```
################################################################

HMAC_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                      20 21222324


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                        20 21222324


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                                     00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


  Key is
                00000000 00000000 00000000 00000000 00000000


  V is
                01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                                     00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    ------------

    V || 0x00 || provided_data is
                                           01 01010101 01010101
        01010101 01010101 01010100 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    K = HMAC(K, V || 0x00 || provided_data) is
                C11B066D 8601D7F1 10C65AE7 750C4937 052014A1
```

```
    V = HMAC(K, V) is
                FB07A09C 7E6E4644 39B497DD F3293B58 35819502


    ------------

    V || 0x01 || provided_data is
                                          FB 07A09C7E 6E464439
        B497DDF3 293B5835 81950201 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    K = HMAC(K, V || 0x01 || provided_data) is
                AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


    V = HMAC(K, V) is
                614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


  Update (Key, V):

    Key is
                AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


    V is
                614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
```

```
                5A7D3B44 9F481CB3 8DF79AD2 B1FCC01E 57F8135E


    temp is
                5A7D3B44 9F481CB3 8DF79AD2 B1FCC01E 57F8135E


  ------------

    V = HMAC(K, V) is
                8C0B22CD 0630BFB0 127FB540 8C8EFC17 A929896E


    temp is
                           5A7D3B44 9F481CB3 8DF79AD2 B1FCC01E
        57F8135E 8C0B22CD 0630BFB0 127FB540 8C8EFC17 A929896E


---------------------------

  returned_bits is
                           5A7D3B44 9F481CB3 8DF79AD2 B1FCC01E
        57F8135E 8C0B22CD 0630BFB0 127FB540 8C8EFC17 A929896E


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              8C 0B22CD06 30BFB012 7FB5408C 8EFC17A9 29896E00


    K = HMAC(K, V || 0x00 || provided_data) is
                7BB18028 E01D0342 DF4F54DA 5122FA5F 2C3A05E4


    V = HMAC(K, V) is
                2F894F28 CC2F5382 9640643A D17B84B0 CD3C7979
```

```
rnd_val is
                          5A7D3B44 9F481CB3 8DF79AD2 B1FCC01E
        57F8135E 8C0B22CD 0630BFB0 127FB540 8C8EFC17 A929896E


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                  82CF772E C3E84B00 FC74F5DF 104EFBFB 2428554E


    temp is
                  82CF772E C3E84B00 FC74F5DF 104EFBFB 2428554E


  ------------

    V = HMAC(K, V) is
                  9CE367D0 3AEADE37 827FA8E9 CB6A0819 6115D948


    temp is
                          82CF772E C3E84B00 FC74F5DF 104EFBFB
        2428554E 9CE367D0 3AEADE37 827FA8E9 CB6A0819 6115D948


---------------------------

  returned_bits is
                          82CF772E C3E84B00 FC74F5DF 104EFBFB
        2428554E 9CE367D0 3AEADE37 827FA8E9 CB6A0819 6115D948


  call Update(additional_input, K, V)
```

```
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              9C E367D03A EADE3782 7FA8E9CB 6A081961 15D94800


    K = HMAC(K, V || 0x00 || provided_data) is
                 3D4D7377 E9172AAF A776B0DD CB894200 4A44B7FD


    V = HMAC(K, V) is
                 1A26BD9B FC9744BD 29F6AEBE 2437E209 F1F71625


rnd_val is
                           82CF772E C3E84B00 FC74F5DF 104EFBFB
         2428554E 9CE367D0 3AEADE37 827FA8E9 CB6A0819 6115D948


################################################################

HMAC_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                    20 21222324


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                                    00010203 04050607 08090A0B
```

```
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


  Key is
                00000000 00000000 00000000 00000000 00000000


  V is
                01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    ------------

    V || 0x00 || provided_data is
                                          01 01010101 01010101
        01010101 01010101 01010100 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    K = HMAC(K, V || 0x00 || provided_data) is
                C11B066D 8601D7F1 10C65AE7 750C4937 052014A1


    V = HMAC(K, V) is
                FB07A09C 7E6E4644 39B497DD F3293B58 35819502


    ------------

    V || 0x01 || provided_data is
                                          FB 07A09C7E 6E464439
        B497DDF3 293B5835 81950201 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


    V = HMAC(K, V) is
                614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


  Update (Key, V):

    Key is
                AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


    V is
                614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                              606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                              606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
```

```
  ------------

  V || 0x00 || provided_data is
                                                        614499EA
      980CFB3D AA2CA86D 65A46BF4 488D8CC5 00606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  K = HMAC(K, V || 0x00 || provided_data) is
               E8C6B0A1 D480E7D6 C3B41065 EBED069A E157CBC3


  V = HMAC(K, V) is
               CBEDC05C 2C54CA75 334BD647 06FC3EF8 7B4E328E


  ------------

  V || 0x01 || provided_data is
                                                        CBEDC05C
      2C54CA75 334BD647 06FC3EF8 7B4E328E 01606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  K = HMAC(K, V || 0x01 || provided_data) is
               48B3AD2B 21D8EF7E A766C6B5 21A2FC3F B1E42935


  V = HMAC(K, V) is
               C5B984AC 3985C236 0E73B018 2F9FBDC7 3251FFD3


------------

  V = HMAC(K, V) is
               C7AAAC58 3C6EF630 0714C2CC 5D06C148 CFFB4044


  temp is
               C7AAAC58 3C6EF630 0714C2CC 5D06C148 CFFB4044


------------
```

```
    V = HMAC(K, V) is
                 9AD0BB26 FAC0497B 5C57E161 E36681BC C930CE80


    temp is
                          C7AAAC58 3C6EF630 0714C2CC 5D06C148
         CFFB4044 9AD0BB26 FAC0497B 5C57E161 E36681BC C930CE80


---------------------------

  returned_bits is
                          C7AAAC58 3C6EF630 0714C2CC 5D06C148
         CFFB4044 9AD0BB26 FAC0497B 5C57E161 E36681BC C930CE80


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                606162 63646566
         6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
         7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                                          9AD0BB26
         FAC0497B 5C57E161 E36681BC C930CE80 00606162 63646566
         6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
         7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                 AC235DC4 2E53D55A 20FAA9F0 6543E29A 799D3DE2


    V = HMAC(K, V) is
                 5106A127 D021DB3E 76AAEC1D 24D4DAAE 7BA91FF2


    ------------
```

```
    V || 0x01 || provided_data is
                                                        5106A127
        D021DB3E 76AAEC1D 24D4DAAE 7BA91FF2 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                 3A062E6B 79FE70DB FFEB3A2B 6BE80323 F7D674C5


    V = HMAC(K, V) is
                 BD363128 BF580D7A 54429DDD 58E8193B 9843BD2B


rnd_val is
                          C7AAAC58 3C6EF630 0714C2CC 5D06C148
        CFFB4044 9AD0BB26 FAC0497B 5C57E161 E36681BC C930CE80


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
  ------------

  V || 0x00 || provided_data is
                                                      BD363128
      BF580D7A 54429DDD 58E8193B 9843BD2B 00A0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x00 || provided_data) is
               D7CDFD76 F19B373F E9FEBC06 115278C8 5DD14375


  V = HMAC(K, V) is
               D06F8199 E16826AF 9EC3486F B76DA833 E2BB11E5


  ------------

  V || 0x01 || provided_data is
                                                      D06F8199
      E16826AF 9EC3486F B76DA833 E2BB11E5 01A0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x01 || provided_data) is
               D1B575BC 767410DB B5E2F7F7 586BB421 CCCD5E22


  V = HMAC(K, V) is
               C4BB579E 7E2A0A94 5A408C61 28446BFF DD211A16


------------

  V = HMAC(K, V) is
               6EBD2B7B 5E0A2AD7 A24B1BF9 A1DBA47D 43271719


  temp is
               6EBD2B7B 5E0A2AD7 A24B1BF9 A1DBA47D 43271719
```

```
  ------------

    V = HMAC(K, V) is
                B9C37B7F E81BA940 45A14A7C B514B446 666EA5A7


    temp is
                           6EBD2B7B 5E0A2AD7 A24B1BF9 A1DBA47D
        43271719 B9C37B7F E81BA940 45A14A7C B514B446 666EA5A7


---------------------------

  returned_bits is
                           6EBD2B7B 5E0A2AD7 A24B1BF9 A1DBA47D
        43271719 B9C37B7F E81BA940 45A14A7C B514B446 666EA5A7


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                                                         B9C37B7F
        E81BA940 45A14A7C B514B446 666EA5A7 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                7FDB1E3A A4B1368E 03C63FC8 F4A05A88 E7A9A11A


    V = HMAC(K, V) is
                D48C4E59 EDA3F929 3282AD19 29A854ED FA128BB7
```

```
    ------------

    V || 0x01 || provided_data is
                                                          D48C4E59
        EDA3F929 3282AD19 29A854ED FA128BB7 01A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                 8AD7E347 72B5FC7C 3B3B2762 4F0B9177 6A8A7112


    V = HMAC(K, V) is
                 D71376A4 6D764B17 C3B73934 7B384E51 51E87E88


rnd_val is
                           6EBD2B7B 5E0A2AD7 A24B1BF9 A1DBA47D
        43271719 B9C37B7F E81BA940 45A14A7C B514B446 666EA5A7


################################################################

HMAC_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
```

DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6

Nonce =
20 21222324

PersonalizationString =
404142 43444546
4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576

AdditionalInput = <empty>

##

****

HMAC_DRBG_Instantiate_algorithm

entropy_input is
000102 03040506
0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536

nonce is
20 21222324

personal_str is
404142 43444546
4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576

prediction_resistance_flag = "No PredictionResistance"

Seed_Material is
000102 03040506 0708090A 0B0C0D0E 0F101112
13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576

Key is
00000000 00000000 00000000 00000000 00000000

V is
01010101 01010101 01010101 01010101 01010101

Update

provided_data
000102 03040506 0708090A 0B0C0D0E 0F101112
13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576

V || 0x00 || provided_data is
01010101 01010101 01010101 01010101
01010101 00000102 03040506 0708090A 0B0C0D0E 0F101112
13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576

K = HMAC(K, V || 0x00 || provided_data) is
3F7A620C 6BED0A29 2CB8E7D7 6DCEA617 67E060D5

V = HMAC(K, V) is
5848B848 182B6499 F6348807 E3CFE186 EE05FE25

V || 0x01 || provided_data is
5848B848 182B6499 F6348807 E3CFE186
EE05FE25 01000102 03040506 0708090A 0B0C0D0E 0F101112
13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A

```
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x01 || provided_data) is
                B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


    V = HMAC(K, V) is
                DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


  Update (Key, V):

    Key is
                B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


    V is
                DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


-----------------------------------------------------------

First call to Generate

***********************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                B3BD0524 6CBA12A6 4735A4E3 FDE599BC 1BE30F43


    temp is
                B3BD0524 6CBA12A6 4735A4E3 FDE599BC 1BE30F43


  ------------
```

```
    V = HMAC(K, V) is
                 9BD06020 8EEA7D71 F9D123DF 47B3CE06 9D98EDE6


    temp is
                           B3BD0524 6CBA12A6 4735A4E3 FDE599BC
         1BE30F43 9BD06020 8EEA7D71 F9D123DF 47B3CE06 9D98EDE6


---------------------------

  returned_bits is
                           B3BD0524 6CBA12A6 4735A4E3 FDE599BC
         1BE30F43 9BD06020 8EEA7D71 F9D123DF 47B3CE06 9D98EDE6


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              9B D060208E EA7D71F9 D123DF47 B3CE069D 98EDE600


    K = HMAC(K, V || 0x00 || provided_data) is
                 87D3828B E03A807D D3402941 BED6DE98 6EE7A286


    V = HMAC(K, V) is
                 6AE1D008 6F53B1B7 63A4515B 1906FEE4 7661FD47


rnd_val is
                           B3BD0524 6CBA12A6 4735A4E3 FDE599BC
         1BE30F43 9BD06020 8EEA7D71 F9D123DF 47B3CE06 9D98EDE6


---------------------------------------------------------------

Second call to Generate
```

```
*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                B5DADA38 0E2872DF 935BCA55 B882C8C9 376902AB


    temp is
                B5DADA38 0E2872DF 935BCA55 B882C8C9 376902AB


  ------------

    V = HMAC(K, V) is
                63976547 2B71ACEB E2EA8B1B 6B49629C B67317E0


    temp is
                           B5DADA38 0E2872DF 935BCA55 B882C8C9
        376902AB 63976547 2B71ACEB E2EA8B1B 6B49629C B67317E0


---------------------------

  returned_bits is
                           B5DADA38 0E2872DF 935BCA55 B882C8C9
        376902AB 63976547 2B71ACEB E2EA8B1B 6B49629C B67317E0


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------
```

```
    V || 0x00 || provided_data is
              63 9765472B 71ACEBE2 EA8B1B6B 49629CB6 7317E000


    K = HMAC(K, V || 0x00 || provided_data) is
                 26ABBF54 B28B93FF 9008670E BFEE86CD D7228ED5


    V = HMAC(K, V) is
                 E9254729 E00204A1 B6C02158 A6C72786 4714F1F7


rnd_val is
                           B5DADA38 0E2872DF 935BCA55 B882C8C9
         376902AB 63976547 2B71ACEB E2EA8B1B 6B49629C B67317E0


##############################################################

HMAC_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                      20 21222324
```

```
    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                  000102 03040506 0708090A 0B0C0D0E 0F101112
```

```
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                00000000 00000000 00000000 00000000 00000000


  V is
                01010101 01010101 01010101 01010101 01010101


----------------------------

  Update

    provided_data
                 000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------

    V || 0x00 || provided_data is
                         01010101 01010101 01010101 01010101
        01010101 00000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x00 || provided_data) is
                3F7A620C 6BED0A29 2CB8E7D7 6DCEA617 67E060D5


    V = HMAC(K, V) is
                5848B848 182B6499 F6348807 E3CFE186 EE05FE25


    ------------
```

```
    V || 0x01 || provided_data is
                          5848B848 182B6499 F6348807 E3CFE186
        EE05FE25 01000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x01 || provided_data) is
                 B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


    V = HMAC(K, V) is
                 DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


  Update (Key, V):

    Key is
                 B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


    V is
                 DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


-----------------------------------------------------------

First call to Generate

***********************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                              606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------
```

```
Update

  provided_data
                                                606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  ------------

  V || 0x00 || provided_data is
                                                        DAB2A718
      83F1005C 5DD03932 4D3C364D 6E18F954 00606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  K = HMAC(K, V || 0x00 || provided_data) is
              94FF0C25 4EAFC7D7 EA314E83 780A09DF 46A5F1A3


  V = HMAC(K, V) is
              7A8FE422 EE665D07 1F63841D CE347CED A6CC07AE


  ------------

  V || 0x01 || provided_data is
                                                        7A8FE422
      EE665D07 1F63841D CE347CED A6CC07AE 01606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  K = HMAC(K, V || 0x01 || provided_data) is
              92AF76A0 7C0A556E 579044B6 A1F19ED9 52727FB6


  V = HMAC(K, V) is
              21BE014B CE5FFB6A 569DDEB6 4F0901F8 469BA704


------------

  V = HMAC(K, V) is
```

```
                1F8FEC7B C7CFA9A8 80345D28 0B13C632 B852770A


    temp is
                1F8FEC7B C7CFA9A8 80345D28 0B13C632 B852770A


  ------------

    V = HMAC(K, V) is
                6DFC302E AD4CE3F5 54C79B0D 44239EBA 56A7EA2D


    temp is
                           1F8FEC7B C7CFA9A8 80345D28 0B13C632
        B852770A 6DFC302E AD4CE3F5 54C79B0D 44239EBA 56A7EA2D


---------------------------

  returned_bits is
                           1F8FEC7B C7CFA9A8 80345D28 0B13C632
        B852770A 6DFC302E AD4CE3F5 54C79B0D 44239EBA 56A7EA2D


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                                         6DFC302E
        AD4CE3F5 54C79B0D 44239EBA 56A7EA2D 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
```

```
                E5B19979 A077728F A891F907 57A39527 1BA998E2


    V = HMAC(K, V) is
                330D2882 2736520F B8C295D8 B853CF90 E6A7F04E


    ------------

    V || 0x01 || provided_data is
                                                        330D2882
        2736520F B8C295D8 B853CF90 E6A7F04E 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                17A5D79F 0767876F 3A45E0C9 C33EC88B 03CEEA13


    V = HMAC(K, V) is
                4D2F3BC7 77505C45 F7E17DCD 3D86BF37 9CB6025E


rnd_val is
                          1F8FEC7B C7CFA9A8 80345D28 0B13C632
        B852770A 6DFC302E AD4CE3F5 54C79B0D 44239EBA 56A7EA2D


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  additional_input <> NULL, call Update(additional_input, K, V)
```

```
---------------------------

  Update

    provided_data
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                                                          4D2F3BC7
        77505C45 F7E17DCD 3D86BF37 9CB6025E 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                 7024EBA2 2F9EFDF9 43CCD4A5 3C3E3EBE 1C328E49


    V = HMAC(K, V) is
                 6EF6820D D3C9BB9C 42D91D32 AC3CF56A 59A7A161


    ------------

    V || 0x01 || provided_data is
                                                          6EF6820D
        D3C9BB9C 42D91D32 AC3CF56A 59A7A161 01A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                 41EDB8EA 2E6E4A25 D9E1A3BC DB40CF35 7976422B


    V = HMAC(K, V) is
                 0E8B49B1 D57E64FE F896BCDB C08920FC 58AC87F8


  ------------
```

```
    V = HMAC(K, V) is
                 AF97CDE1 E8AB322A 2EACA8E6 F4E5BF78 A11BDEF7


    temp is
                 AF97CDE1 E8AB322A 2EACA8E6 F4E5BF78 A11BDEF7


  ------------

    V = HMAC(K, V) is
                 DC91215D 44B107B4 D5A77901 59250976 5280F969


    temp is
                          AF97CDE1 E8AB322A 2EACA8E6 F4E5BF78
        A11BDEF7 DC91215D 44B107B4 D5A77901 59250976 5280F969


---------------------------

  returned_bits is
                          AF97CDE1 E8AB322A 2EACA8E6 F4E5BF78
        A11BDEF7 DC91215D 44B107B4 D5A77901 59250976 5280F969


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                                                       DC91215D
        44B107B4 D5A77901 59250976 5280F969 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
    K = HMAC(K, V || 0x00 || provided_data) is
                 2CCF0DC9 D717135E 3D52BEC8 82B48902 B559A2B5


    V = HMAC(K, V) is
                 16609755 A8B2C412 E44C47F5 891FBAF6 645505E8


    ------------

    V || 0x01 || provided_data is
                                                        16609755
        A8B2C412 E44C47F5 891FBAF6 645505E8 01A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                 079B57D9 406E11C2 F87C8C82 8C8C6FA7 6E40EA01


    V = HMAC(K, V) is
                 A654FE72 F8A77BB8 F03DFF07 C79A5153 009EDDDA


rnd_val is
                          AF97CDE1 E8AB322A 2EACA8E6 F4E5BF78
        A11BDEF7 DC91215D 44B107B4 D5A77901 59250976 5280F969


################################################################

HMAC_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                               000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
```

```
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                      20 21222324


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                      20 21222324


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


  Key is
```

```
                00000000 00000000 00000000 00000000 00000000

  V is
                01010101 01010101 01010101 01010101 01010101

---------------------------

  Update

    provided_data
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    ------------

    V || 0x00 || provided_data is
                                           01 01010101 01010101
        01010101 01010101 01010100 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    K = HMAC(K, V || 0x00 || provided_data) is
                C11B066D 8601D7F1 10C65AE7 750C4937 052014A1


    V = HMAC(K, V) is
                FB07A09C 7E6E4644 39B497DD F3293B58 35819502


    ------------

    V || 0x01 || provided_data is
                                           FB 07A09C7E 6E464439
        B497DDF3 293B5835 81950201 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    K = HMAC(K, V || 0x01 || provided_data) is
                AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9
```

```
    V = HMAC(K, V) is
                614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


  Update (Key, V):

    Key is
                AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


    V is
                614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is  <empty>

  Seed_Material is
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

Key is
AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9

V is
614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5

Update

provided_data
808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

V || 0x00 || provided_data is
614499EA
980CFB3D AA2CA86D 65A46BF4 488D8CC5 00808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

K = HMAC(K, V || 0x00 || provided_data) is
B365E8D2 ABCB06AE EF8094A3 768F6FA5 8402966D

V = HMAC(K, V) is
91EC2556 8078AA94 0A447074 33004BB0 A388B056

V || 0x01 || provided_data is
91EC2556
8078AA94 0A447074 33004BB0 A388B056 01808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

K = HMAC(K, V || 0x01 || provided_data) is
CD4CAB38 C8AD6571 22BF5D3D 00D0AC9B 13D629BB

V = HMAC(K, V) is
F660E23E 91006B62 C6543AB1 344D23A3 1AB4CF2C

Update (Key, V):

Key is
CD4CAB38 C8AD6571 22BF5D3D 00D0AC9B 13D629BB

V is
F660E23E 91006B62 C6543AB1 344D23A3 1AB4CF2C

****

HMAC_DRBG_Generate

requested_number_of_bits = 320

additional_input is <empty>

V = HMAC(K, V) is
FEC4597F 06A3A8CC 8529D595 57B9E661 053809C0

temp is
FEC4597F 06A3A8CC 8529D595 57B9E661 053809C0

V = HMAC(K, V) is
BC0EFC28 2ABD8760 5CC90CBA 9B8633DC B1DAE02E

temp is
FEC4597F 06A3A8CC 8529D595 57B9E661
053809C0 BC0EFC28 2ABD8760 5CC90CBA 9B8633DC B1DAE02E

```
  returned_bits is
                          FEC4597F 06A3A8CC 8529D595 57B9E661
        053809C0 BC0EFC28 2ABD8760 5CC90CBA 9B8633DC B1DAE02E


  call Update(additional_input, K, V)
----------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              BC 0EFC282A BD87605C C90CBA9B 8633DCB1 DAE02E00


    K = HMAC(K, V || 0x00 || provided_data) is
                587FD821 EF6C9DA4 A83C1921 1F1056CA CD23FC1A


    V = HMAC(K, V) is
                848FD14C 13B7EA93 720CCFDE 71F2F644 39DB795D


rnd_val is
                          FEC4597F 06A3A8CC 8529D595 57B9E661
        053809C0 BC0EFC28 2ABD8760 5CC90CBA 9B8633DC B1DAE02E


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************
```

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6

    additional_input is <empty>

  Seed_Material is
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6

  Key is
                587FD821 EF6C9DA4 A83C1921 1F1056CA CD23FC1A

  V is
                848FD14C 13B7EA93 720CCFDE 71F2F644 39DB795D

  Update

    provided_data
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6

    V || 0x00 || provided_data is
                                                            848FD14C
        13B7EA93 720CCFDE 71F2F644 39DB795D 00C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6

    K = HMAC(K, V || 0x00 || provided_data) is
                E99B2A74 468B6877 0F2F00C0 9C1F5850 BE543344

```
    V = HMAC(K, V) is
                42138429 41CC9219 A1D0C6D0 E0C96DA3 DF303937


    ------------

    V || 0x01 || provided_data is
                                                        42138429
        41CC9219 A1D0C6D0 E0C96DA3 DF303937 01C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    K = HMAC(K, V || 0x01 || provided_data) is
                DBA1CFF4 879546A0 38A559B2 A24DF2C0 30089A41


    V = HMAC(K, V) is
                2F883C46 48E131E8 6DDF9DCA 0D74F30C A1CE6EFB


  Update (Key, V):

    Key is
                DBA1CFF4 879546A0 38A559B2 A24DF2C0 30089A41


    V is
                2F883C46 48E131E8 6DDF9DCA 0D74F30C A1CE6EFB


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                84ADD5E2 D2041C01 723A4DE4 335B13EF DF16B0E5
```

```
    temp is
                 84ADD5E2 D2041C01 723A4DE4 335B13EF DF16B0E5


  ------------

    V = HMAC(K, V) is
                 1A0AD39B D15E862E 644F31E4 A2D7D843 E57C5968


    temp is
                           84ADD5E2 D2041C01 723A4DE4 335B13EF
         DF16B0E5 1A0AD39B D15E862E 644F31E4 A2D7D843 E57C5968


----------------------------

  returned_bits is
                           84ADD5E2 D2041C01 723A4DE4 335B13EF
         DF16B0E5 1A0AD39B D15E862E 644F31E4 A2D7D843 E57C5968


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              1A 0AD39BD1 5E862E64 4F31E4A2 D7D843E5 7C596800


    K = HMAC(K, V || 0x00 || provided_data) is
                 F939A5AB 08A39F23 1070B0D4 C96DC237 90BA0153


    V = HMAC(K, V) is
                 CE6D08B4 AE2CE383 FDABB01E AAFC9C8E 76A0D472


rnd_val is
                           84ADD5E2 D2041C01 723A4DE4 335B13EF
```

```
        DF16B0E5 1A0AD39B D15E862E 644F31E4 A2D7D843 E57C5968


###############################################################

HMAC_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                      20 21222324


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                       20 21222324


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


  Key is
                00000000 00000000 00000000 00000000 00000000


  V is
                01010101 01010101 01010101 01010101 01010101


--------------------------

  Update

    provided_data
                                    00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324
```

```
    ------------

    V || 0x00 || provided_data is
                                          01 01010101 01010101
        01010101 01010101 01010100 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    K = HMAC(K, V || 0x00 || provided_data) is
                 C11B066D 8601D7F1 10C65AE7 750C4937 052014A1


    V = HMAC(K, V) is
                 FB07A09C 7E6E4644 39B497DD F3293B58 35819502


    ------------

    V || 0x01 || provided_data is
                                          FB 07A09C7E 6E464439
        B497DDF3 293B5835 81950201 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F 20212223
        24252627 28292A2B 2C2D2E2F 30313233 34353620 21222324


    K = HMAC(K, V || 0x01 || provided_data) is
                 AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


    V = HMAC(K, V) is
                 614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


  Update (Key, V):

    Key is
                 AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


    V is
                 614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5


-----------------------------------------------------------------
```

```
First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Seed_Material is
                             8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Key is
                AB160DD2 1C30980C A3CA5A9C 77B7BDF0 50E64EE9


  V is
                614499EA 980CFB3D AA2CA86D 65A46BF4 488D8CC5
```

```
---------------------------

  Update

    provided_data
                                8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                      614499 EA980CFB 3DAA2CA8
        6D65A46B F4488D8C C5008081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                 580F7D3D 738FBF1C 8D9ACE0D 52CB00C4 B490CE86


    V = HMAC(K, V) is
                 1F06F616 E7D08B5B F2947CB1 DC295B71 46ED65CE


    ------------

    V || 0x01 || provided_data is
                                      1F06F6 16E7D08B 5BF2947C
        B1DC295B 7146ED65 CE018081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                 5228A4B6 A4469290 5EC044BF F0BB4E25 A387CAC1
```

```
    V = HMAC(K, V) is
                  247732D0 4CB84ED4 1ADD95A4 B78B50CD 9B3D3F32


  Update (Key, V):

    Key is
                  5228A4B6 A4469290 5EC044BF F0BB4E25 A387CAC1


    V is
                  247732D0 4CB84ED4 1ADD95A4 B78B50CD 9B3D3F32


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                  A1BA8FA5 8BB5013F 43F7B6ED 52B4539F A16DC779


    temp is
                  A1BA8FA5 8BB5013F 43F7B6ED 52B4539F A16DC779


  ------------

    V = HMAC(K, V) is
                  57AEE815 B9C07004 C7E992EB 8C7E5919 64AFEEA2


    temp is
                           A1BA8FA5 8BB5013F 43F7B6ED 52B4539F
        A16DC779 57AEE815 B9C07004 C7E992EB 8C7E5919 64AFEEA2


---------------------------
```

```
  returned_bits is
                           A1BA8FA5 8BB5013F 43F7B6ED 52B4539F
        A16DC779 57AEE815 B9C07004 C7E992EB 8C7E5919 64AFEEA2


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              57 AEE815B9 C07004C7 E992EB8C 7E591964 AFEEA200


    K = HMAC(K, V || 0x00 || provided_data) is
                 AB3DD489 5BC8CD22 71DEBA5F 3C136352 6B8B7452


    V = HMAC(K, V) is
                 A866C5EF F2AF042B 11864494 45237F9C 02449864


rnd_val is
                           A1BA8FA5 8BB5013F 43F7B6ED 52B4539F
        A16DC779 57AEE815 B9C07004 C7E992EB 8C7E5919 64AFEEA2


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Seed_Material is
                             C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Key is
                AB3DD489 5BC8CD22 71DEBA5F 3C136352 6B8B7452


  V is
                A866C5EF F2AF042B 11864494 45237F9C 02449864


---------------------------

  Update

    provided_data
                             C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
  ------------

  V || 0x00 || provided_data is
                                    A866C5 EFF2AF04 2B118644
      9445237F 9C024498 6400C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
      CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
      E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x00 || provided_data) is
                C908BF7E 4FC908C3 17B20887 77CC961F 8173EACB


  V = HMAC(K, V) is
                915C0615 0BC71C0D 01B8B479 3E01367E 59F8BE44


  ------------

  V || 0x01 || provided_data is
                                    915C06 150BC71C 0D01B8B4
      793E0136 7E59F8BE 4401C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
      CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
      E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x01 || provided_data) is
                E5739F9C F7FF4384 D1273E02 6B453121 36494F41


  V = HMAC(K, V) is
                30C34305 C2C648B0 57A64022 1B5C5657 26CD32B2


Update (Key, V):

  Key is
                E5739F9C F7FF4384 D1273E02 6B453121 36494F41


  V is
                30C34305 C2C648B0 57A64022 1B5C5657 26CD32B2
```

```
**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                 84264A73 A818C95C 2F424B37 D3CC990B 046FB50C


    temp is
                 84264A73 A818C95C 2F424B37 D3CC990B 046FB50C


  ------------

    V = HMAC(K, V) is
                 2DC64A16 4211889A 010F2471 A0912FFE A1BF0195


    temp is
                           84264A73 A818C95C 2F424B37 D3CC990B
        046FB50C 2DC64A16 4211889A 010F2471 A0912FFE A1BF0195


---------------------------

  returned_bits is
                           84264A73 A818C95C 2F424B37 D3CC990B
        046FB50C 2DC64A16 4211889A 010F2471 A0912FFE A1BF0195


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------
```

```
    V || 0x00 || provided_data is
              2D C64A1642 11889A01 0F2471A0 912FFEA1 BF019500


    K = HMAC(K, V || 0x00 || provided_data) is
                 6191CA9B F000D10A 71690AC1 0E09FFC8 92ABDE9A


    V = HMAC(K, V) is
                 1EC0490F A0B76552 7E5EA18B 5322B28B DD0E7BC0


rnd_val is
                           84264A73 A818C95C 2F424B37 D3CC990B
        046FB50C 2DC64A16 4211889A 010F2471 A0912FFE A1BF0195


################################################################

HMAC_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
```

```
                                                    20 21222324


    PersonalizationString =
                                                   404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                   000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                    20 21222324


    personal_str is
                                                   404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                  000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                00000000 00000000 00000000 00000000 00000000
```

```
  V is
                01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                   000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------

    V || 0x00 || provided_data is
                          01010101 01010101 01010101 01010101
        01010101 00000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x00 || provided_data) is
                3F7A620C 6BED0A29 2CB8E7D7 6DCEA617 67E060D5


    V = HMAC(K, V) is
                5848B848 182B6499 F6348807 E3CFE186 EE05FE25


    ------------

    V || 0x01 || provided_data is
                          5848B848 182B6499 F6348807 E3CFE186
        EE05FE25 01000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C

    V = HMAC(K, V) is
                DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954

  Update (Key, V):

    Key is
                B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C

    V is
                DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954

-----------------------------------------------------------------

First call to Generate

*****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

Generate FAILED: Reseed is required
*****************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

    additional_input is  <empty>

  Seed_Material is
                                              808182 83848586
```

```
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  Key is
                B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


  V is
                DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


---------------------------

  Update

    provided_data
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    ------------

    V || 0x00 || provided_data is
                                                          DAB2A718
        83F1005C 5DD03932 4D3C364D 6E18F954 00808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    K = HMAC(K, V || 0x00 || provided_data) is
                F5044986 F825EB14 7DB35FE8 0666DB09 A7773C4C


    V = HMAC(K, V) is
                9C4D0729 7D6631D9 504721BD 21C8A102 C632306C


    ------------

    V || 0x01 || provided_data is
                                                          9C4D0729
        7D6631D9 504721BD 21C8A102 C632306C 01808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                 B9254D8A ACBA43FB DAE6394F 2B3AFC5D 580800BF


    V = HMAC(K, V) is
                 28403B60 3638D07D 7966661E F67B9D39 05F46DB9


  Update (Key, V):

    Key is
                 B9254D8A ACBA43FB DAE6394F 2B3AFC5D 580800BF


    V is
                 28403B60 3638D07D 7966661E F67B9D39 05F46DB9


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                 6C37FDD7 29AA40F8 0BC6AB08 CA7CC649 794F6998


    temp is
                 6C37FDD7 29AA40F8 0BC6AB08 CA7CC649 794F6998


  ------------

    V = HMAC(K, V) is
                 B57081E4 220F22C5 C283E2C9 1B8E305A B869C625


    temp is
                         6C37FDD7 29AA40F8 0BC6AB08 CA7CC649
```

```
        794F6998 B57081E4 220F22C5 C283E2C9 1B8E305A B869C625


---------------------------

  returned_bits is
                          6C37FDD7 29AA40F8 0BC6AB08 CA7CC649
        794F6998 B57081E4 220F22C5 C283E2C9 1B8E305A B869C625


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              B5 7081E422 0F22C5C2 83E2C91B 8E305AB8 69C62500


    K = HMAC(K, V || 0x00 || provided_data) is
                64FE074A 6E7797D1 A435DA89 64484D6C F8BDC01B


    V = HMAC(K, V) is
                43E0C052 1586E947 3B060D87 D08A2325 FAE149D1


rnd_val is
                          6C37FDD7 29AA40F8 0BC6AB08 CA7CC649
        794F6998 B57081E4 220F22C5 C283E2C9 1B8E305A B869C625


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320
```

```
    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is  <empty>

  Seed_Material is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  Key is
                64FE074A 6E7797D1 A435DA89 64484D6C F8BDC01B


  V is
                43E0C052 1586E947 3B060D87 D08A2325 FAE149D1


---------------------------

  Update

    provided_data
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    ------------

    V || 0x00 || provided_data is
                                                        43E0C052
        1586E947 3B060D87 D08A2325 FAE149D1 00C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
```

```
    K = HMAC(K, V || 0x00 || provided_data) is
                C25BF4F6 DF4271AC 796CC694 F61D7EEF 0BA4B13F


    V = HMAC(K, V) is
                E1A4863E 97118850 8DD8413B 07610B55 EFCFE0C2


    ------------

    V || 0x01 || provided_data is
                                                        E1A4863E
        97118850 8DD8413B 07610B55 EFCFE0C2 01C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    K = HMAC(K, V || 0x01 || provided_data) is
                02BC577F D10EF719 3C1DB098 BD5B75C7 C4B67959


    V = HMAC(K, V) is
                BCBDF052 E0E02AE8 9A776794 3F9865B8 B722902D


  Update (Key, V):

    Key is
                02BC577F D10EF719 3C1DB098 BD5B75C7 C4B67959


    V is
                BCBDF052 E0E02AE8 9A776794 3F9865B8 B722902D

**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------
```

```
    V = HMAC(K, V) is
                 CAF57DCF EA393B92 36BF691F A456FEA7 FDF1DF83


    temp is
                 CAF57DCF EA393B92 36BF691F A456FEA7 FDF1DF83


  ------------

    V = HMAC(K, V) is
                 61482CA5 4D5FA723 F4C88B4F A504BF03 277FA783


    temp is
                           CAF57DCF EA393B92 36BF691F A456FEA7
        FDF1DF83 61482CA5 4D5FA723 F4C88B4F A504BF03 277FA783


---------------------------

  returned_bits is
                           CAF57DCF EA393B92 36BF691F A456FEA7
        FDF1DF83 61482CA5 4D5FA723 F4C88B4F A504BF03 277FA783


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              61 482CA54D 5FA723F4 C88B4FA5 04BF0327 7FA78300


    K = HMAC(K, V || 0x00 || provided_data) is
                 1AA4241C 695E29C0 A59AD18A 6070E338 A548BE92


    V = HMAC(K, V) is
                 0347359B C9C7F88C C8330D4F 59FBC770 B0B77B03
```

```
rnd_val is
                          CAF57DCF EA393B92 36BF691F A456FEA7
        FDF1DF83 61482CA5 4D5FA723 F4C88B4F A504BF03 277FA783


################################################################

HMAC_DRBG

    Requested Security Strength = 80

    Requested Hash Algorithm = SHA-1

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                     20 21222324


    PersonalizationString =
                                                 404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                 606162 63646566
```

```
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##############################################################

**************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                              000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                   20 21222324


    personal_str is
                                              404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                  000102 03040506 0708090A 0B0C0D0E 0F101112
        13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
        2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                00000000 00000000 00000000 00000000 00000000
```

V is
01010101 01010101 01010101 01010101 01010101

Update

provided_data
000102 03040506 0708090A 0B0C0D0E 0F101112
13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576

V || 0x00 || provided_data is
01010101 01010101 01010101 01010101
01010101 00000102 03040506 0708090A 0B0C0D0E 0F101112
13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576

K = HMAC(K, V || 0x00 || provided_data) is
3F7A620C 6BED0A29 2CB8E7D7 6DCEA617 67E060D5

V = HMAC(K, V) is
5848B848 182B6499 F6348807 E3CFE186 EE05FE25

V || 0x01 || provided_data is
5848B848 182B6499 F6348807 E3CFE186
EE05FE25 01000102 03040506 0708090A 0B0C0D0E 0F101112
13141516 1718191A 1B1C1D1E 1F202122 23242526 2728292A
2B2C2D2E 2F303132 33343536 20212223 24404142 43444546
4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576

```
    K = HMAC(K, V || 0x01 || provided_data) is
                 B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


    V = HMAC(K, V) is
                 DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


  Update (Key, V):

    Key is
                 B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


    V is
                 DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                              606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is
```

```
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Seed_Material is
                               8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Key is
                B7D966D7 0D4E27A7 FA838F7D 61126C0E DC84761C


  V is
                DAB2A718 83F1005C 5DD03932 4D3C364D 6E18F954


--------------------------

  Update

    provided_data
                               8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                     DAB2A7 1883F100 5C5DD039
        324D3C36 4D6E18F9 54008081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                B02FB0AE F02B9D35 01597640 32641425 F7AB0780
```

```
    V = HMAC(K, V) is
                0D23D81F 8626C01D FA230E23 B6AD0A2C CAEA3180


    ------------

    V || 0x01 || provided_data is
                                      0D23D8 1F8626C0 1DFA230E
        23B6AD0A 2CCAEA31 80018081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                C09548C0 D3C861D7 40F2837D 72B50723 5C26DB82


    V = HMAC(K, V) is
                174B3F84 C3531F7C 0A2E5421 234EA16B 708DDF0D


  Update (Key, V):

    Key is
                C09548C0 D3C861D7 40F2837D 72B50723 5C26DB82


    V is
                174B3F84 C3531F7C 0A2E5421 234EA16B 708DDF0D


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
```

```
                BD07C25C FD7C5E3A 4EAA6E2E DC5AB7EA 4942A091


    temp is
                BD07C25C FD7C5E3A 4EAA6E2E DC5AB7EA 4942A091


  ------------

    V = HMAC(K, V) is
                3471FDA5 5C6DDD2C 03EFA3B9 643AB3BB 22F6C9F2


    temp is
                          BD07C25C FD7C5E3A 4EAA6E2E DC5AB7EA
        4942A091 3471FDA5 5C6DDD2C 03EFA3B9 643AB3BB 22F6C9F2


---------------------------

  returned_bits is
                          BD07C25C FD7C5E3A 4EAA6E2E DC5AB7EA
        4942A091 3471FDA5 5C6DDD2C 03EFA3B9 643AB3BB 22F6C9F2


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              34 71FDA55C 6DDD2C03 EFA3B964 3AB3BB22 F6C9F200


    K = HMAC(K, V || 0x00 || provided_data) is
                603F0949 279C70E8 C66C0F56 37C0F375 6007E5AC


    V = HMAC(K, V) is
                F2B33B21 151FAF61 20018310 F44E4CD0 BFE368EA
```

```
rnd_val is
                          BD07C25C FD7C5E3A 4EAA6E2E DC5AB7EA
        4942A091 3471FDA5 5C6DDD2C 03EFA3B9 643AB3BB 22F6C9F2


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                 C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Seed_Material is
                             C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
```

```
  Key is
                603F0949 279C70E8 C66C0F56 37C0F375 6007E5AC


  V is
                F2B33B21 151FAF61 20018310 F44E4CD0 BFE368EA


---------------------------

  Update

    provided_data
                              C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                                    F2B33B 21151FAF 61200183
        10F44E4C D0BFE368 EA00C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                66638E61 B8F0D692 C5D300BA 7D0237DD CE94F587


    V = HMAC(K, V) is
                80EFA2CF 6DB37996 B4147204 724649BF CB0C6C79


    ------------

    V || 0x01 || provided_data is
                                    80EFA2 CF6DB379 96B41472
        04724649 BFCB0C6C 7901C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
```

```
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                 8942A54F 349E281B 84AA4695 87FBDDAF 9D114082


    V = HMAC(K, V) is
                 07730E3C BFFD3CAF D7A8AAE2 BF01D601 4301E24D


  Update (Key, V):

    Key is
                 8942A54F 349E281B 84AA4695 87FBDDAF 9D114082


    V is
                 07730E3C BFFD3CAF D7A8AAE2 BF01D601 4301E24D

**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 320

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                 D1A9C1A2 2C84FC23 FF2227EF 98EC8BA9 DF2A209B


    temp is
                 D1A9C1A2 2C84FC23 FF2227EF 98EC8BA9 DF2A209B


  ------------

    V = HMAC(K, V) is
                 A1DB0980 9F57BFEA E5B3E5F1 46C75F2D 8DBB5E4A
```

```
    temp is
                           D1A9C1A2 2C84FC23 FF2227EF 98EC8BA9
         DF2A209B A1DB0980 9F57BFEA E5B3E5F1 46C75F2D 8DBB5E4A


---------------------------

  returned_bits is
                           D1A9C1A2 2C84FC23 FF2227EF 98EC8BA9
         DF2A209B A1DB0980 9F57BFEA E5B3E5F1 46C75F2D 8DBB5E4A


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
              A1 DB09809F 57BFEAE5 B3E5F146 C75F2D8D BB5E4A00


    K = HMAC(K, V || 0x00 || provided_data) is
                 BDE1B46C DC5413B3 D9F735AC DB80B13C 57BFE473


    V = HMAC(K, V) is
                 725A3C78 20DE1A06 D095819C CF6F2C9B 3A67F2CE


rnd_val is
                           D1A9C1A2 2C84FC23 FF2227EF 98EC8BA9
         DF2A209B A1DB0980 9F57BFEA E5B3E5F1 46C75F2D 8DBB5E4A
```

```
###############################################################

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                  202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


  Key is
                                                        00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                        01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    ------------

    V || 0x00 || provided_data is
                    010101 01010101 01010101 01010101 01010101
        01010101 01010101 01000001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        B1F7F90A
```

```
        6FFA27B5 34FB2454 58934840 532A856D 5FC3E322 5AD0C4EE


    V = HMAC(K, V) is
                                                        F679095D
        7D62ED32 D35CC35C F8209B48 BA2463EF E19F5416 4825ADB5


    ------------

    V || 0x01 || provided_data is
                   F67909 5D7D62ED 32D35CC3 5CF8209B 48BA2463
        EFE19F54 164825AD B5010001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    K = HMAC(K, V || 0x01 || provided_data) is
                                                        69E16A0D
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


    V = HMAC(K, V) is
                                                        BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


  Update (Key, V):

    Key is
                                                        69E16A0D
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


    V is
                                                        BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate
```

```
  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                          2444F876
        2695FE82 C2CA72C9 C5834B94 8C9C334C C922A81A EABC53D9


    temp is
                                                          2444F876
        2695FE82 C2CA72C9 C5834B94 8C9C334C C922A81A EABC53D9


  ------------

    V = HMAC(K, V) is
                                                          4962FF27
        345EF1E3 E199DDE5 E586800E 40C4B369 8F84FFE1 580EA6A9


    temp is
                                                 2444F876 2695FE82
        C2CA72C9 C5834B94 8C9C334C C922A81A EABC53D9 4962FF27
        345EF1E3 E199DDE5 E586800E 40C4B369 8F84FFE1 580EA6A9


---------------------------

  returned_bits is
                                                 2444F876 2695FE82
        C2CA72C9 C5834B94 8C9C334C C922A81A EABC53D9 4962FF27
        345EF1E3 E199DDE5 E586800E 40C4B369 8F84FFE1 580EA6A9


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------
```

```
    V || 0x00 || provided_data is
                                                        49 62FF2734
        5EF1E3E1 99DDE5E5 86800E40 C4B3698F 84FFE158 0EA6A900


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          CB3DFDD4
        13A75233 0768D47A 0F63EC98 E5A16D2D 8DA28CD6 ABC9BEE0


    V = HMAC(K, V) is
                                                          43F9FE36
        663484FF 28F83061 90496111 1D919505 0C6268CE 07F86D55


rnd_val is
                                              2444F876 2695FE82
        C2CA72C9 C5834B94 8C9C334C C922A81A EABC53D9 4962FF27
        345EF1E3 E199DDE5 E586800E 40C4B369 8F84FFE1 580EA6A9


----------------------------------------------------------------

Second call to Generate

****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                          C2FD2E69
        DD13C1AB 0B9E4182 4109E257 22DC2248 3ADFE7C1 C556D924


    temp is
                                                          C2FD2E69
        DD13C1AB 0B9E4182 4109E257 22DC2248 3ADFE7C1 C556D924
```

```
  ------------

    V = HMAC(K, V) is
                                                          45EDDEB3
        C98DC11C 51F59F2A A00F9DC2 C22DC9BD 3050F06E B516B98D


    temp is
                                              C2FD2E69 DD13C1AB
        0B9E4182 4109E257 22DC2248 3ADFE7C1 C556D924 45EDDEB3
        C98DC11C 51F59F2A A00F9DC2 C22DC9BD 3050F06E B516B98D


---------------------------

  returned_bits is
                                              C2FD2E69 DD13C1AB
        0B9E4182 4109E257 22DC2248 3ADFE7C1 C556D924 45EDDEB3
        C98DC11C 51F59F2A A00F9DC2 C22DC9BD 3050F06E B516B98D


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                       45 EDDEB3C9
        8DC11C51 F59F2AA0 0F9DC2C2 2DC9BD30 50F06EB5 16B98D00


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          0D7D695F
        79040A7D B6A96BB9 CAB37A2D B22D43D6 E96FCDA2 581B6D4E


    V = HMAC(K, V) is
                                                          BDB549A1
        495B54BB 36F670C6 2DCD0699 903211BE 4A3506B9 5EE8F8C7


rnd_val is
```

```
                                                C2FD2E69 DD13C1AB
        0B9E4182 4109E257 22DC2248 3ADFE7C1 C556D924 45EDDEB3
        C98DC11C 51F59F2A A00F9DC2 C22DC9BD 3050F06E B516B98D


##############################################################

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                  A0A1A2 A3A4A5A6
```

```
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                 202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                              0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


  Key is
                                                       00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                       01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                              0001 02030405 06070809 0A0B0C0D
```

```
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


  ------------

  V || 0x00 || provided_data is
                 010101 01010101 01010101 01010101 01010101
    01010101 01010101 01000001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


  K = HMAC(K, V || 0x00 || provided_data) is
                                                    B1F7F90A
    6FFA27B5 34FB2454 58934840 532A856D 5FC3E322 5AD0C4EE


  V = HMAC(K, V) is
                                                    F679095D
    7D62ED32 D35CC35C F8209B48 BA2463EF E19F5416 4825ADB5


  ------------

  V || 0x01 || provided_data is
                 F67909 5D7D62ED 32D35CC3 5CF8209B 48BA2463
    EFE19F54 164825AD B5010001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


  K = HMAC(K, V || 0x01 || provided_data) is
                                                    69E16A0D
    59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


  V = HMAC(K, V) is
                                                    BE23F2F3
    66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


Update (Key, V):

  Key is
                                                    69E16A0D
```

```
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


    V is
                                                          BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                   BE23F2F3 66C83C79 D6A17791
        99855104 4B6479EB 3C1F18E6 E3975E06 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          C2B0B628
```

```
      4B609F8C F9C532F2 3A4FBC51 80B893E9 9377214A 14029FE4


  V = HMAC(K, V) is
                                                        B574BE90
      67E03706 A28C8AA4 B2C5E0C0 95434964 2439A2DD 5E8DB295


  ------------

  V || 0x01 || provided_data is
                                  B574BE90 67E03706 A28C8AA4
      B2C5E0C0 95434964 2439A2DD 5E8DB295 01606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  K = HMAC(K, V || 0x01 || provided_data) is
                                                        7FF56354
      5662FD74 EA9F2E45 9C5685A8 258DFEE3 5420638C 333617E0


  V = HMAC(K, V) is
                                                        EA32E139
      1A80FD6F 6CD28207 C229C386 E68499F3 9A1D432A B303BAC0


------------

  V = HMAC(K, V) is
                                                        F9CA2486
      FCBED54C F88DFAA8 B87959D7 0BD1048E CD01FA2E B4375028


  temp is
                                                        F9CA2486
      FCBED54C F88DFAA8 B87959D7 0BD1048E CD01FA2E B4375028


------------

  V = HMAC(K, V) is
                                                        8860ACC0
      1EF2DC2C 47D29FD9 9B353754 EA45EF0F 45074520 B4591045
```

```
    temp is
                                                F9CA2486 FCBED54C
        F88DFAA8 B87959D7 0BD1048E CD01FA2E B4375028 8860ACC0
        1EF2DC2C 47D29FD9 9B353754 EA45EF0F 45074520 B4591045


---------------------------

  returned_bits is
                                                F9CA2486 FCBED54C
        F88DFAA8 B87959D7 0BD1048E CD01FA2E B4375028 8860ACC0
        1EF2DC2C 47D29FD9 9B353754 EA45EF0F 45074520 B4591045


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                    8860ACC0 1EF2DC2C 47D29FD9
        9B353754 EA45EF0F 45074520 B4591045 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          279D1B68
        E24558AE 38BF95EC A2095AB3 32520665 0571DC01 D727770E


    V = HMAC(K, V) is
                                                          BBDADA2A
        0BAFC0AB 43FF2F3E F8323A11 1C06AA01 CB4AE54C 6522409D


    ------------
```

```
    V || 0x01 || provided_data is
                                    BBDADA2A 0BAFC0AB 43FF2F3E
        F8323A11 1C06AA01 CB4AE54C 6522409D 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                                                        8F137BBC
        45EB987E 7610C142 7E0A42CC 9DE74BAC F04B8E7B AB144EC0


    V = HMAC(K, V) is
                                                        CC72D1CB
        867CBE33 96B27783 6C3DA456 6D01E5C3 F9B37262 1C3C4094


rnd_val is
                                               F9CA2486 FCBED54C
        F88DFAA8 B87959D7 0BD1048E CD01FA2E B4375028 8860ACC0
        1EF2DC2C 47D29FD9 9B353754 EA45EF0F 45074520 B4591045


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                 A0A1A2 A3A4A5A6
```

```
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  ------------

  V || 0x00 || provided_data is
                                CC72D1CB 867CBE33 96B27783
    6C3DA456 6D01E5C3 F9B37262 1C3C4094 00A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x00 || provided_data) is
                                                    BADF9387
    FF7212EE DAE531DD F1D69F9E 2938BB4D 837DF2AD 07E3F89B


  V = HMAC(K, V) is
                                                    36FB6EAE
    622876D7 DE3E66B1 D3295F5E 373419CF 11FF31C6 568E00B5


  ------------

  V || 0x01 || provided_data is
                                36FB6EAE 622876D7 DE3E66B1
    D3295F5E 373419CF 11FF31C6 568E00B5 01A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x01 || provided_data) is
                                                    83EF49A7
    A1758EAE 37E40BE9 F7A87929 C2702BC2 AB7244DD 527B86AC


  V = HMAC(K, V) is
                                                    C2E02384
    8D14026B 8CC97914 E9E9DA72 298F6334 AA012B34 9A8D4792


------------

  V = HMAC(K, V) is
                                                    96D23972
```

```
        60FA9F7D 085F9CDC B3EBAA39 A0B2E4B4 8C5858B9 88357FE6


    temp is
                                                        96D23972
        60FA9F7D 085F9CDC B3EBAA39 A0B2E4B4 8C5858B9 88357FE6


  ------------

    V = HMAC(K, V) is
                                                        32985C91
        FC3A8A58 3441856D 0C1B1059 C7153B91 1DE34048 425E3A42


    temp is
                                                96D23972 60FA9F7D
        085F9CDC B3EBAA39 A0B2E4B4 8C5858B9 88357FE6 32985C91
        FC3A8A58 3441856D 0C1B1059 C7153B91 1DE34048 425E3A42


--------------------------

  returned_bits is
                                                96D23972 60FA9F7D
        085F9CDC B3EBAA39 A0B2E4B4 8C5858B9 88357FE6 32985C91
        FC3A8A58 3441856D 0C1B1059 C7153B91 1DE34048 425E3A42


  call Update(additional_input, K, V)
--------------------------

  Update

    provided_data
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                                    32985C91 FC3A8A58 3441856D
        0C1B1059 C7153B91 1DE34048 425E3A42 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
```

```
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        47D94E6B
        04AFC62D 1F5C2D66 C423787F 3117AAFE BE0A1DDE 420377DC


    V = HMAC(K, V) is
                                                        ECAF7807
        CD949FD7 30B12F60 927CCFA1 F3EBE260 DE99E007 E49FEF48


    ------------

    V || 0x01 || provided_data is
                                    ECAF7807 CD949FD7 30B12F60
        927CCFA1 F3EBE260 DE99E007 E49FEF48 01A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                                                        BC8C708C
        E66DA5EC D09AD5C5 75A56079 EF34217A FBC4CD18 697C739A


    V = HMAC(K, V) is
                                                        D8B3E4BE
        638D71E2 D7B691E8 81680E60 69B3E4D9 9FCA0557 6D0203F7


rnd_val is
                                               96D23972 60FA9F7D
        085F9CDC B3EBAA39 A0B2E4B4 8C5858B9 88357FE6 32985C91
        FC3A8A58 3441856D 0C1B1059 C7153B91 1DE34048 425E3A42


################################################################

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224
```

```
    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                  202122 23242526
```

```
    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                                        00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                        01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------

    V || 0x00 || provided_data is
                                                          0101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010000 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
```

```
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        B45032CF
        6A06E937 50DBD791 1C1F7701 11FA85E4 522863CA 4B8B66E7


    V = HMAC(K, V) is
                                                        A00F5F20
        C0D5BC5D CCDFDEC7 8839E0D5 376D22CC A1ABEB9A 2FC53CAC


    ------------

    V || 0x01 || provided_data is
                                                            A00F
        5F20C0D5 BC5DCCDF DEC78839 E0D5376D 22CCA1AB EB9A2FC5
        3CAC0100 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x01 || provided_data) is
                                                        4F7FCBA2
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


    V = HMAC(K, V) is
                                                        D0DE6F99
        D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


Update (Key, V):

    Key is
                                                        4F7FCBA2
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


    V is
                                                        D0DE6F99
```

```
        D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                        CC52B803
        A2BE29C1 3669C492 60C80FAB A2C8079E 12D929B0 19A229A2


    temp is
                                                        CC52B803
        A2BE29C1 3669C492 60C80FAB A2C8079E 12D929B0 19A229A2


  ------------

    V = HMAC(K, V) is
                                                        3EBC03FA
        0962232F 6D92E3E4 432DCD20 B62A1F3B AC98B7C2 5A85A1C9


    temp is
                                               CC52B803 A2BE29C1
        3669C492 60C80FAB A2C8079E 12D929B0 19A229A2 3EBC03FA
        0962232F 6D92E3E4 432DCD20 B62A1F3B AC98B7C2 5A85A1C9


---------------------------

  returned_bits is
                                               CC52B803 A2BE29C1
        3669C492 60C80FAB A2C8079E 12D929B0 19A229A2 3EBC03FA
        0962232F 6D92E3E4 432DCD20 B62A1F3B AC98B7C2 5A85A1C9
```

```
  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                        3E BC03FA09
        62232F6D 92E3E443 2DCD20B6 2A1F3BAC 98B7C25A 85A1C900


    K = HMAC(K, V || 0x00 || provided_data) is
                                                       BE844670
        9C81C7A0 818B6639 84595EC1 EDCCA3F7 C6205C42 2A32061F


    V = HMAC(K, V) is
                                                       F6A634C4
        8CA0EA19 687D5438 656915AF CF76AC73 B3386CBC BD093016


rnd_val is
                                               CC52B803 A2BE29C1
        3669C492 60C80FAB A2C8079E 12D929B0 19A229A2 3EBC03FA
        0962232F 6D92E3E4 432DCD20 B62A1F3B AC98B7C2 5A85A1C9


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------
```

```
    V = HMAC(K, V) is
                                                          1A6131F5
        FBE23C94 750185A4 F496EFB4 108F5125 CEBDCF02 746B32FD


    temp is
                                                          1A6131F5
        FBE23C94 750185A4 F496EFB4 108F5125 CEBDCF02 746B32FD


  ------------

    V = HMAC(K, V) is
                                                          952AEC16
        BD2538AB E16C2C99 245C8B3C 3A2E77CC 8BC86FAC 26CE278F


    temp is
                                                 1A6131F5 FBE23C94
        750185A4 F496EFB4 108F5125 CEBDCF02 746B32FD 952AEC16
        BD2538AB E16C2C99 245C8B3C 3A2E77CC 8BC86FAC 26CE278F


---------------------------

  returned_bits is
                                                 1A6131F5 FBE23C94
        750185A4 F496EFB4 108F5125 CEBDCF02 746B32FD 952AEC16
        BD2538AB E16C2C99 245C8B3C 3A2E77CC 8BC86FAC 26CE278F


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                       95 2AEC16BD
        2538ABE1 6C2C9924 5C8B3C3A 2E77CC8B C86FAC26 CE278F00


    K = HMAC(K, V || 0x00 || provided_data) is
```

                                                    2E7B1838
        458F0B0B 989DD5C1 6E4CAC18 25A5D73B 6B957C70 6F3B9941

    V = HMAC(K, V) is
                                                    81046D3D
        D2F3DFA4 5BD97475 49EB1880 7CA55CE0 1F3FEB35 837C2530

rnd_val is
                                            1A6131F5 FBE23C94
        750185A4 F496EFB4 108F5125 CEBDCF02 746B32FD 952AEC16
        BD2538AB E16C2C99 245C8B3C 3A2E77CC 8BC86FAC 26CE278F

##

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                              000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536

    EntropyInput1 (for Reseed1) =
                                              808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

    EntropyInput2 (for Reseed2) =
                                              C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6

    Nonce =
                                              202122 23242526

```
    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                202122 23242526


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
               00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
```

```
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                                          00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                          01010101
        01010101 01010101 01010101 01010101 01010101 01010101


----------------------------

  Update

    provided_data
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------

    V || 0x00 || provided_data is
                                                            0101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010000 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          B45032CF
        6A06E937 50DBD791 1C1F7701 11FA85E4 522863CA 4B8B66E7


    V = HMAC(K, V) is
                                                          A00F5F20
        C0D5BC5D CCDFDEC7 8839E0D5 376D22CC A1ABEB9A 2FC53CAC
```

```
    ------------

    V || 0x01 || provided_data is
                                                            A00F
        5F20C0D5 BC5DCCDF DEC78839 E0D5376D 22CCA1AB EB9A2FC5
        3CAC0100 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x01 || provided_data) is
                                                        4F7FCBA2
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


    V = HMAC(K, V) is
                                                        D0DE6F99
        D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


  Update (Key, V):

    Key is
                                                        4F7FCBA2
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


    V is
                                                        D0DE6F99
        D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


-----------------------------------------------------------

First call to Generate

***********************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448
```

```
    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                  D0DE6F99 D9E7DF8C 07E9F4D7
        5E05B73E FDE0834B 2E19CC1F DC0FC853 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        DBA3E0DA
        7D398C32 BA5CB4CE FEC678BC 42C2E23F 51458216 227EDD6E


    V = HMAC(K, V) is
                                                        D20CD00C
        4C59B384 24D4421A 4294D0CC 4946A992 42B842B8 467D7C74


    ------------

    V || 0x01 || provided_data is
                                  D20CD00C 4C59B384 24D4421A
        4294D0CC 4946A992 42B842B8 467D7C74 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
```

```
                                                        36EAE5C0
        D729D9D4 37311A3D 9E412E01 E3B10E2C E727C770 2DCFD9ED


    V = HMAC(K, V) is
                                                        D1CFC04F
        A80E88F6 849054F3 20CB84E5 DB77F3B7 EBBE820A F16F006A


  ------------

    V = HMAC(K, V) is
                                                        499A959D
        E618773D F17A5372 074DA0AA 7A7B121C D31DA444 F65F9782


    temp is
                                                        499A959D
        E618773D F17A5372 074DA0AA 7A7B121C D31DA444 F65F9782


  ------------

    V = HMAC(K, V) is
                                                        801EAFE1
        ED3A3D40 06C3A321 C5FA1261 CA596C75 E25CBC26 23189FC4


    temp is
                                            499A959D E618773D
        F17A5372 074DA0AA 7A7B121C D31DA444 F65F9782 801EAFE1
        ED3A3D40 06C3A321 C5FA1261 CA596C75 E25CBC26 23189FC4


---------------------------

  returned_bits is
                                            499A959D E618773D
        F17A5372 074DA0AA 7A7B121C D31DA444 F65F9782 801EAFE1
        ED3A3D40 06C3A321 C5FA1261 CA596C75 E25CBC26 23189FC4


  call Update(additional_input, K, V)
---------------------------

  Update
```

```
    provided_data
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                                   801EAFE1 ED3A3D40 06C3A321
        C5FA1261 CA596C75 E25CBC26 23189FC4 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        3CCE29FF
        4BB898B5 F67EFC0B 1D967D19 8D39C0C8 E7B4AB49 2C5B17D9


    V = HMAC(K, V) is
                                                        3E97F0F4
        27AF7B10 F40CC786 0E9A5E04 1B1CC7EB D670E8A9 55BCFEC8


    ------------

    V || 0x01 || provided_data is
                                   3E97F0F4 27AF7B10 F40CC786
        0E9A5E04 1B1CC7EB D670E8A9 55BCFEC8 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                                                        F433D100
        3FBFAB7B 3708531F 206D93EB 0A4F9FD8 43F3BF00 9D9815A1


    V = HMAC(K, V) is
                                                        2F61B62E
        88FDA431 B829880A DC472F8B 44BAA571 D27878F0 36D72ED2


rnd_val is
```

```
                                                499A959D E618773D
        F17A5372 074DA0AA 7A7B121C D31DA444 F65F9782 801EAFE1
        ED3A3D40 06C3A321 C5FA1261 CA596C75 E25CBC26 23189FC4


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                                  2F61B62E 88FDA431 B829880A
        DC472F8B 44BAA571 D27878F0 36D72ED2 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        5F2F354C
        E2992DAF E9FF8612 013C50B3 A38F5AED E8B88F87 84EAD08C
```

```
  V = HMAC(K, V) is
                                                      8C5574C7
      9376296E E2463C2B CB39BB3D 85F80542 BE686350 2C0AC1F8


  ------------

  V || 0x01 || provided_data is
                                  8C5574C7 9376296E E2463C2B
      CB39BB3D 85F80542 BE686350 2C0AC1F8 01A0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x01 || provided_data) is
                                                      3D854845
      99F8D48D A11C61F6 E954A100 DA4149D9 DCA75625 911A42A5


  V = HMAC(K, V) is
                                                      15536D25
      35361578 6B563F02 64CFF800 00D75389 4C5A23AE 34403B13


------------

  V = HMAC(K, V) is
                                                      0AD161E1
      9C70E4F5 29A31D94 D4913162 9A24E77B 5545AE91 F23A7D1C


  temp is
                                                      0AD161E1
      9C70E4F5 29A31D94 D4913162 9A24E77B 5545AE91 F23A7D1C


------------

  V = HMAC(K, V) is
                                                      6FFB0C00
      19640D0F 75B62D31 431557E9 A87A6714 0F9C1BA3 917A510C


  temp is
                                              0AD161E1 9C70E4F5
      29A31D94 D4913162 9A24E77B 5545AE91 F23A7D1C 6FFB0C00
```

```
        19640D0F 75B62D31 431557E9 A87A6714 0F9C1BA3 917A510C


--------------------------

  returned_bits is
                                                0AD161E1 9C70E4F5
        29A31D94 D4913162 9A24E77B 5545AE91 F23A7D1C 6FFB0C00
        19640D0F 75B62D31 431557E9 A87A6714 0F9C1BA3 917A510C


  call Update(additional_input, K, V)
--------------------------

  Update

    provided_data
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                                    6FFB0C00 19640D0F 75B62D31
        431557E9 A87A6714 0F9C1BA3 917A510C 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        E7CB8EB0
        7E6A6CA3 1F44AB18 B09D9772 C8D0C54E 1909B375 BA3FE64F


    V = HMAC(K, V) is
                                                        C5CDA955
        5D4E8307 1F0DDC95 9D996CB1 88DCF23A 41953C90 28196F9E


    ------------

    V || 0x01 || provided_data is
                                    C5CDA955 5D4E8307 1F0DDC95
        9D996CB1 88DCF23A 41953C90 28196F9E 01A0A1A2 A3A4A5A6
```

```
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                                                        BFB6AFF8
        B2F1096D 92E05777 68B85EB7 32037CC1 B8775A71 3A0CE3BA


    V = HMAC(K, V) is
                                                        71BA6980
        76B9E948 8636D427 7A382EA7 D6774CE2 BE10F390 DA3F92D6


rnd_val is
                                              0AD161E1 9C70E4F5
        29A31D94 D4913162 9A24E77B 5545AE91 F23A7D1C 6FFB0C00
        19640D0F 75B62D31 431557E9 A87A6714 0F9C1BA3 917A510C


###############################################################

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
```

```
    Nonce =
                                                202122 23242526


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                              0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


  Key is
                                                        00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                        01010101
        01010101 01010101 01010101 01010101 01010101 01010101


--------------------------
```

Update

provided_data
                          0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526

V || 0x00 || provided_data is
              010101 01010101 01010101 01010101 01010101
    01010101 01010101 01000001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526

K = HMAC(K, V || 0x00 || provided_data) is
                                                    B1F7F90A
    6FFA27B5 34FB2454 58934840 532A856D 5FC3E322 5AD0C4EE

V = HMAC(K, V) is
                                                    F679095D
    7D62ED32 D35CC35C F8209B48 BA2463EF E19F5416 4825ADB5

V || 0x01 || provided_data is
                F67909 5D7D62ED 32D35CC3 5CF8209B 48BA2463
    EFE19F54 164825AD B5010001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526

K = HMAC(K, V || 0x01 || provided_data) is
                                                    69E16A0D
    59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1

V = HMAC(K, V) is
                                                    BE23F2F3
    66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06

```
  Update (Key, V):

    Key is
                                                        69E16A0D
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


    V is
                                                        BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is  <empty>

  Seed_Material is
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  Key is
                                                        69E16A0D
```

```
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


  V is
                                                           BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


---------------------------

  Update

    provided_data
                                                    808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    ------------

    V || 0x00 || provided_data is
                                  BE23F2F3 66C83C79 D6A17791
        99855104 4B6479EB 3C1F18E6 E3975E06 00808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                           2216735C
        C98E7189 2680E0C4 13B68700 5752DBFF E5AEA7A0 BCFA0244


    V = HMAC(K, V) is
                                                           3776E0E0
        CFF312C1 5551DC10 FA8B40E3 226C9C02 48544531 020DC532


    ------------

    V || 0x01 || provided_data is
                                  3776E0E0 CFF312C1 5551DC10
        FA8B40E3 226C9C02 48544531 020DC532 01808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                                                          95603C76
        4BC3CB23 7C2FC6B0 651F858F 2DB9378A B26ADB6E 2632437C


    V = HMAC(K, V) is
                                                          7DC1DD01
        33C30D6B 4862D627 09514D76 DD15699C 598C173B BB7F8129


  Update (Key, V):

    Key is
                                                          95603C76
        4BC3CB23 7C2FC6B0 651F858F 2DB9378A B26ADB6E 2632437C


    V is
                                                          7DC1DD01
        33C30D6B 4862D627 09514D76 DD15699C 598C173B BB7F8129


*****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                          A07AA4CC
        1716E214 96DB43E3 05B00400 578D3227 E224ED5F 08D881B7


    temp is
                                                          A07AA4CC
        1716E214 96DB43E3 05B00400 578D3227 E224ED5F 08D881B7


  ------------

    V = HMAC(K, V) is
                                                          04CA6EFF
```

```
        3E9CA847 C90660DF 36517813 AC13913B AC1E822B 5883281A


    temp is
                                                A07AA4CC 1716E214
        96DB43E3 05B00400 578D3227 E224ED5F 08D881B7 04CA6EFF
        3E9CA847 C90660DF 36517813 AC13913B AC1E822B 5883281A


---------------------------

  returned_bits is
                                                A07AA4CC 1716E214
        96DB43E3 05B00400 578D3227 E224ED5F 08D881B7 04CA6EFF
        3E9CA847 C90660DF 36517813 AC13913B AC1E822B 5883281A


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                      04 CA6EFF3E
        9CA847C9 0660DF36 517813AC 13913BAC 1E822B58 83281A00


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        707AB325
        EC6269F7 8B43B0CB B6D18E20 B78944EF 3028763E 3C9D6486


    V = HMAC(K, V) is
                                                        0494DEDA
        33EE314C 09879164 4E23201A 8AC6D0CB 6085548C B89260B8


rnd_val is
                                                A07AA4CC 1716E214
        96DB43E3 05B00400 578D3227 E224ED5F 08D881B7 04CA6EFF
        3E9CA847 C90660DF 36517813 AC13913B AC1E822B 5883281A
```

```
------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is  <empty>

  Seed_Material is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  Key is
                                                        707AB325
        EC6269F7 8B43B0CB B6D18E20 B78944EF 3028763E 3C9D6486


  V is
                                                        0494DEDA
        33EE314C 09879164 4E23201A 8AC6D0CB 6085548C B89260B8


---------------------------

  Update
```

```
  provided_data
                                                  C0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  ------------

  V || 0x00 || provided_data is
                                0494DEDA 33EE314C 09879164
      4E23201A 8AC6D0CB 6085548C B89260B8 00C0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x00 || provided_data) is
                                                        4EABCEE2
      A40FED76 141D2FF2 77F6B4C4 F16BF785 DC98CE03 8D8634C6


  V = HMAC(K, V) is
                                                        E0493CBD
      0E533288 16113396 BF703F25 B9AD4748 19E1D904 5D4540FA


  ------------

  V || 0x01 || provided_data is
                                E0493CBD 0E533288 16113396
      BF703F25 B9AD4748 19E1D904 5D4540FA 01C0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x01 || provided_data) is
                                                        61ED54C4
      6DE78330 A4E25662 8A1F8417 70C049F7 F9DE7C39 040ADA10


  V = HMAC(K, V) is
                                                        D0758ED6
      5D5C2F3D BFA33CD2 408125FA 8AB1C03F 0A4DB8C7 3D607F53


Update (Key, V):
```

```
    Key is
                                                        61ED54C4
        6DE78330 A4E25662 8A1F8417 70C049F7 F9DE7C39 040ADA10


    V is
                                                        D0758ED6
        5D5C2F3D BFA33CD2 408125FA 8AB1C03F 0A4DB8C7 3D607F53


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                        1FCC850D
        8F3E8B56 98D03900 F3D6BE3F 3EAD1260 09BCE060 4D0B60DF


    temp is
                                                        1FCC850D
        8F3E8B56 98D03900 F3D6BE3F 3EAD1260 09BCE060 4D0B60DF


  ------------

    V = HMAC(K, V) is
                                                        CE17F743
        CE0913AB CAF36FC3 082F89D2 F8AD52A8 A0DF633F A3C108A7


    temp is
                                                1FCC850D 8F3E8B56
        98D03900 F3D6BE3F 3EAD1260 09BCE060 4D0B60DF CE17F743
        CE0913AB CAF36FC3 082F89D2 F8AD52A8 A0DF633F A3C108A7


---------------------------

  returned_bits is
```

```
                                                1FCC850D 8F3E8B56
        98D03900 F3D6BE3F 3EAD1260 09BCE060 4D0B60DF CE17F743
        CE0913AB CAF36FC3 082F89D2 F8AD52A8 A0DF633F A3C108A7


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                      CE 17F743CE
        0913ABCA F36FC308 2F89D2F8 AD52A8A0 DF633FA3 C108A700


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        B4838859
        F3630EFF 7568590A 01D2E40C 42EABF47 43C03872 682F5B64


    V = HMAC(K, V) is
                                                        074F3021
        F6A0D2FF 03FAEA1C 94F63BD1 8CB9F9E0 5058DDE6 7D81AE13


rnd_val is
                                                1FCC850D 8F3E8B56
        98D03900 F3D6BE3F 3EAD1260 09BCE060 4D0B60DF CE17F743
        CE0913AB CAF36FC3 082F89D2 F8AD52A8 A0DF633F A3C108A7


#############################################################

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
```

```
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                202122 23242526


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                202122 23242526


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


  Key is
                                                        00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                        01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                               0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    ------------

    V || 0x00 || provided_data is
                    010101 01010101 01010101 01010101 01010101
        01010101 01010101 01000001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        B1F7F90A
        6FFA27B5 34FB2454 58934840 532A856D 5FC3E322 5AD0C4EE
```

```
    V = HMAC(K, V) is
                                                          F679095D
        7D62ED32 D35CC35C F8209B48 BA2463EF E19F5416 4825ADB5


    ------------

    V || 0x01 || provided_data is
                   F67909 5D7D62ED 32D35CC3 5CF8209B 48BA2463
        EFE19F54 164825AD B5010001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2E2F3031 32333435 36202122 23242526


    K = HMAC(K, V || 0x01 || provided_data) is
                                                          69E16A0D
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


    V = HMAC(K, V) is
                                                          BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


  Update (Key, V):

    Key is
                                                          69E16A0D
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


    V is
                                                          BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


-----------------------------------------------------------------

First call to Generate

*****************************************************************

HMAC_DRBG_Generate
```

```
  requested_number_of_bits = 448

    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Seed_Material is
                             8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Key is
                                                      69E16A0D
        59DD6B13 0C941512 AFAE8492 C4ECFAA0 95B89282 5E814FF1


  V is
                                                      BE23F2F3
        66C83C79 D6A17791 99855104 4B6479EB 3C1F18E6 E3975E06


---------------------------

  Update
```

```
provided_data
                          8081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


------------

V || 0x00 || provided_data is
               BE23F2 F366C83C 79D6A177 91998551 044B6479
    EB3C1F18 E6E3975E 06008081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


K = HMAC(K, V || 0x00 || provided_data) is
                                                    FA5BDF71
    2EB399A3 81F352A3 D22DFFD5 47F205D4 9C4D85C2 8433BE8D


V = HMAC(K, V) is
                                                    EAB91B1F
    72E91DCC 52F897BD 0725D58E 8761300A 8ADBF928 67325DFC


------------

V || 0x01 || provided_data is
               EAB91B 1F72E91D CC52F897 BD0725D5 8E876130
    0A8ADBF9 2867325D FC018081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


K = HMAC(K, V || 0x01 || provided_data) is
                                                    091ED0A7
    D134660B 75769A07 F26DAD14 5CB66631 C18A01FB BFB92C60
```

```
    V = HMAC(K, V) is
                                                        994C10C0
        F06B1287 0E8AEE05 D92245DB FCCB6067 21E3D98A 00B74C0C

  Update (Key, V):

    Key is
                                                        091ED0A7
        D134660B 75769A07 F26DAD14 5CB66631 C18A01FB BFB92C60

    V is
                                                        994C10C0
        F06B1287 0E8AEE05 D92245DB FCCB6067 21E3D98A 00B74C0C

**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                        E28DA53A
        461C412D 7E57C3A2 E4A93A82 13EFC9E7 A9BD99CD F8624A25

    temp is
                                                        E28DA53A
        461C412D 7E57C3A2 E4A93A82 13EFC9E7 A9BD99CD F8624A25

  ------------

    V = HMAC(K, V) is
                                                        1EE9B715
        33C5D916 05FA2C6B 14C50A75 2DF39B9B 0DE877B7 645A3D2F

    temp is
                                                E28DA53A 461C412D
```

```
        7E57C3A2 E4A93A82 13EFC9E7 A9BD99CD F8624A25 1EE9B715
        33C5D916 05FA2C6B 14C50A75 2DF39B9B 0DE877B7 645A3D2F


---------------------------

  returned_bits is
                                              E28DA53A 461C412D
        7E57C3A2 E4A93A82 13EFC9E7 A9BD99CD F8624A25 1EE9B715
        33C5D916 05FA2C6B 14C50A75 2DF39B9B 0DE877B7 645A3D2F


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                    1E E9B71533
        C5D91605 FA2C6B14 C50A752D F39B9B0D E877B764 5A3D2F00


    K = HMAC(K, V || 0x00 || provided_data) is
                                                      D3CE8637
        D87C38FB 1ABC374D E9CDDC6A A77892F2 FAD5D8A6 F008A917


    V = HMAC(K, V) is
                                                      45C6F054
        BBC02940 DE40A451 F276E995 CBC10660 AB1658B6 6B89B1C6


rnd_val is
                                              E28DA53A 461C412D
        7E57C3A2 E4A93A82 13EFC9E7 A9BD99CD F8624A25 1EE9B715
        33C5D916 05FA2C6B 14C50A75 2DF39B9B 0DE877B7 645A3D2F


-------------------------------------------------------------

Second call to Generate
```

```
***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Seed_Material is
                             C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Key is
                                                        D3CE8637
        D87C38FB 1ABC374D E9CDDC6A A77892F2 FAD5D8A6 F008A917


  V is
                                                        45C6F054
        BBC02940 DE40A451 F276E995 CBC10660 AB1658B6 6B89B1C6
```

```
---------------------------

  Update

    provided_data
                              C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                   45C6F0 54BBC029 40DE40A4 51F276E9 95CBC106
        60AB1658 B66B89B1 C600C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        7AA2ABB4
        10E64C6A 30A48CEC 96A95766 F0CB5574 709B6540 EB41ED8F


    V = HMAC(K, V) is
                                                        0C27DF08
        5E23EC39 6E5D6D06 EED6B0FE 2F9A24E8 7E52F526 B15E2633


    ------------

    V || 0x01 || provided_data is
                   0C27DF 085E23EC 396E5D6D 06EED6B0 FE2F9A24
        E87E52F5 26B15E26 3301C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
```

```
                                                          159FA328
        4A1E65D9 0AD889A0 9BAD44DA D0197935 E66C772E 68F2A468


    V = HMAC(K, V) is
                                                          FC104C95
        577F4259 7113809C 66AADAD8 998A788D E93B937F 70746973


  Update (Key, V):

    Key is
                                                          159FA328
        4A1E65D9 0AD889A0 9BAD44DA D0197935 E66C772E 68F2A468


    V is
                                                          FC104C95
        577F4259 7113809C 66AADAD8 998A788D E93B937F 70746973


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                          0A2E074D
        FF196BD8 2B8CC309 1A1C99C7 2220B0D2 154594EE 103398B8


    temp is
                                                          0A2E074D
        FF196BD8 2B8CC309 1A1C99C7 2220B0D2 154594EE 103398B8


  ------------

    V = HMAC(K, V) is
                                                          774050F6
        87EE6090 D0B415DD 1D3D9027 E9CB59AE 831EF109 C415BB4A
```

```
    temp is
                                                0A2E074D FF196BD8
        2B8CC309 1A1C99C7 2220B0D2 154594EE 103398B8 774050F6
        87EE6090 D0B415DD 1D3D9027 E9CB59AE 831EF109 C415BB4A


----------------------------

  returned_bits is
                                                0A2E074D FF196BD8
        2B8CC309 1A1C99C7 2220B0D2 154594EE 103398B8 774050F6
        87EE6090 D0B415DD 1D3D9027 E9CB59AE 831EF109 C415BB4A


  call Update(additional_input, K, V)
----------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                      77 4050F687
        EE6090D0 B415DD1D 3D9027E9 CB59AE83 1EF109C4 15BB4A00


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        36767608
        2B1FCB6D 186B60A2 BE241915 AB140381 7E759FAD F64064AC


    V = HMAC(K, V) is
                                                        FCB677C9
        D39629C3 EE57FA1D 81938307 A2AFFC50 7713068A 6F8F7BB4


rnd_val is
                                                0A2E074D FF196BD8
        2B8CC309 1A1C99C7 2220B0D2 154594EE 103398B8 774050F6
        87EE6090 D0B415DD 1D3D9027 E9CB59AE 831EF109 C415BB4A
```

```
###############################################################

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                  202122 23242526


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
```

```
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                  202122 23242526


    personal_str is
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                                        00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                        01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576
```

```
  ------------

  V || 0x00 || provided_data is
                                                              0101
      01010101 01010101 01010101 01010101 01010101 01010101
      01010000 01020304 05060708 090A0B0C 0D0E0F10 11121314
      15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
      2D2E2F30 31323334 35362021 22232425 26404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x00 || provided_data) is
                                                            B45032CF
      6A06E937 50DBD791 1C1F7701 11FA85E4 522863CA 4B8B66E7


  V = HMAC(K, V) is
                                                            A00F5F20
      C0D5BC5D CCDFDEC7 8839E0D5 376D22CC A1ABEB9A 2FC53CAC


  ------------

  V || 0x01 || provided_data is
                                                              A00F
      5F20C0D5 BC5DCCDF DEC78839 E0D5376D 22CCA1AB EB9A2FC5
      3CAC0100 01020304 05060708 090A0B0C 0D0E0F10 11121314
      15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
      2D2E2F30 31323334 35362021 22232425 26404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x01 || provided_data) is
                                                            4F7FCBA2
      3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


  V = HMAC(K, V) is
                                                            D0DE6F99
      D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


Update (Key, V):
```

```
    Key is
                                                          4F7FCBA2
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


    V is
                                                          D0DE6F99
        D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                               808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is  <empty>

  Seed_Material is
                                               808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  Key is
                                                          4F7FCBA2
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A
```

```
  V is
                                                          D0DE6F99
       D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


---------------------------

  Update

    provided_data
                                                 808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    ------------

    V || 0x00 || provided_data is
                                  D0DE6F99 D9E7DF8C 07E9F4D7
        5E05B73E FDE0834B 2E19CC1F DC0FC853 00808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          AC86F578
        BC8A381E D3D91289 BA72063E 7567F07D 8C7D2A0F 879FBD32


    V = HMAC(K, V) is
                                                          6AC3E086
        9913D864 5EA47BBD 8891ECC9 F41F7ED4 B129B9D3 E85995D6


    ------------

    V || 0x01 || provided_data is
                                  6AC3E086 9913D864 5EA47BBD
        8891ECC9 F41F7ED4 B129B9D3 E85995D6 01808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    K = HMAC(K, V || 0x01 || provided_data) is
                                                          5F540144
```

```
        2A22561B 2611D127 F6A18BEE FE11289D E4BF06A7 C9EA1E8F


    V = HMAC(K, V) is
                                                        1F7D5CBC
        DFFB3585 91ABDF03 42EBAF04 399A4D0B 3CB047FF 0179FA4D


  Update (Key, V):

    Key is
                                                        5F540144
        2A22561B 2611D127 F6A18BEE FE11289D E4BF06A7 C9EA1E8F


    V is
                                                        1F7D5CBC
        DFFB3585 91ABDF03 42EBAF04 399A4D0B 3CB047FF 0179FA4D


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                        ACD797A0
        7B378D0A D9A8FBE2 1683E7BB 8A3DF9CB 1346FF43 2EA75B47


    temp is
                                                        ACD797A0
        7B378D0A D9A8FBE2 1683E7BB 8A3DF9CB 1346FF43 2EA75B47


  ------------

    V = HMAC(K, V) is
                                                        66B7C754
        C4D06F4C 257537CC D9A399E5 986BBD30 085EEC86 01582911
```

```
    temp is
                                                ACD797A0 7B378D0A
        D9A8FBE2 1683E7BB 8A3DF9CB 1346FF43 2EA75B47 66B7C754
        C4D06F4C 257537CC D9A399E5 986BBD30 085EEC86 01582911


---------------------------

  returned_bits is
                                                ACD797A0 7B378D0A
        D9A8FBE2 1683E7BB 8A3DF9CB 1346FF43 2EA75B47 66B7C754
        C4D06F4C 257537CC D9A399E5 986BBD30 085EEC86 01582911


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                      66 B7C754C4
        D06F4C25 7537CCD9 A399E598 6BBD3008 5EEC8601 58291100


    K = HMAC(K, V || 0x00 || provided_data) is
                                                        DF30730C
        59996936 44B98F12 22B7F33A E6856E8E 13F74BBD BF9D1F48


    V = HMAC(K, V) is
                                                        92C3122C
        4EF67B98 1F418241 3D718E9B A800A2D7 A45F9E6E 07C9C86B


rnd_val is
                                                ACD797A0 7B378D0A
        D9A8FBE2 1683E7BB 8A3DF9CB 1346FF43 2EA75B47 66B7C754
        C4D06F4C 257537CC D9A399E5 986BBD30 085EEC86 01582911


-------------------------------------------------------------
```

```
Second call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is  <empty>

  Seed_Material is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  Key is
                                                        DF30730C
        59996936 44B98F12 22B7F33A E6856E8E 13F74BBD BF9D1F48


  V is
                                                        92C3122C
        4EF67B98 1F418241 3D718E9B A800A2D7 A45F9E6E 07C9C86B


---------------------------

  Update

    provided_data
                                                C0C1C2 C3C4C5C6
```

```
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  ------------

  V || 0x00 || provided_data is
                                92C3122C 4EF67B98 1F418241
    3D718E9B A800A2D7 A45F9E6E 07C9C86B 00C0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x00 || provided_data) is
                                                  4F2B28A0
    087B3D6D 2547F378 D7F9C755 9964D055 1645831E 741B6BA5


  V = HMAC(K, V) is
                                                  4C5DB5ED
    89B9E3C3 35D79EFB 4EF5B0F4 A1F4E9D0 F3EFA1D1 D086A7BE


  ------------

  V || 0x01 || provided_data is
                                4C5DB5ED 89B9E3C3 35D79EFB
    4EF5B0F4 A1F4E9D0 F3EFA1D1 D086A7BE 01C0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x01 || provided_data) is
                                                  4B1DC621
    0B96E8E4 2657BF25 CC14B415 9F740014 2491860B D9AA7A00


  V = HMAC(K, V) is
                                                  ED0C4699
    3DDFEB91 A7EF6E4E E9EDB613 9A4C283C 5D493EDB 482390D7


Update (Key, V):

  Key is
                                                  4B1DC621
```

```
        0B96E8E4 2657BF25 CC14B415 9F740014 2491860B D9AA7A00


    V is
                                                           ED0C4699
        3DDFEB91 A7EF6E4E E9EDB613 9A4C283C 5D493EDB 482390D7


***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                           3531CEE9
        F51FBCA7 361CD991 0AD3A973 416EA587 4A5E5868 3E81BA3B


    temp is
                                                           3531CEE9
        F51FBCA7 361CD991 0AD3A973 416EA587 4A5E5868 3E81BA3B


  ------------

    V = HMAC(K, V) is
                                                           A36A191C
        0B74EDCF 25803D0F 046B3071 738648A8 DC0D4ABC 8C3E5A20


    temp is
                                                 3531CEE9 F51FBCA7
        361CD991 0AD3A973 416EA587 4A5E5868 3E81BA3B A36A191C
        0B74EDCF 25803D0F 046B3071 738648A8 DC0D4ABC 8C3E5A20


---------------------------

  returned_bits is
                                                 3531CEE9 F51FBCA7
        361CD991 0AD3A973 416EA587 4A5E5868 3E81BA3B A36A191C
```

```
        0B74EDCF 25803D0F 046B3071 738648A8 DC0D4ABC 8C3E5A20


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                      A3 6A191C0B
        74EDCF25 803D0F04 6B307173 8648A8DC 0D4ABC8C 3E5A2000


    K = HMAC(K, V || 0x00 || provided_data) is
                                                     CC792D62
        9EC9C4C8 C7983EFA B1E76661 57D43B4F 2CE63DC9 7AE979B3


    V = HMAC(K, V) is
                                                     00EBEB5A
        D8543B8E 5070F6FE 05CB7072 F7D30B47 29B2F718 6841DCB5


rnd_val is
                                                3531CEE9 F51FBCA7
        361CD991 0AD3A973 416EA587 4A5E5868 3E81BA3B A36A191C
        0B74EDCF 25803D0F 046B3071 738648A8 DC0D4ABC 8C3E5A20


################################################################

HMAC_DRBG

    Requested Security Strength = 112

    Requested Hash Algorithm = SHA-224

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                202122 23242526


    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                202122 23242526


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                                        00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                        01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
              00 01020304 05060708 090A0B0C 0D0E0F10 11121314
        15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
        2D2E2F30 31323334 35362021 22232425 26404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------
```

```
  V || 0x00 || provided_data is
                                                              0101
      01010101 01010101 01010101 01010101 01010101 01010101
      01010000 01020304 05060708 090A0B0C 0D0E0F10 11121314
      15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
      2D2E2F30 31323334 35362021 22232425 26404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x00 || provided_data) is
                                                            B45032CF
      6A06E937 50DBD791 1C1F7701 11FA85E4 522863CA 4B8B66E7


  V = HMAC(K, V) is
                                                            A00F5F20
      C0D5BC5D CCDFDEC7 8839E0D5 376D22CC A1ABEB9A 2FC53CAC


  ------------

  V || 0x01 || provided_data is
                                                              A00F
      5F20C0D5 BC5DCCDF DEC78839 E0D5376D 22CCA1AB EB9A2FC5
      3CAC0100 01020304 05060708 090A0B0C 0D0E0F10 11121314
      15161718 191A1B1C 1D1E1F20 21222324 25262728 292A2B2C
      2D2E2F30 31323334 35362021 22232425 26404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x01 || provided_data) is
                                                            4F7FCBA2
      3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


  V = HMAC(K, V) is
                                                            D0DE6F99
      D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


Update (Key, V):

  Key is
                                                            4F7FCBA2
```

```
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


    V is
                                                          D0DE6F99
        D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Seed_Material is
                             8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
```

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Key is
                                                          4F7FCBA2
        3A6D7557 A0D657F7 57E3EBA4 6093D3BD F5D86BCF D941B53A


  V is
                                                          D0DE6F99
        D9E7DF8C 07E9F4D7 5E05B73E FDE0834B 2E19CC1F DC0FC853


---------------------------

  Update

    provided_data
                              8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                   D0DE6F 99D9E7DF 8C07E9F4 D75E05B7 3EFDE083
        4B2E19CC 1FDC0FC8 53008081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          7B84E441
        10AEB20F 7E6B716C C1CC579B 83DD4D9E 8ECB38BF 5F6525C3


    V = HMAC(K, V) is
                                                          A027489C
        623DFED2 455551AC 37A813AD 12D21A5D 0E886088 883BC831
```

```
    ------------

    V || 0x01 || provided_data is
                  A02748 9C623DFE D2455551 AC37A813 AD12D21A
        5D0E8860 88883BC8 31018081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                                                       56C32756
        61E13129 CBB88B5D 29C98DD9 FC5FC3E1 68A84827 0A1AF27E


    V = HMAC(K, V) is
                                                       A62217F1
        E0DDF482 4D64B43D 8A2493B8 7E366BCE 3688E103 059FC6A3


  Update (Key, V):

    Key is
                                                       56C32756
        61E13129 CBB88B5D 29C98DD9 FC5FC3E1 68A84827 0A1AF27E


    V is
                                                       A62217F1
        E0DDF482 4D64B43D 8A2493B8 7E366BCE 3688E103 059FC6A3


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                       C1DA29D0
        48DDBED3 DCCE1040 DCF74E66 0FC2D883 269E65B4 9DBFAD8E
```

```
    temp is
                                                          C1DA29D0
        48DDBED3 DCCE1040 DCF74E66 0FC2D883 269E65B4 9DBFAD8E


  ------------

    V = HMAC(K, V) is
                                                          C99CECB6
        5C4EE17A BC3E3A93 342750DC 623A92A8 2A12A05F 0E59B714


    temp is
                                                C1DA29D0 48DDBED3
        DCCE1040 DCF74E66 0FC2D883 269E65B4 9DBFAD8E C99CECB6
        5C4EE17A BC3E3A93 342750DC 623A92A8 2A12A05F 0E59B714


---------------------------

  returned_bits is
                                                C1DA29D0 48DDBED3
        DCCE1040 DCF74E66 0FC2D883 269E65B4 9DBFAD8E C99CECB6
        5C4EE17A BC3E3A93 342750DC 623A92A8 2A12A05F 0E59B714


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                       C9 9CECB65C
        4EE17ABC 3E3A9334 2750DC62 3A92A82A 12A05F0E 59B71400


    K = HMAC(K, V || 0x00 || provided_data) is
                                                          B2AA116E
        3C7B57EC 08806FC0 3A223326 0A5EA550 D83F0AFB 2390C539
```

```
    V = HMAC(K, V) is
                                                            B96A8DB8
        006DAF12 C4D23EAF 36935AB7 8FE914FD DD0D79BF A33D7465


rnd_val is
                                                C1DA29D0 48DDBED3
        DCCE1040 DCF74E66 0FC2D883 269E65B4 9DBFAD8E C99CECB6
        5C4EE17A BC3E3A93 342750DC 623A92A8 2A12A05F 0E59B714


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is
                                                  A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Seed_Material is
```

```
                            C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Key is
                                                    B2AA116E
        3C7B57EC 08806FC0 3A223326 0A5EA550 D83F0AFB 2390C539


  V is
                                                    B96A8DB8
        006DAF12 C4D23EAF 36935AB7 8FE914FD DD0D79BF A33D7465


---------------------------

  Update

    provided_data
                            C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                  B96A8D B8006DAF 12C4D23E AF36935A B78FE914
        FDDD0D79 BFA33D74 6500C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                    8D7799DF
        5B9F1037 ED8D020E BCE90603 FCEE0235 01078635 04B69414


    V = HMAC(K, V) is
```

```
                                                        8DDAAFC4
        6B81D406 918BD1EF CB37742E 43077C81 4D4D5879 2FB8B8FA


    ------------

    V || 0x01 || provided_data is
                   8DDAAF C46B81D4 06918BD1 EFCB3774 2E43077C
        814D4D58 792FB8B8 FA01C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                                                        2C50D3C3
        468AAE25 80069E95 CEA6AE36 9F46D9FA 42DBCFA1 78599093


    V = HMAC(K, V) is
                                                        DC2EAE8F
        7B370072 D450D431 86813E8A CA306B16 A27F5A2C 51464A0E


  Update (Key, V):

    Key is
                                                        2C50D3C3
        468AAE25 80069E95 CEA6AE36 9F46D9FA 42DBCFA1 78599093


    V is
                                                        DC2EAE8F
        7B370072 D450D431 86813E8A CA306B16 A27F5A2C 51464A0E


****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 448

    additional_input is  <empty>

  ------------
```

```
    V = HMAC(K, V) is
                                                          62CB0F78
        6098110C 817975BA 4AAB395E 2E7D2B7F B0CDD094 59693A1A


    temp is
                                                          62CB0F78
        6098110C 817975BA 4AAB395E 2E7D2B7F B0CDD094 59693A1A


  ------------

    V = HMAC(K, V) is
                                                          952AD057
        CA66E306 F283E5F8 AAAB2087 B0B8A2E1 6DEDF4C3 C5EE8B71


    temp is
                                                 62CB0F78 6098110C
        817975BA 4AAB395E 2E7D2B7F B0CDD094 59693A1A 952AD057
        CA66E306 F283E5F8 AAAB2087 B0B8A2E1 6DEDF4C3 C5EE8B71


---------------------------

  returned_bits is
                                                 62CB0F78 6098110C
        817975BA 4AAB395E 2E7D2B7F B0CDD094 59693A1A 952AD057
        CA66E306 F283E5F8 AAAB2087 B0B8A2E1 6DEDF4C3 C5EE8B71


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                       95 2AD057CA
        66E306F2 83E5F8AA AB2087B0 B8A2E16D EDF4C3C5 EE8B7100
```

```
    K = HMAC(K, V || 0x00 || provided_data) is
                                                        5CE58637
        BE1FD995 D54EA9C7 1C3CFB3F 40709465 40E2C717 BBC70669


    V = HMAC(K, V) is
                                                        577AEE11
        6868CE4D CA699C4D E3276E5F DBAEB601 594E6CF8 27A67EF2


rnd_val is
                                              62CB0F78 6098110C
        817975BA 4AAB395E 2E7D2B7F B0CDD094 59693A1A 952AD057
        CA66E306 F283E5F8 AAAB2087 B0B8A2E1 6DEDF4C3 C5EE8B71
```

```
###############################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                              000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                              000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    ------------

    V || 0x00 || provided_data is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 00000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    K = HMAC(K, V || 0x00 || provided_data) is
                                                44AD352A 3BEE9247
```

```
        C10F06B0 7EAA3983 C163F7D1 2FD023C7 72F45B84 66477910


    V = HMAC(K, V) is
                                                8E900608 F34F1504
        5D31A80E 9D699577 BF327E45 DBC501BC 4F45BA26 A9B4C4BC


    ------------

    V || 0x01 || provided_data is
        8E900608 F34F1504 5D31A80E 9D699577 BF327E45 DBC501BC
        4F45BA26 A9B4C4BC 01000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    K = HMAC(K, V || 0x01 || provided_data) is
                                                3DDA543E 7EEF14F9
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


    V = HMAC(K, V) is
                                                2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


  Update (Key, V):

    Key is
                                                3DDA543E 7EEF14F9
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


    V is
                                                2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


------------------------------------------------------------

First call to Generate

************************************************************

HMAC_DRBG_Generate
```

```
  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                              D67B8C17 34F46FA3
        F763CF57 C6F9F4F2 DC1089BD 8BC1F6F0 23950BFC 56176352


    temp is
                                              D67B8C17 34F46FA3
        F763CF57 C6F9F4F2 DC1089BD 8BC1F6F0 23950BFC 56176352


  ------------

    V = HMAC(K, V) is
                                              08C85012 38AD7A44
        00DEFEE4 6C640B61 AF77C2D1 A3BFAA90 EDE5D207 406E5403


    temp is
                          D67B8C17 34F46FA3 F763CF57 C6F9F4F2
        DC1089BD 8BC1F6F0 23950BFC 56176352 08C85012 38AD7A44
        00DEFEE4 6C640B61 AF77C2D1 A3BFAA90 EDE5D207 406E5403


---------------------------

  returned_bits is
                          D67B8C17 34F46FA3 F763CF57 C6F9F4F2
        DC1089BD 8BC1F6F0 23950BFC 56176352 08C85012 38AD7A44
        00DEFEE4 6C640B61 AF77C2D1 A3BFAA90 EDE5D207 406E5403


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------
```

```
    V || 0x00 || provided_data is
                                          08 C8501238 AD7A4400
        DEFEE46C 640B61AF 77C2D1A3 BFAA90ED E5D20740 6E540300


    K = HMAC(K, V || 0x00 || provided_data) is
                                          DD309579 353802CC
        DD4399C3 691C9DD9 09DD3B2D D003CCD5 9D6F08D8 5F2E3509


    V = HMAC(K, V) is
                                          A1C20FF2 70A39D2B
        8D03D659 B9DDD011 C2CCDF24 48557EF6 A1A915D1 8940A688


rnd_val is
                         D67B8C17 34F46FA3 F763CF57 C6F9F4F2
        DC1089BD 8BC1F6F0 23950BFC 56176352 08C85012 38AD7A44
        00DEFEE4 6C640B61 AF77C2D1 A3BFAA90 EDE5D207 406E5403


----------------------------------------------------------------

Second call to Generate

****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                          8FDAEC20 F8B42140
        7059E358 8920DA7E DA9DCE3C F8274DFA 1C59C108 C1D0AA9B


    temp is
                                          8FDAEC20 F8B42140
        7059E358 8920DA7E DA9DCE3C F8274DFA 1C59C108 C1D0AA9B
```

```
  ------------

    V = HMAC(K, V) is
                                                0FA38DA5 C792037C
        4D33CD07 0CA7CD0C 5608DBA8 B8856546 39DE2187 B74CB263


    temp is
                            8FDAEC20 F8B42140 7059E358 8920DA7E
        DA9DCE3C F8274DFA 1C59C108 C1D0AA9B 0FA38DA5 C792037C
        4D33CD07 0CA7CD0C 5608DBA8 B8856546 39DE2187 B74CB263


----------------------------

  returned_bits is
                            8FDAEC20 F8B42140 7059E358 8920DA7E
        DA9DCE3C F8274DFA 1C59C108 C1D0AA9B 0FA38DA5 C792037C
        4D33CD07 0CA7CD0C 5608DBA8 B8856546 39DE2187 B74CB263


  call Update(additional_input, K, V)
----------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                           0F A38DA5C7 92037C4D
        33CD070C A7CD0C56 08DBA8B8 85654639 DE2187B7 4CB26300


    K = HMAC(K, V || 0x00 || provided_data) is
                                                5CD5E50A 3E448A07
        C3D2F2A3 F9DEBCC0 465F9CF1 1CA136E9 B504B4D3 1C7FF1B8


    V = HMAC(K, V) is
                                                33B309F2 FF01CE10
        4B4429B6 75FAFA19 011E348B 2812715A 7637F6A6 E63B5D57


rnd_val is
```

```
                        8FDAEC20 F8B42140 7059E358 8920DA7E
        DA9DCE3C F8274DFA 1C59C108 C1D0AA9B 0FA38DA5 C792037C
        4D33CD07 0CA7CD0C 5608DBA8 B8856546 39DE2187 B74CB263


###############################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                              20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
```

```
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                               20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  Key is
                                               00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                               01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                            000102 03040506 0708090A 0B0C0D0E
```

```
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    ------------

    V || 0x00 || provided_data is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 00000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    K = HMAC(K, V || 0x00 || provided_data) is
                                            44AD352A 3BEE9247
        C10F06B0 7EAA3983 C163F7D1 2FD023C7 72F45B84 66477910


    V = HMAC(K, V) is
                                            8E900608 F34F1504
        5D31A80E 9D699577 BF327E45 DBC501BC 4F45BA26 A9B4C4BC


    ------------

    V || 0x01 || provided_data is
        8E900608 F34F1504 5D31A80E 9D699577 BF327E45 DBC501BC
        4F45BA26 A9B4C4BC 01000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    K = HMAC(K, V || 0x01 || provided_data) is
                                            3DDA543E 7EEF14F9
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


    V = HMAC(K, V) is
                                            2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


Update (Key, V):

    Key is
                                            3DDA543E 7EEF14F9
```

```
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


    V is
                                                2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                          2D02C2F8 22517D54 B817279A 59491C41
        A1989B3E 382DEBE8 0D2C7F66 0F4476C4 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                                BC43CACB 4AFF5D2D
```

```
      A0C65825 D013B674 E6950B8D 926F5E57 18F8D9BA 839FC4EE


  V = HMAC(K, V) is
                                                 C5FF9271 0AE3ECB8
      6D76A3EB 1C5100C3 B79F8E19 B943E1E6 C76ABB92 756B59BC


  ------------

  V || 0x01 || provided_data is
                         C5FF9271 0AE3ECB8 6D76A3EB 1C5100C3
      B79F8E19 B943E1E6 C76ABB92 756B59BC 01606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  K = HMAC(K, V || 0x01 || provided_data) is
                                                 08B5732C FC2C5F8C
      9EA915AE 8F6419AB 5383373E 6EE0DBF0 37325E82 1C548A66


  V = HMAC(K, V) is
                                                 CD58D9B9 850EB9DD
      1EC6C827 5A41F6AF 0153AB5E 5C0E3654 0FB4D618 BBFE0640


------------

  V = HMAC(K, V) is
                                                 41878735 8135419B
      93813353 5306176A FB251CDD 2BA37988 59B566A0 5CFB1D68


  temp is
                                                 41878735 8135419B
      93813353 5306176A FB251CDD 2BA37988 59B566A0 5CFB1D68


------------

  V = HMAC(K, V) is
                                                 0EA92585 6D5B84D5
      6ADAE870 45A6BA28 D2C908AB 75B7CC41 431FAC59 F38918A3
```

```
    temp is
                            41878735 8135419B 93813353 5306176A
        FB251CDD 2BA37988 59B566A0 5CFB1D68 0EA92585 6D5B84D5
        6ADAE870 45A6BA28 D2C908AB 75B7CC41 431FAC59 F38918A3


---------------------------

  returned_bits is
                            41878735 8135419B 93813353 5306176A
        FB251CDD 2BA37988 59B566A0 5CFB1D68 0EA92585 6D5B84D5
        6ADAE870 45A6BA28 D2C908AB 75B7CC41 431FAC59 F38918A3


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                  606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                            0EA92585 6D5B84D5 6ADAE870 45A6BA28
        D2C908AB 75B7CC41 431FAC59 F38918A3 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                                  19D384D9 A9A7F8F5
        401C181E BDEDD94E 297AC090 5FD44A97 5AB78132 36CB8D2A


    V = HMAC(K, V) is
                                                  06461517 E829ADA4
        E5AB4523 EBA1514B 56A141D7 94C3877F EFAA7CB2 07C2BBC7


    ------------
```

```
    V || 0x01 || provided_data is
                            06461517 E829ADA4 E5AB4523 EBA1514B
        56A141D7 94C3877F EFAA7CB2 07C2BBC7 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                                               791D3144 B302AD6C
        E4324134 4210AAD0 D399EDB7 B5906FB2 51DB1CB6 0004EA51


    V = HMAC(K, V) is
                                               58FD965F 4F99893C
        17E6A33C B8E90415 B516D006 14A449D4 06E03C68 5BD859BD


rnd_val is
                            41878735 8135419B 93813353 5306176A
        FB251CDD 2BA37988 59B566A0 5CFB1D68 0EA92585 6D5B84D5
        6ADAE870 45A6BA28 D2C908AB 75B7CC41 431FAC59 F38918A3


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                 A0A1A2 A3A4A5A6
```

```
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  ------------

  V || 0x00 || provided_data is
                       58FD965F 4F99893C 17E6A33C B8E90415
    B516D006 14A449D4 06E03C68 5BD859BD 00A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x00 || provided_data) is
                                          FC15C8FD 1A937961
    D6880278 84E31C1A 679694A2 4543B65E CDAA24A5 457AFF6E


  V = HMAC(K, V) is
                                          F72F8818 3AFCE0AE
    B1B53151 962AFAB7 D2C87E51 97B1E21C 25D2CC83 C2F20801


  ------------

  V || 0x01 || provided_data is
                       F72F8818 3AFCE0AE B1B53151 962AFAB7
    D2C87E51 97B1E21C 25D2CC83 C2F20801 01A0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x01 || provided_data) is
                                          36A2F9CE A0B5E314
    CBE70BD5 E8D81916 2498C734 4F50FB34 D8879990 E2985CDA


  V = HMAC(K, V) is
                                          1FAF36AE BAFF731D
    99921019 DB901FBC 62C562AF E1C535A6 7EE281D3 8CF1FA40


------------

  V = HMAC(K, V) is
                                          7C067BDD CA817248
```

```
        23D64C69 829285BD BFF53771 6102C188 2E202250 E0FA5EF3


    temp is
                                                7C067BDD CA817248
        23D64C69 829285BD BFF53771 6102C188 2E202250 E0FA5EF3


  ------------

    V = HMAC(K, V) is
                                               A384CD34 A20FFD1F
        BC91E0C5 32A8A421 BC4AFE3C D47F2232 3EB4BAE1 A0078981


    temp is
                           7C067BDD CA817248 23D64C69 829285BD
        BFF53771 6102C188 2E202250 E0FA5EF3 A384CD34 A20FFD1F
        BC91E0C5 32A8A421 BC4AFE3C D47F2232 3EB4BAE1 A0078981


---------------------------

  returned_bits is
                           7C067BDD CA817248 23D64C69 829285BD
        BFF53771 6102C188 2E202250 E0FA5EF3 A384CD34 A20FFD1F
        BC91E0C5 32A8A421 BC4AFE3C D47F2232 3EB4BAE1 A0078981


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                           A384CD34 A20FFD1F BC91E0C5 32A8A421
        BC4AFE3C D47F2232 3EB4BAE1 A0078981 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
```

```
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                              F7EE5EE9 3CE673E2
        48886523 A03B5F16 580ADD46 C62F4CC9 2B6F870E E6F503F2


    V = HMAC(K, V) is
                                              721BE504 190DBE91
        CD17E519 1C0885FC 8B7C9060 352B08EB FEB1DB58 55B4B040


    ------------

    V || 0x01 || provided_data is
                           721BE504 190DBE91 CD17E519 1C0885FC
        8B7C9060 352B08EB FEB1DB58 55B4B040 01A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                                              E7458FB4 4A369A65
        3F2F8F57 7BF975C4 B362C4FE 618B2F1F F6769B13 C94DECF4


    V = HMAC(K, V) is
                                              19334B8C 31B74932
        DDD7B2A4 68F6436D F92E100D 39D3ACB3 68C7029C B883EC89


rnd_val is
                           7C067BDD CA817248 23D64C69 829285BD
        BFF53771 6102C188 2E202250 E0FA5EF3 A384CD34 A20FFD1F
        BC91E0C5 32A8A421 BC4AFE3C D47F2232 3EB4BAE1 A0078981


################################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256
```

```
    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                             20212223 24252627


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                             20212223 24252627
```

```
    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                               00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                               01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------

    V || 0x00 || provided_data is
                                                 010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
```

```
      2E2F3031 32333435 36202122 23242526 27404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x00 || provided_data) is
                                           E48294AE A5171B5D
      6A091450 868B39C4 B14D4E1A 9B29F128 416E1E14 81D10F69


  V = HMAC(K, V) is
                                           40987A58 C3E1346C
      0023F00F 417FA7BD 09C72FED A9738670 993392DF 490E94E2


  ------------

  V || 0x01 || provided_data is
                                             40987A 58C3E134
      6C0023F0 0F417FA7 BD09C72F EDA97386 70993392 DF490E94
      E2010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
      16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
      2E2F3031 32333435 36202122 23242526 27404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x01 || provided_data) is
                                           65673C34 8E51CFAC
      C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


  V = HMAC(K, V) is
                                           E0F91AC9 9630EEE6
      7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


Update (Key, V):

  Key is
                                           65673C34 8E51CFAC
      C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


  V is
                                           E0F91AC9 9630EEE6
```

```
        7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


------------------------------------------------------------

First call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                0DD9C855 89F357C3
        89D6AF8D E9D734A9 17C771EF 2D8816B9 82596ED1 2DB45D73


    temp is
                                                0DD9C855 89F357C3
        89D6AF8D E9D734A9 17C771EF 2D8816B9 82596ED1 2DB45D73


  ------------

    V = HMAC(K, V) is
                                                4A626808 35C02FDA
        66B08E1A 369AE218 F26D5210 AD564248 872D7A28 784159C3


    temp is
                           0DD9C855 89F357C3 89D6AF8D E9D734A9
        17C771EF 2D8816B9 82596ED1 2DB45D73 4A626808 35C02FDA
        66B08E1A 369AE218 F26D5210 AD564248 872D7A28 784159C3


---------------------------

  returned_bits is
                           0DD9C855 89F357C3 89D6AF8D E9D734A9
        17C771EF 2D8816B9 82596ED1 2DB45D73 4A626808 35C02FDA
        66B08E1A 369AE218 F26D5210 AD564248 872D7A28 784159C3
```

```
  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                          4A 62680835 C02FDA66
        B08E1A36 9AE218F2 6D5210AD 56424887 2D7A2878 4159C300


    K = HMAC(K, V || 0x00 || provided_data) is
                                            F0B2F242 CAD992A7
        24F7E559 1D2F3B0C 2157AE70 D5327899 40F16445 9B00C749


    V = HMAC(K, V) is
                                            1A03F91C 5120BACA
        2BF6C64D D73AB11D F6FD3FF1 AC3B5720 A3F7FBE3 9E7E7FE9


rnd_val is
                         0DD9C855 89F357C3 89D6AF8D E9D734A9
        17C771EF 2D8816B9 82596ED1 2DB45D73 4A626808 35C02FDA
        66B08E1A 369AE218 F26D5210 AD564248 872D7A28 784159C3


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------
```

```
    V = HMAC(K, V) is
                                                46B4F475 6AE715E0
        E51681AB 2932DE15 23BE5D13 BAF0F458 8B11FE37 2FDA37AB


    temp is
                                                46B4F475 6AE715E0
        E51681AB 2932DE15 23BE5D13 BAF0F458 8B11FE37 2FDA37AB


  ------------

    V = HMAC(K, V) is
                                                E3683173 41BC8BA9
        1FC5D85B 7FB8CA8F BC309A75 8FD6FCA9 DF43C766 0B221322


    temp is
                            46B4F475 6AE715E0 E51681AB 2932DE15
        23BE5D13 BAF0F458 8B11FE37 2FDA37AB E3683173 41BC8BA9
        1FC5D85B 7FB8CA8F BC309A75 8FD6FCA9 DF43C766 0B221322


---------------------------

  returned_bits is
                            46B4F475 6AE715E0 E51681AB 2932DE15
        23BE5D13 BAF0F458 8B11FE37 2FDA37AB E3683173 41BC8BA9
        1FC5D85B 7FB8CA8F BC309A75 8FD6FCA9 DF43C766 0B221322


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                              E3 68317341 BC8BA91F
        C5D85B7F B8CA8FBC 309A758F D6FCA9DF 43C7660B 22132200


    K = HMAC(K, V || 0x00 || provided_data) is
```

```
                                                5C0DEC09 3708C17C
        A76B57C0 CB60CF88 9DCC47AD 10BD64BC 6A14B23F 2026078A


    V = HMAC(K, V) is
                                                456752A5 11B848BD
        05F1819B 9F6B1542 C7D5ECF9 32733926 7A0C7723 5B87DC5A


rnd_val is
                           46B4F475 6AE715E0 E51681AB 2932DE15
        23BE5D13 BAF0F458 8B11FE37 2FDA37AB E3683173 41BC8BA9
        1FC5D85B 7FB8CA8F BC309A75 8FD6FCA9 DF43C766 0B221322


################################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                                20212223 24252627
```

```
    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##############################################################

**************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                              20212223 24252627


    personal_str is
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
```

```
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                                 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


----------------------------

  Update

    provided_data
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------

    V || 0x00 || provided_data is
                                                   010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x00 || provided_data) is
                                                 E48294AE A5171B5D
        6A091450 868B39C4 B14D4E1A 9B29F128 416E1E14 81D10F69


    V = HMAC(K, V) is
                                                 40987A58 C3E1346C
        0023F00F 417FA7BD 09C72FED A9738670 993392DF 490E94E2
```

```
    ------------

    V || 0x01 || provided_data is
                                                40987A 58C3E134
        6C0023F0 0F417FA7 BD09C72F EDA97386 70993392 DF490E94
        E2010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    K = HMAC(K, V || 0x01 || provided_data) is
                                               65673C34 8E51CFAC
        C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


    V = HMAC(K, V) is
                                               E0F91AC9 9630EEE6
        7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


  Update (Key, V):

    Key is
                                               65673C34 8E51CFAC
        C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


    V is
                                               E0F91AC9 9630EEE6
        7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


-----------------------------------------------------------

First call to Generate

***********************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512
```

```
    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                           E0F91AC9 9630EEE6 7CF830CF D5044FEB
        F55C0C11 5007997A DA11296F C4164A9A 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                               AEC2D8F1 47E486D9
        02BFCBD5 3348C149 1E4D2FFB 1926867A ACA29FD0 C71DCFB7


    V = HMAC(K, V) is
                                               E6C969EE 096C8EE7
        B90A0AB5 587F435F DE8C4AFB 657910D4 B7B5E522 23C31FC1


    ------------

    V || 0x01 || provided_data is
                           E6C969EE 096C8EE7 B90A0AB5 587F435F
        DE8C4AFB 657910D4 B7B5E522 23C31FC1 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
```

```
                                                80B2F215 13E4279D
        F0A8C63F 985E14CE D2DEB415 821EA82A 716AAB4C 2552C49D


    V = HMAC(K, V) is
                                                4C16A0FC 00C35B53
        B152AA1E 430F241D 63B4F167 DF65CC92 FC3F4821 F0FBF71C


  ------------

    V = HMAC(K, V) is
                                                1478F29E 94B02CB4
        0D3AAB86 245557CE 13A8CA2F DB657D98 EFC19234 6B9FAC33


    temp is
                                                1478F29E 94B02CB4
        0D3AAB86 245557CE 13A8CA2F DB657D98 EFC19234 6B9FAC33


  ------------

    V = HMAC(K, V) is
                                                EA58ADA2 CCA432CC
        DEFBCDAA 8B82F553 EF966134 E2CD139F 15F01CAD 568565A8


    temp is
                            1478F29E 94B02CB4 0D3AAB86 245557CE
        13A8CA2F DB657D98 EFC19234 6B9FAC33 EA58ADA2 CCA432CC
        DEFBCDAA 8B82F553 EF966134 E2CD139F 15F01CAD 568565A8


---------------------------

  returned_bits is
                            1478F29E 94B02CB4 0D3AAB86 245557CE
        13A8CA2F DB657D98 EFC19234 6B9FAC33 EA58ADA2 CCA432CC
        DEFBCDAA 8B82F553 EF966134 E2CD139F 15F01CAD 568565A8


  call Update(additional_input, K, V)
---------------------------

  Update
```

```
    provided_data
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
                           EA58ADA2 CCA432CC DEFBCDAA 8B82F553
        EF966134 E2CD139F 15F01CAD 568565A8 00606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                               584491D3 53B81040
        53EA0BD3 F436510C 5FD38433 939A1951 F4983744 A6C8E5AB


    V = HMAC(K, V) is
                                               E625EAF3 5BB58168
        F208A9EE 65A4A531 F3072BA6 7921D2F3 6838C3E1 6B4B7A69


    ------------

    V || 0x01 || provided_data is
                           E625EAF3 5BB58168 F208A9EE 65A4A531
        F3072BA6 7921D2F3 6838C3E1 6B4B7A69 01606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                                               572C0374 C1A10125
        BFA6AECD 7CEBFE32 F752C3FB 316731B7 CFDBDEC2 6356932B


    V = HMAC(K, V) is
                                               D68BF041 F3EB5088
        088D8B8E 712C36AE 9583BB08 FD1F9034 A4E942E9 A6747CE7


rnd_val is
```

```
                        1478F29E 94B02CB4 0D3AAB86 245557CE
        13A8CA2F DB657D98 EFC19234 6B9FAC33 EA58ADA2 CCA432CC
        DEFBCDAA 8B82F553 EF966134 E2CD139F 15F01CAD 568565A8


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                        D68BF041 F3EB5088 088D8B8E 712C36AE
        9583BB08 FD1F9034 A4E942E9 A6747CE7 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                 39B0DA85 112EE543
        27721EEA A7A16965 F6E0975F F81F312A 7C88E79B 8F0F98E9
```

```
  V = HMAC(K, V) is
                                                B189B4DF 841734E7
      8B3D482E 9A082D36 16F5D674 23EADAE7 ED966B72 8EA10C56


  ------------

  V || 0x01 || provided_data is
                          B189B4DF 841734E7 8B3D482E 9A082D36
      16F5D674 23EADAE7 ED966B72 8EA10C56 01A0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  K = HMAC(K, V || 0x01 || provided_data) is
                                                D88F4E3B DAB9404B
      817B0EBD 27330511 E2B4C257 753CF527 CDA90871 4C73BC0D


  V = HMAC(K, V) is
                                                9CE06AB1 8AEC3612
      5C6E9029 156DDDD0 936072E1 78168681 1A6B57DE D8473E04


------------

  V = HMAC(K, V) is
                                                497C7A16 E88A6411
      F8FCE10E F56763C6 1025801D 8F51A743 52D682CC 23A0A8E6


  temp is
                                                497C7A16 E88A6411
      F8FCE10E F56763C6 1025801D 8F51A743 52D682CC 23A0A8E6


------------

  V = HMAC(K, V) is
                                                73CAE032 28939064
      7DC683B7 342885D6 B76AB1DA 696D3E97 E22DFFDD FFFD8DF0


  temp is
                          497C7A16 E88A6411 F8FCE10E F56763C6
      1025801D 8F51A743 52D682CC 23A0A8E6 73CAE032 28939064
```

```
        7DC683B7 342885D6 B76AB1DA 696D3E97 E22DFFDD FFFD8DF0


---------------------------

  returned_bits is
                         497C7A16 E88A6411 F8FCE10E F56763C6
        1025801D 8F51A743 52D682CC 23A0A8E6 73CAE032 28939064
        7DC683B7 342885D6 B76AB1DA 696D3E97 E22DFFDD FFFD8DF0


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                                                 A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
                         73CAE032 28939064 7DC683B7 342885D6
        B76AB1DA 696D3E97 E22DFFDD FFFD8DF0 00A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                 F8F5E360 854BAA38
        A7F3F443 12D2475A 0752C0CA 57643724 CFF0431C 0F93BD61


    V = HMAC(K, V) is
                                                 DC2F83C9 DA2605D2
        1E026EF0 6E008D53 34B51534 3CA1E918 472E7F81 D7E37EF5


    ------------

    V || 0x01 || provided_data is
                         DC2F83C9 DA2605D2 1E026EF0 6E008D53
        34B51534 3CA1E918 472E7F81 D7E37EF5 01A0A1A2 A3A4A5A6
```

```
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                                              282E0734 80809375
        58B1392E 95AB91E7 C1F622B2 4FFB8720 A5F0A5E0 7550C7C2


    V = HMAC(K, V) is
                                              DFC3BDB5 F3BCF1AA
        68298E79 0D720A67 A76E31B9 2B9B35A8 E5471BB1 7E303C6B


rnd_val is
                         497C7A16 E88A6411 F8FCE10E F56763C6
        1025801D 8F51A743 52D682CC 23A0A8E6 73CAE032 28939064
        7DC683B7 342885D6 B76AB1DA 696D3E97 E22DFFDD FFFD8DF0


################################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
```

```
    Nonce =
                                                20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput = <empty>

################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


--------------------------
```

```
Update

  provided_data
                           000102 03040506 0708090A 0B0C0D0E
      0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
      2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  ------------

  V || 0x00 || provided_data is
      01010101 01010101 01010101 01010101 01010101 01010101
      01010101 01010101 00000102 03040506 0708090A 0B0C0D0E
      0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
      2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  K = HMAC(K, V || 0x00 || provided_data) is
                                           44AD352A 3BEE9247
      C10F06B0 7EAA3983 C163F7D1 2FD023C7 72F45B84 66477910


  V = HMAC(K, V) is
                                           8E900608 F34F1504
      5D31A80E 9D699577 BF327E45 DBC501BC 4F45BA26 A9B4C4BC


  ------------

  V || 0x01 || provided_data is
      8E900608 F34F1504 5D31A80E 9D699577 BF327E45 DBC501BC
      4F45BA26 A9B4C4BC 01000102 03040506 0708090A 0B0C0D0E
      0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
      2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  K = HMAC(K, V || 0x01 || provided_data) is
                                           3DDA543E 7EEF14F9
      36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


  V = HMAC(K, V) is
                                           2D02C2F8 22517D54
      B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4
```

```
  Update (Key, V):

    Key is
                                                3DDA543E 7EEF14F9
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


    V is
                                                2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is  <empty>

  Seed_Material is
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  Key is
                                                3DDA543E 7EEF14F9
```

```
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


  V is
                                                 2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


---------------------------

  Update

    provided_data
                                                   808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    ------------

    V || 0x00 || provided_data is
                          2D02C2F8 22517D54 B817279A 59491C41
        A1989B3E 382DEBE8 0D2C7F66 0F4476C4 00808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                 E7F1346E 1B837375
        0DFF7840 DCD97C74 25F85732 87B91151 CD5C3C2A 37B06B0C


    V = HMAC(K, V) is
                                                 5775A709 1255E890
        3B575A25 6C0DE34E A959CDB4 F8ABEE3E D5C21D59 8243C185


    ------------

    V || 0x01 || provided_data is
                          5775A709 1255E890 3B575A25 6C0DE34E
        A959CDB4 F8ABEE3E D5C21D59 8243C185 01808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                                                B84007E3 E27F34F9
        A7820B7A B59BBEFC D0C4ACAE DE4B0B36 B147B897 79FD749D


    V = HMAC(K, V) is
                                                A72B8FEE 92392F0A
        9D2D61BF 09A4DFCC 9DE69A16 A5F15022 4C3EF604 2D1521FC


  Update (Key, V):

    Key is
                                                B84007E3 E27F34F9
        A7820B7A B59BBEFC D0C4ACAE DE4B0B36 B147B897 79FD749D


    V is
                                                A72B8FEE 92392F0A
        9D2D61BF 09A4DFCC 9DE69A16 A5F15022 4C3EF604 2D1521FC


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                FABD0AE2 5C69DC2E
        FDEFB7F2 0C5A31B5 7AC938AB 771AA19B F8F5F146 8F665C93


    temp is
                                                FABD0AE2 5C69DC2E
        FDEFB7F2 0C5A31B5 7AC938AB 771AA19B F8F5F146 8F665C93


  ------------

    V = HMAC(K, V) is
                                                8C9A1A5D F0628A56
```

```
        90F15A1A D8A613F3 1BBD65EE AD5457D5 D26947F2 9FE91AA7


    temp is
                            FABD0AE2 5C69DC2E FDEFB7F2 0C5A31B5
        7AC938AB 771AA19B F8F5F146 8F665C93 8C9A1A5D F0628A56
        90F15A1A D8A613F3 1BBD65EE AD5457D5 D26947F2 9FE91AA7


---------------------------

  returned_bits is
                            FABD0AE2 5C69DC2E FDEFB7F2 0C5A31B5
        7AC938AB 771AA19B F8F5F146 8F665C93 8C9A1A5D F0628A56
        90F15A1A D8A613F3 1BBD65EE AD5457D5 D26947F2 9FE91AA7


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                           8C 9A1A5DF0 628A5690
        F15A1AD8 A613F31B BD65EEAD 5457D5D2 6947F29F E91AA700


    K = HMAC(K, V || 0x00 || provided_data) is
                                           4348AF84 20842FA0
        77B9D3DB A8DCE9B3 E1DF734F FCE1BEA5 B9E2B154 DC5EC615


    V = HMAC(K, V) is
                                           D2C1AC27 885D4332
        76713146 32EA6043 3CCA7273 04569EA7 D471FEA7 DB7D315D


rnd_val is
                            FABD0AE2 5C69DC2E FDEFB7F2 0C5A31B5
        7AC938AB 771AA19B F8F5F146 8F665C93 8C9A1A5D F0628A56
        90F15A1A D8A613F3 1BBD65EE AD5457D5 D26947F2 9FE91AA7
```

```
------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is  <empty>

  Seed_Material is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  Key is
                                              4348AF84 20842FA0
        77B9D3DB A8DCE9B3 E1DF734F FCE1BEA5 B9E2B154 DC5EC615


  V is
                                              D2C1AC27 885D4332
        76713146 32EA6043 3CCA7273 04569EA7 D471FEA7 DB7D315D


---------------------------

  Update
```

```
  provided_data
                                                C0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  ------------

  V || 0x00 || provided_data is
                        D2C1AC27 885D4332 76713146 32EA6043
      3CCA7273 04569EA7 D471FEA7 DB7D315D 00C0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x00 || provided_data) is
                                               668B28ED 146DAB9E
      561501C6 544536C8 34259891 4A444CDB 484E709A 41E5C10F


  V = HMAC(K, V) is
                                               D19D64C7 941B480A
      C3444F46 A3771FD3 E3D204B1 270F33AD 6482D293 E1300249


  ------------

  V || 0x01 || provided_data is
                        D19D64C7 941B480A C3444F46 A3771FD3
      E3D204B1 270F33AD 6482D293 E1300249 01C0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x01 || provided_data) is
                                               BFA02CE7 E92DE92B
      18242886 890E586F 836906AC E9E554F1 B0ED6357 3CB8B503


  V = HMAC(K, V) is
                                               D32403EE A9DCE161
      6E4E1155 B923D884 2CC6E784 C67A9385 B2A637F1 02FA45D5


Update (Key, V):
```

```
    Key is
                                                BFA02CE7 E92DE92B
        18242886 890E586F 836906AC E9E554F1 B0ED6357 3CB8B503


    V is
                                                D32403EE A9DCE161
        6E4E1155 B923D884 2CC6E784 C67A9385 B2A637F1 02FA45D5


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                6BD925B0 E1C232EF
        D67CCD84 F722E927 ECB46AB2 B7400147 77AF14BA 0BBF53A4


    temp is
                                                6BD925B0 E1C232EF
        D67CCD84 F722E927 ECB46AB2 B7400147 77AF14BA 0BBF53A4


  ------------

    V = HMAC(K, V) is
                                                5BDBB62B 3F7D0B9C
        8EEAD057 C0EC754E F8B53E60 A1F434F0 5946A8B6 86AFBC7A


    temp is
                            6BD925B0 E1C232EF D67CCD84 F722E927
        ECB46AB2 B7400147 77AF14BA 0BBF53A4 5BDBB62B 3F7D0B9C
        8EEAD057 C0EC754E F8B53E60 A1F434F0 5946A8B6 86AFBC7A


---------------------------

  returned_bits is
```

```
                          6BD925B0 E1C232EF D67CCD84 F722E927
        ECB46AB2 B7400147 77AF14BA 0BBF53A4 5BDBB62B 3F7D0B9C
        8EEAD057 C0EC754E F8B53E60 A1F434F0 5946A8B6 86AFBC7A


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                          5B DBB62B3F 7D0B9C8E
        EAD057C0 EC754EF8 B53E60A1 F434F059 46A8B686 AFBC7A00


    K = HMAC(K, V || 0x00 || provided_data) is
                                          8121F776 4C081EE9
        D1171ED1 87BAE088 95CAE230 D0A25E37 39C57D54 16109B82


    V = HMAC(K, V) is
                                          3784977C C0E59FBC
        9CDA4E11 92475C6E FAF80720 19862122 CB6BCEAA CC4A175E


rnd_val is
                          6BD925B0 E1C232EF D67CCD84 F722E927
        ECB46AB2 B7400147 77AF14BA 0BBF53A4 5BDBB62B 3F7D0B9C
        8EEAD057 C0EC754E F8B53E60 A1F434F0 5946A8B6 86AFBC7A


##############################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                            000102 03040506
```

```
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                              20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


  Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    ------------

    V || 0x00 || provided_data is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 00000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    K = HMAC(K, V || 0x00 || provided_data) is
                                                44AD352A 3BEE9247
        C10F06B0 7EAA3983 C163F7D1 2FD023C7 72F45B84 66477910
```

```
    V = HMAC(K, V) is
                                                8E900608 F34F1504
        5D31A80E 9D699577 BF327E45 DBC501BC 4F45BA26 A9B4C4BC


    ------------

    V || 0x01 || provided_data is
        8E900608 F34F1504 5D31A80E 9D699577 BF327E45 DBC501BC
        4F45BA26 A9B4C4BC 01000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 20212223 24252627


    K = HMAC(K, V || 0x01 || provided_data) is
                                                3DDA543E 7EEF14F9
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


    V = HMAC(K, V) is
                                                2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


  Update (Key, V):

    Key is
                                                3DDA543E 7EEF14F9
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


    V is
                                                2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


------------------------------------------------------------

First call to Generate

************************************************************

HMAC_DRBG_Generate
```

```
  requested_number_of_bits = 512

    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Seed_Material is
                             8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Key is
                                               3DDA543E 7EEF14F9
        36237BE6 5D094B4D DC969C0B 2B5EAFB5 D805E86C FA64D741


  V is
                                               2D02C2F8 22517D54
        B817279A 59491C41 A1989B3E 382DEBE8 0D2C7F66 0F4476C4


---------------------------

  Update
```

```
provided_data
                          8081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


------------

V || 0x00 || provided_data is
      2D02C2 F822517D 54B81727 9A59491C 41A1989B 3E382DEB
    E80D2C7F 660F4476 C4008081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


K = HMAC(K, V || 0x00 || provided_data) is
                                        A61BAEFD DC0C56E3
    E0851C60 F83FDBB3 C9A8B56F 2B5ADA3B FD70228E FBC8EBCC


V = HMAC(K, V) is
                                        E1C3045A 91B61344
    A9493879 32B94894 A0D41A9D 873F2C61 A897D512 4AE95D27


------------

V || 0x01 || provided_data is
      E1C304 5A91B613 44A94938 7932B948 94A0D41A 9D873F2C
    61A897D5 124AE95D 27018081 82838485 86878889 8A8B8C8D
    8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
    A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


K = HMAC(K, V || 0x01 || provided_data) is
                                        C125EA99 758EBB9A
    6F69AE31 2AC204B5 94C00AB6 8B816E3A 52128E02 78A584AC
```

```
    V = HMAC(K, V) is
                                                B2CB2B89 123F5B4A
        F587B8F6 BDC5427A 991419D3 53077C68 5E707ACD F8E9FDA9


  Update (Key, V):

    Key is
                                                C125EA99 758EBB9A
        6F69AE31 2AC204B5 94C00AB6 8B816E3A 52128E02 78A584AC


    V is
                                                B2CB2B89 123F5B4A
        F587B8F6 BDC5427A 991419D3 53077C68 5E707ACD F8E9FDA9


****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                085D57AF 6BABCF2B
        9AEEF387 D531650E 6A505C54 406AB37A 52899E0E CAB3632B


    temp is
                                                085D57AF 6BABCF2B
        9AEEF387 D531650E 6A505C54 406AB37A 52899E0E CAB3632B


  ------------

    V = HMAC(K, V) is
                                                7A068A28 14C6DF6A
        E532B658 D0D9741C 84775FEE 45B684CD BDC25FBC B4D8F310


    temp is
                            085D57AF 6BABCF2B 9AEEF387 D531650E
```

```
        6A505C54 406AB37A 52899E0E CAB3632B 7A068A28 14C6DF6A
        E532B658 D0D9741C 84775FEE 45B684CD BDC25FBC B4D8F310


---------------------------

  returned_bits is
                         085D57AF 6BABCF2B 9AEEF387 D531650E
        6A505C54 406AB37A 52899E0E CAB3632B 7A068A28 14C6DF6A
        E532B658 D0D9741C 84775FEE 45B684CD BDC25FBC B4D8F310


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                          7A 068A2814 C6DF6AE5
        32B658D0 D9741C84 775FEE45 B684CDBD C25FBCB4 D8F31000


    K = HMAC(K, V || 0x00 || provided_data) is
                                          C6ED8FED 7157A4D0
        9EA1DDE8 946B5443 3ECC5449 A4A352AF 45764EE6 734BBB04


    V = HMAC(K, V) is
                                          EBC77525 6BB78124
        1E9C70BB CF732BDC 90AD10D9 DD3A896E CC12B92F FB6345AB


rnd_val is
                         085D57AF 6BABCF2B 9AEEF387 D531650E
        6A505C54 406AB37A 52899E0E CAB3632B 7A068A28 14C6DF6A
        E532B658 D0D9741C 84775FEE 45B684CD BDC25FBC B4D8F310


-------------------------------------------------------------

Second call to Generate
```

```
***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Seed_Material is
                             C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Key is
                                               C6ED8FED 7157A4D0
        9EA1DDE8 946B5443 3ECC5449 A4A352AF 45764EE6 734BBB04


  V is
                                               EBC77525 6BB78124
        1E9C70BB CF732BDC 90AD10D9 DD3A896E CC12B92F FB6345AB
```

```
---------------------------

  Update

    provided_data
                              C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
          EBC775 256BB781 241E9C70 BBCF732B DC90AD10 D9DD3A89
        6ECC12B9 2FFB6345 AB00C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                              EC9957E0 75B59A8B
        ABE0F473 DB8348C7 FDDB3291 39AAA1D9 81E7027A 8BF6F94D


    V = HMAC(K, V) is
                                              5D2D543E 1CB4E397
        FFD81958 E452D31E 951EEBBE 05AD5C68 6958E58B 1961275C


    ------------

    V || 0x01 || provided_data is
          5D2D54 3E1CB4E3 97FFD819 58E452D3 1E951EEB BE05AD5C
        686958E5 8B196127 5C01C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
```

```
                                                FC51DA84 F9696BCC
        84C8F2AC B924BCDF 72F82EA2 CA643F08 3B0C16C3 634EFC62


    V = HMAC(K, V) is
                                                B974E437 0AD576BB
        99C4E49E A680BFF9 8DE9E12F ECD013DE D43C80F6 9A7ADE8A


  Update (Key, V):

    Key is
                                                FC51DA84 F9696BCC
        84C8F2AC B924BCDF 72F82EA2 CA643F08 3B0C16C3 634EFC62


    V is
                                                B974E437 0AD576BB
        99C4E49E A680BFF9 8DE9E12F ECD013DE D43C80F6 9A7ADE8A


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                9B219FD9 0DE2A08E
        493405CF 874417B5 826770F3 94481555 DC668ACD 96B9A3E5


    temp is
                                                9B219FD9 0DE2A08E
        493405CF 874417B5 826770F3 94481555 DC668ACD 96B9A3E5


  ------------

    V = HMAC(K, V) is
                                                6F9D2C32 5E26D47C
        1DFCFC8F BF86126F 40A1E639 60F62749 342ECDB7 1B240DC6
```

```
    temp is
                            9B219FD9 0DE2A08E 493405CF 874417B5
        826770F3 94481555 DC668ACD 96B9A3E5 6F9D2C32 5E26D47C
        1DFCFC8F BF86126F 40A1E639 60F62749 342ECDB7 1B240DC6


----------------------------

  returned_bits is
                            9B219FD9 0DE2A08E 493405CF 874417B5
        826770F3 94481555 DC668ACD 96B9A3E5 6F9D2C32 5E26D47C
        1DFCFC8F BF86126F 40A1E639 60F62749 342ECDB7 1B240DC6


  call Update(additional_input, K, V)
----------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                          6F 9D2C325E 26D47C1D
        FCFC8FBF 86126F40 A1E63960 F6274934 2ECDB71B 240DC600


    K = HMAC(K, V || 0x00 || provided_data) is
                                          56A2B446 32CB8FC3
        A64009BF D6EC95E5 6CEF8E7C 912AA82B 16F61491 5D9CD6E3


    V = HMAC(K, V) is
                                          B5B396A0 1576B0FE
        42F40844 556C4CF4 B6804C94 DE9D6238 F1F7E7AF 5C7257F3


rnd_val is
                            9B219FD9 0DE2A08E 493405CF 874417B5
        826770F3 94481555 DC668ACD 96B9A3E5 6F9D2C32 5E26D47C
        1DFCFC8F BF86126F 40A1E639 60F62749 342ECDB7 1B240DC6
```

```
###############################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    EntropyInput1 (for Reseed1) =
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                  C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                              20212223 24252627


    PersonalizationString =
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
```

```
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536


    nonce is
                                                20212223 24252627


    personal_str is
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576
```

```
  ------------

  V || 0x00 || provided_data is
                                                 010101 01010101
      01010101 01010101 01010101 01010101 01010101 01010101
      01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
      16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
      2E2F3031 32333435 36202122 23242526 27404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x00 || provided_data) is
                                               E48294AE A5171B5D
      6A091450 868B39C4 B14D4E1A 9B29F128 416E1E14 81D10F69


  V = HMAC(K, V) is
                                               40987A58 C3E1346C
      0023F00F 417FA7BD 09C72FED A9738670 993392DF 490E94E2


  ------------

  V || 0x01 || provided_data is
                                                 40987A 58C3E134
      6C0023F0 0F417FA7 BD09C72F EDA97386 70993392 DF490E94
      E2010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
      16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
      2E2F3031 32333435 36202122 23242526 27404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x01 || provided_data) is
                                               65673C34 8E51CFAC
      C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


  V = HMAC(K, V) is
                                               E0F91AC9 9630EEE6
      7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


Update (Key, V):
```

```
    Key is
                                                65673C34 8E51CFAC
        C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


    V is
                                                E0F91AC9 9630EEE6
        7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


-----------------------------------------------------------------

First call to Generate

*****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

Generate FAILED: Reseed is required
*****************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    additional_input is  <empty>

  Seed_Material is
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


  Key is
                                                65673C34 8E51CFAC
        C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042
```

```
  V is
                                                E0F91AC9 9630EEE6
        7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


---------------------------

  Update

    provided_data
                                                  808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    ------------

    V || 0x00 || provided_data is
                           E0F91AC9 9630EEE6 7CF830CF D5044FEB
        F55C0C11 5007997A DA11296F C4164A9A 00808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    K = HMAC(K, V || 0x00 || provided_data) is
                                                6F9B62E0 F7918FD9
        251248F2 F8EBA1C3 DC736788 8BD5668A 08E773E3 4A197989


    V = HMAC(K, V) is
                                                54C051C9 1B500C9B
        798A021F E4B482AE 5D757F4F DFAA3502 489D1CEB A04D87DB


    ------------

    V || 0x01 || provided_data is
                           54C051C9 1B500C9B 798A021F E4B482AE
        5D757F4F DFAA3502 489D1CEB A04D87DB 01808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    K = HMAC(K, V || 0x01 || provided_data) is
                                                4476C6D1 1FC35D44
```

```
        09D9032E 453B0F0D C3314DB8 62CBDB60 9C560220 8D4C88D8


    V = HMAC(K, V) is
                                                95EF785A 61C2F7B3
        6BC596BA 4BA208A5 2C6DC203 636D8F17 87453B85 2B7E49EC


  Update (Key, V):

    Key is
                                                4476C6D1 1FC35D44
        09D9032E 453B0F0D C3314DB8 62CBDB60 9C560220 8D4C88D8


    V is
                                                95EF785A 61C2F7B3
        6BC596BA 4BA208A5 2C6DC203 636D8F17 87453B85 2B7E49EC


****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                D8B67130 714194FF
        E5B2A35D BCD5E1A2 9942AD5C 68F3DEB9 4ADD9E9E BAD86067


    temp is
                                                D8B67130 714194FF
        E5B2A35D BCD5E1A2 9942AD5C 68F3DEB9 4ADD9E9E BAD86067


  ------------

    V = HMAC(K, V) is
                                                EDF04915 FB40C391
        EAE70C65 9EAAE7EF 11A3D46A 5B085EDD 90CC72CE A989210B
```

```
    temp is
                           D8B67130 714194FF E5B2A35D BCD5E1A2
        9942AD5C 68F3DEB9 4ADD9E9E BAD86067 EDF04915 FB40C391
        EAE70C65 9EAAE7EF 11A3D46A 5B085EDD 90CC72CE A989210B


---------------------------

  returned_bits is
                           D8B67130 714194FF E5B2A35D BCD5E1A2
        9942AD5C 68F3DEB9 4ADD9E9E BAD86067 EDF04915 FB40C391
        EAE70C65 9EAAE7EF 11A3D46A 5B085EDD 90CC72CE A989210B


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                          ED F04915FB 40C391EA
        E70C659E AAE7EF11 A3D46A5B 085EDD90 CC72CEA9 89210B00


    K = HMAC(K, V || 0x00 || provided_data) is
                                          0DF9110E 2F225898
        24A9476C 8E32088E 51A0DA36 633F8CD1 F7547DFF 696E4B29


    V = HMAC(K, V) is
                                          C0E3C8ED 5A8B579E
        3FEF9DF3 B7C2C212 980717CC 91AE1866 45FABB2C C784D5D7


rnd_val is
                           D8B67130 714194FF E5B2A35D BCD5E1A2
        9942AD5C 68F3DEB9 4ADD9E9E BAD86067 EDF04915 FB40C391
        EAE70C65 9EAAE7EF 11A3D46A 5B085EDD 90CC72CE A989210B


-------------------------------------------------------------
```

```
Second call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is  <empty>

  Seed_Material is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  Key is
                                               0DF9110E 2F225898
        24A9476C 8E32088E 51A0DA36 633F8CD1 F7547DFF 696E4B29


  V is
                                               C0E3C8ED 5A8B579E
        3FEF9DF3 B7C2C212 980717CC 91AE1866 45FABB2C C784D5D7


---------------------------

  Update

    provided_data
                                                C0C1C2 C3C4C5C6
```

```
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  ------------

  V || 0x00 || provided_data is
                       C0E3C8ED 5A8B579E 3FEF9DF3 B7C2C212
    980717CC 91AE1866 45FABB2C C784D5D7 00C0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x00 || provided_data) is
                                          C1A605C2 002F91FD
    0D0CAAD2 8F6DC96D 0D0C0362 404C9B6F 41EB52F4 5A61204C


  V = HMAC(K, V) is
                                          A9EFDB92 95BD1AE4
    A9C00AFF 6D03ED60 697D8F5A 067F1B2F 1826A94D 42060E21


  ------------

  V || 0x01 || provided_data is
                       A9EFDB92 95BD1AE4 A9C00AFF 6D03ED60
    697D8F5A 067F1B2F 1826A94D 42060E21 01C0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


  K = HMAC(K, V || 0x01 || provided_data) is
                                          3D7763E5 303DB54B
    E20544A8 1E9F00CA DCFC1CB2 8DECB9CF C699F61D BAF88021


  V = HMAC(K, V) is
                                          FEBC0279 B7710DEC
    5C067EBE FA068E4B 5967491B 7EEF9475 83506D04 97CE67BA


Update (Key, V):

  Key is
                                          3D7763E5 303DB54B
```

```
        E20544A8 1E9F00CA DCFC1CB2 8DECB9CF C699F61D BAF88021


    V is
                                                FEBC0279 B7710DEC
        5C067EBE FA068E4B 5967491B 7EEF9475 83506D04 97CE67BA


****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                                8BBA71C2 583F2530
        C259C907 84A59AC4 4D1C8056 917CCF38 8788102D 73824C6C


    temp is
                                                8BBA71C2 583F2530
        C259C907 84A59AC4 4D1C8056 917CCF38 8788102D 73824C6C


  ------------

    V = HMAC(K, V) is
                                                11D5D63B E1F01017
        D884CD69 D9334B9E BC01E7BD 8FDF2A8E 52572293 DC21C0E1


    temp is
                           8BBA71C2 583F2530 C259C907 84A59AC4
        4D1C8056 917CCF38 8788102D 73824C6C 11D5D63B E1F01017
        D884CD69 D9334B9E BC01E7BD 8FDF2A8E 52572293 DC21C0E1


----------------------------

  returned_bits is
                           8BBA71C2 583F2530 C259C907 84A59AC4
        4D1C8056 917CCF38 8788102D 73824C6C 11D5D63B E1F01017
```

```
        D884CD69 D9334B9E BC01E7BD 8FDF2A8E 52572293 DC21C0E1


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                          11 D5D63BE1 F01017D8
        84CD69D9 334B9EBC 01E7BD8F DF2A8E52 572293DC 21C0E100


    K = HMAC(K, V || 0x00 || provided_data) is
                                          2D21AC94 992FD82B
        0980D3D5 9551B9D0 7C8D54B2 52B61628 9344F8AC 869ED35B


    V = HMAC(K, V) is
                                          610C34CD BF6F7533
        547F2332 EAC57EE3 1E724FB2 9255566B 59783316 6CD0399F


rnd_val is
                         8BBA71C2 583F2530 C259C907 84A59AC4
        4D1C8056 917CCF38 8788102D 73824C6C 11D5D63B E1F01017
        D884CD69 D9334B9E BC01E7BD 8FDF2A8E 52572293 DC21C0E1


##############################################################

HMAC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                            000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    EntropyInput1 (for Reseed1) =
                                                808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6


    EntropyInput2 (for Reseed2) =
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    Nonce =
                                             20212223 24252627


    PersonalizationString =
                                                404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    AdditionalInput1 =
                                                606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    AdditionalInput2 =
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


##################################################################

******************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                                                000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    nonce is
                                                20212223 24252627


    personal_str is
                                                  404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                                                01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36202122 23242526 27404142 43444546
        4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
        5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


    ------------
```

```
  V || 0x00 || provided_data is
                                                 010101 01010101
      01010101 01010101 01010101 01010101 01010101 01010101
      01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
      16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
      2E2F3031 32333435 36202122 23242526 27404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x00 || provided_data) is
                                                E48294AE A5171B5D
      6A091450 868B39C4 B14D4E1A 9B29F128 416E1E14 81D10F69


  V = HMAC(K, V) is
                                                40987A58 C3E1346C
      0023F00F 417FA7BD 09C72FED A9738670 993392DF 490E94E2


  ------------

  V || 0x01 || provided_data is
                                                  40987A 58C3E134
      6C0023F0 0F417FA7 BD09C72F EDA97386 70993392 DF490E94
      E2010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
      16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
      2E2F3031 32333435 36202122 23242526 27404142 43444546
      4748494A 4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E
      5F606162 63646566 6768696A 6B6C6D6E 6F707172 73747576


  K = HMAC(K, V || 0x01 || provided_data) is
                                                65673C34 8E51CFAC
      C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


  V = HMAC(K, V) is
                                                E0F91AC9 9630EEE6
      7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


Update (Key, V):

  Key is
                                                65673C34 8E51CFAC
```

C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042

V is
E0F91AC9 9630EEE6
7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A

First call to Generate

****

HMAC_DRBG_Generate

requested_number_of_bits = 512

additional_input is
606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596

Generate FAILED: Reseed is required
****

HMAC_DRBG_Reseed_algorithm

entropy_input is
808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6

additional_input is
606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596

Seed_Material is
8081 82838485 86878889 8A8B8C8D
8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


  Key is
                                             65673C34 8E51CFAC
        C410BD20 0249A59A 9D6BAE77 6904271B B1F718DA 1D182042


  V is
                                             E0F91AC9 9630EEE6
        7CF830CF D5044FEB F55C0C11 5007997A DA11296F C4164A9A


---------------------------

  Update

    provided_data
                              8081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    ------------

    V || 0x00 || provided_data is
          E0F91A C99630EE E67CF830 CFD5044F EBF55C0C 11500799
        7ADA1129 6FC4164A 9A008081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x00 || provided_data) is
                                             3F5556FC 1A11F18F
        5A33BA25 176B9620 EAD725FA C9BDB742 C14FE54A 98009E8A


    V = HMAC(K, V) is
                                             8B023A87 012038CA
        F38F39C5 F120B858 5668FE6C D263A944 EBEA32F9 020D365C
```

```
    ------------

    V || 0x01 || provided_data is
          8B023A 87012038 CAF38F39 C5F120B8 585668FE 6CD263A9
        44EBEA32 F9020D36 5C018081 82838485 86878889 8A8B8C8D
        8E8F9091 92939495 96979899 9A9B9C9D 9E9FA0A1 A2A3A4A5
        A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5 B6606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596


    K = HMAC(K, V || 0x01 || provided_data) is
                                            B381388C 1D7CFD56
        5930993B D9269066 5088D9B8 39969B87 F16DB6DF 4E4300D7


    V = HMAC(K, V) is
                                            FA042564 00E342E6
        55F43326 94E3B24C 04FB85BF 878021E4 52E73B8F 46D4BDC6


  Update (Key, V):

    Key is
                                            B381388C 1D7CFD56
        5930993B D9269066 5088D9B8 39969B87 F16DB6DF 4E4300D7


    V is
                                            FA042564 00E342E6
        55F43326 94E3B24C 04FB85BF 878021E4 52E73B8F 46D4BDC6


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                                            44D78BBC 3EB67C59
        C22F6C31 003D212A 7837CCD8 4C438B55 150FD013 A8A78FE8
```

```
    temp is
                                                44D78BBC 3EB67C59
        C22F6C31 003D212A 7837CCD8 4C438B55 150FD013 A8A78FE8


  ------------

    V = HMAC(K, V) is
                                                EDEA81C6 72E4B8DD
        C8183886 E69C2E17 7DF574C1 F190DF27 1850F8CE 55EF20B8


    temp is
                           44D78BBC 3EB67C59 C22F6C31 003D212A
        7837CCD8 4C438B55 150FD013 A8A78FE8 EDEA81C6 72E4B8DD
        C8183886 E69C2E17 7DF574C1 F190DF27 1850F8CE 55EF20B8


---------------------------

  returned_bits is
                           44D78BBC 3EB67C59 C22F6C31 003D212A
        7837CCD8 4C438B55 150FD013 A8A78FE8 EDEA81C6 72E4B8DD
        C8183886 E69C2E17 7DF574C1 F190DF27 1850F8CE 55EF20B8


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                             ED EA81C672 E4B8DDC8
        183886E6 9C2E177D F574C1F1 90DF2718 50F8CE55 EF20B800


    K = HMAC(K, V || 0x00 || provided_data) is
                                                D41F6F33 65822170
        50B1F659 28FD6E94 CBC94568 FE3B6B53 389E1E3A 5B49E101
```

```
    V = HMAC(K, V) is
                                              A655C9E7 D133F1CD
        8B1161F2 7D54E75A 7E7C8042 BF74D47F 9FFD60E2 45EBA57E


rnd_val is
                          44D78BBC 3EB67C59 C22F6C31 003D212A
        7837CCD8 4C438B55 150FD013 A8A78FE8 EDEA81C6 72E4B8DD
        C8183886 E69C2E17 7DF574C1 F190DF27 1850F8CE 55EF20B8


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                                                C0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6


    additional_input is
                                                A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Seed_Material is
```

```
                            C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


  Key is
                                            D41F6F33 65822170
        50B1F659 28FD6E94 CBC94568 FE3B6B53 389E1E3A 5B49E101


  V is
                                            A655C9E7 D133F1CD
        8B1161F2 7D54E75A 7E7C8042 BF74D47F 9FFD60E2 45EBA57E


----------------------------

  Update

    provided_data
                            C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    ------------

    V || 0x00 || provided_data is
          A655C9 E7D133F1 CD8B1161 F27D54E7 5A7E7C80 42BF74D4
        7F9FFD60 E245EBA5 7E00C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x00 || provided_data) is
                                            5C2A1146 F81ABA3A
        CFFBF538 A8BDFACC 7BF1FCBC E131B8C5 1138877A 7701B1CD


    V = HMAC(K, V) is
```

```
                                                2E7BF1B5 D13386DA
        220B6E1F BA67B999 D3CC7DDC F939FD50 4D1A1534 6ABC94D2


    ------------

    V || 0x01 || provided_data is
          2E7BF1 B5D13386 DA220B6E 1FBA67B9 99D3CC7D DCF939FD
        504D1A15 346ABC94 D201C0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5 F6A0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6


    K = HMAC(K, V || 0x01 || provided_data) is
                                                FBA80545 3E3C9A73
        64585CED BCD29230 FBC93D6F 129D21ED DDF6613B 3A8FF283


    V = HMAC(K, V) is
                                                83647A33 8C153CBA
        F0E49A54 A44FEA66 70CFD7C1 714D4AB3 5F11123D F27B69CF


  Update (Key, V):

    Key is
                                                FBA80545 3E3C9A73
        64585CED BCD29230 FBC93D6F 129D21ED DDF6613B 3A8FF283


    V is
                                                83647A33 8C153CBA
        F0E49A54 A44FEA66 70CFD7C1 714D4AB3 5F11123D F27B69CF


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 512

    additional_input is  <empty>

  ------------
```

```
    V = HMAC(K, V) is
                                                917780DC 0CE9989F
        EE6C0806 D6DA123A 18252947 58D4E1B5 82687231 780A2A9C


    temp is
                                                917780DC 0CE9989F
        EE6C0806 D6DA123A 18252947 58D4E1B5 82687231 780A2A9C


  ------------

    V = HMAC(K, V) is
                                                33F1D156 CCAD3277
        64B29A4C B2690177 AE96EF9E E92AD0C3 40BA0FD1 203C02C6


    temp is
                            917780DC 0CE9989F EE6C0806 D6DA123A
        18252947 58D4E1B5 82687231 780A2A9C 33F1D156 CCAD3277
        64B29A4C B2690177 AE96EF9E E92AD0C3 40BA0FD1 203C02C6


---------------------------

  returned_bits is
                            917780DC 0CE9989F EE6C0806 D6DA123A
        18252947 58D4E1B5 82687231 780A2A9C 33F1D156 CCAD3277
        64B29A4C B2690177 AE96EF9E E92AD0C3 40BA0FD1 203C02C6


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                          33 F1D156CC AD327764
        B29A4CB2 690177AE 96EF9EE9 2AD0C340 BA0FD120 3C02C600
```

```
    K = HMAC(K, V || 0x00 || provided_data) is
                                                AE59C70A 7C60ED49
        8378EA84 5BE97D8F F881E0EA 372E265F A6728429 3E1A46AC


    V = HMAC(K, V) is
                                                E2F04DE3 CE217961
        AE2B2D20 A7BA7C6C 820B5B14 926E5956 AE6DFA2E D1D63993


rnd_val is
                          917780DC 0CE9989F EE6C0806 D6DA123A
        18252947 58D4E1B5 82687231 780A2A9C 33F1D156 CCAD3277
        64B29A4C B2690177 AE96EF9E E92AD0C3 40BA0FD1 203C02C6
```

```
###############################################################

HMAC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                   20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


--------------------------

  Update

    provided_data
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
```

```
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


------------

V || 0x00 || provided_data is
                                                    01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 00000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


K = HMAC(K, V || 0x00 || provided_data) is
    E5675B81 A558502A 38EBFD09 A9753D3E F31388D1 EF8EFC89
    1808526C D64ABF8C 3502D83F 20CE07DB 68F0FA99 22789E4C


V = HMAC(K, V) is
    F70F7FF2 45023323 7528314F A8EBF4D2 50B95649 06F0EF58
    41402759 CD72F743 72924730 1F85C172 1CCB323D 4D8B887F


------------

V || 0x01 || provided_data is
                                                    F70F7FF2
    45023323 7528314F A8EBF4D2 50B95649 06F0EF58 41402759
    CD72F743 72924730 1F85C172 1CCB323D 4D8B887F 01000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


K = HMAC(K, V || 0x01 || provided_data) is
    DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
    4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


V = HMAC(K, V) is
    D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
```

```
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


  Update (Key, V):

    Key is
        DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
        4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


    V is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        FF08EED5 0F04D543 FAE5C9C8 FB31D784 89FE82C9 F77F60ED
        A91A86E5 5EFADB6B 3431BF08 86BC1A63 C44FAD9B 9715C092


    temp is
        FF08EED5 0F04D543 FAE5C9C8 FB31D784 89FE82C9 F77F60ED
        A91A86E5 5EFADB6B 3431BF08 86BC1A63 C44FAD9B 9715C092


  ------------

    V = HMAC(K, V) is
        6C24AA45 76A94444 23BF6B55 8CEA09FD BADCE2A5 C05BD480
        F8DEF079 75826DAA 53EF71EC 7E28CB38 1D10A7B0 C09A1D15
```

```
    temp is
        FF08EED5 0F04D543 FAE5C9C8 FB31D784 89FE82C9 F77F60ED
        A91A86E5 5EFADB6B 3431BF08 86BC1A63 C44FAD9B 9715C092
        6C24AA45 76A94444 23BF6B55 8CEA09FD BADCE2A5 C05BD480
        F8DEF079 75826DAA 53EF71EC 7E28CB38 1D10A7B0 C09A1D15


---------------------------

  returned_bits is
        FF08EED5 0F04D543 FAE5C9C8 FB31D784 89FE82C9 F77F60ED
        A91A86E5 5EFADB6B 3431BF08 86BC1A63 C44FAD9B 9715C092
        6C24AA45 76A94444 23BF6B55 8CEA09FD BADCE2A5 C05BD480
        F8DEF079 75826DAA 53EF71EC 7E28CB38 1D10A7B0 C09A1D15


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                            6C
        24AA4576 A9444423 BF6B558C EA09FDBA DCE2A5C0 5BD480F8
        DEF07975 826DAA53 EF71EC7E 28CB381D 10A7B0C0 9A1D1500


    K = HMAC(K, V || 0x00 || provided_data) is
        18ABF78C 40CBE6E8 600D08EA F18D1BF7 0843B2B0 7A15B490
        3E94462E 7F56DBB5 C5138A34 28860A33 0FDCF44E CA1CCCF4


    V = HMAC(K, V) is
        DD77E6C8 006B2F77 53357544 3B15471A 32442ACF 231FD04B
        A91F6650 4735CE0F 51BEC2CE 3D9A9B6E 0719E730 63B93FAA


rnd_val is
        FF08EED5 0F04D543 FAE5C9C8 FB31D784 89FE82C9 F77F60ED
        A91A86E5 5EFADB6B 3431BF08 86BC1A63 C44FAD9B 9715C092
        6C24AA45 76A94444 23BF6B55 8CEA09FD BADCE2A5 C05BD480
        F8DEF079 75826DAA 53EF71EC 7E28CB38 1D10A7B0 C09A1D15
```

```
------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        1B3D9FAB 561E4C87 B78EABAC 0773E0CE 6AF93E9B B67B7719
        C6176752 7000351D D7D6910F 3AA375B7 70D38CF2 0270CBB1


    temp is
        1B3D9FAB 561E4C87 B78EABAC 0773E0CE 6AF93E9B B67B7719
        C6176752 7000351D D7D6910F 3AA375B7 70D38CF2 0270CBB1


  ------------

    V = HMAC(K, V) is
        147AE249 F9DADB7A 5B4B6380 12C14ECA DCA32FBD DA8ED4BF
        73586EE5 DC9D543F 210437D4 866F7A2E FD326447 CAF4F68C


    temp is
        1B3D9FAB 561E4C87 B78EABAC 0773E0CE 6AF93E9B B67B7719
        C6176752 7000351D D7D6910F 3AA375B7 70D38CF2 0270CBB1
        147AE249 F9DADB7A 5B4B6380 12C14ECA DCA32FBD DA8ED4BF
        73586EE5 DC9D543F 210437D4 866F7A2E FD326447 CAF4F68C


---------------------------

  returned_bits is
        1B3D9FAB 561E4C87 B78EABAC 0773E0CE 6AF93E9B B67B7719
        C6176752 7000351D D7D6910F 3AA375B7 70D38CF2 0270CBB1
        147AE249 F9DADB7A 5B4B6380 12C14ECA DCA32FBD DA8ED4BF
```

```
        73586EE5 DC9D543F 210437D4 866F7A2E FD326447 CAF4F68C


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                                  14
        7AE249F9 DADB7A5B 4B638012 C14ECADC A32FBDDA 8ED4BF73
        586EE5DC 9D543F21 0437D486 6F7A2EFD 326447CA F4F68C00


    K = HMAC(K, V || 0x00 || provided_data) is
        E53CFF8F DA284692 96F3D2D6 88164204 CC767F00 2107AEB6
        9EB94ACB 0AC7C5C5 AD431FDF D7367E09 2C0E78B5 E59964AA


    V = HMAC(K, V) is
        D24F1437 9D37B5AF 5EA4FF2D B78051D6 609007A7 86E2579C
        690997DF 3E82B760 437A98E4 59F10497 9C6A6209 D56F72FD


rnd_val is
        1B3D9FAB 561E4C87 B78EABAC 0773E0CE 6AF93E9B B67B7719
        C6176752 7000351D D7D6910F 3AA375B7 70D38CF2 0270CBB1
        147AE249 F9DADB7A 5B4B6380 12C14ECA DCA32FBD DA8ED4BF
        73586EE5 DC9D543F 210437D4 866F7A2E FD326447 CAF4F68C


##############################################################

HMAC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
```

```
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                              808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                              C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput1 =
                              606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                              A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


##############################################################
```

```
**************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                              000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
```

```
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


------------

V || 0x00 || provided_data is
                                                    01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 00000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


K = HMAC(K, V || 0x00 || provided_data) is
    E5675B81 A558502A 38EBFD09 A9753D3E F31388D1 EF8EFC89
    1808526C D64ABF8C 3502D83F 20CE07DB 68F0FA99 22789E4C


V = HMAC(K, V) is
    F70F7FF2 45023323 7528314F A8EBF4D2 50B95649 06F0EF58
    41402759 CD72F743 72924730 1F85C172 1CCB323D 4D8B887F


------------

V || 0x01 || provided_data is
                                                    F70F7FF2
    45023323 7528314F A8EBF4D2 50B95649 06F0EF58 41402759
    CD72F743 72924730 1F85C172 1CCB323D 4D8B887F 01000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


K = HMAC(K, V || 0x01 || provided_data) is
    DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
    4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7
```

```
    V = HMAC(K, V) is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


  Update (Key, V):

    Key is
        DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
        4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


    V is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

```
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


------------

V || 0x00 || provided_data is
                      D6F45225 560DF998 B7006216 D4FFAE27
    44D97518 D7585280 09A9DCE6 1D50A2FF B4C53C9E D7B405C5
    6692FDA8 5523EC69 00606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
    5BA16AA7 BD2432F2 F1553EFA 42AFFEB9 6E429977 94C4F924
    F924BD53 C2571A12 2164A46A 9D760495 F2B4E83D 484C047A


V = HMAC(K, V) is
    71DA2378 FC0B0FB7 CBEB0FC0 252EE2E2 443DF2B2 CF9EE746
    94886FC9 45D7996E 85CFFEDC C9DBCF44 3AEE92FF BEC95804


------------

V || 0x01 || provided_data is
                      71DA2378 FC0B0FB7 CBEB0FC0 252EE2E2
    443DF2B2 CF9EE746 94886FC9 45D7996E 85CFFEDC C9DBCF44
    3AEE92FF BEC95804 01606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x01 || provided_data) is
    3089EB25 D72DB470 D0BC6DEA BA31774E 0E4C8C50 E95D8B34
    6008395E BC21568A E7A2E89F A6507D97 591887EB 1D94D037


V = HMAC(K, V) is
    A22922DE 91403C5A 2A65EF5E 53586775 96A3B2C7 CA75F99F
    C90789BD 0B7A4444 A361FE0B B058B244 5B79E361 BF5E70D9
```

```
  ------------

    V = HMAC(K, V) is
        52DCD4A4 07EE8506 D9CFF5B0 1F938959 73D45E58 52AFA29A
        8F11ADFC CDF21274 57C3BAB6 D6A0EC28 7DAB83C6 1011D311


    temp is
        52DCD4A4 07EE8506 D9CFF5B0 1F938959 73D45E58 52AFA29A
        8F11ADFC CDF21274 57C3BAB6 D6A0EC28 7DAB83C6 1011D311


  ------------

    V = HMAC(K, V) is
        D3CC40D6 FE744874 4A13E811 ABE42206 9118240B 09B4E330
        FB7EB1E1 C1871B73 92C5B7EF A753EDA2 260D41ED A4B0A8EE


    temp is
        52DCD4A4 07EE8506 D9CFF5B0 1F938959 73D45E58 52AFA29A
        8F11ADFC CDF21274 57C3BAB6 D6A0EC28 7DAB83C6 1011D311
        D3CC40D6 FE744874 4A13E811 ABE42206 9118240B 09B4E330
        FB7EB1E1 C1871B73 92C5B7EF A753EDA2 260D41ED A4B0A8EE


---------------------------

  returned_bits is
        52DCD4A4 07EE8506 D9CFF5B0 1F938959 73D45E58 52AFA29A
        8F11ADFC CDF21274 57C3BAB6 D6A0EC28 7DAB83C6 1011D311
        D3CC40D6 FE744874 4A13E811 ABE42206 9118240B 09B4E330
        FB7EB1E1 C1871B73 92C5B7EF A753EDA2 260D41ED A4B0A8EE


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
```

B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

V || 0x00 || provided_data is
D3CC40D6 FE744874 4A13E811 ABE42206
9118240B 09B4E330 FB7EB1E1 C1871B73 92C5B7EF A753EDA2
260D41ED A4B0A8EE 00606162 63646566 6768696A 6B6C6D6E
6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

K = HMAC(K, V || 0x00 || provided_data) is
771D7ECC 7123E344 3ADB89D1 B603E562 388ED87D 0AEB880C
E39C5C7A 2A89E4D8 204CDA7D 9F004C3B 6667B4D4 E8618AB8

V = HMAC(K, V) is
3D063B7D AAD0ADB7 0C47A2BF 1B230784 DA404A4C 12B938D7
62B69E88 79B63A71 53501820 15D3228D 2E06722D 79BD737E

V || 0x01 || provided_data is
3D063B7D AAD0ADB7 0C47A2BF 1B230784
DA404A4C 12B938D7 62B69E88 79B63A71 53501820 15D3228D
2E06722D 79BD737E 01606162 63646566 6768696A 6B6C6D6E
6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

K = HMAC(K, V || 0x01 || provided_data) is
FDB20FD7 B77F2156 4502583E AC235F3B 21C20A19 4560D1BD
FDC2C11F FB5E080E B489EF00 21B03C0A 40408DA1 111FB993

V = HMAC(K, V) is
27CE0060 D10422FB 7B643CE0 629E9DB5 6A1DE24B C240E025
417CDA29 8C34D886 FA41695C 9FD4364B A8E8044A 6CD95873

```
rnd_val is
        52DCD4A4 07EE8506 D9CFF5B0 1F938959 73D45E58 52AFA29A
        8F11ADFC CDF21274 57C3BAB6 D6A0EC28 7DAB83C6 1011D311
        D3CC40D6 FE744874 4A13E811 ABE42206 9118240B 09B4E330
        FB7EB1E1 C1871B73 92C5B7EF A753EDA2 260D41ED A4B0A8EE


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    ------------

    V || 0x00 || provided_data is
                          27CE0060 D10422FB 7B643CE0 629E9DB5
        6A1DE24B C240E025 417CDA29 8C34D886 FA41695C 9FD4364B
        A8E8044A 6CD95873 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
```

```
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  K = HMAC(K, V || 0x00 || provided_data) is
      517B62B9 F5FFA061 2AEBEAAA 197F0182 81A2A93A E972E47A
      874D25CC D2968468 9513584D 05A59A34 1A063F05 F49F628A


  V = HMAC(K, V) is
      8E003226 D59AC8C3 057114CC 583643DC 5B30CB9B AB9CE09E
      CB0FCBA5 E9D3767E 40B57B67 C7B9B627 371D7EF0 EBE01D9E


  ------------

  V || 0x01 || provided_data is
                       8E003226 D59AC8C3 057114CC 583643DC
      5B30CB9B AB9CE09E CB0FCBA5 E9D3767E 40B57B67 C7B9B627
      371D7EF0 EBE01D9E 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  K = HMAC(K, V || 0x01 || provided_data) is
      B403259D 1B927583 94D8AF63 84D8548E C962457B 14005AB0
      B3C49530 77365A85 895CE8A9 247B3EA1 32308830 FEBBE984


  V = HMAC(K, V) is
      89BC4ADF F69AC101 B3B83AA8 4BBF0F0E 3880BFA4 97C19D27
      39C1D876 47225AF9 DD545E9F 9DED4011 E2D2F74E 322D1D34


------------

  V = HMAC(K, V) is
      A8E2404D 14F6AE1F A9B66686 3D4C0265 2B806170 3F958798
      870032C9 D6D3CA10 302DC1C5 FE0F5B21 1F760EFB 4177684B


  temp is
      A8E2404D 14F6AE1F A9B66686 3D4C0265 2B806170 3F958798
```

```
        870032C9 D6D3CA10 302DC1C5 FE0F5B21 1F760EFB 4177684B


  ------------

    V = HMAC(K, V) is
        A5056D84 B35B9FCC E4C44818 080346AD CC9AC610 E4719575
        B0D1713D DF30C671 99EA0A17 B1592E9B 75390462 D3059C35


    temp is
        A8E2404D 14F6AE1F A9B66686 3D4C0265 2B806170 3F958798
        870032C9 D6D3CA10 302DC1C5 FE0F5B21 1F760EFB 4177684B
        A5056D84 B35B9FCC E4C44818 080346AD CC9AC610 E4719575
        B0D1713D DF30C671 99EA0A17 B1592E9B 75390462 D3059C35


---------------------------

  returned_bits is
        A8E2404D 14F6AE1F A9B66686 3D4C0265 2B806170 3F958798
        870032C9 D6D3CA10 302DC1C5 FE0F5B21 1F760EFB 4177684B
        A5056D84 B35B9FCC E4C44818 080346AD CC9AC610 E4719575
        B0D1713D DF30C671 99EA0A17 B1592E9B 75390462 D3059C35


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    ------------

    V || 0x00 || provided_data is
                          A5056D84 B35B9FCC E4C44818 080346AD
        CC9AC610 E4719575 B0D1713D DF30C671 99EA0A17 B1592E9B
        75390462 D3059C35 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
```

```
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x00 || provided_data) is
        C1BE3D41 76D35248 9193251F 10D37B56 65045FA1 013AEF3F
        5A37A984 8FD2387A 59B33F9B 575F73A5 192FDCC7 3B0FA53E


    V = HMAC(K, V) is
        C5DE0CEC 4C36EDB0 228BCCC9 9AA5EBC9 9286C1A9 3735E767
        10AF8539 A99F3452 FD9DB65A 2F4A5CA1 F517B0D5 31824731


    ------------

    V || 0x01 || provided_data is
                          C5DE0CEC 4C36EDB0 228BCCC9 9AA5EBC9
        9286C1A9 3735E767 10AF8539 A99F3452 FD9DB65A 2F4A5CA1
        F517B0D5 31824731 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x01 || provided_data) is
        BB28D41B A296C891 577EBB93 4C0E5275 24BC193A 4D7D710A
        9E265304 82B810FF C829B71C 13A933D8 A4EE193D 9DDDC831


    V = HMAC(K, V) is
        5B6628DF 4BBE2767 1ECED5EF 03ECEDA7 FB399DA3 E756658F
        8F86A6F0 D115F17E A973BEEF B2BE905B 9115AACD EE5AB92A


rnd_val is
        A8E2404D 14F6AE1F A9B66686 3D4C0265 2B806170 3F958798
        870032C9 D6D3CA10 302DC1C5 FE0F5B21 1F760EFB 4177684B
        A5056D84 B35B9FCC E4C44818 080346AD CC9AC610 E4719575
        B0D1713D DF30C671 99EA0A17 B1592E9B 75390462 D3059C35


################################################################
```

```
HMAC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

##################################################################
```

```
************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                  20212223 24252627 28292A2B


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                      0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
```

```
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                    0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    ------------

    V || 0x00 || provided_data is
                  010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01000001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x00 || provided_data) is
        759FC2E2 D33686FF B43AB4F9 27A9E74D 7C30CE89 05C5AEDF
        7A84FF76 479BD8B6 D930A267 6D76D9BC B2F420A3 4B76654A


    V = HMAC(K, V) is
        D873522C B0FC9099 33B67222 16975EA8 B7EA9349 6647EB8B
        BC9A0873 5DE801C3 6D01ABE8 52B764E9 9514935A 9567A39D
```

```
    ------------

    V || 0x01 || provided_data is
                   D87352 2CB0FC90 9933B672 2216975E A8B7EA93
        496647EB 8BBC9A08 735DE801 C36D01AB E852B764 E9951493
        5A9567A3 9D010001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x01 || provided_data) is
        085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


    V = HMAC(K, V) is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


  Update (Key, V):

    Key is
        085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


    V is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


---------------------------------------------------------------

First call to Generate

***************************************************************
```

```
HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        03AB8BCE 4D1DBBB6 36C5C5B7 E1C58499 FEB1C619 CDD11D35
        CD6CF6BB 8F20EF27 B6F5F905 4FF900DB 9EBF7BF3 0ED4DCBB


    temp is
        03AB8BCE 4D1DBBB6 36C5C5B7 E1C58499 FEB1C619 CDD11D35
        CD6CF6BB 8F20EF27 B6F5F905 4FF900DB 9EBF7BF3 0ED4DCBB


  ------------

    V = HMAC(K, V) is
        BC8D5B51 C965EA22 6FFEE2CA 5AB2EFD0 0754DC32 F357BF7A
        E42275E0 F7704DC4 4E50A522 0AD05AB6 98A22640 AC634829


    temp is
        03AB8BCE 4D1DBBB6 36C5C5B7 E1C58499 FEB1C619 CDD11D35
        CD6CF6BB 8F20EF27 B6F5F905 4FF900DB 9EBF7BF3 0ED4DCBB
        BC8D5B51 C965EA22 6FFEE2CA 5AB2EFD0 0754DC32 F357BF7A
        E42275E0 F7704DC4 4E50A522 0AD05AB6 98A22640 AC634829


---------------------------

  returned_bits is
        03AB8BCE 4D1DBBB6 36C5C5B7 E1C58499 FEB1C619 CDD11D35
        CD6CF6BB 8F20EF27 B6F5F905 4FF900DB 9EBF7BF3 0ED4DCBB
        BC8D5B51 C965EA22 6FFEE2CA 5AB2EFD0 0754DC32 F357BF7A
        E42275E0 F7704DC4 4E50A522 0AD05AB6 98A22640 AC634829


  call Update(additional_input, K, V)
---------------------------

  Update
```

```
    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                                BC
        8D5B51C9 65EA226F FEE2CA5A B2EFD007 54DC32F3 57BF7AE4
        2275E0F7 704DC44E 50A5220A D05AB698 A22640AC 63482900


    K = HMAC(K, V || 0x00 || provided_data) is
        6FF4623B 22742731 AD3855C1 446809EA 9EC2015B 75140D0C
        C47CFEAD 2F520948 78BFB048 F4FC4C8A 47E52D96 64ADF033


    V = HMAC(K, V) is
        0D61885B 765A2E62 04BC92F5 BFBF4FA5 4ABB7668 245399A0
        B87B4771 0E75CF2A D8A089EF 7827EF56 19CEF3AB 668708C1


rnd_val is
        03AB8BCE 4D1DBBB6 36C5C5B7 E1C58499 FEB1C619 CDD11D35
        CD6CF6BB 8F20EF27 B6F5F905 4FF900DB 9EBF7BF3 0ED4DCBB
        BC8D5B51 C965EA22 6FFEE2CA 5AB2EFD0 0754DC32 F357BF7A
        E42275E0 F7704DC4 4E50A522 0AD05AB6 98A22640 AC634829


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        B907E771 44FD55A5 4E9BA1A6 A0EED0AA C780020C 41A15DD8
        9A6C1638 30BA1D09 4E6A1710 0FF71EE3 0A96E1EE 04D2A966
```

```
    temp is
        B907E771 44FD55A5 4E9BA1A6 A0EED0AA C780020C 41A15DD8
        9A6C1638 30BA1D09 4E6A1710 0FF71EE3 0A96E1EE 04D2A966


  ------------

    V = HMAC(K, V) is
        03832A4E 404F1966 C2B5F4CB 61B9927E 8D12AC1E 1A24CF23
        88C14E8E C96C3518 1EAEE32A AA46330D EAAFE5E7 CE783C74


    temp is
        B907E771 44FD55A5 4E9BA1A6 A0EED0AA C780020C 41A15DD8
        9A6C1638 30BA1D09 4E6A1710 0FF71EE3 0A96E1EE 04D2A966
        03832A4E 404F1966 C2B5F4CB 61B9927E 8D12AC1E 1A24CF23
        88C14E8E C96C3518 1EAEE32A AA46330D EAAFE5E7 CE783C74


---------------------------

  returned_bits is
        B907E771 44FD55A5 4E9BA1A6 A0EED0AA C780020C 41A15DD8
        9A6C1638 30BA1D09 4E6A1710 0FF71EE3 0A96E1EE 04D2A966
        03832A4E 404F1966 C2B5F4CB 61B9927E 8D12AC1E 1A24CF23
        88C14E8E C96C3518 1EAEE32A AA46330D EAAFE5E7 CE783C74


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                            03
        832A4E40 4F1966C2 B5F4CB61 B9927E8D 12AC1E1A 24CF2388
        C14E8EC9 6C35181E AEE32AAA 46330DEA AFE5E7CE 783C7400


    K = HMAC(K, V || 0x00 || provided_data) is
        EC249919 FFD99A78 321BBC13 DD7C3718 DC349F49 A255AC62
```

```
        D691306F B5BAFBDD 035BEADD 49D42B0C 7D4EA325 A0649B04


    V = HMAC(K, V) is
        5CE2AAC0 55EA1A0D 199DAF5C F250EB3E E8711ED5 5D2589E3
        AED9FF62 9F47199D 7EB1669E 7CE6CD51 90C528D5 63D72107


rnd_val is
        B907E771 44FD55A5 4E9BA1A6 A0EED0AA C780020C 41A15DD8
        9A6C1638 30BA1D09 4E6A1710 0FF71EE3 0A96E1EE 04D2A966
        03832A4E 404F1966 C2B5F4CB 61B9927E 8D12AC1E 1A24CF23
        88C14E8E C96C3518 1EAEE32A AA46330D EAAFE5E7 CE783C74


################################################################

HMAC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E
```

```
    Nonce =
                                  20212223 24252627 28292A2B


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput1 =
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


##################################################################

******************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                  20212223 24252627 28292A2B
```

```
    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                     0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                     0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
```

```
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


------------

V || 0x00 || provided_data is
                010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01000001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


K = HMAC(K, V || 0x00 || provided_data) is
    759FC2E2 D33686FF B43AB4F9 27A9E74D 7C30CE89 05C5AEDF
    7A84FF76 479BD8B6 D930A267 6D76D9BC B2F420A3 4B76654A


V = HMAC(K, V) is
    D873522C B0FC9099 33B67222 16975EA8 B7EA9349 6647EB8B
    BC9A0873 5DE801C3 6D01ABE8 52B764E9 9514935A 9567A39D


------------

V || 0x01 || provided_data is
                D87352 2CB0FC90 9933B672 2216975E A8B7EA93
    496647EB 8BBC9A08 735DE801 C36D01AB E852B764 E9951493
    5A9567A3 9D010001 02030405 06070809 0A0B0C0D 0E0F1011
    12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
    2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
    42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
    5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
    23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
```

```
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x01 || provided_data) is
        085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


    V = HMAC(K, V) is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


  Update (Key, V):

    Key is
        085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


    V is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------
```

```
Update

  provided_data
                          606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  ------------

  V || 0x00 || provided_data is
                        8E065B64 B430910B 4950528A F23A9FA2
      866F8DAA 9106B72E 38BA0B93 D033B851 04485F29 D1AD7EB6
      FF1643D6 9129654D 00606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  K = HMAC(K, V || 0x00 || provided_data) is
      40F45F9B DB63CE2D C49A99E2 22EB624D 1392BF1E 31F6BE87
      E4FBA82F 7BB4F4B6 1A26C174 B21EBBB7 843E7378 31F2D481


  V = HMAC(K, V) is
      BB1F9B0F 08693EE1 512D9E7E 94CED7F8 4CCA5D1F 07B74BCB
      4D988A48 4E6CABDD 0BDBCAA7 0073F85D D3B981FE 6F0588DE


  ------------

  V || 0x01 || provided_data is
                        BB1F9B0F 08693EE1 512D9E7E 94CED7F8
      4CCA5D1F 07B74BCB 4D988A48 4E6CABDD 0BDBCAA7 0073F85D
      D3B981FE 6F0588DE 01606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  K = HMAC(K, V || 0x01 || provided_data) is
```

```
        F43A39BD 8EBD1620 2FD2A304 EE4D3F5A C29A8855 98BD4370
        E3EC8A77 8F45378E DFF8936C D073D36A 6AC105FF A2BE704C


    V = HMAC(K, V) is
        F2B03FB9 BA930DE3 71C08DD4 D1D26541 2A7AC84A B2314D89
        2C30AFC9 BA96423A CD267E78 F84671DE 43B61E79 6C6687D1


  ------------

    V = HMAC(K, V) is
        3918F6DF 5E50B922 CDD7D0FB 87967822 33141EEE 8A14AB69
        B2B3970A F1D30D9F 344225A1 5384869B 208ADB4B 5674C6DA


    temp is
        3918F6DF 5E50B922 CDD7D0FB 87967822 33141EEE 8A14AB69
        B2B3970A F1D30D9F 344225A1 5384869B 208ADB4B 5674C6DA


  ------------

    V = HMAC(K, V) is
        0C9ED74F 56BC8FB4 8145FB36 90FDA956 1AD6038A 5B1E0BA2
        AC09FCC5 D35E5898 3570F37C CE516D76 407A2342 F802CCB9


    temp is
        3918F6DF 5E50B922 CDD7D0FB 87967822 33141EEE 8A14AB69
        B2B3970A F1D30D9F 344225A1 5384869B 208ADB4B 5674C6DA
        0C9ED74F 56BC8FB4 8145FB36 90FDA956 1AD6038A 5B1E0BA2
        AC09FCC5 D35E5898 3570F37C CE516D76 407A2342 F802CCB9


---------------------------

  returned_bits is
        3918F6DF 5E50B922 CDD7D0FB 87967822 33141EEE 8A14AB69
        B2B3970A F1D30D9F 344225A1 5384869B 208ADB4B 5674C6DA
        0C9ED74F 56BC8FB4 8145FB36 90FDA956 1AD6038A 5B1E0BA2
        AC09FCC5 D35E5898 3570F37C CE516D76 407A2342 F802CCB9


  call Update(additional_input, K, V)
---------------------------
```

Update

  provided_data
                          606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

  V || 0x00 || provided_data is
                        0C9ED74F 56BC8FB4 8145FB36 90FDA956
      1AD6038A 5B1E0BA2 AC09FCC5 D35E5898 3570F37C CE516D76
      407A2342 F802CCB9 00606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

  K = HMAC(K, V || 0x00 || provided_data) is
      B28EF895 0D1F0F9E 7528FE77 60ADBCFD 3EE1100C 1DE8173B
      D09B070B 44526378 83FC310B 32FA6C16 700AA4FE 61A0A397

  V = HMAC(K, V) is
      0A4B15DE 6B992614 D3502202 23171C33 DD4553F1 C068F00D
      59D3FCB8 73635241 79C956AA 281FFD6B 350C8ECB 35EB71A4

  V || 0x01 || provided_data is
                        0A4B15DE 6B992614 D3502202 23171C33
      DD4553F1 C068F00D 59D3FCB8 73635241 79C956AA 281FFD6B
      350C8ECB 35EB71A4 01606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

  K = HMAC(K, V || 0x01 || provided_data) is

```
        1D99B92D E9846C92 22D0EE91 E7423C62 C165B662 B6B29D59
        8D0AAA82 D354FC3F C3AC2D65 E92D43A5 012A494D D8995AEB


    V = HMAC(K, V) is
        A86E8815 2A533A42 829B9F7E 2589A79B B4FBACF9 51349F14
        FF9D2538 0669EB08 683F1B0F BE45F5FF D3DB2A6D 5412522B


rnd_val is
        3918F6DF 5E50B922 CDD7D0FB 87967822 33141EEE 8A14AB69
        B2B3970A F1D30D9F 344225A1 5384869B 208ADB4B 5674C6DA
        0C9ED74F 56BC8FB4 8145FB36 90FDA956 1AD6038A 5B1E0BA2
        AC09FCC5 D35E5898 3570F37C CE516D76 407A2342 F802CCB9


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
  ------------

  V || 0x00 || provided_data is
                        A86E8815 2A533A42 829B9F7E 2589A79B
      B4FBACF9 51349F14 FF9D2538 0669EB08 683F1B0F BE45F5FF
      D3DB2A6D 5412522B 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  K = HMAC(K, V || 0x00 || provided_data) is
      D8618675 35A0AC79 ECA3C968 6BDE77B8 BF7D52A0 EE50D8D3
      B089D770 8B60F0C3 72234ACA 2B791B75 5B31E7AC E515336B


  V = HMAC(K, V) is
      3072E24D 08F157E1 F0446641 BDCEAB60 1BBE5209 059DE17E
      98927025 BBCF3B82 BB82B0BF 7440DBC6 7C891877 9D86858D


  ------------

  V || 0x01 || provided_data is
                        3072E24D 08F157E1 F0446641 BDCEAB60
      1BBE5209 059DE17E 98927025 BBCF3B82 BB82B0BF 7440DBC6
      7C891877 9D86858D 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  K = HMAC(K, V || 0x01 || provided_data) is
      E070149D 96AD5AE2 CAED9BC9 3A875FD8 B6291122 58E92889
      CDC186B7 A843F3F6 848C8502 CC688B04 3556C54D 3CD5A28A


  V = HMAC(K, V) is
      9FA62895 A425AD21 F19FFC95 6341DEAB 7B940EBE E5A2E475
      0BC6EBAD E3F1793A 41422A7E 078B98D8 C740D638 E0C6526A


------------
```

```
    V = HMAC(K, V) is
        BFFE3657 BE463125 BC247C54 B3A5B608 A7198008 78F5058A
        34ECAC69 2837F275 F0449FB1 5B04C2F1 2F12A189 87FF1E5B


    temp is
        BFFE3657 BE463125 BC247C54 B3A5B608 A7198008 78F5058A
        34ECAC69 2837F275 F0449FB1 5B04C2F1 2F12A189 87FF1E5B


  ------------

    V = HMAC(K, V) is
        10370288 FF0074CA 6D99DD0B 5912AE3A B2875B18 201626E6
        1D2E3A0C FF95F45E 49B02FB8 CFBDE860 0B222872 82E01DF3


    temp is
        BFFE3657 BE463125 BC247C54 B3A5B608 A7198008 78F5058A
        34ECAC69 2837F275 F0449FB1 5B04C2F1 2F12A189 87FF1E5B
        10370288 FF0074CA 6D99DD0B 5912AE3A B2875B18 201626E6
        1D2E3A0C FF95F45E 49B02FB8 CFBDE860 0B222872 82E01DF3


---------------------------

  returned_bits is
        BFFE3657 BE463125 BC247C54 B3A5B608 A7198008 78F5058A
        34ECAC69 2837F275 F0449FB1 5B04C2F1 2F12A189 87FF1E5B
        10370288 FF0074CA 6D99DD0B 5912AE3A B2875B18 201626E6
        1D2E3A0C FF95F45E 49B02FB8 CFBDE860 0B222872 82E01DF3


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
    ------------

    V || 0x00 || provided_data is
                          10370288 FF0074CA 6D99DD0B 5912AE3A
        B2875B18 201626E6 1D2E3A0C FF95F45E 49B02FB8 CFBDE860
        0B222872 82E01DF3 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x00 || provided_data) is
        0E744D90 FE08D1BD 53AC0DEE E23659C5 A07BCC3E FE9FA961
        63352A8C 17ED67D3 90FE4950 C7DA111B 2555A82A D3BFCE5D


    V = HMAC(K, V) is
        12677BF7 2691959E 9C09F5F2 AA618376 97E0E4C1 51873C3A
        BAFF4230 FCE4F512 19B29624 9348EFC8 A1130840 4625EA69


    ------------

    V || 0x01 || provided_data is
                          12677BF7 2691959E 9C09F5F2 AA618376
        97E0E4C1 51873C3A BAFF4230 FCE4F512 19B29624 9348EFC8
        A1130840 4625EA69 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x01 || provided_data) is
        0B77DD3B ED4BFFE4 F6494C1B 7522F2AB 93EE1338 ED89CFC1
        6CF81218 4E133482 A04F7007 BF4A4D85 FA138745 1B6D8BE3


    V = HMAC(K, V) is
        020E9776 277D8B88 4E16E40D 7B7AF404 4952A9B9 5DA33382
        2ADB6417 D726E901 46142F6E B388A3A3 7A669D27 9432DACD


rnd_val is
```

BFFE3657 BE463125 BC247C54 B3A5B608 A7198008 78F5058A
34ECAC69 2837F275 F0449FB1 5B04C2F1 2F12A189 87FF1E5B
10370288 FF0074CA 6D99DD0B 5912AE3A B2875B18 201626E6
1D2E3A0C FF95F45E 49B02FB8 CFBDE860 0B222872 82E01DF3

##

HMAC_DRBG

Requested Security Strength = 192

Requested Hash Algorithm = SHA-384

prediction_resistance_flag = "ENABLED"
EntropyInput =
000102 03040506 0708090A 0B0C0D0E
0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E

EntropyInput1 (for Reseed1) =
808182 83848586 8788898A 8B8C8D8E
8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE

EntropyInput2 (for Reseed2) =
C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E

Nonce =
20212223 24252627 28292A2B

PersonalizationString = <empty>

AdditionalInput = <empty>

```
################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                              000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update
```

provided_data
                                                          000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B

V || 0x00 || provided_data is
                                                        01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 00000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B

K = HMAC(K, V || 0x00 || provided_data) is
    E5675B81 A558502A 38EBFD09 A9753D3E F31388D1 EF8EFC89
    1808526C D64ABF8C 3502D83F 20CE07DB 68F0FA99 22789E4C

V = HMAC(K, V) is
    F70F7FF2 45023323 7528314F A8EBF4D2 50B95649 06F0EF58
    41402759 CD72F743 72924730 1F85C172 1CCB323D 4D8B887F

V || 0x01 || provided_data is
                                                        F70F7FF2
    45023323 7528314F A8EBF4D2 50B95649 06F0EF58 41402759
    CD72F743 72924730 1F85C172 1CCB323D 4D8B887F 01000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B

K = HMAC(K, V || 0x01 || provided_data) is

```
        DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
        4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


    V = HMAC(K, V) is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


  Update (Key, V):

    Key is
        DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
        4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


    V is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE
```

```
    additional_input is  <empty>

  Seed_Material is
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  Key is
        DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
        4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


  V is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


---------------------------

  Update

    provided_data
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    ------------

    V || 0x00 || provided_data is
                           D6F45225 560DF998 B7006216 D4FFAE27
        44D97518 D7585280 09A9DCE6 1D50A2FF B4C53C9E D7B405C5
        6692FDA8 5523EC69 00808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    K = HMAC(K, V || 0x00 || provided_data) is
        4BEF4E9F 3D8105E6 700CBA90 8ABA29CB 42D3F72D 9EEF2FE3
```

```
        DE136559 1A50E527 21318D64 8944859C A97B12C7 672BD3E3


    V = HMAC(K, V) is
        7FFBC5F8 8ABDF011 517370E2 D6081072 C680E523 14F66156
        42F38C60 CF73C071 13F90D9F A85FC132 B24753DC 119FBF74


    ------------

    V || 0x01 || provided_data is
                          7FFBC5F8 8ABDF011 517370E2 D6081072
        C680E523 14F66156 42F38C60 CF73C071 13F90D9F A85FC132
        B24753DC 119FBF74 01808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    K = HMAC(K, V || 0x01 || provided_data) is
        F51761FD 6C4C10BC 6843A51A FE40EFE9 2AC78D7C 2CE62FFA
        562E530C 40F165CB 58EA3DF8 447FB5CA 75A4A0C9 7004431E


    V = HMAC(K, V) is
        5279E3F8 A1887F7C 0CE2A9FC 1CCE90B1 E3B8021A 8FFACEE2
        66F1D4CB F8589D67 05D0FE7B 6B7EAFC6 70B73EC3 60A5BD35


  Update (Key, V):

    Key is
        F51761FD 6C4C10BC 6843A51A FE40EFE9 2AC78D7C 2CE62FFA
        562E530C 40F165CB 58EA3DF8 447FB5CA 75A4A0C9 7004431E


    V is
        5279E3F8 A1887F7C 0CE2A9FC 1CCE90B1 E3B8021A 8FFACEE2
        66F1D4CB F8589D67 05D0FE7B 6B7EAFC6 70B73EC3 60A5BD35


**************************************************************

HMAC_DRBG_Generate
```

```
  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        0DC4AC80 D862FBB4 83980077 5BF1E7D3 7AE1E195 A9A30C44
        3A4229B2 8D277E2A BE8E7E41 AC5A870E F3824657 4203FD0D


    temp is
        0DC4AC80 D862FBB4 83980077 5BF1E7D3 7AE1E195 A9A30C44
        3A4229B2 8D277E2A BE8E7E41 AC5A870E F3824657 4203FD0D


  ------------

    V = HMAC(K, V) is
        0C68069F 3DE0F533 57F8B80A FE695876 C731D774 E80CCDA5
        8927FE45 F6168BE8 BC56F876 8ED2065D 0C5829D7 8694EDCF


    temp is
        0DC4AC80 D862FBB4 83980077 5BF1E7D3 7AE1E195 A9A30C44
        3A4229B2 8D277E2A BE8E7E41 AC5A870E F3824657 4203FD0D
        0C68069F 3DE0F533 57F8B80A FE695876 C731D774 E80CCDA5
        8927FE45 F6168BE8 BC56F876 8ED2065D 0C5829D7 8694EDCF


---------------------------

  returned_bits is
        0DC4AC80 D862FBB4 83980077 5BF1E7D3 7AE1E195 A9A30C44
        3A4229B2 8D277E2A BE8E7E41 AC5A870E F3824657 4203FD0D
        0C68069F 3DE0F533 57F8B80A FE695876 C731D774 E80CCDA5
        8927FE45 F6168BE8 BC56F876 8ED2065D 0C5829D7 8694EDCF


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>
```

```
    ------------

    V || 0x00 || provided_data is
                                                              0C
        68069F3D E0F53357 F8B80AFE 695876C7 31D774E8 0CCDA589
        27FE45F6 168BE8BC 56F8768E D2065D0C 5829D786 94EDCF00


    K = HMAC(K, V || 0x00 || provided_data) is
        24CBF22F 1D9D609B 057D661F FA38E1FE 4C3A248F 6703EF33
        7AC3342E 16764CC0 9FA53F01 F7A89CED 3543C990 0A4A84AB


    V = HMAC(K, V) is
        CC054BC6 66BF8793 429D4B82 E23059CC BAD4ABB4 F9368AF2
        0D54F4C5 63C1BE92 5DADF8E3 B039D3C8 A1FE432A DC573A31


rnd_val is
        0DC4AC80 D862FBB4 83980077 5BF1E7D3 7AE1E195 A9A30C44
        3A4229B2 8D277E2A BE8E7E41 AC5A870E F3824657 4203FD0D
        0C68069F 3DE0F533 57F8B80A FE695876 C731D774 E80CCDA5
        8927FE45 F6168BE8 BC56F876 8ED2065D 0C5829D7 8694EDCF


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                             C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
```

```
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    additional_input is  <empty>

  Seed_Material is
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  Key is
        24CBF22F 1D9D609B 057D661F FA38E1FE 4C3A248F 6703EF33
        7AC3342E 16764CC0 9FA53F01 F7A89CED 3543C990 0A4A84AB


  V is
        CC054BC6 66BF8793 429D4B82 E23059CC BAD4ABB4 F9368AF2
        0D54F4C5 63C1BE92 5DADF8E3 B039D3C8 A1FE432A DC573A31


---------------------------

  Update

    provided_data
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    ------------

    V || 0x00 || provided_data is
                          CC054BC6 66BF8793 429D4B82 E23059CC
        BAD4ABB4 F9368AF2 0D54F4C5 63C1BE92 5DADF8E3 B039D3C8
        A1FE432A DC573A31 00C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E
```

```
  K = HMAC(K, V || 0x00 || provided_data) is
      53C01F08 5511CBB7 900AC343 096A1F10 988EA942 C044BBA8
      6847CEFF 981966B6 6E254A9B 8219CDDF E4FE3B41 226FD5CF


  V = HMAC(K, V) is
      A7006AEE 57CEEEF0 B6D4D886 C9B31281 18544E30 397D36E5
      CC9971B2 66C425AF D106A34E 220282EA 831153CE 6654A4F2


  ------------

  V || 0x01 || provided_data is
                        A7006AEE 57CEEEF0 B6D4D886 C9B31281
      18544E30 397D36E5 CC9971B2 66C425AF D106A34E 220282EA
      831153CE 6654A4F2 01C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
      CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
      E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
      FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
      1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  K = HMAC(K, V || 0x01 || provided_data) is
      B05A00CE 2CFD708F 3ACB9092 0F152F8A D9CE740A 76C8A56E
      2C8220C0 B1C02396 4A0CA788 B4CFE25A 70938AA8 D5FF6525


  V = HMAC(K, V) is
      C9B3C782 6FFA7EFD E6E30723 E87F5A4C EC563A14 91789FE1
      1A7083A2 711E5366 866502D2 A74C64D0 71CCEFC0 5CEB3CBA


Update (Key, V):

  Key is
      B05A00CE 2CFD708F 3ACB9092 0F152F8A D9CE740A 76C8A56E
      2C8220C0 B1C02396 4A0CA788 B4CFE25A 70938AA8 D5FF6525


  V is
      C9B3C782 6FFA7EFD E6E30723 E87F5A4C EC563A14 91789FE1
      1A7083A2 711E5366 866502D2 A74C64D0 71CCEFC0 5CEB3CBA
```

```
***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        018413E2 105E8803 FA13F8E8 65D538B4 747B3297 2577F180
        70A3F1B6 49986781 027DC908 210BAD0F 0E1DA470 A0450EFD


    temp is
        018413E2 105E8803 FA13F8E8 65D538B4 747B3297 2577F180
        70A3F1B6 49986781 027DC908 210BAD0F 0E1DA470 A0450EFD


  ------------

    V = HMAC(K, V) is
        0EC93DC0 06D24E95 BC6BA656 7AB36074 A29F2C93 B836FAF9
        62F80560 E44D759F F920BCFA 83EF4595 16F7196D 0885C522


    temp is
        018413E2 105E8803 FA13F8E8 65D538B4 747B3297 2577F180
        70A3F1B6 49986781 027DC908 210BAD0F 0E1DA470 A0450EFD
        0EC93DC0 06D24E95 BC6BA656 7AB36074 A29F2C93 B836FAF9
        62F80560 E44D759F F920BCFA 83EF4595 16F7196D 0885C522


---------------------------

  returned_bits is
        018413E2 105E8803 FA13F8E8 65D538B4 747B3297 2577F180
        70A3F1B6 49986781 027DC908 210BAD0F 0E1DA470 A0450EFD
        0EC93DC0 06D24E95 BC6BA656 7AB36074 A29F2C93 B836FAF9
        62F80560 E44D759F F920BCFA 83EF4595 16F7196D 0885C522


  call Update(additional_input, K, V)
---------------------------
```

```
  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                                  0E
        C93DC006 D24E95BC 6BA6567A B36074A2 9F2C93B8 36FAF962
        F80560E4 4D759FF9 20BCFA83 EF459516 F7196D08 85C52200


    K = HMAC(K, V || 0x00 || provided_data) is
        9AA45364 6096D875 09CE753A CBA6D6B9 00C28240 41340F09
        92F198E8 96F4A311 3AFE97D7 BF59F066 9BBF7C98 80D24887


    V = HMAC(K, V) is
        735DA3B1 0D10469D 49B2D2DE B56CB890 275222E1 59BD3570
        DEE47333 7721C8AA BFC94350 775D25FB 5DFB3581 A048241F


rnd_val is
        018413E2 105E8803 FA13F8E8 65D538B4 747B3297 2577F180
        70A3F1B6 49986781 027DC908 210BAD0F 0E1DA470 A0450EFD
        0EC93DC0 06D24E95 BC6BA656 7AB36074 A29F2C93 B836FAF9
        62F80560 E44D759F F920BCFA 83EF4595 16F7196D 0885C522


################################################################

HMAC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E
```

```
    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                  20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput1 =
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


##################################################################

******************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
```

```
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


--------------------------

  Update

    provided_data
                                                          000102
        03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
        1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
        33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
        4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
        63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B
```

```
------------

V || 0x00 || provided_data is
                                                    01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 00000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


K = HMAC(K, V || 0x00 || provided_data) is
    E5675B81 A558502A 38EBFD09 A9753D3E F31388D1 EF8EFC89
    1808526C D64ABF8C 3502D83F 20CE07DB 68F0FA99 22789E4C


V = HMAC(K, V) is
    F70F7FF2 45023323 7528314F A8EBF4D2 50B95649 06F0EF58
    41402759 CD72F743 72924730 1F85C172 1CCB323D 4D8B887F


------------

V || 0x01 || provided_data is
                                                    F70F7FF2
    45023323 7528314F A8EBF4D2 50B95649 06F0EF58 41402759
    CD72F743 72924730 1F85C172 1CCB323D 4D8B887F 01000102
    03040506 0708090A 0B0C0D0E 0F101112 13141516 1718191A
    1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E 2F303132
    33343536 3738393A 3B3C3D3E 3F404142 43444546 4748494A
    4B4C4D4E 4F505152 53545556 5758595A 5B5C5D5E 5F606162
    63646566 6768696A 6B6C6D6E 20212223 24252627 28292A2B


K = HMAC(K, V || 0x01 || provided_data) is
    DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
    4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


V = HMAC(K, V) is
    D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
    09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69
```

```
  Update (Key, V):

    Key is
        DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
        4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


    V is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    additional_input is
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
```

```
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  Seed_Material is
                                                 8081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  Key is
        DE2451BA AF677086 D7C6FBDB 53638AC0 0FE1E7E9 B1CF6A30
        4ABC2005 D1A8A726 77A4E48A B5B3D2D1 35BA251A 764C77C7


  V is
        D6F45225 560DF998 B7006216 D4FFAE27 44D97518 D7585280
        09A9DCE6 1D50A2FF B4C53C9E D7B405C5 6692FDA8 5523EC69


---------------------------

  Update

    provided_data
                                                 8081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    ------------
```

```
V || 0x00 || provided_data is
                                                  D6F452 25560DF9
    98B70062 16D4FFAE 2744D975 18D75852 8009A9DC E61D50A2
    FFB4C53C 9ED7B405 C56692FD A85523EC 69008081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
    9FADF2CA B5F52BCD 4ED1DDC8 3A7A3333 F94771A6 C45949C2
    4F4D09DD 0156984F 7AE3882D 6B938BCD 30A657B3 74B8FB9F


V = HMAC(K, V) is
    0B4AEB0C 12A47693 2ED81E9F B8981807 CF0B35B7 94F53FAA
    1CEB37A0 DA9EB792 87C3BA50 F9F23E28 8A5B4F20 F3ED87A3


------------

V || 0x01 || provided_data is
                                                  0B4AEB 0C12A476
    932ED81E 9FB89818 07CF0B35 B794F53F AA1CEB37 A0DA9EB7
    9287C3BA 50F9F23E 288A5B4F 20F3ED87 A3018081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x01 || provided_data) is
    17C9901C CA056D1D 21D8D70B 9893574B 451CFF6F 385AB5CC
    7B931108 1F0A9F3A 2D4BF499 CC551F63 7D693B66 9433E536
```

```
    V = HMAC(K, V) is
        6B29D52D E3BB63A9 8642E78B 2BE7703D 2A35750F FB9EAA1C
        3D3EFBF1 BB6C0AB1 8564DB62 D3B60133 397B0EDB B2C06D53


  Update (Key, V):

    Key is
        17C9901C CA056D1D 21D8D70B 9893574B 451CFF6F 385AB5CC
        7B931108 1F0A9F3A 2D4BF499 CC551F63 7D693B66 9433E536


    V is
        6B29D52D E3BB63A9 8642E78B 2BE7703D 2A35750F FB9EAA1C
        3D3EFBF1 BB6C0AB1 8564DB62 D3B60133 397B0EDB B2C06D53


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        61AA7FC4 4CD9D28E 5A19092C 5ADBA05D F7A4EADC FBBB920F
        2A2EF8DC 1692F203 EC3EAC8D 38FD917D 13CA80AC A874003E


    temp is
        61AA7FC4 4CD9D28E 5A19092C 5ADBA05D F7A4EADC FBBB920F
        2A2EF8DC 1692F203 EC3EAC8D 38FD917D 13CA80AC A874003E


  ------------

    V = HMAC(K, V) is
        CD556DD9 954C5802 4AA6B155 1049E612 D548C6EA CACC5C26
        0CACCD88 47CFE880 8B5B57D2 F3405ECD 1DD84756 585E8FBE
```

```
    temp is
        61AA7FC4 4CD9D28E 5A19092C 5ADBA05D F7A4EADC FBBB920F
        2A2EF8DC 1692F203 EC3EAC8D 38FD917D 13CA80AC A874003E
        CD556DD9 954C5802 4AA6B155 1049E612 D548C6EA CACC5C26
        0CACCD88 47CFE880 8B5B57D2 F3405ECD 1DD84756 585E8FBE


---------------------------

  returned_bits is
        61AA7FC4 4CD9D28E 5A19092C 5ADBA05D F7A4EADC FBBB920F
        2A2EF8DC 1692F203 EC3EAC8D 38FD917D 13CA80AC A874003E
        CD556DD9 954C5802 4AA6B155 1049E612 D548C6EA CACC5C26
        0CACCD88 47CFE880 8B5B57D2 F3405ECD 1DD84756 585E8FBE


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                            CD
        556DD995 4C58024A A6B15510 49E612D5 48C6EACA CC5C260C
        ACCD8847 CFE8808B 5B57D2F3 405ECD1D D8475658 5E8FBE00


    K = HMAC(K, V || 0x00 || provided_data) is
        5B78D72D D7D4EFB3 F45AC31B 89802B49 0FF3CFB4 D324A419
        EC6D0385 DF1E750C 08D0B874 B3A3814E 521B229B B6C67497


    V = HMAC(K, V) is
        758EFB2B 4B1FCD20 CBA02F0A E71F3A3E EDD9B1D1 CC7CA8AE
        5838BD43 DB6C42AE DE8CE9BD 4B3827F1 1B1806BA A22275E9


rnd_val is
        61AA7FC4 4CD9D28E 5A19092C 5ADBA05D F7A4EADC FBBB920F
        2A2EF8DC 1692F203 EC3EAC8D 38FD917D 13CA80AC A874003E
        CD556DD9 954C5802 4AA6B155 1049E612 D548C6EA CACC5C26
        0CACCD88 47CFE880 8B5B57D2 F3405ECD 1DD84756 585E8FBE
```

```
---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    additional_input is
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  Seed_Material is
                                                C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
```

```
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  Key is
        5B78D72D D7D4EFB3 F45AC31B 89802B49 0FF3CFB4 D324A419
        EC6D0385 DF1E750C 08D0B874 B3A3814E 521B229B B6C67497


  V is
        758EFB2B 4B1FCD20 CBA02F0A E71F3A3E EDD9B1D1 CC7CA8AE
        5838BD43 DB6C42AE DE8CE9BD 4B3827F1 1B1806BA A22275E9


---------------------------

  Update

    provided_data
                                                C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    ------------

    V || 0x00 || provided_data is
                                              758EFB 2B4B1FCD
        20CBA02F 0AE71F3A 3EEDD9B1 D1CC7CA8 AE5838BD 43DB6C42
        AEDE8CE9 BD4B3827 F11B1806 BAA22275 E900C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  K = HMAC(K, V || 0x00 || provided_data) is
      0AF353E9 02F91380 C592800E A2C074F0 C27BDC69 519AA7B5
      1114AE83 51925AD7 7AC74BBE 516FD004 D590A0D6 66FFC44F


  V = HMAC(K, V) is
      3A34E67C 3AF1808B 134C4EBA 578CFC96 B21F4942 7EA7474A
      9E42E096 E981B82B 8C86E9E6 0FC184F1 8FD68D74 2561E441


  ------------

  V || 0x01 || provided_data is
                                                3A34E6 7C3AF180
      8B134C4E BA578CFC 96B21F49 427EA747 4A9E42E0 96E981B8
      2B8C86E9 E60FC184 F18FD68D 742561E4 4101C0C1 C2C3C4C5
      C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
      DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
      F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
      0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
      26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  K = HMAC(K, V || 0x01 || provided_data) is
      DDE62D1D 19862D57 3E96719E 2E783954 C8D7CC72 DA242C94
      E1FC41C2 FCA96B44 29F41F62 5B19769B 7454FC6E C0133D85


  V = HMAC(K, V) is
      7F4C4B95 7AF571A9 C7178615 C105D370 10F02FFB BF35A3B3
      E553BC9A 22A790CF B55AD5B6 B6A9F995 89CB230F 70C43A5D


Update (Key, V):

  Key is
```

DDE62D1D 19862D57 3E96719E 2E783954 C8D7CC72 DA242C94
E1FC41C2 FCA96B44 29F41F62 5B19769B 7454FC6E C0133D85

V is
7F4C4B95 7AF571A9 C7178615 C105D370 10F02FFB BF35A3B3
E553BC9A 22A790CF B55AD5B6 B6A9F995 89CB230F 70C43A5D

****

HMAC_DRBG_Generate

requested_number_of_bits = 768

additional_input is <empty>

V = HMAC(K, V) is
8659E679 E61EF663 2374C514 07F7DDA2 7DC0CE8D 8A444EB8
CA912CE1 3BB20D88 9E880E65 71913D67 2498DE90 2B71CEDA

temp is
8659E679 E61EF663 2374C514 07F7DDA2 7DC0CE8D 8A444EB8
CA912CE1 3BB20D88 9E880E65 71913D67 2498DE90 2B71CEDA

V = HMAC(K, V) is
5D644344 C63CD4D9 43CB6872 30867D60 F4712AEC 962EB77C
CDB141F6 678C622A 65A0B2B3 E3DBD812 891EA5FC F09D2F19

temp is
8659E679 E61EF663 2374C514 07F7DDA2 7DC0CE8D 8A444EB8
CA912CE1 3BB20D88 9E880E65 71913D67 2498DE90 2B71CEDA
5D644344 C63CD4D9 43CB6872 30867D60 F4712AEC 962EB77C
CDB141F6 678C622A 65A0B2B3 E3DBD812 891EA5FC F09D2F19

---

returned_bits is

```
        8659E679 E61EF663 2374C514 07F7DDA2 7DC0CE8D 8A444EB8
        CA912CE1 3BB20D88 9E880E65 71913D67 2498DE90 2B71CEDA
        5D644344 C63CD4D9 43CB6872 30867D60 F4712AEC 962EB77C
        CDB141F6 678C622A 65A0B2B3 E3DBD812 891EA5FC F09D2F19


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                            5D
        644344C6 3CD4D943 CB687230 867D60F4 712AEC96 2EB77CCD
        B141F667 8C622A65 A0B2B3E3 DBD81289 1EA5FCF0 9D2F1900


    K = HMAC(K, V || 0x00 || provided_data) is
        8650C034 55987FF7 37FDB25C B0B5587A 88BE8DFB 57B3C993
        396F7E3F 194FCC9F 6E609234 15784F56 E77D9046 6225D4B2


    V = HMAC(K, V) is
        B3D93B3A 3FAFCB35 81C2E98F 1B06B4DE 9C31142F 0F047C08
        EEE7F281 A9A6129F 0EB9F380 A9E3DF62 E2DD2CCB 735DC4E2


rnd_val is
        8659E679 E61EF663 2374C514 07F7DDA2 7DC0CE8D 8A444EB8
        CA912CE1 3BB20D88 9E880E65 71913D67 2498DE90 2B71CEDA
        5D644344 C63CD4D9 43CB6872 30867D60 F4712AEC 962EB77C
        CDB141F6 678C622A 65A0B2B3 E3DBD812 891EA5FC F09D2F19


##############################################################

HMAC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384
```

```
    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                                  20212223 24252627 28292A2B


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

##################################################################

******************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
```

```
                          000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                  20212223 24252627 28292A2B


    personal_str is
                          404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                     0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------
```

Update

provided_data
0001 02030405 06070809 0A0B0C0D 0E0F1011
12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE

V || 0x00 || provided_data is
010101 01010101 01010101 01010101 01010101
01010101 01010101 01010101 01010101 01010101 01010101
01010101 01000001 02030405 06070809 0A0B0C0D 0E0F1011
12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE

K = HMAC(K, V || 0x00 || provided_data) is
759FC2E2 D33686FF B43AB4F9 27A9E74D 7C30CE89 05C5AEDF
7A84FF76 479BD8B6 D930A267 6D76D9BC B2F420A3 4B76654A

V = HMAC(K, V) is
D873522C B0FC9099 33B67222 16975EA8 B7EA9349 6647EB8B
BC9A0873 5DE801C3 6D01ABE8 52B764E9 9514935A 9567A39D

V || 0x01 || provided_data is
D87352 2CB0FC90 9933B672 2216975E A8B7EA93

```
        496647EB 8BBC9A08 735DE801 C36D01AB E852B764 E9951493
        5A9567A3 9D010001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x01 || provided_data) is
        085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


    V = HMAC(K, V) is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


  Update (Key, V):

    Key is
        085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


    V is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>
```

```
Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    additional_input is  <empty>

  Seed_Material is
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  Key is
        085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


  V is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


---------------------------

  Update

    provided_data
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE
```

```
  ------------

  V || 0x00 || provided_data is
                       8E065B64 B430910B 4950528A F23A9FA2
      866F8DAA 9106B72E 38BA0B93 D033B851 04485F29 D1AD7EB6
      FF1643D6 9129654D 00808182 83848586 8788898A 8B8C8D8E
      8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
      D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  K = HMAC(K, V || 0x00 || provided_data) is
      1C9FA6D8 1D8DFE6C F9BB52AA ABBFD392 0E64EBB5 D4ECA0CB
      43732C17 7E16D25F E60376EC 2B288F9A 83263608 FD02235D


  V = HMAC(K, V) is
      636BA84D AEECE502 2D2D64C9 DE0FA460 01291377 3B0A12D2
      D5E684A4 ED30DEFC 4B52F771 A1FAF136 D27B13D7 C3C89A27


  ------------

  V || 0x01 || provided_data is
                       636BA84D AEECE502 2D2D64C9 DE0FA460
      01291377 3B0A12D2 D5E684A4 ED30DEFC 4B52F771 A1FAF136
      D27B13D7 C3C89A27 01808182 83848586 8788898A 8B8C8D8E
      8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
      A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
      BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
      D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  K = HMAC(K, V || 0x01 || provided_data) is
      4D2276F7 3EA64903 043B719C A9070167 CDCCCC14 4C0112E4
      2C9A74A2 88E692B8 AAFA77E9 7E5BA72B 33F9212F B358347D


  V = HMAC(K, V) is
      A0F9444C 406CB1F5 474077CE B92954A5 01EEBB4F C46C8757
      58367BA6 48D99E24 75994FF3 AA4F9C3E FADD63B7 0B67EE71


Update (Key, V):
```

```
    Key is
        4D2276F7 3EA64903 043B719C A9070167 CDCCCC14 4C0112E4
        2C9A74A2 88E692B8 AAFA77E9 7E5BA72B 33F9212F B358347D


    V is
        A0F9444C 406CB1F5 474077CE B92954A5 01EEBB4F C46C8757
        58367BA6 48D99E24 75994FF3 AA4F9C3E FADD63B7 0B67EE71


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        804A3AD7 20F4FCE8 738D0632 514FEF16 430CB7D6 3A8DF1A5
        F02A3CE3 BD7ED6A6 68B69E63 E2BB93F0 96EE753D 6194A0F1


    temp is
        804A3AD7 20F4FCE8 738D0632 514FEF16 430CB7D6 3A8DF1A5
        F02A3CE3 BD7ED6A6 68B69E63 E2BB93F0 96EE753D 6194A0F1


  ------------

    V = HMAC(K, V) is
        A3271106 36530096 36337D22 167CC440 2D019AC2 16FA574F
        091CF6EA 283568D7 37A77BE3 8E8F0938 2C69E76B 142ABC3A


    temp is
        804A3AD7 20F4FCE8 738D0632 514FEF16 430CB7D6 3A8DF1A5
        F02A3CE3 BD7ED6A6 68B69E63 E2BB93F0 96EE753D 6194A0F1
        A3271106 36530096 36337D22 167CC440 2D019AC2 16FA574F
        091CF6EA 283568D7 37A77BE3 8E8F0938 2C69E76B 142ABC3A


---------------------------
```

```
  returned_bits is
        804A3AD7 20F4FCE8 738D0632 514FEF16 430CB7D6 3A8DF1A5
        F02A3CE3 BD7ED6A6 68B69E63 E2BB93F0 96EE753D 6194A0F1
        A3271106 36530096 36337D22 167CC440 2D019AC2 16FA574F
        091CF6EA 283568D7 37A77BE3 8E8F0938 2C69E76B 142ABC3A


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                              A3
        27110636 53009636 337D2216 7CC4402D 019AC216 FA574F09
        1CF6EA28 3568D737 A77BE38E 8F09382C 69E76B14 2ABC3A00


    K = HMAC(K, V || 0x00 || provided_data) is
        E2C0EF35 375E7405 0B95DC11 BEAA9A8B 336FFC44 478234D7
        0DDCD0CD 58C798E0 FBE0A03D 9D2110F7 024C6D88 E7497BB0


    V = HMAC(K, V) is
        062FD25F 4544B9F9 C1A6AC78 E0909B18 B447332D C1E4D48B
        EDF84413 1D0213C6 70480F0A 5308D2AE 001BA8EB ABFB8E3F


rnd_val is
        804A3AD7 20F4FCE8 738D0632 514FEF16 430CB7D6 3A8DF1A5
        F02A3CE3 BD7ED6A6 68B69E63 E2BB93F0 96EE753D 6194A0F1
        A3271106 36530096 36337D22 167CC440 2D019AC2 16FA574F
        091CF6EA 283568D7 37A77BE3 8E8F0938 2C69E76B 142ABC3A


-------------------------------------------------------------

Second call to Generate

*************************************************************

HMAC_DRBG_Generate
```

```
  requested_number_of_bits = 768

    additional_input is  <empty>

Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    additional_input is  <empty>

  Seed_Material is
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  Key is
        E2C0EF35 375E7405 0B95DC11 BEAA9A8B 336FFC44 478234D7
        0DDCD0CD 58C798E0 FBE0A03D 9D2110F7 024C6D88 E7497BB0


  V is
        062FD25F 4544B9F9 C1A6AC78 E0909B18 B447332D C1E4D48B
        EDF84413 1D0213C6 70480F0A 5308D2AE 001BA8EB ABFB8E3F


---------------------------

  Update

    provided_data
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
```

FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E

V || 0x00 || provided_data is
062FD25F 4544B9F9 C1A6AC78 E0909B18
B447332D C1E4D48B EDF84413 1D0213C6 70480F0A 5308D2AE
001BA8EB ABFB8E3F 00C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E

K = HMAC(K, V || 0x00 || provided_data) is
BAFFB234 45445961 91E1AAA1 6E7B3E61 F9828D06 EA466F4C
2B53A319 5F55C0D7 BAF86AE7 CAAD72F5 66CB9048 E88E8700

V = HMAC(K, V) is
99E49A1C 9CBCFF92 46FBE4D8 2149EF06 75759443 CEF5A876
F856A566 B5ADA088 40B845B8 4A170D65 E4565CD6 224D46F7

V || 0x01 || provided_data is
99E49A1C 9CBCFF92 46FBE4D8 2149EF06
75759443 CEF5A876 F856A566 B5ADA088 40B845B8 4A170D65
E4565CD6 224D46F7 01C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E

K = HMAC(K, V || 0x01 || provided_data) is
938C379D EBC9F6E7 E31F9D37 20BDF8A9 F6DF97D9 1D56E1E4
A42D48CF 5CC0048B E7593F8F 621C3A11 3D6AEA12 3BE358A1

V = HMAC(K, V) is
A1E2B41D 1A621E6E B4444042 B18E0E93 4084F074 6694E764
904155E7 7C3E555D 80C5F9FB 7A550F71 8150E52F 3B0DEB34

```
  Update (Key, V):

    Key is
        938C379D EBC9F6E7 E31F9D37 20BDF8A9 F6DF97D9 1D56E1E4
        A42D48CF 5CC0048B E7593F8F 621C3A11 3D6AEA12 3BE358A1


    V is
        A1E2B41D 1A621E6E B4444042 B18E0E93 4084F074 6694E764
        904155E7 7C3E555D 80C5F9FB 7A550F71 8150E52F 3B0DEB34


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        73B8E55C 75320217 6A17B9B9 754A9FE6 F23B0186 1FCD4059
        6AEAA301 AF1AEF8A F0EAF22F BF34541E FFAB1431 666ACACC


    temp is
        73B8E55C 75320217 6A17B9B9 754A9FE6 F23B0186 1FCD4059
        6AEAA301 AF1AEF8A F0EAF22F BF34541E FFAB1431 666ACACC


  ------------

    V = HMAC(K, V) is
        759338C7 E2867281 9D53CFEF 10A3E19D AFBD5329 5F1980A9
        F491504A 27255067 84B7AC82 6D92C838 A8668171 CAAA86E7


    temp is
        73B8E55C 75320217 6A17B9B9 754A9FE6 F23B0186 1FCD4059
        6AEAA301 AF1AEF8A F0EAF22F BF34541E FFAB1431 666ACACC
        759338C7 E2867281 9D53CFEF 10A3E19D AFBD5329 5F1980A9
        F491504A 27255067 84B7AC82 6D92C838 A8668171 CAAA86E7
```

```
---------------------------

  returned_bits is
        73B8E55C 75320217 6A17B9B9 754A9FE6 F23B0186 1FCD4059
        6AEAA301 AF1AEF8A F0EAF22F BF34541E FFAB1431 666ACACC
        759338C7 E2867281 9D53CFEF 10A3E19D AFBD5329 5F1980A9
        F491504A 27255067 84B7AC82 6D92C838 A8668171 CAAA86E7


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                           75
        9338C7E2 8672819D 53CFEF10 A3E19DAF BD53295F 1980A9F4
        91504A27 25506784 B7AC826D 92C838A8 668171CA AA86E700


    K = HMAC(K, V || 0x00 || provided_data) is
        06F77A08 C07BABD4 ACC6761F 0726141B E48E3DA0 D140EB8A
        7B05E053 168F92A1 C66B625D A046E9D0 31E414E1 21AB0033


    V = HMAC(K, V) is
        FC7C27C8 34FBE90C 6539863F DF9B9478 3A98D67D E8CF1BD5
        4682E95F 80B48AC7 6935E0E2 B6E2876E 24DB08D4 72A65292


rnd_val is
        73B8E55C 75320217 6A17B9B9 754A9FE6 F23B0186 1FCD4059
        6AEAA301 AF1AEF8A F0EAF22F BF34541E FFAB1431 666ACACC
        759338C7 E2867281 9D53CFEF 10A3E19D AFBD5329 5F1980A9
        F491504A 27255067 84B7AC82 6D92C838 A8668171 CAAA86E7


################################################################

HMAC_DRBG
```

```
Requested Security Strength = 192

Requested Hash Algorithm = SHA-384

prediction_resistance_flag = "ENABLED"
EntropyInput =
                        000102 03040506 0708090A 0B0C0D0E
    0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
    2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
    3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
    5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


EntropyInput1 (for Reseed1) =
                        808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


EntropyInput2 (for Reseed2) =
                        C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Nonce =
                               20212223 24252627 28292A2B


PersonalizationString =
                        404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


AdditionalInput1 =
                        606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
```

```
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


##############################################################

**************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                                  20212223 24252627 28292A2B


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                      0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
```

```
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Key is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


----------------------------

  Update

    provided_data
                     0001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    ------------

    V || 0x00 || provided_data is
                   010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01000001 02030405 06070809 0A0B0C0D 0E0F1011
        12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
        2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
        42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
        5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
        23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
```

```
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
      9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  K = HMAC(K, V || 0x00 || provided_data) is
      759FC2E2 D33686FF B43AB4F9 27A9E74D 7C30CE89 05C5AEDF
      7A84FF76 479BD8B6 D930A267 6D76D9BC B2F420A3 4B76654A


  V = HMAC(K, V) is
      D873522C B0FC9099 33B67222 16975EA8 B7EA9349 6647EB8B
      BC9A0873 5DE801C3 6D01ABE8 52B764E9 9514935A 9567A39D


  ------------

  V || 0x01 || provided_data is
                 D87352 2CB0FC90 9933B672 2216975E A8B7EA93
      496647EB 8BBC9A08 735DE801 C36D01AB E852B764 E9951493
      5A9567A3 9D010001 02030405 06070809 0A0B0C0D 0E0F1011
      12131415 16171819 1A1B1C1D 1E1F2021 22232425 26272829
      2A2B2C2D 2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041
      42434445 46474849 4A4B4C4D 4E4F5051 52535455 56575859
      5A5B5C5D 5E5F6061 62636465 66676869 6A6B6C6D 6E202122
      23242526 2728292A 2B404142 43444546 4748494A 4B4C4D4E
      4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
      9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  K = HMAC(K, V || 0x01 || provided_data) is
      085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
      2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


  V = HMAC(K, V) is
      8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
      38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


Update (Key, V):

  Key is
      085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
```

```
        2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448


    V is
        8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
        38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    additional_input is
                           606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

Seed_Material is

```
                                                  8081 82838485
      86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
      9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
      B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
      CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
      E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

Key is

```
      085987EF 2F1BD2B4 01CF188A EF3E3428 9AB194F5 803FB7E5
      2A0072E2 A4B86949 38AD044F BEDCEAAD EB9618C7 D7393448
```

V is

```
      8E065B64 B430910B 4950528A F23A9FA2 866F8DAA 9106B72E
      38BA0B93 D033B851 04485F29 D1AD7EB6 FF1643D6 9129654D
```

Update

provided_data

```
                                                  8081 82838485
      86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
      9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
      B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
      CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
      E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

V || 0x00 || provided_data is

```
                                                8E065B 64B43091
      0B495052 8AF23A9F A2866F8D AA9106B7 2E38BA0B 93D033B8
```

```
    5104485F 29D1AD7E B6FF1643 D6912965 4D008081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
    840E795F 167DF10E 956213C5 2BC483BC B6ECD132 849DF730
    C3E8D9CC 54F19C6B 3B09B80C 5C001A83 67F69B16 016B20DD


V = HMAC(K, V) is
    E02485E8 1B0E2312 7D733900 A6D9A67A C5255B9A B7EC719A
    8AD3B2B1 24806654 30DBC1EA 8BD5CF05 25895C0F 1C24C4B8


------------

V || 0x01 || provided_data is
                                            E02485 E81B0E23
    127D7339 00A6D9A6 7AC5255B 9AB7EC71 9A8AD3B2 B1248066
    5430DBC1 EA8BD5CF 0525895C 0F1C24C4 B8018081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x01 || provided_data) is
    82F6395B 724D720E 5C3A4AD0 FEDD38BF 78642799 23646108
    BC7F9542 E557E84D C5F034FC 6A33D4A7 288B2A28 CD3CB6B6


V = HMAC(K, V) is
    34CA293B AE154FA0 3531B6B0 A17F7D54 2BE4C52C 2AF71CB2
```

```
        9372160E 34403801 FF392CAB DE4B6332 F3C508A3 AB4B404C


  Update (Key, V):

    Key is
        82F6395B 724D720E 5C3A4AD0 FEDD38BF 78642799 23646108
        BC7F9542 E557E84D C5F034FC 6A33D4A7 288B2A28 CD3CB6B6


    V is
        34CA293B AE154FA0 3531B6B0 A17F7D54 2BE4C52C 2AF71CB2
        9372160E 34403801 FF392CAB DE4B6332 F3C508A3 AB4B404C


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        5EDACD29 898A1E8F B0E32CCD 77EF56C6 CBD0D9BD 7027CFF5
        3FEF9050 047682C6 9CE18B27 31CEDEF6 7E9066B9 4EDD2CAF


    temp is
        5EDACD29 898A1E8F B0E32CCD 77EF56C6 CBD0D9BD 7027CFF5
        3FEF9050 047682C6 9CE18B27 31CEDEF6 7E9066B9 4EDD2CAF


  ------------

    V = HMAC(K, V) is
        6683302E 3FB51FF8 6767A6FD B607BFD8 744DA141 E67E8326
        7850F789 7C927DE7 D4A27EEA 9A7A8131 C4C22D76 9CCA49E0


    temp is
        5EDACD29 898A1E8F B0E32CCD 77EF56C6 CBD0D9BD 7027CFF5
        3FEF9050 047682C6 9CE18B27 31CEDEF6 7E9066B9 4EDD2CAF
        6683302E 3FB51FF8 6767A6FD B607BFD8 744DA141 E67E8326
```

```
        7850F789 7C927DE7 D4A27EEA 9A7A8131 C4C22D76 9CCA49E0


---------------------------

  returned_bits is
        5EDACD29 898A1E8F B0E32CCD 77EF56C6 CBD0D9BD 7027CFF5
        3FEF9050 047682C6 9CE18B27 31CEDEF6 7E9066B9 4EDD2CAF
        6683302E 3FB51FF8 6767A6FD B607BFD8 744DA141 E67E8326
        7850F789 7C927DE7 D4A27EEA 9A7A8131 C4C22D76 9CCA49E0


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                           66
        83302E3F B51FF867 67A6FDB6 07BFD874 4DA141E6 7E832678
        50F7897C 927DE7D4 A27EEA9A 7A8131C4 C22D769C CA49E000


    K = HMAC(K, V || 0x00 || provided_data) is
        3893A359 D9196DC2 3573E2B6 CC3677FF 6D8175AF 71E93A4F
        C90DFE43 970E006A D6BCDC8A 7AC450D8 06E9E4A4 65D507F2


    V = HMAC(K, V) is
        A0D9C554 9FF79334 491E459B 6409ED7B A0641663 082F4BEB
        9FBC0B80 43FD87F5 29077B50 15CE5689 40E903A2 3BA509E6


rnd_val is
        5EDACD29 898A1E8F B0E32CCD 77EF56C6 CBD0D9BD 7027CFF5
        3FEF9050 047682C6 9CE18B27 31CEDEF6 7E9066B9 4EDD2CAF
        6683302E 3FB51FF8 6767A6FD B607BFD8 744DA141 E67E8326
        7850F789 7C927DE7 D4A27EEA 9A7A8131 C4C22D76 9CCA49E0


-------------------------------------------------------------
```

```
Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    additional_input is
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  Seed_Material is
                                                 C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
```

```
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  Key is
        3893A359 D9196DC2 3573E2B6 CC3677FF 6D8175AF 71E93A4F
        C90DFE43 970E006A D6BCDC8A 7AC450D8 06E9E4A4 65D507F2


  V is
        A0D9C554 9FF79334 491E459B 6409ED7B A0641663 082F4BEB
        9FBC0B80 43FD87F5 29077B50 15CE5689 40E903A2 3BA509E6


---------------------------

  Update

    provided_data
                                                  C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    ------------

    V || 0x00 || provided_data is
                                                A0D9C5 549FF793
        34491E45 9B6409ED 7BA06416 63082F4B EB9FBC0B 8043FD87
        F529077B 5015CE56 8940E903 A23BA509 E600C0C1 C2C3C4C5
        C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
        DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
        F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
        0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
        26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
  K = HMAC(K, V || 0x00 || provided_data) is
      0C11B5B3 6E11FA9C 5A935C54 770D810A 207C2640 D61EF548
      90EE1E80 84705589 9F95E9D9 DB32E433 8A8F830D 03142E55


  V = HMAC(K, V) is
      94181C3E 1EBB1828 E2570709 FC31E329 134F34F6 1A03FCE3
      A194B127 E37A12DD 53D32F7E E7BB2679 12B3E260 BF77A2AD


  ------------

  V || 0x01 || provided_data is
                                              94181C 3E1EBB18
      28E25707 09FC31E3 29134F34 F61A03FC E3A194B1 27E37A12
      DD53D32F 7EE7BB26 7912B3E2 60BF77A2 AD01C0C1 C2C3C4C5
      C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
      DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
      F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
      0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
      26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  K = HMAC(K, V || 0x01 || provided_data) is
      374602CC 90D287DA 7C4A8F59 50108A83 AD5B6F0D 5A388ADB
      B0DC7AE2 59FA400B D2833624 BFB66E63 7C9BB152 B857CF75


  V = HMAC(K, V) is
      C9501771 CEF5FDA8 DE964F9F 2FF1E606 65736893 D2EF5E5E
      A75DBC11 02911BD8 BCCFAF0C AED2FA24 5FFE038C 0302F4A7


Update (Key, V):

  Key is
      374602CC 90D287DA 7C4A8F59 50108A83 AD5B6F0D 5A388ADB
      B0DC7AE2 59FA400B D2833624 BFB66E63 7C9BB152 B857CF75
```

```
    V is
        C9501771 CEF5FDA8 DE964F9F 2FF1E606 65736893 D2EF5E5E
        A75DBC11 02911BD8 BCCFAF0C AED2FA24 5FFE038C 0302F4A7


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 768

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
        EFE5120A 69A85539 27016001 03492DFF 3D7F253E 83765107
        E2301DFA 51DCB14C 2F61DB1B 0030BF70 CCA6FB38 9BD34914


    temp is
        EFE5120A 69A85539 27016001 03492DFF 3D7F253E 83765107
        E2301DFA 51DCB14C 2F61DB1B 0030BF70 CCA6FB38 9BD34914


  ------------

    V = HMAC(K, V) is
        8929CC00 CCC8CA6F B9138FD4 5BB0A9BA 136D0E2B 9CE54D63
        4BC4D139 B238A097 1883C693 B9958354 A2CAFAFE 3654958D


    temp is
        EFE5120A 69A85539 27016001 03492DFF 3D7F253E 83765107
        E2301DFA 51DCB14C 2F61DB1B 0030BF70 CCA6FB38 9BD34914
        8929CC00 CCC8CA6F B9138FD4 5BB0A9BA 136D0E2B 9CE54D63
        4BC4D139 B238A097 1883C693 B9958354 A2CAFAFE 3654958D


---------------------------

  returned_bits is
        EFE5120A 69A85539 27016001 03492DFF 3D7F253E 83765107
        E2301DFA 51DCB14C 2F61DB1B 0030BF70 CCA6FB38 9BD34914
        8929CC00 CCC8CA6F B9138FD4 5BB0A9BA 136D0E2B 9CE54D63
        4BC4D139 B238A097 1883C693 B9958354 A2CAFAFE 3654958D
```

```
  call Update(additional_input, K, V)
--------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                                                                    89
        29CC00CC C8CA6FB9 138FD45B B0A9BA13 6D0E2B9C E54D634B
        C4D139B2 38A09718 83C693B9 958354A2 CAFAFE36 54958D00


    K = HMAC(K, V || 0x00 || provided_data) is
        8B7EDEA8 A8777A75 56CAD70E 21211E04 DEB8819F 6940BFDF
        373A03D2 8CDD8B22 990B6749 798F211B A8369112 AB0817CB


    V = HMAC(K, V) is
        3E747542 B9607748 97B0F107 523DEC6A E21FE528 86E471B1
        B8711BEB 10A653DB F3A00DF5 9F18AF74 7C6BBCC4 20208C6E


rnd_val is
        EFE5120A 69A85539 27016001 03492DFF 3D7F253E 83765107
        E2301DFA 51DCB14C 2F61DB1B 0030BF70 CCA6FB38 9BD34914
        8929CC00 CCC8CA6F B9138FD4 5BB0A9BA 136D0E2B 9CE54D63
        4BC4D139 B238A097 1883C693 B9958354 A2CAFAFE 3654958D
```

```
###############################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                           20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm
```

```
    entropy_input is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


  Key is
                           00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                           01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                                                 000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
    3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


------------

V || 0x00 || provided_data is
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 00000102 03040506
    0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
    1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
    3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


K = HMAC(K, V || 0x00 || provided_data) is
                        45A111E3 AB3725B8 D02D1D8C A0AED099
    D32CF71C 2CA703C8 3708DDC3 AB0BDBEC 23719C1A 4C7273A8
    EB06EC14 B05853A0 793D492D C256DD1C 7DA4D148 BE8516CD


V = HMAC(K, V) is
                        B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F
    37948762 32662A75 B91B6150 E5BB1802 C68698C7 1E5BBCEB
    2C39FB40 CE3EF53D 4F092229 4CA844A1 6E67E2B2 710250CA


------------

V || 0x01 || provided_data is
    B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F 37948762 32662A75
    B91B6150 E5BB1802 C68698C7 1E5BBCEB 2C39FB40 CE3EF53D
    4F092229 4CA844A1 6E67E2B2 710250CA 01000102 03040506
    0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
    1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
    3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


K = HMAC(K, V || 0x01 || provided_data) is
                        A7E118A5 31DEF956 DCFF94BB 3D801F77
    5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
```

```
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V = HMAC(K, V) is
                         110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


  Update (Key, V):

    Key is
                         A7E118A5 31DEF956 DCFF94BB 3D801F77
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V is
                         110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


-------------------------------------------------------------

First call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                         A463395A A79F237A 22E5BD24 462BD303
        E1BE5103 BA37299B ED170E10 713EE9CD A62FABD5 171231E1
        F6D82629 BC521D41 178D002D 92918F39 7824E449 004E9AE1


    temp is
                         A463395A A79F237A 22E5BD24 462BD303
        E1BE5103 BA37299B ED170E10 713EE9CD A62FABD5 171231E1
```

```
        F6D82629 BC521D41 178D002D 92918F39 7824E449 004E9AE1


  ------------

    V = HMAC(K, V) is
                           851F7BFA 11CD616E F519A9E2 A05951D9
        108AB389 59CA7E9E 80B18ADF CC622389 495795CB FB7D39AF
        6C8571DD CE035CA6 890C7A1A F80861F0 629EF1B6 952BA206


    temp is
                                                A463395A A79F237A
        22E5BD24 462BD303 E1BE5103 BA37299B ED170E10 713EE9CD
        A62FABD5 171231E1 F6D82629 BC521D41 178D002D 92918F39
        7824E449 004E9AE1 851F7BFA 11CD616E F519A9E2 A05951D9
        108AB389 59CA7E9E 80B18ADF CC622389 495795CB FB7D39AF
        6C8571DD CE035CA6 890C7A1A F80861F0 629EF1B6 952BA206


----------------------------

  returned_bits is
                                                A463395A A79F237A
        22E5BD24 462BD303 E1BE5103 BA37299B ED170E10 713EE9CD
        A62FABD5 171231E1 F6D82629 BC521D41 178D002D 92918F39
        7824E449 004E9AE1 851F7BFA 11CD616E F519A9E2 A05951D9
        108AB389 59CA7E9E 80B18ADF CC622389 495795CB FB7D39AF
        6C8571DD CE035CA6 890C7A1A F80861F0 629EF1B6 952BA206


  call Update(additional_input, K, V)
----------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                         85 1F7BFA11 CD616EF5 19A9E2A0 5951D910
        8AB38959 CA7E9E80 B18ADFCC 62238949 5795CBFB 7D39AF6C
        8571DDCE 035CA689 0C7A1AF8 0861F062 9EF1B695 2BA20600
```

```
    K = HMAC(K, V || 0x00 || provided_data) is
                          8B4FD7FC B0ECB6E6 28F90F71 57A26D11
        58B7269B 5FA2C7F5 54C49FFE 1E24F566 9F69B0F8 6D83FBE8
        DCA24E24 E6F652E2 EEE97482 8DC99CD1 05D12D5D 6D539188


    V = HMAC(K, V) is
                          27383F81 81766C53 A67EBA6D 822DF9F3
        6EF30976 0F1CAA2D 1D41F5B4 EA54D4C3 B9FFCC0C F8303EFA
        6803D7E9 F722F8D1 500E0E83 5AB8CC8F 7B3F3B99 C9472DB2


rnd_val is
                                              A463395A A79F237A
        22E5BD24 462BD303 E1BE5103 BA37299B ED170E10 713EE9CD
        A62FABD5 171231E1 F6D82629 BC521D41 178D002D 92918F39
        7824E449 004E9AE1 851F7BFA 11CD616E F519A9E2 A05951D9
        108AB389 59CA7E9E 80B18ADF CC622389 495795CB FB7D39AF
        6C8571DD CE035CA6 890C7A1A F80861F0 629EF1B6 952BA206


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                          FB5BD98D 2CB25EC4 955CD152 04D68C49
        7281CA0C E2201DAC A5E412DD FDEBAF98 D724D216 62E45ABA
        9AE200D9 41C4CF76 039808F2 9A800034 6A6CC97D 44417737


    temp is
                          FB5BD98D 2CB25EC4 955CD152 04D68C49
        7281CA0C E2201DAC A5E412DD FDEBAF98 D724D216 62E45ABA
        9AE200D9 41C4CF76 039808F2 9A800034 6A6CC97D 44417737
```

```
  ------------

    V = HMAC(K, V) is
                           A89F9047 2AC6088B 45C666C5 61686F19
        1745228F 11ED556A 519DA9AA 1646D15B 901382D8 7726D17D
        C5139FDE E1E8BDB0 F328D4B1 05865BD1 D815641E 6B1DBA23


    temp is
                                              FB5BD98D 2CB25EC4
        955CD152 04D68C49 7281CA0C E2201DAC A5E412DD FDEBAF98
        D724D216 62E45ABA 9AE200D9 41C4CF76 039808F2 9A800034
        6A6CC97D 44417737 A89F9047 2AC6088B 45C666C5 61686F19
        1745228F 11ED556A 519DA9AA 1646D15B 901382D8 7726D17D
        C5139FDE E1E8BDB0 F328D4B1 05865BD1 D815641E 6B1DBA23


---------------------------

  returned_bits is
                                              FB5BD98D 2CB25EC4
        955CD152 04D68C49 7281CA0C E2201DAC A5E412DD FDEBAF98
        D724D216 62E45ABA 9AE200D9 41C4CF76 039808F2 9A800034
        6A6CC97D 44417737 A89F9047 2AC6088B 45C666C5 61686F19
        1745228F 11ED556A 519DA9AA 1646D15B 901382D8 7726D17D
        C5139FDE E1E8BDB0 F328D4B1 05865BD1 D815641E 6B1DBA23


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                         A8 9F90472A C6088B45 C666C561 686F1917
        45228F11 ED556A51 9DA9AA16 46D15B90 1382D877 26D17DC5
        139FDEE1 E8BDB0F3 28D4B105 865BD1D8 15641E6B 1DBA2300


    K = HMAC(K, V || 0x00 || provided_data) is
                           1A8D4FBF B9FCE595 14C1CDB3 A025DE7E
```

```
        FEAA60ED EF3E73A1 B4518CC6 003A67C3 C9E4837E FE0E84B2
        C98C0E87 6D2F6D2A AF583347 01261298 CA98D068 FEF520B8


    V = HMAC(K, V) is
                           8A43F190 1A6ACFFF F8D60A0C 1BC02E47
        48088B30 DFEF309B E595FE60 BCA7DC9D EA918356 4EE4A5B8
        005D6435 39D9976F 270DD2D2 91CCE62A E56788F8 CC1CAEB5


rnd_val is
                                                 FB5BD98D 2CB25EC4
        955CD152 04D68C49 7281CA0C E2201DAC A5E412DD FDEBAF98
        D724D216 62E45ABA 9AE200D9 41C4CF76 039808F2 9A800034
        6A6CC97D 44417737 A89F9047 2AC6088B 45C666C5 61686F19
        1745228F 11ED556A 519DA9AA 1646D15B 901382D8 7726D17D
        C5139FDE E1E8BDB0 F328D4B1 05865BD1 D815641E 6B1DBA23


################################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                             808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                             C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput1 =
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F
```

```
    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


  Key is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                          01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    ------------

    V || 0x00 || provided_data is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 00000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
```

```
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    K = HMAC(K, V || 0x00 || provided_data) is
                          45A111E3 AB3725B8 D02D1D8C A0AED099
        D32CF71C 2CA703C8 3708DDC3 AB0BDBEC 23719C1A 4C7273A8
        EB06EC14 B05853A0 793D492D C256DD1C 7DA4D148 BE8516CD


    V = HMAC(K, V) is
                          B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F
        37948762 32662A75 B91B6150 E5BB1802 C68698C7 1E5BBCEB
        2C39FB40 CE3EF53D 4F092229 4CA844A1 6E67E2B2 710250CA


    ------------

    V || 0x01 || provided_data is
        B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F 37948762 32662A75
        B91B6150 E5BB1802 C68698C7 1E5BBCEB 2C39FB40 CE3EF53D
        4F092229 4CA844A1 6E67E2B2 710250CA 01000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    K = HMAC(K, V || 0x01 || provided_data) is
                          A7E118A5 31DEF956 DCFF94BB 3D801F77
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V = HMAC(K, V) is
                          110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


Update (Key, V):

    Key is
                          A7E118A5 31DEF956 DCFF94BB 3D801F77
```

```
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V is
                          110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  additional_input <> NULL, call Update(additional_input, K, V)
----------------------------

  Update

    provided_data
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    ------------

    V || 0x00 || provided_data is
                                              110793EA A60DC9DB
        CD420810 4088A23D AECC1226 EAF1D03B BA9D83A6 95999165
```

```
    71907346 B15A0439 362B9C8E E330E52D EACC639B 98E8030A
    95780CD7 C24B04D5 00606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
                      613F9906 1E248B2D E05965D5 362A900C
    E20476AE 34433771 BD38AD34 B9307F5A EE280580 6EB35336
    9A5FB4BF 74FF9BB6 C5357745 927ACC89 99D9C257 34F9A35D


V = HMAC(K, V) is
                      0B92DBD0 91064624 8985C9F6 21C23574
    26F1E13F C24FF4CD 554DE629 A77853C8 B65D91B9 56DBC5E7
    4CE12E6A E9197529 043CA90E 0232D6A9 7F26DC5B 32E53822


------------

V || 0x01 || provided_data is
                                          0B92DBD0 91064624
    8985C9F6 21C23574 26F1E13F C24FF4CD 554DE629 A77853C8
    B65D91B9 56DBC5E7 4CE12E6A E9197529 043CA90E 0232D6A9
    7F26DC5B 32E53822 01606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x01 || provided_data) is
                      5284605C F2AFEB0D BAE2129E B7BFFE7C
    14332DB8 F74B92E9 82458FD9 32E18B0C 29F0B522 D9A02E6B
    09054ACF 9E932A02 AADD3EE3 3378E452 E2FAB625 0FB919AC


V = HMAC(K, V) is
                      0AB65B16 AE880563 F94A9459 30747960
    130144BE FA7C6298 D2BCFC44 02E29199 E5899F19 1A74F635
    727D3220 2C3300BD 48EB39F6 F9870C18 B407E507 BE14E15C


------------
```

```
    V = HMAC(K, V) is
                          0469527C F922093E 80F7C35F 96A4AA78
        D57144E0 C55E2B17 AE42BD79 FB2BE771 A19A474E EAE90D73
        E28FEA0C E1EB2ED7 EA727875 11384F8C 8033B56E F4F8545D


    temp is
                          0469527C F922093E 80F7C35F 96A4AA78
        D57144E0 C55E2B17 AE42BD79 FB2BE771 A19A474E EAE90D73
        E28FEA0C E1EB2ED7 EA727875 11384F8C 8033B56E F4F8545D


  ------------

    V = HMAC(K, V) is
                          E7AC23F4 88A8BBBE C676D614 E9572429
        F0378106 0C66A36A 604AEE6E F22E5E1F 78E5BE71 61D51308
        E1C8D6CF EF2DE302 453C4CE9 20175EDA F99664C2 339D9F07


    temp is
                                                   0469527C F922093E
        80F7C35F 96A4AA78 D57144E0 C55E2B17 AE42BD79 FB2BE771
        A19A474E EAE90D73 E28FEA0C E1EB2ED7 EA727875 11384F8C
        8033B56E F4F8545D E7AC23F4 88A8BBBE C676D614 E9572429
        F0378106 0C66A36A 604AEE6E F22E5E1F 78E5BE71 61D51308
        E1C8D6CF EF2DE302 453C4CE9 20175EDA F99664C2 339D9F07


--------------------------

  returned_bits is
                                                   0469527C F922093E
        80F7C35F 96A4AA78 D57144E0 C55E2B17 AE42BD79 FB2BE771
        A19A474E EAE90D73 E28FEA0C E1EB2ED7 EA727875 11384F8C
        8033B56E F4F8545D E7AC23F4 88A8BBBE C676D614 E9572429
        F0378106 0C66A36A 604AEE6E F22E5E1F 78E5BE71 61D51308
        E1C8D6CF EF2DE302 453C4CE9 20175EDA F99664C2 339D9F07


  call Update(additional_input, K, V)
--------------------------

  Update
```

```
provided_data
                        606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


------------

V || 0x00 || provided_data is
                                          E7AC23F4 88A8BBBE
    C676D614 E9572429 F0378106 0C66A36A 604AEE6E F22E5E1F
    78E5BE71 61D51308 E1C8D6CF EF2DE302 453C4CE9 20175EDA
    F99664C2 339D9F07 00606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
                       052FF2F9 9579ABDD 989F7EC2 2A8ACFA6
    5AA83978 810A2F22 41A24CA4 0FF4468A 01775B2A 36D2600E
    817FD4B3 EDFCF755 E3E4BDBC A4109F1C 7F941774 13F91D0F


V = HMAC(K, V) is
                       6EFD8779 2A059B91 9F4E190C 1FE488F6
    5138C747 C2F76CC7 06E2C8F4 181FE8E3 36B464E6 518901A5
    03BC97AB 65E83467 C8C0FE34 EF0BD9DE CBFB4063 B4A30A40


------------

V || 0x01 || provided_data is
                                          6EFD8779 2A059B91
    9F4E190C 1FE488F6 5138C747 C2F76CC7 06E2C8F4 181FE8E3
    36B464E6 518901A5 03BC97AB 65E83467 C8C0FE34 EF0BD9DE
    CBFB4063 B4A30A40 01606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                            8C1D655B 79BB63C8 591A3016 D01F8122
        06557FEC 61DC13A6 1701CD4C 6A4597BF 13B908EB 9BA30A81
        D10DCB71 8364CD6B EC343E27 3F6AD936 B2A2598E 173F61DF


    V = HMAC(K, V) is
                            53BC68C9 F6692CD1 A94C8376 AB7C076C
        5EFE2681 26197A3F 2A3045B1 4E9B1AE3 A3BD944C 254BDCF1
        94A81F9A 70EE34F9 8DCF0D92 B63C4B2C 2DFA523C DC32B6CF


rnd_val is
                                                0469527C F922093E
        80F7C35F 96A4AA78 D57144E0 C55E2B17 AE42BD79 FB2BE771
        A19A474E EAE90D73 E28FEA0C E1EB2ED7 EA727875 11384F8C
        8033B56E F4F8545D E7AC23F4 88A8BBBE C676D614 E9572429
        F0378106 0C66A36A 604AEE6E F22E5E1F 78E5BE71 61D51308
        E1C8D6CF EF2DE302 453C4CE9 20175EDA F99664C2 339D9F07


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is
                              A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  additional_input <> NULL, call Update(additional_input, K, V)
----------------------------

  Update

    provided_data
                              A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


------------

V || 0x00 || provided_data is
                                          53BC68C9 F6692CD1
    A94C8376 AB7C076C 5EFE2681 26197A3F 2A3045B1 4E9B1AE3
    A3BD944C 254BDCF1 94A81F9A 70EE34F9 8DCF0D92 B63C4B2C
    2DFA523C DC32B6CF 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


K = HMAC(K, V || 0x00 || provided_data) is
                      040A763E 76ED2B13 78C2DEF1 AB37EFAF
    0A7E261E DC0D1415 48AE54AA 04139348 65F599E4 FB22CB2E
    13A72696 DBF90774 38CA4C18 40B9F97E C68C766E B05B5951


V = HMAC(K, V) is
                      9F3CCCA2 F3A2C033 AA36E1E2 3DA30378
    0BAABBC3 4E1C3687 FC2EC11A 09F20BD5 319EA959 8EEB0865
    6AB44A9E AD95F5C0 E2B0412A F918773C 07E0EB42 76D44191


------------

V || 0x01 || provided_data is
                                          9F3CCCA2 F3A2C033
    AA36E1E2 3DA30378 0BAABBC3 4E1C3687 FC2EC11A 09F20BD5
    319EA959 8EEB0865 6AB44A9E AD95F5C0 E2B0412A F918773C
    07E0EB42 76D44191 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


K = HMAC(K, V || 0x01 || provided_data) is
                      D4ECAA91 73A92CA6 3E0AFB0B 827518FA
```

```
        3868168A A43E877B A66F64FC A4D1AFCD EF0CCC2E 214A2ED2
        BA11BB2F 7D611FB9 5F4D0D8E 104EE0D6 512B8FEE 0EE593C5


    V = HMAC(K, V) is
                          020FD4F6 C9F76CB6 5CD6E603 1AB79A5A
        A8230594 7D8960FD 7080DD0E B4C7B81B 6BBCB568 1C4BC066
        50E3BCAB 5DF3A7C7 8EB729A3 CB440BF5 0276F507 D3591177


  ------------

    V = HMAC(K, V) is
                          15A45211 78CE9F71 D62DF426 ED92B3DA
        BD884880 A71405D7 D37217EB 0195FEC1 3B82C599 A9D5E22D
        9E577BC8 4FCF85D7 D490798B 1F3033DB 0A86D8BB 4B5C59D4


    temp is
                          15A45211 78CE9F71 D62DF426 ED92B3DA
        BD884880 A71405D7 D37217EB 0195FEC1 3B82C599 A9D5E22D
        9E577BC8 4FCF85D7 D490798B 1F3033DB 0A86D8BB 4B5C59D4


  ------------

    V = HMAC(K, V) is
                          8733D44B 4C9D831E B844329F A0B1C6B9
        56427905 30846F3A B4019E60 D6E7241C 17AA0710 9BBB6A8E
        D1E2B917 F7A7FA86 CCEA498F F18181E6 E1BED9F0 7B2F612F


    temp is
                                               15A45211 78CE9F71
        D62DF426 ED92B3DA BD884880 A71405D7 D37217EB 0195FEC1
        3B82C599 A9D5E22D 9E577BC8 4FCF85D7 D490798B 1F3033DB
        0A86D8BB 4B5C59D4 8733D44B 4C9D831E B844329F A0B1C6B9
        56427905 30846F3A B4019E60 D6E7241C 17AA0710 9BBB6A8E
        D1E2B917 F7A7FA86 CCEA498F F18181E6 E1BED9F0 7B2F612F


---------------------------

  returned_bits is
                                               15A45211 78CE9F71
        D62DF426 ED92B3DA BD884880 A71405D7 D37217EB 0195FEC1
```

```
        3B82C599 A9D5E22D 9E577BC8 4FCF85D7 D490798B 1F3033DB
        0A86D8BB 4B5C59D4 8733D44B 4C9D831E B844329F A0B1C6B9
        56427905 30846F3A B4019E60 D6E7241C 17AA0710 9BBB6A8E
        D1E2B917 F7A7FA86 CCEA498F F18181E6 E1BED9F0 7B2F612F


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    ------------

    V || 0x00 || provided_data is
                                              8733D44B 4C9D831E
        B844329F A0B1C6B9 56427905 30846F3A B4019E60 D6E7241C
        17AA0710 9BBB6A8E D1E2B917 F7A7FA86 CCEA498F F18181E6
        E1BED9F0 7B2F612F 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x00 || provided_data) is
                           95B0CAB3 9F589D71 C81F354A 7BB3AA72
        7FDAA35D DC5CEAF4 63158597 72CDF13C 34361836 23C73D2F
        77F5DFD4 90FDF012 49F825B0 24114FCA 5465E874 8D0B8878


    V = HMAC(K, V) is
                           6F7C0C89 81F9D7F3 03E99987 4D0AC1F2
        F37E8D01 7D119FF6 06F072F8 59EB1E54 BDB3F6F6 9F4A3DAF
        D85328D7 F99ECA8F C4046803 47A33EC7 E9D017B0 735BD55E


    ------------
```

```
    V || 0x01 || provided_data is
                                            6F7C0C89 81F9D7F3
        03E99987 4D0AC1F2 F37E8D01 7D119FF6 06F072F8 59EB1E54
        BDB3F6F6 9F4A3DAF D85328D7 F99ECA8F C4046803 47A33EC7
        E9D017B0 735BD55E 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x01 || provided_data) is
                          3216E702 D2ECD57A E0FC73CE 801F088D
        6274ED97 9F0BA437 4093215F 6B53D0F1 408B0D2D 79C81EAC
        2B194436 0A940B23 457BC989 C5C24EE3 5BD24312 04F5C950


    V = HMAC(K, V) is
                          75E0C067 A35850E0 CAAA84AE 4D61B409
        8D58EFF7 1118F6B2 065DC4AA 89FA3A44 6C49E753 59DC7F5F
        E9CC26E6 CBEBB461 1142DBBA 9DD102EF 67D6E7AF 981F969A


rnd_val is
                                            15A45211 78CE9F71
        D62DF426 ED92B3DA BD884880 A71405D7 D37217EB 0195FEC1
        3B82C599 A9D5E22D 9E577BC8 4FCF85D7 D490798B 1F3033DB
        0A86D8BB 4B5C59D4 8733D44B 4C9D831E B844329F A0B1C6B9
        56427905 30846F3A B4019E60 D6E7241C 17AA0710 9BBB6A8E
        D1E2B917 F7A7FA86 CCEA498F F18181E6 E1BED9F0 7B2F612F


#############################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
```

```
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

##################################################################

******************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E
```

```
    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "No PredictionResistance"

  Seed_Material is
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Key is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                          01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
```

```
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


------------

V || 0x00 || provided_data is
                        010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


K = HMAC(K, V || 0x00 || provided_data) is
                       8FE3241B 7CEC3C91 831FEBC5 664A324E
    CE7885EC 0CFB79F0 A110CDDA 5C25FBDF 2724481F E501C813
    656BAC39 9CE61ABA DA1D0D75 7B2AB666 F4C98216 C1482F59


V = HMAC(K, V) is
                       496DABED 7FE15C71 16E221B4 30EE825C
    72A53FC3 49091FBF 5060584F CF9BAA56 70592E2F BB7E0E5A
    AD170616 E98B6DC8 BC4D77A2 EA17DFDE 4E64B0DF 260D9DCB


------------

V || 0x01 || provided_data is
                         496DAB ED7FE15C 7116E221 B430EE82
    5C72A53F C349091F BF506058 4FCF9BAA 5670592E 2FBB7E0E
```

```
        5AAD1706 16E98B6D C8BC4D77 A2EA17DF DE4E64B0 DF260D9D
        CB010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x01 || provided_data) is
                        96477F38 6DC67E91 FBE26228 31E00384
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


    V = HMAC(K, V) is
                        FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


  Update (Key, V):

    Key is
                        96477F38 6DC67E91 FBE26228 31E00384
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


    V is
                        FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate
```

```
  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                          2A5FF652 0C20F66E D5EA431B D4AEAC58
        F975EEC9 A015137D 5C94B73A A09CB8B5 9D611DDE ECEB34A5
        2BB99942 4009EB9E AC5353F9 2A6699D2 0A02164E EBBC6492


    temp is
                          2A5FF652 0C20F66E D5EA431B D4AEAC58
        F975EEC9 A015137D 5C94B73A A09CB8B5 9D611DDE ECEB34A5
        2BB99942 4009EB9E AC5353F9 2A6699D2 0A02164E EBBC6492


  ------------

    V = HMAC(K, V) is
                          941E1042 63238984 65DFD731 C7E04730
        60A5AA89 73841FDF 3446FB6E 72A58DA8 BDA2A57A 36F3DD98
        6DF85C8A 5C6FF31C DE660BF8 A841B21D D6AA9D3A C356B87B


    temp is
                                             2A5FF652 0C20F66E
        D5EA431B D4AEAC58 F975EEC9 A015137D 5C94B73A A09CB8B5
        9D611DDE ECEB34A5 2BB99942 4009EB9E AC5353F9 2A6699D2
        0A02164E EBBC6492 941E1042 63238984 65DFD731 C7E04730
        60A5AA89 73841FDF 3446FB6E 72A58DA8 BDA2A57A 36F3DD98
        6DF85C8A 5C6FF31C DE660BF8 A841B21D D6AA9D3A C356B87B


---------------------------

  returned_bits is
                                             2A5FF652 0C20F66E
        D5EA431B D4AEAC58 F975EEC9 A015137D 5C94B73A A09CB8B5
        9D611DDE ECEB34A5 2BB99942 4009EB9E AC5353F9 2A6699D2
        0A02164E EBBC6492 941E1042 63238984 65DFD731 C7E04730
        60A5AA89 73841FDF 3446FB6E 72A58DA8 BDA2A57A 36F3DD98
        6DF85C8A 5C6FF31C DE660BF8 A841B21D D6AA9D3A C356B87B
```

```
  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                       94 1E104263 23898465 DFD731C7 E0473060
        A5AA8973 841FDF34 46FB6E72 A58DA8BD A2A57A36 F3DD986D
        F85C8A5C 6FF31CDE 660BF8A8 41B21DD6 AA9D3AC3 56B87B00


    K = HMAC(K, V || 0x00 || provided_data) is
                         C2A6A666 D6EBF5F6 A96D1EDA 13AFA820
        8D388E17 C2DAE33A F5614506 C3686998 FA9728AC 17361C26
        6FB28BB6 54D73642 DA5FD913 3B9BCA86 6920A66F 332ADE84


    V = HMAC(K, V) is
                         F644A36F 1D274552 CCA57438 296DB616
        9C727402 7367C3D2 E3BD1A99 8DD31B10 9401B2A9 E7D5E5DF
        C05F5AA4 677B3D6F 7867E944 81922620 8F607119 ED71709A


rnd_val is
                                             2A5FF652 0C20F66E
        D5EA431B D4AEAC58 F975EEC9 A015137D 5C94B73A A09CB8B5
        9D611DDE ECEB34A5 2BB99942 4009EB9E AC5353F9 2A6699D2
        0A02164E EBBC6492 941E1042 63238984 65DFD731 C7E04730
        60A5AA89 73841FDF 3446FB6E 72A58DA8 BDA2A57A 36F3DD98
        6DF85C8A 5C6FF31C DE660BF8 A841B21D D6AA9D3A C356B87B


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024
```

```
    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                          0EDC8D7D 7CEEC7FE 36333FB3 0C0A9A4B
        27AA0BEC BF075568 B006C1C3 693B1C29 0F84769C 213F98EB
        5880909E DF068FDA 6BFC4350 3987BBBD 4FC23AFB E982FE4B


    temp is
                          0EDC8D7D 7CEEC7FE 36333FB3 0C0A9A4B
        27AA0BEC BF075568 B006C1C3 693B1C29 0F84769C 213F98EB
        5880909E DF068FDA 6BFC4350 3987BBBD 4FC23AFB E982FE4B


  ------------

    V = HMAC(K, V) is
                          4B007910 CC4874EE C2174054 21C8D8A1
        BA87EC68 4D0AF9A6 101D9DB7 87AE82C3 A6A25ED4 78DF1B12
        212CEC32 5466F3AC 7C48A561 66DD0B11 9C8673A1 A9D54F67


    temp is
                                              0EDC8D7D 7CEEC7FE
        36333FB3 0C0A9A4B 27AA0BEC BF075568 B006C1C3 693B1C29
        0F84769C 213F98EB 5880909E DF068FDA 6BFC4350 3987BBBD
        4FC23AFB E982FE4B 4B007910 CC4874EE C2174054 21C8D8A1
        BA87EC68 4D0AF9A6 101D9DB7 87AE82C3 A6A25ED4 78DF1B12
        212CEC32 5466F3AC 7C48A561 66DD0B11 9C8673A1 A9D54F67


---------------------------

  returned_bits is
                                              0EDC8D7D 7CEEC7FE
        36333FB3 0C0A9A4B 27AA0BEC BF075568 B006C1C3 693B1C29
        0F84769C 213F98EB 5880909E DF068FDA 6BFC4350 3987BBBD
        4FC23AFB E982FE4B 4B007910 CC4874EE C2174054 21C8D8A1
        BA87EC68 4D0AF9A6 101D9DB7 87AE82C3 A6A25ED4 78DF1B12
        212CEC32 5466F3AC 7C48A561 66DD0B11 9C8673A1 A9D54F67


  call Update(additional_input, K, V)
```

```
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                      4B 007910CC 4874EEC2 17405421 C8D8A1BA
        87EC684D 0AF9A610 1D9DB787 AE82C3A6 A25ED478 DF1B1221
        2CEC3254 66F3AC7C 48A56166 DD0B119C 8673A1A9 D54F6700


    K = HMAC(K, V || 0x00 || provided_data) is
                           AB5E2153 B7DFBE45 7FCE345B 7DADCA8D
        5BFB3C98 58C36ECD F124C147 23B4CD39 F446E749 440FE69D
        D05E625F DC4625AC 8B7A47C5 465590E6 4662DB37 986C1335


    V = HMAC(K, V) is
                           02D99E7B 03B96288 2D288D60 AF87C466
        82FB7E21 13461E2B 3652EDF4 86DCE759 1BD5BE18 A78CFD69
        5E5B5C51 F72AC509 5DB5D786 C432EE91 FE8B292C 2309E470


rnd_val is
                                                0EDC8D7D 7CEEC7FE
        36333FB3 0C0A9A4B 27AA0BEC BF075568 B006C1C3 693B1C29
        0F84769C 213F98EB 5880909E DF068FDA 6BFC4350 3987BBBD
        4FC23AFB E982FE4B 4B007910 CC4874EE C2174054 21C8D8A1
        BA87EC68 4D0AF9A6 101D9DB7 87AE82C3 A6A25ED4 78DF1B12
        212CEC32 5466F3AC 7C48A561 66DD0B11 9C8673A1 A9D54F67


##############################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                             000102 03040506 0708090A 0B0C0D0E
```

```
    0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
    2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
    3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
    5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


EntropyInput1 (for Reseed1) =
                         808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


EntropyInput2 (for Reseed2) =
                         C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Nonce =
                       20212223 24252627 28292A2B 2C2D2E2F


PersonalizationString =
                         404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


AdditionalInput1 =
                         606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


AdditionalInput2 =
                         A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
```

DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E

##

****

HMAC_DRBG_Instantiate_algorithm

entropy_input is
000102 03040506 0708090A 0B0C0D0E
0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E

nonce is
20212223 24252627 28292A2B 2C2D2E2F

personal_str is
404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE

prediction_resistance_flag = "No PredictionResistance"

Seed_Material is
0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE

Key is

```
                        00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                        01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    ------------

    V || 0x00 || provided_data is
                           010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
  K = HMAC(K, V || 0x00 || provided_data) is
                        8FE3241B 7CEC3C91 831FEBC5 664A324E
      CE7885EC 0CFB79F0 A110CDDA 5C25FBDF 2724481F E501C813
      656BAC39 9CE61ABA DA1D0D75 7B2AB666 F4C98216 C1482F59


  V = HMAC(K, V) is
                        496DABED 7FE15C71 16E221B4 30EE825C
      72A53FC3 49091FBF 5060584F CF9BAA56 70592E2F BB7E0E5A
      AD170616 E98B6DC8 BC4D77A2 EA17DFDE 4E64B0DF 260D9DCB


  ------------

  V || 0x01 || provided_data is
                          496DAB ED7FE15C 7116E221 B430EE82
      5C72A53F C349091F BF506058 4FCF9BAA 5670592E 2FBB7E0E
      5AAD1706 16E98B6D C8BC4D77 A2EA17DF DE4E64B0 DF260D9D
      CB010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
      16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
      2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
      46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
      5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
      2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
      4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
      6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
      7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
      9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  K = HMAC(K, V || 0x01 || provided_data) is
                        96477F38 6DC67E91 FBE26228 31E00384
      E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
      EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


  V = HMAC(K, V) is
                        FAE68E0C ED06928D 3D6EC078 2D3FF3ED
      D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
      8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


Update (Key, V):

  Key is
                        96477F38 6DC67E91 FBE26228 31E00384
```

```
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


    V is
                            FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is
                              606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  additional_input <> NULL, call Update(additional_input, K, V)
----------------------------

  Update

    provided_data
                              606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    ------------

    V || 0x00 || provided_data is
                                              FAE68E0C ED06928D
        3D6EC078 2D3FF3ED D3E6D364 B11EF22B 715D26C4 4850F01D
```

```
    7074E6C8 13109CD4 8BD91FC8 678E972C 205511E4 3622F079
    72ADB6BC 61BE4F7E 00606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
                      519297BD B0EDA5D1 084F8B3B C203347D
    0C930D32 CEE2E49D F4BACBC6 D83AF8D9 EBD72991 B42C248E
    CD4EFAE9 1021F388 381D8659 A2ECBEEE F3E41952 E7A2451A


V = HMAC(K, V) is
                      D7DA4ED0 3A73A57B 54BF8D1D 33A1593D
    69FFDCA4 D66D74D9 89301F48 A8922EC0 E221977F 8F470A9B
    9486B5B6 DC9D7214 59A2A371 444894DE 0C09A8C8 9E599256


------------

V || 0x01 || provided_data is
                                          D7DA4ED0 3A73A57B
    54BF8D1D 33A1593D 69FFDCA4 D66D74D9 89301F48 A8922EC0
    E221977F 8F470A9B 9486B5B6 DC9D7214 59A2A371 444894DE
    0C09A8C8 9E599256 01606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x01 || provided_data) is
                      CEFBD1FE AB9E394C 0BB8AEEA A0432A7F
    6F1B3A0B 3ECB72E9 D08AF37E 1DC7D7B9 7C173D7D B2711ECA
    EA8AFD3F 138E7097 13401FCC D1E813A9 0BFA720E 39A765CB


V = HMAC(K, V) is
                      653FED49 BF632DDF 3EC4182C 3ECB3BE1
    CE9C05A8 231E90F1 7BA624C7 366131F9 876CB3E9 C27C453C
    1DF40471 07BADDD9 81D09078 C2D9C3FC 094A2BDC 0A8405BB


------------
```

```
    V = HMAC(K, V) is
                          7AE31A2D EC31075F E5972660 C16D22EC
        C0D415C5 693001BE 5A468B59 0BC1AE2C 43F647F8 D681AEEA
        0D87B79B 0B4E5D08 9CA2C9D3 27534234 0254E6B0 4690D77A


    temp is
                          7AE31A2D EC31075F E5972660 C16D22EC
        C0D415C5 693001BE 5A468B59 0BC1AE2C 43F647F8 D681AEEA
        0D87B79B 0B4E5D08 9CA2C9D3 27534234 0254E6B0 4690D77A


  ------------

    V = HMAC(K, V) is
                          71A294DA 9568479E EF8BB2A2 110F18B6
        22F60F35 235DE0E8 F9D7E981 05D84AA2 4AF0757A F005DFD5
        2FA51DE3 F44FCE0C 5F3A27FC E8B0F6E4 A3F7C7B5 3CE34A3D


    temp is
                                              7AE31A2D EC31075F
        E5972660 C16D22EC C0D415C5 693001BE 5A468B59 0BC1AE2C
        43F647F8 D681AEEA 0D87B79B 0B4E5D08 9CA2C9D3 27534234
        0254E6B0 4690D77A 71A294DA 9568479E EF8BB2A2 110F18B6
        22F60F35 235DE0E8 F9D7E981 05D84AA2 4AF0757A F005DFD5
        2FA51DE3 F44FCE0C 5F3A27FC E8B0F6E4 A3F7C7B5 3CE34A3D


---------------------------

  returned_bits is
                                              7AE31A2D EC31075F
        E5972660 C16D22EC C0D415C5 693001BE 5A468B59 0BC1AE2C
        43F647F8 D681AEEA 0D87B79B 0B4E5D08 9CA2C9D3 27534234
        0254E6B0 4690D77A 71A294DA 9568479E EF8BB2A2 110F18B6
        22F60F35 235DE0E8 F9D7E981 05D84AA2 4AF0757A F005DFD5
        2FA51DE3 F44FCE0C 5F3A27FC E8B0F6E4 A3F7C7B5 3CE34A3D


  call Update(additional_input, K, V)
---------------------------

  Update
```

```
provided_data
                        606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


------------

V || 0x00 || provided_data is
                                          71A294DA 9568479E
    EF8BB2A2 110F18B6 22F60F35 235DE0E8 F9D7E981 05D84AA2
    4AF0757A F005DFD5 2FA51DE3 F44FCE0C 5F3A27FC E8B0F6E4
    A3F7C7B5 3CE34A3D 00606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
                        40587E1D 5EB9F3D1 A6811767 EFA6A242
    1122DF2D EF5CC623 0A987605 7513A4F0 0ADB49E4 4A98478F
    6ED3A236 232B748E BAD48809 19D8C114 F8B02820 35763FE2


V = HMAC(K, V) is
                        58D27756 7DFE2227 FB9D105E 672EB72B
    CB08C9B5 EBCA5F19 753AE981 FCCFA587 00DC0586 87E29642
    D7E7CC30 10C82510 079EB2F4 DF4795B8 E1FF6499 E05551F1


------------

V || 0x01 || provided_data is
                                          58D27756 7DFE2227
    FB9D105E 672EB72B CB08C9B5 EBCA5F19 753AE981 FCCFA587
    00DC0586 87E29642 D7E7CC30 10C82510 079EB2F4 DF4795B8
    E1FF6499 E05551F1 01606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                          C64282B6 5A169138 8C94D85B 470D6FB3
        9DA80F71 A59D1160 C96B1FFC 0F77EDF9 11553ADC 552FC5B9
        9BDE010F 861FB90E 1EC9CD69 BA6B0C62 490D43FD 9FA6FE19


    V = HMAC(K, V) is
                          F12FA531 40E9A7DE 07D1EA08 3E31AF42
        5836A08F B59D2B1C 463263AD D1D4FCAD 5DA77F94 BE3E1A6A
        ACFC8845 33A2B5F6 685D6F66 F77D333A 43A119D9 56577B47


rnd_val is
                                              7AE31A2D EC31075F
        E5972660 C16D22EC C0D415C5 693001BE 5A468B59 0BC1AE2C
        43F647F8 D681AEEA 0D87B79B 0B4E5D08 9CA2C9D3 27534234
        0254E6B0 4690D77A 71A294DA 9568479E EF8BB2A2 110F18B6
        22F60F35 235DE0E8 F9D7E981 05D84AA2 4AF0757A F005DFD5
        2FA51DE3 F44FCE0C 5F3A27FC E8B0F6E4 A3F7C7B5 3CE34A3D


------------------------------------------------------------

Second call to Generate

************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  additional_input <> NULL, call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


------------

V || 0x00 || provided_data is
                                        F12FA531 40E9A7DE
    07D1EA08 3E31AF42 5836A08F B59D2B1C 463263AD D1D4FCAD
    5DA77F94 BE3E1A6A ACFC8845 33A2B5F6 685D6F66 F77D333A
    43A119D9 56577B47 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


K = HMAC(K, V || 0x00 || provided_data) is
                        66CDD877 BDBC01F0 B8C593E6 DB68698D
    3EA26EC3 D7EACB28 48091406 E371CFFD DE5FD3A7 D0F689AA
    C754C53C 9F5F51B4 A876BA90 25E6812B 15DF9C94 B4513C3C


V = HMAC(K, V) is
                        CB042B0E F4D993CF 753DBDAE E68D7E0E
    1E361D00 0EEE983F E53293AB 859E90E8 B12F7C18 85AD2795
    E8D52968 48C450C2 0942DA83 130898BE 39A9FCAB 49C7D4FE


------------

V || 0x01 || provided_data is
                                        CB042B0E F4D993CF
    753DBDAE E68D7E0E 1E361D00 0EEE983F E53293AB 859E90E8
    B12F7C18 85AD2795 E8D52968 48C450C2 0942DA83 130898BE
    39A9FCAB 49C7D4FE 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


K = HMAC(K, V || 0x01 || provided_data) is
                        EA829A96 FF1A6598 A63F82AC 4683837D
```

```
        46957868 3AF5D469 47146C05 16A1B3BC 7F32B337 EC80B0DF
        D40F7A56 F2520441 A7EBC2F5 F449FA1C 9F80B624 189FE4DF


    V = HMAC(K, V) is
                         4A97F3E7 84A888F2 CF6ACE46 3C0AA6C1
        5F3F2E58 7AA021B7 4DB140D4 C629E42F 87D3A5CE 78BCA47A
        A30CAB16 91020EF2 A5C40821 871D9C21 343DCE92 988697BE


  ------------

    V = HMAC(K, V) is
                         D83A8084 630F286D A4DB49B9 F6F608C8
        993F7F13 97EA0D6F 4A72CF3E F2733A11 AB823C29 F2EBDEC3
        EDE962F9 3D920A1D B59C84E1 E879C29F 5F9995FC 3A6A3AF9


    temp is
                         D83A8084 630F286D A4DB49B9 F6F608C8
        993F7F13 97EA0D6F 4A72CF3E F2733A11 AB823C29 F2EBDEC3
        EDE962F9 3D920A1D B59C84E1 E879C29F 5F9995FC 3A6A3AF9


  ------------

    V = HMAC(K, V) is
                         B587CA7C 13EA197D 423E81E1 D6469942
        B6E2CA83 A97E91F6 B298266A C148A180 9776C26A F5E239A5
        5A2BEB9E 752203A6 94E1F3FE 2B3E6A0C 9C314421 CDB55FBD


    temp is
                                             D83A8084 630F286D
        A4DB49B9 F6F608C8 993F7F13 97EA0D6F 4A72CF3E F2733A11
        AB823C29 F2EBDEC3 EDE962F9 3D920A1D B59C84E1 E879C29F
        5F9995FC 3A6A3AF9 B587CA7C 13EA197D 423E81E1 D6469942
        B6E2CA83 A97E91F6 B298266A C148A180 9776C26A F5E239A5
        5A2BEB9E 752203A6 94E1F3FE 2B3E6A0C 9C314421 CDB55FBD


--------------------------

  returned_bits is
                                             D83A8084 630F286D
        A4DB49B9 F6F608C8 993F7F13 97EA0D6F 4A72CF3E F2733A11
```

```
        AB823C29 F2EBDEC3 EDE962F9 3D920A1D B59C84E1 E879C29F
        5F9995FC 3A6A3AF9 B587CA7C 13EA197D 423E81E1 D6469942
        B6E2CA83 A97E91F6 B298266A C148A180 9776C26A F5E239A5
        5A2BEB9E 752203A6 94E1F3FE 2B3E6A0C 9C314421 CDB55FBD


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    ------------

    V || 0x00 || provided_data is
                                              B587CA7C 13EA197D
        423E81E1 D6469942 B6E2CA83 A97E91F6 B298266A C148A180
        9776C26A F5E239A5 5A2BEB9E 752203A6 94E1F3FE 2B3E6A0C
        9C314421 CDB55FBD 00A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x00 || provided_data) is
                            715D6185 7CE5456B 7FABA13E ABA449AB
        EE0D7EA0 EA9B2530 62733A9F DAF8EB82 A2896F50 6F71B24A
        1A765247 7051C55C A3FA8C92 8D47B5B2 4EBF0FE3 144CF727


    V = HMAC(K, V) is
                            44894C5E D321DD8E 80C4171B 1C97965D
        E5BBCF20 33ECCE57 1F0EBF27 1FF4559A 42D39CFD 2473F47E
        6FB9BF00 32DB08FA 5702D025 FD52FC7D ECEAA4FB AADED3A1


    ------------
```

```
    V || 0x01 || provided_data is
                                                44894C5E D321DD8E
        80C4171B 1C97965D E5BBCF20 33ECCE57 1F0EBF27 1FF4559A
        42D39CFD 2473F47E 6FB9BF00 32DB08FA 5702D025 FD52FC7D
        ECEAA4FB AADED3A1 01A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x01 || provided_data) is
                           43175BC3 737F59B4 6EE92380 8CF3DA53
        68933814 772FA1E8 4EFB1B7E E0F7C62E 0525A3D7 3D951FF4
        C9BE97DA D3722D12 ACA772FB D41D5100 5E50943F C5C95D6F


    V = HMAC(K, V) is
                           5575680B D05BA728 92CB32C4 7D8288E3
        8A0746C4 A23CECA7 5DFD1573 52165638 EFFBEA34 03DD40F1
        58B7B369 663D4B8C C1D280ED C34A1AB7 621746B1 DC0B924F


rnd_val is
                                                D83A8084 630F286D
        A4DB49B9 F6F608C8 993F7F13 97EA0D6F 4A72CF3E F2733A11
        AB823C29 F2EBDEC3 EDE962F9 3D920A1D B59C84E1 E879C29F
        5F9995FC 3A6A3AF9 B587CA7C 13EA197D 423E81E1 D6469942
        B6E2CA83 A97E91F6 B298266A C148A180 9776C26A F5E239A5
        5A2BEB9E 752203A6 94E1F3FE 2B3E6A0C 9C314421 CDB55FBD


##############################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
```

5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E

EntropyInput1 (for Reseed1) =
808182 83848586 8788898A 8B8C8D8E
8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE

EntropyInput2 (for Reseed2) =
C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E

Nonce =
20212223 24252627 28292A2B 2C2D2E2F

PersonalizationString = <empty>

AdditionalInput = <empty>

##

****

HMAC_DRBG_Instantiate_algorithm

entropy_input is
000102 03040506 0708090A 0B0C0D0E
0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E

nonce is
20212223 24252627 28292A2B 2C2D2E2F

personal_str is <empty>

```
    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


  Key is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                          01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    ------------

    V || 0x00 || provided_data is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 00000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
```

```
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    K = HMAC(K, V || 0x00 || provided_data) is
                          45A111E3 AB3725B8 D02D1D8C A0AED099
        D32CF71C 2CA703C8 3708DDC3 AB0BDBEC 23719C1A 4C7273A8
        EB06EC14 B05853A0 793D492D C256DD1C 7DA4D148 BE8516CD


    V = HMAC(K, V) is
                          B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F
        37948762 32662A75 B91B6150 E5BB1802 C68698C7 1E5BBCEB
        2C39FB40 CE3EF53D 4F092229 4CA844A1 6E67E2B2 710250CA


    ------------

    V || 0x01 || provided_data is
        B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F 37948762 32662A75
        B91B6150 E5BB1802 C68698C7 1E5BBCEB 2C39FB40 CE3EF53D
        4F092229 4CA844A1 6E67E2B2 710250CA 01000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    K = HMAC(K, V || 0x01 || provided_data) is
                          A7E118A5 31DEF956 DCFF94BB 3D801F77
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V = HMAC(K, V) is
                          110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


Update (Key, V):

    Key is
                          A7E118A5 31DEF956 DCFF94BB 3D801F77
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
```

```
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V is
                         110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


------------------------------------------------------------

First call to Generate

**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

Generate FAILED: Reseed is required
**************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    additional_input is  <empty>

  Seed_Material is
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  Key is
                         A7E118A5 31DEF956 DCFF94BB 3D801F77
```

```
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


  V is
                         110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


---------------------------

  Update

    provided_data
                           808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    ------------

    V || 0x00 || provided_data is
                                              110793EA A60DC9DB
        CD420810 4088A23D AECC1226 EAF1D03B BA9D83A6 95999165
        71907346 B15A0439 362B9C8E E330E52D EACC639B 98E8030A
        95780CD7 C24B04D5 00808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    K = HMAC(K, V || 0x00 || provided_data) is
                         55630E7A 8BD664AE AA8B1CE6 1EF6BF5B
        24656B8A 9F0667C9 C81A89E7 CB1269C8 408BD712 7A0E46D2
        4C2E03EC E2B62A08 B93045CC C808DC2B 9C195647 4790C2B3


    V = HMAC(K, V) is
                         4247B361 AF91E466 DC4C3C35 86EC9F3C
        FC6DAD2A 7C46902B 7A7FFC6C C618B605 0A48953C BBA0CF78
        0CBC76D6 E60B5FC6 9965D59F 6F8B66FB 4A2EAF68 99EC5447
```

```
    ------------

    V || 0x01 || provided_data is
                                                4247B361 AF91E466
        DC4C3C35 86EC9F3C FC6DAD2A 7C46902B 7A7FFC6C C618B605
        0A48953C BBA0CF78 0CBC76D6 E60B5FC6 9965D59F 6F8B66FB
        4A2EAF68 99EC5447 01808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    K = HMAC(K, V || 0x01 || provided_data) is
                           06CE30C3 A6C36878 BDE5C626 37F9454F
        A6F034FB A6751139 1DF82E7F F076B2DE CBCAC10F 15744E3F
        075C1DDF 46E934C6 EDDADDB9 CFC68587 467E2296 1D9166DC


    V = HMAC(K, V) is
                           59133BDF 3FEFAE3C AC734B81 F307CA18
        6D6E6228 2CD1BFFE 3F48E3FE 672C81BB 1325ACED 3AE6B1FF
        C386DC6A ECC8BB03 58CE2F43 7CE38674 4014A3BC 0CFAD33B


  Update (Key, V):

    Key is
                           06CE30C3 A6C36878 BDE5C626 37F9454F
        A6F034FB A6751139 1DF82E7F F076B2DE CBCAC10F 15744E3F
        075C1DDF 46E934C6 EDDADDB9 CFC68587 467E2296 1D9166DC


    V is
                           59133BDF 3FEFAE3C AC734B81 F307CA18
        6D6E6228 2CD1BFFE 3F48E3FE 672C81BB 1325ACED 3AE6B1FF
        C386DC6A ECC8BB03 58CE2F43 7CE38674 4014A3BC 0CFAD33B


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024
```

```
    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                          28FD6060 C4F35F4D 317AB206 0EE32019
        E0DAA330 F3F5650B BCA57CB6 7EE6AF1C 6F25D1B0 1F3601ED
        A85DC2ED 29A9B2BA 4C85CF49 1CE7185F 1A2BD937 8AE3C655


    temp is
                          28FD6060 C4F35F4D 317AB206 0EE32019
        E0DAA330 F3F5650B BCA57CB6 7EE6AF1C 6F25D1B0 1F3601ED
        A85DC2ED 29A9B2BA 4C85CF49 1CE7185F 1A2BD937 8AE3C655


  ------------

    V = HMAC(K, V) is
                          BD1CEC2E E108AE7F C382989F 6D4FEA8A
        B0149969 7C2F0794 5CE02C5E D617D042 87FEAF3B A638A4CE
        F3BB6B82 7E40AF16 279580FC F1FDAD83 0930F7FD E341E2AF


    temp is
                                              28FD6060 C4F35F4D
        317AB206 0EE32019 E0DAA330 F3F5650B BCA57CB6 7EE6AF1C
        6F25D1B0 1F3601ED A85DC2ED 29A9B2BA 4C85CF49 1CE7185F
        1A2BD937 8AE3C655 BD1CEC2E E108AE7F C382989F 6D4FEA8A
        B0149969 7C2F0794 5CE02C5E D617D042 87FEAF3B A638A4CE
        F3BB6B82 7E40AF16 279580FC F1FDAD83 0930F7FD E341E2AF


---------------------------

  returned_bits is
                                              28FD6060 C4F35F4D
        317AB206 0EE32019 E0DAA330 F3F5650B BCA57CB6 7EE6AF1C
        6F25D1B0 1F3601ED A85DC2ED 29A9B2BA 4C85CF49 1CE7185F
        1A2BD937 8AE3C655 BD1CEC2E E108AE7F C382989F 6D4FEA8A
        B0149969 7C2F0794 5CE02C5E D617D042 87FEAF3B A638A4CE
        F3BB6B82 7E40AF16 279580FC F1FDAD83 0930F7FD E341E2AF


  call Update(additional_input, K, V)
---------------------------
```

```
  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                        BD 1CEC2EE1 08AE7FC3 82989F6D 4FEA8AB0
        1499697C 2F07945C E02C5ED6 17D04287 FEAF3BA6 38A4CEF3
        BB6B827E 40AF1627 9580FCF1 FDAD8309 30F7FDE3 41E2AF00


    K = HMAC(K, V || 0x00 || provided_data) is
                           744B3A07 D75D8FA7 C894A730 C642D564
        71291E34 A93CE631 8BB20CC0 576F1142 1F332C9A 2A596B2D
        410ED227 DAD3520A 9D6C8A72 2CDDC825 B4C5DEF3 87FABF86


    V = HMAC(K, V) is
                           5918A9CE AA04C275 3BD95BD2 4BDA176C
        7A73E42E A519AC98 B95BB900 5D7065AD 715D9F55 0C95D4DB
        3A4E6774 B352DBC6 5344B54A 828727F8 86D67426 DB5E1997


rnd_val is
                                              28FD6060 C4F35F4D
        317AB206 0EE32019 E0DAA330 F3F5650B BCA57CB6 7EE6AF1C
        6F25D1B0 1F3601ED A85DC2ED 29A9B2BA 4C85CF49 1CE7185F
        1A2BD937 8AE3C655 BD1CEC2E E108AE7F C382989F 6D4FEA8A
        B0149969 7C2F0794 5CE02C5E D617D042 87FEAF3B A638A4CE
        F3BB6B82 7E40AF16 279580FC F1FDAD83 0930F7FD E341E2AF


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>
```

```
Generate FAILED: Reseed is required
************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    additional_input is  <empty>

  Seed_Material is
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  Key is
                          744B3A07 D75D8FA7 C894A730 C642D564
        71291E34 A93CE631 8BB20CC0 576F1142 1F332C9A 2A596B2D
        410ED227 DAD3520A 9D6C8A72 2CDDC825 B4C5DEF3 87FABF86


  V is
                          5918A9CE AA04C275 3BD95BD2 4BDA176C
        7A73E42E A519AC98 B95BB900 5D7065AD 715D9F55 0C95D4DB
        3A4E6774 B352DBC6 5344B54A 828727F8 86D67426 DB5E1997


---------------------------

  Update

    provided_data
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E
```

```
------------

V || 0x00 || provided_data is
                                          5918A9CE AA04C275
    3BD95BD2 4BDA176C 7A73E42E A519AC98 B95BB900 5D7065AD
    715D9F55 0C95D4DB 3A4E6774 B352DBC6 5344B54A 828727F8
    86D67426 DB5E1997 00C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


K = HMAC(K, V || 0x00 || provided_data) is
                      E21D7EEC 44625C70 56119BB4 C3D19587
    E72E44B3 CC75F1B3 0AA15AA5 69DF6CEF B25A7E73 F5C0D643
    2CEC282C 8A4223DA 10A228C1 4FF8F48F 32477C40 A0C68E3F


V = HMAC(K, V) is
                      6E7B9E62 F29C3F65 5F09DB28 9EAA8F92
    D7BD2C9E 88DB90E9 C4FEF91F 0D45F67B 6330E12F 1345BF1C
    DBE19BE6 D0017B92 CDC06E6A F84D056A 815EB4EF 2F8847F7


------------

V || 0x01 || provided_data is
                                          6E7B9E62 F29C3F65
    5F09DB28 9EAA8F92 D7BD2C9E 88DB90E9 C4FEF91F 0D45F67B
    6330E12F 1345BF1C DBE19BE6 D0017B92 CDC06E6A F84D056A
    815EB4EF 2F8847F7 01C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


K = HMAC(K, V || 0x01 || provided_data) is
                      5B7FDA36 07BFB790 442F742F 147E1722
    AB8880F3 66491ADB 3E338343 3E0D3238 F67146F6 96968B5F
    C2CF696F 3CBBE826 1167EF87 6A176071 23FE23E6 BBB8F891


V = HMAC(K, V) is
```

```
                        25069D7D 3C99972A D1816407 9061C5FC
        B12AA76F DB71519C 5C009B63 1DB75344 DB55BF4C A1080FE8
        893036DD 60C38A1B E0B8DB65 2E11B679 ACC3BD38 6DF6995B


  Update (Key, V):

    Key is
                        5B7FDA36 07BFB790 442F742F 147E1722
        AB8880F3 66491ADB 3E338343 3E0D3238 F67146F6 96968B5F
        C2CF696F 3CBBE826 1167EF87 6A176071 23FE23E6 BBB8F891


    V is
                        25069D7D 3C99972A D1816407 9061C5FC
        B12AA76F DB71519C 5C009B63 1DB75344 DB55BF4C A1080FE8
        893036DD 60C38A1B E0B8DB65 2E11B679 ACC3BD38 6DF6995B


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                        C0B1601A FE39338B 58DC2BE7 C256AEBE
        3C21C5A9 39BEEC7E 97B3528A C420F0C6 34184718 7666E0FF
        578A8EB0 A37809F8 77365A28 DF2FA0F0 6354A6F0 24967473


    temp is
                        C0B1601A FE39338B 58DC2BE7 C256AEBE
        3C21C5A9 39BEEC7E 97B3528A C420F0C6 34184718 7666E0FF
        578A8EB0 A37809F8 77365A28 DF2FA0F0 6354A6F0 24967473


  ------------

    V = HMAC(K, V) is
                        69375B9A 9D6B756F DC4A8FB3 08E08256
        9D79A85B B960F747 25662638 9A3B45B0 ABE7ECBC 39D5CD7B
```

```
        2C18DF2E 5FDE8C9B 8D43474C 54B6F983 94684459 29B438C7


    temp is
                                               C0B1601A FE39338B
        58DC2BE7 C256AEBE 3C21C5A9 39BEEC7E 97B3528A C420F0C6
        34184718 7666E0FF 578A8EB0 A37809F8 77365A28 DF2FA0F0
        6354A6F0 24967473 69375B9A 9D6B756F DC4A8FB3 08E08256
        9D79A85B B960F747 25662638 9A3B45B0 ABE7ECBC 39D5CD7B
        2C18DF2E 5FDE8C9B 8D43474C 54B6F983 94684459 29B438C7


---------------------------

  returned_bits is
                                               C0B1601A FE39338B
        58DC2BE7 C256AEBE 3C21C5A9 39BEEC7E 97B3528A C420F0C6
        34184718 7666E0FF 578A8EB0 A37809F8 77365A28 DF2FA0F0
        6354A6F0 24967473 69375B9A 9D6B756F DC4A8FB3 08E08256
        9D79A85B B960F747 25662638 9A3B45B0 ABE7ECBC 39D5CD7B
        2C18DF2E 5FDE8C9B 8D43474C 54B6F983 94684459 29B438C7


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                      69 375B9A9D 6B756FDC 4A8FB308 E082569D
        79A85BB9 60F74725 6626389A 3B45B0AB E7ECBC39 D5CD7B2C
        18DF2E5F DE8C9B8D 43474C54 B6F98394 68445929 B438C700


    K = HMAC(K, V || 0x00 || provided_data) is
                           3E88DDDE D73D0F04 35F64858 4E5FCA52
        9DD2DA82 71DD4977 48932721 71D40ACD 8F97E19B 1DC644B1
        49DFE2FB 46085F2D 62F99535 FC1C1B38 2684CFA0 1412AB09


    V = HMAC(K, V) is
                           E36E1391 DEE6220C 5CC7D84B B0D7DBB4
```

```
        1CC88316 5EF43866 E02F30C3 EE2AF4EC CF13F324 C69FF0C5
        0963BDA7 FAB59647 FC06E343 8F3A06D3 A4E48ABD 7ED1BA99


rnd_val is
                                              C0B1601A FE39338B
        58DC2BE7 C256AEBE 3C21C5A9 39BEEC7E 97B3528A C420F0C6
        34184718 7666E0FF 578A8EB0 A37809F8 77365A28 DF2FA0F0
        6354A6F0 24967473 69375B9A 9D6B756F DC4A8FB3 08E08256
        9D79A85B B960F747 25662638 9A3B45B0 ABE7ECBC 39D5CD7B
        2C18DF2E 5FDE8C9B 8D43474C 54B6F983 94684459 29B438C7


################################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E
```

```
    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput1 =
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    AdditionalInput2 =
                            A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
                                               000102 03040506
```

```
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


  Key is
                         00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                         01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
                                                  000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    ------------

    V || 0x00 || provided_data is
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 00000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    K = HMAC(K, V || 0x00 || provided_data) is
```

```
                        45A111E3 AB3725B8 D02D1D8C A0AED099
        D32CF71C 2CA703C8 3708DDC3 AB0BDBEC 23719C1A 4C7273A8
        EB06EC14 B05853A0 793D492D C256DD1C 7DA4D148 BE8516CD


    V = HMAC(K, V) is
                        B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F
        37948762 32662A75 B91B6150 E5BB1802 C68698C7 1E5BBCEB
        2C39FB40 CE3EF53D 4F092229 4CA844A1 6E67E2B2 710250CA


    ------------

    V || 0x01 || provided_data is
        B4F4EAD4 4D45EF54 6C9CE52C C9B0B50F 37948762 32662A75
        B91B6150 E5BB1802 C68698C7 1E5BBCEB 2C39FB40 CE3EF53D
        4F092229 4CA844A1 6E67E2B2 710250CA 01000102 03040506
        0708090A 0B0C0D0E 0F101112 13141516 1718191A 1B1C1D1E
        1F202122 23242526 2728292A 2B2C2D2E 2F303132 33343536
        3738393A 3B3C3D3E 3F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 20212223 24252627 28292A2B 2C2D2E2F


    K = HMAC(K, V || 0x01 || provided_data) is
                        A7E118A5 31DEF956 DCFF94BB 3D801F77
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V = HMAC(K, V) is
                        110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


Update (Key, V):

    Key is
                        A7E118A5 31DEF956 DCFF94BB 3D801F77
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


    V is
                        110793EA A60DC9DB CD420810 4088A23D
```

AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5

First call to Generate

****

HMAC_DRBG_Generate

requested_number_of_bits = 1024

additional_input is
606162 63646566 6768696A 6B6C6D6E
6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

Generate FAILED: Reseed is required
****

HMAC_DRBG_Reseed_algorithm

entropy_input is
808182 83848586 8788898A 8B8C8D8E
8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE

additional_input is
606162 63646566 6768696A 6B6C6D6E
6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE

Seed_Material is
8081 82838485
86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D

```
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


  Key is
                        A7E118A5 31DEF956 DCFF94BB 3D801F77
        5DC68F91 696A434C C25E270E 639044E1 A7240266 D3AA202D
        46C1054B 61024753 5007DF12 CFC8DA45 982A587F C81C47D5


  V is
                        110793EA A60DC9DB CD420810 4088A23D
        AECC1226 EAF1D03B BA9D83A6 95999165 71907346 B15A0439
        362B9C8E E330E52D EACC639B 98E8030A 95780CD7 C24B04D5


---------------------------

  Update

    provided_data
                                                  8081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
        9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
        B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
        CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
        E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


    ------------

    V || 0x00 || provided_data is
          110793 EAA60DC9 DBCD4208 104088A2 3DAECC12 26EAF1D0
        3BBA9D83 A6959991 65719073 46B15A04 39362B9C 8EE330E5
        2DEACC63 9B98E803 0A95780C D7C24B04 D5008081 82838485
        86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
```

```
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
                      4886B37A A9D553BD 09ED84EF 277C1F08
    B7CE7FC5 8AB92D89 68D23154 7407016B 44402F9E 69404796
    C0FD87DB D1A9A4BE DB3247F0 900EE1EB 39DDB7CD B712EB23


V = HMAC(K, V) is
                      8EC05CF1 396D4E82 2B03E445 0859CE0F
    A9A1D9DA 3AB15FB7 7EC1B0A6 0E447853 836E64B8 34C46B04
    59DBD08F DB6EA145 AFAAD2FC 939584A2 91F141CF 55E8DFD4


------------

V || 0x01 || provided_data is
      8EC05C F1396D4E 822B03E4 450859CE 0FA9A1D9 DA3AB15F
    B77EC1B0 A60E4478 53836E64 B834C46B 0459DBD0 8FDB6EA1
    45AFAAD2 FC939584 A291F141 CF55E8DF D4018081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x01 || provided_data) is
                      91529DF9 C5C21BD7 141E05DB E7F3678C
    F4531EB0 110ED597 EBF65048 8EBEB6D1 B6D129F2 47697693
    2D2BD4CB 93F05DE7 40AAA7AF 28485952 1E06108F ABA4806C


V = HMAC(K, V) is
```

```
                        8C03B0DB 21C3F1F0 54027000 0CB3821E
        3D3C853A 90202E25 BD4AF86A 33A1A2CE 679A9006 C8A6054E
        84E2DF90 EEADDC78 EC20AC3C 7745B890 5AB4ED53 927BD958


  Update (Key, V):

    Key is
                        91529DF9 C5C21BD7 141E05DB E7F3678C
        F4531EB0 110ED597 EBF65048 8EBEB6D1 B6D129F2 47697693
        2D2BD4CB 93F05DE7 40AAA7AF 28485952 1E06108F ABA4806C


    V is
                        8C03B0DB 21C3F1F0 54027000 0CB3821E
        3D3C853A 90202E25 BD4AF86A 33A1A2CE 679A9006 C8A6054E
        84E2DF90 EEADDC78 EC20AC3C 7745B890 5AB4ED53 927BD958


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                        72691D21 03FB567C CD303707 15B36666
        F6343008 7B1C6882 81CA0974 DB456BDB A7EB5C48 CFF62EA0
        5F9508F3 B530CE99 5A272B11 EC079C13 923EEF8E 011A93C1


    temp is
                        72691D21 03FB567C CD303707 15B36666
        F6343008 7B1C6882 81CA0974 DB456BDB A7EB5C48 CFF62EA0
        5F9508F3 B530CE99 5A272B11 EC079C13 923EEF8E 011A93C1


  ------------

    V = HMAC(K, V) is
                        9B58CC67 16BC7CB8 BD886CAA 60C14D85
        C023348B D77738C4 75D6C7E1 D9BFF4B1 2C43D8CC 73F838DC
```

```
        4F8BD476 CF8328EE B71B3D87 3D6B7B85 9C9B2106 5638FF95


    temp is
                                               72691D21 03FB567C
        CD303707 15B36666 F6343008 7B1C6882 81CA0974 DB456BDB
        A7EB5C48 CFF62EA0 5F9508F3 B530CE99 5A272B11 EC079C13
        923EEF8E 011A93C1 9B58CC67 16BC7CB8 BD886CAA 60C14D85
        C023348B D77738C4 75D6C7E1 D9BFF4B1 2C43D8CC 73F838DC
        4F8BD476 CF8328EE B71B3D87 3D6B7B85 9C9B2106 5638FF95


---------------------------

  returned_bits is
                                               72691D21 03FB567C
        CD303707 15B36666 F6343008 7B1C6882 81CA0974 DB456BDB
        A7EB5C48 CFF62EA0 5F9508F3 B530CE99 5A272B11 EC079C13
        923EEF8E 011A93C1 9B58CC67 16BC7CB8 BD886CAA 60C14D85
        C023348B D77738C4 75D6C7E1 D9BFF4B1 2C43D8CC 73F838DC
        4F8BD476 CF8328EE B71B3D87 3D6B7B85 9C9B2106 5638FF95


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                       9B 58CC6716 BC7CB8BD 886CAA60 C14D85C0
        23348BD7 7738C475 D6C7E1D9 BFF4B12C 43D8CC73 F838DC4F
        8BD476CF 8328EEB7 1B3D873D 6B7B859C 9B210656 38FF9500


    K = HMAC(K, V || 0x00 || provided_data) is
                            9648218E 7084C7B9 4678C2DC 7495AC1C
        B8812E4C 7FD238E2 F1AE5C52 71649A36 8FF93E09 BD03465E
        8E11E568 7296575E 05972C3C A8F5ED9B 4D37817F 135FF5E2


    V = HMAC(K, V) is
                            509C5F6A ABABA9EA 799C530F 01EE5423
```

```
        8E6013B1 6DC1DB7A 4F6E36ED 2E0ED112 07E94187 C10AF321
        449765D1 63DFA6B8 B4A6A629 70D7D4E1 9DB67A89 F6FE098D


rnd_val is
                                            72691D21 03FB567C
        CD303707 15B36666 F6343008 7B1C6882 81CA0974 DB456BDB
        A7EB5C48 CFF62EA0 5F9508F3 B530CE99 5A272B11 EC079C13
        923EEF8E 011A93C1 9B58CC67 16BC7CB8 BD886CAA 60C14D85
        C023348B D77738C4 75D6C7E1 D9BFF4B1 2C43D8CC 73F838DC
        4F8BD476 CF8328EE B71B3D87 3D6B7B85 9C9B2106 5638FF95


-------------------------------------------------------------

Second call to Generate

*************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
*************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    additional_input is
                           A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  Seed_Material is
                                                C0C1 C2C3C4C5
      C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
      DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
      F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
      0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
      26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  Key is
                        9648218E 7084C7B9 4678C2DC 7495AC1C
      B8812E4C 7FD238E2 F1AE5C52 71649A36 8FF93E09 BD03465E
      8E11E568 7296575E 05972C3C A8F5ED9B 4D37817F 135FF5E2


  V is
                        509C5F6A ABABA9EA 799C530F 01EE5423
      8E6013B1 6DC1DB7A 4F6E36ED 2E0ED112 07E94187 C10AF321
      449765D1 63DFA6B8 B4A6A629 70D7D4E1 9DB67A89 F6FE098D


---------------------------

  Update

    provided_data
                                                C0C1 C2C3C4C5
      C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
      DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
      F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
      0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
      26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
------------

V || 0x00 || provided_data is
      509C5F 6AABABA9 EA799C53 0F01EE54 238E6013 B16DC1DB
    7A4F6E36 ED2E0ED1 1207E941 87C10AF3 21449765 D163DFA6
    B8B4A6A6 2970D7D4 E19DB67A 89F6FE09 8D00C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


K = HMAC(K, V || 0x00 || provided_data) is
                      E4550E14 6FA955BA 46A1DAA7 95A96A8A
    17603D79 BF97BA11 15445EA8 CBD036A5 4C2F1452 407A59F5
    EA0B78E8 9196552F 2C59EB4A 59424229 79F77768 905933D7


V = HMAC(K, V) is
                      C39717D6 DB739945 60D8F8B8 77E50871
    0FAEB012 07958974 7DBCD12F 8334E2EA DDEE361E 69D52AAA
    6DC0B1E3 2EF28F54 798C7DCD 8CCE64B8 773525DE DDEB4F28


------------

V || 0x01 || provided_data is
      C39717 D6DB7399 4560D8F8 B877E508 710FAEB0 12079589
    747DBCD1 2F8334E2 EADDEE36 1E69D52A AA6DC0B1 E32EF28F
    54798C7D CD8CCE64 B8773525 DEDDEB4F 2801C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
    K = HMAC(K, V || 0x01 || provided_data) is
                          3D8DA1FA D6F226D4 C5B8F1F1 B4A595B2
        21F33E44 62F8ABA2 F0D3CBC8 D27360C6 B295803F D893A019
        E96E4DD6 C0C56301 EB7D2DBD B67585FC 3AC3AA85 74CBC463


    V = HMAC(K, V) is
                          27E8D349 BC72C165 1861847B 585BCE91
        46D5FA9A 9FBE2820 106ECAC3 1E8B4525 A2FF70D5 2A1D25A3
        F42277B5 3564C37D D745B0F8 39D2CFD1 35B08DF6 54E68323


  Update (Key, V):

    Key is
                          3D8DA1FA D6F226D4 C5B8F1F1 B4A595B2
        21F33E44 62F8ABA2 F0D3CBC8 D27360C6 B295803F D893A019
        E96E4DD6 C0C56301 EB7D2DBD B67585FC 3AC3AA85 74CBC463


    V is
                          27E8D349 BC72C165 1861847B 585BCE91
        46D5FA9A 9FBE2820 106ECAC3 1E8B4525 A2FF70D5 2A1D25A3
        F42277B5 3564C37D D745B0F8 39D2CFD1 35B08DF6 54E68323


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                          8570DA3D 47E1E160 5CF3E44B 8D328B99
        5EFC6410 7B6292D1 B1036B5F 88CE3160 2F12BEB7 1D801C09
        42E7C086 4B3DB67A 9356DB20 3490D881 24FE86BC E38AC226


    temp is
                          8570DA3D 47E1E160 5CF3E44B 8D328B99
```

```
        5EFC6410 7B6292D1 B1036B5F 88CE3160 2F12BEB7 1D801C09
        42E7C086 4B3DB67A 9356DB20 3490D881 24FE86BC E38AC226


  ------------

    V = HMAC(K, V) is
                           9B4FDA6A BAA88403 9DF80A03 36A24D79
        1EB3067C 8F5F0CF0 F18DD73B 66A7B316 FB19E028 35CC6293
        65FCD1D3 BE640178 ED9093B9 1B36E1D6 8135F278 5BFF505C


    temp is
                                              8570DA3D 47E1E160
        5CF3E44B 8D328B99 5EFC6410 7B6292D1 B1036B5F 88CE3160
        2F12BEB7 1D801C09 42E7C086 4B3DB67A 9356DB20 3490D881
        24FE86BC E38AC226 9B4FDA6A BAA88403 9DF80A03 36A24D79
        1EB3067C 8F5F0CF0 F18DD73B 66A7B316 FB19E028 35CC6293
        65FCD1D3 BE640178 ED9093B9 1B36E1D6 8135F278 5BFF505C


---------------------------

  returned_bits is
                                              8570DA3D 47E1E160
        5CF3E44B 8D328B99 5EFC6410 7B6292D1 B1036B5F 88CE3160
        2F12BEB7 1D801C09 42E7C086 4B3DB67A 9356DB20 3490D881
        24FE86BC E38AC226 9B4FDA6A BAA88403 9DF80A03 36A24D79
        1EB3067C 8F5F0CF0 F18DD73B 66A7B316 FB19E028 35CC6293
        65FCD1D3 BE640178 ED9093B9 1B36E1D6 8135F278 5BFF505C


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                         9B 4FDA6ABA A884039D F80A0336 A24D791E
        B3067C8F 5F0CF0F1 8DD73B66 A7B316FB 19E02835 CC629365
        FCD1D3BE 640178ED 9093B91B 36E1D681 35F2785B FF505C00
```

```
    K = HMAC(K, V || 0x00 || provided_data) is
                          5ECC11F5 000DF823 E91EA756 E3F917C0
        0AD8B95C 526EABEE A1EDBCBF D38DA649 F762EBE0 B8FFA062
        B0715DD7 635206B7 A746CC4A FC7A54F4 33DB4428 F6212E53


    V = HMAC(K, V) is
                          FFA84AA8 DB1089F7 16ECEF15 9C628AF2
        48300647 39D87AF4 CBC64C48 6EB2DF2C F58EDB53 D3D3DE89
        C58E88CD DB569E57 DF32CC37 D3B3CC82 88786494 0273CB6E


rnd_val is
                                              8570DA3D 47E1E160
        5CF3E44B 8D328B99 5EFC6410 7B6292D1 B1036B5F 88CE3160
        2F12BEB7 1D801C09 42E7C086 4B3DB67A 9356DB20 3490D881
        24FE86BC E38AC226 9B4FDA6A BAA88403 9DF80A03 36A24D79
        1EB3067C 8F5F0CF0 F18DD73B 66A7B316 FB19E028 35CC6293
        65FCD1D3 BE640178 ED9093B9 1B36E1D6 8135F278 5BFF505C


################################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    EntropyInput1 (for Reseed1) =
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE
```

```
    EntropyInput2 (for Reseed2) =
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString =
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    AdditionalInput = <empty>

###############################################################

***************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                            000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                            404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
```

```
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Key is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                          01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


--------------------------

  Update

    provided_data
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
------------

V || 0x00 || provided_data is
                         010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01010101 01010101 01010101 01010101 01010101 01010101
    01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


K = HMAC(K, V || 0x00 || provided_data) is
                       8FE3241B 7CEC3C91 831FEBC5 664A324E
    CE7885EC 0CFB79F0 A110CDDA 5C25FBDF 2724481F E501C813
    656BAC39 9CE61ABA DA1D0D75 7B2AB666 F4C98216 C1482F59


V = HMAC(K, V) is
                       496DABED 7FE15C71 16E221B4 30EE825C
    72A53FC3 49091FBF 5060584F CF9BAA56 70592E2F BB7E0E5A
    AD170616 E98B6DC8 BC4D77A2 EA17DFDE 4E64B0DF 260D9DCB


------------

V || 0x01 || provided_data is
                         496DAB ED7FE15C 7116E221 B430EE82
    5C72A53F C349091F BF506058 4FCF9BAA 5670592E 2FBB7E0E
    5AAD1706 16E98B6D C8BC4D77 A2EA17DF DE4E64B0 DF260D9D
    CB010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
    16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
    2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
    46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
    5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
    2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
```

```
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x01 || provided_data) is
                          96477F38 6DC67E91 FBE26228 31E00384
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


    V = HMAC(K, V) is
                          FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


  Update (Key, V):

    Key is
                          96477F38 6DC67E91 FBE26228 31E00384
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


    V is
                          FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


----------------------------------------------------------------

First call to Generate

****************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

Generate FAILED: Reseed is required
****************************************************************

HMAC_DRBG_Reseed_algorithm
```

```
    entropy_input is
                              808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    additional_input is  <empty>

  Seed_Material is
                              808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


  Key is
                            96477F38 6DC67E91 FBE26228 31E00384
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


  V is
                            FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


--------------------------

  Update

    provided_data
                              808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    ------------

    V || 0x00 || provided_data is
                                              FAE68E0C ED06928D
```

```
    3D6EC078 2D3FF3ED D3E6D364 B11EF22B 715D26C4 4850F01D
    7074E6C8 13109CD4 8BD91FC8 678E972C 205511E4 3622F079
    72ADB6BC 61BE4F7E 00808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


K = HMAC(K, V || 0x00 || provided_data) is
                      1F9C99C0 D27D726B F887D144 314EDE3B
    FB85FF51 DA2D8147 2C38432F 9592ABA2 A49E4194 A9D2EA4E
    2DF0141B B4EE22BA C263029D 8A1EA7DC 7AB8332D A48C9E66


V = HMAC(K, V) is
                      B63CF883 05CF1F68 986F1E96 3CBB5FE8
    C1ACA6B9 5DE8AFAF 4857BABE 48121DF7 42D1A6B6 1556F1B6
    09032ECA 7B4844BE 70F337FF FBECAE48 F772E2FF B1D840C2


------------

V || 0x01 || provided_data is
                                          B63CF883 05CF1F68
    986F1E96 3CBB5FE8 C1ACA6B9 5DE8AFAF 4857BABE 48121DF7
    42D1A6B6 1556F1B6 09032ECA 7B4844BE 70F337FF FBECAE48
    F772E2FF B1D840C2 01808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


K = HMAC(K, V || 0x01 || provided_data) is
                      E1E5F34B EF791518 4C9E49D1 2518A591
    C077845D 89C9DA00 A2C83950 43148800 818AE9CF 467A7A45
    DA939E96 E3064D99 1848F7AF 5911CA23 FACBD738 16ED0ED4


V = HMAC(K, V) is
                      A089C037 3C58AD2A 465E444D 33269678
    8C28F5BA FE54889B ADF0FEA3 46303EA4 F1933433 7836DB7B
    CB1FFF31 86EDE3B2 C3A8DEA7 D825D3CB 4714C0E1 90269466
```

```
  Update (Key, V):

    Key is
                          E1E5F34B EF791518 4C9E49D1 2518A591
        C077845D 89C9DA00 A2C83950 43148800 818AE9CF 467A7A45
        DA939E96 E3064D99 1848F7AF 5911CA23 FACBD738 16ED0ED4


    V is
                          A089C037 3C58AD2A 465E444D 33269678
        8C28F5BA FE54889B ADF0FEA3 46303EA4 F1933433 7836DB7B
        CB1FFF31 86EDE3B2 C3A8DEA7 D825D3CB 4714C0E1 90269466


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                          AAE4DC3C 9ECC74D9 061DD527 117EF3D2
        9E1E52B2 6853C539 D6CA797E 8DA3D0BB 171D8E30 B8B194D8
        C28F7F6B E3B986B8 8506DC6A 01B294A7 165DD1C3 470F7BE7


    temp is
                          AAE4DC3C 9ECC74D9 061DD527 117EF3D2
        9E1E52B2 6853C539 D6CA797E 8DA3D0BB 171D8E30 B8B194D8
        C28F7F6B E3B986B8 8506DC6A 01B294A7 165DD1C3 470F7BE7


  ------------

    V = HMAC(K, V) is
                          B396AA0D B7D50C40 51E7C7E1 C8A7D21A
        2B5878C0 BCB163CA A79366E7 A1162FDC 88429616 CD3E6977
        8D327520 A6BBBF71 D8AA2E03 EC4A9DAA 0E77CF93 E1EE30D2


    temp is
                                              AAE4DC3C 9ECC74D9
```

```
        061DD527 117EF3D2 9E1E52B2 6853C539 D6CA797E 8DA3D0BB
        171D8E30 B8B194D8 C28F7F6B E3B986B8 8506DC6A 01B294A7
        165DD1C3 470F7BE7 B396AA0D B7D50C40 51E7C7E1 C8A7D21A
        2B5878C0 BCB163CA A79366E7 A1162FDC 88429616 CD3E6977
        8D327520 A6BBBF71 D8AA2E03 EC4A9DAA 0E77CF93 E1EE30D2


---------------------------

  returned_bits is
                                            AAE4DC3C 9ECC74D9
        061DD527 117EF3D2 9E1E52B2 6853C539 D6CA797E 8DA3D0BB
        171D8E30 B8B194D8 C28F7F6B E3B986B8 8506DC6A 01B294A7
        165DD1C3 470F7BE7 B396AA0D B7D50C40 51E7C7E1 C8A7D21A
        2B5878C0 BCB163CA A79366E7 A1162FDC 88429616 CD3E6977
        8D327520 A6BBBF71 D8AA2E03 EC4A9DAA 0E77CF93 E1EE30D2


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                       B3 96AA0DB7 D50C4051 E7C7E1C8 A7D21A2B
        5878C0BC B163CAA7 9366E7A1 162FDC88 429616CD 3E69778D
        327520A6 BBBF71D8 AA2E03EC 4A9DAA0E 77CF93E1 EE30D200


    K = HMAC(K, V || 0x00 || provided_data) is
                            275F4A02 431A1B30 6DCA0A37 3BB9EA85
        039B1DE3 08227752 F9633D57 7854C73A 84886B9A 3C25819C
        EBDE8F16 8C1C8B06 3482BB6A 8AB54870 59A3876C 7710ACB4


    V = HMAC(K, V) is
                            FDA1F0F3 8D1D0BB7 0D29E9CC 05A4190E
        9D9D49CC 24000C8D F12CFC09 D4325714 C0F78B13 EC7A12D6
        EF1A380B 0C7B0563 0CD08D7F C77E43A8 755F47A5 B01A9E48


rnd_val is
```

```
                                                AAE4DC3C 9ECC74D9
        061DD527 117EF3D2 9E1E52B2 6853C539 D6CA797E 8DA3D0BB
        171D8E30 B8B194D8 C28F7F6B E3B986B8 8506DC6A 01B294A7
        165DD1C3 470F7BE7 B396AA0D B7D50C40 51E7C7E1 C8A7D21A
        2B5878C0 BCB163CA A79366E7 A1162FDC 88429616 CD3E6977
        8D327520 A6BBBF71 D8AA2E03 EC4A9DAA 0E77CF93 E1EE30D2


-----------------------------------------------------------

Second call to Generate

***********************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

Generate FAILED: Reseed is required
***********************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    additional_input is  <empty>

  Seed_Material is
                            C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


  Key is
                          275F4A02 431A1B30 6DCA0A37 3BB9EA85
        039B1DE3 08227752 F9633D57 7854C73A 84886B9A 3C25819C
```

```
        EBDE8F16 8C1C8B06 3482BB6A 8AB54870 59A3876C 7710ACB4


  V is
                         FDA1F0F3 8D1D0BB7 0D29E9CC 05A4190E
        9D9D49CC 24000C8D F12CFC09 D4325714 C0F78B13 EC7A12D6
        EF1A380B 0C7B0563 0CD08D7F C77E43A8 755F47A5 B01A9E48


--------------------------

  Update

    provided_data
                           C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    ------------

    V || 0x00 || provided_data is
                                               FDA1F0F3 8D1D0BB7
        0D29E9CC 05A4190E 9D9D49CC 24000C8D F12CFC09 D4325714
        C0F78B13 EC7A12D6 EF1A380B 0C7B0563 0CD08D7F C77E43A8
        755F47A5 B01A9E48 00C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    K = HMAC(K, V || 0x00 || provided_data) is
                         2F4B184F 21910B66 079269B5 2708880D
        FFB6A73D 37962656 B91DB6CC 1157B4BA 65955979 373F928A
        B86269C1 DC89A604 B047B65F 5EB1AA11 D636E58A 5D13F645


    V = HMAC(K, V) is
                         2EB12A07 23BF0EE7 F0CE6B73 08510C62
        2C00D617 F3E5994E EBA9913B 87D01D28 17C82DFB FD3CB1DE
        D99E2C7D 4C9212D4 A95D492D 99E61F6E 4F9CEC02 490A6919
```

```
    ------------

    V || 0x01 || provided_data is
                                              2EB12A07 23BF0EE7
        F0CE6B73 08510C62 2C00D617 F3E5994E EBA9913B 87D01D28
        17C82DFB FD3CB1DE D99E2C7D 4C9212D4 A95D492D 99E61F6E
        4F9CEC02 490A6919 01C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


    K = HMAC(K, V || 0x01 || provided_data) is
                          3C666E58 0DE3F6DB 662E8C00 EC31B6D9
        8F7DFB8A BB4DB1AD D0AA989C C2E71EF2 C5D41166 FAC63729
        E23B591C 0D1F11E7 D10AE714 6687CD2E 0ED9B738 9CD7DD35


    V = HMAC(K, V) is
                          26DBEAEF BCC48F41 D41077C2 ED286F67
        49FDC109 E24D372E 7DC20F0F 87037E4D FACCD39A 77807D5C
        8586CACE AEE75863 C9351C96 5678E46F DB77A739 FD123189


  Update (Key, V):

    Key is
                          3C666E58 0DE3F6DB 662E8C00 EC31B6D9
        8F7DFB8A BB4DB1AD D0AA989C C2E71EF2 C5D41166 FAC63729
        E23B591C 0D1F11E7 D10AE714 6687CD2E 0ED9B738 9CD7DD35


    V is
                          26DBEAEF BCC48F41 D41077C2 ED286F67
        49FDC109 E24D372E 7DC20F0F 87037E4D FACCD39A 77807D5C
        8586CACE AEE75863 C9351C96 5678E46F DB77A739 FD123189


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>
```

```
  ------------

    V = HMAC(K, V) is
                          129FF6D3 1A23FFBC 870632B3 5EE477C2
        280DDD2E CDABEDB9 00C78418 BE2D243B B9D8E509 3ECE7B6B
        F48638D8 F704D134 ADDEB7F4 E9D5C142 CD05683E 72B51648


    temp is
                          129FF6D3 1A23FFBC 870632B3 5EE477C2
        280DDD2E CDABEDB9 00C78418 BE2D243B B9D8E509 3ECE7B6B
        F48638D8 F704D134 ADDEB7F4 E9D5C142 CD05683E 72B51648


  ------------

    V = HMAC(K, V) is
                          6AF24AEC 15D61E81 E270DD4E BED91B62
        12EB8896 A6250D5C 8BC3A4A1 2F7E3068 FBDF856F 47EB23D3
        79F82C1E BCD1585F B260B9C0 C42625FB CEE68CAD 773CD5B1


    temp is
                                              129FF6D3 1A23FFBC
        870632B3 5EE477C2 280DDD2E CDABEDB9 00C78418 BE2D243B
        B9D8E509 3ECE7B6B F48638D8 F704D134 ADDEB7F4 E9D5C142
        CD05683E 72B51648 6AF24AEC 15D61E81 E270DD4E BED91B62
        12EB8896 A6250D5C 8BC3A4A1 2F7E3068 FBDF856F 47EB23D3
        79F82C1E BCD1585F B260B9C0 C42625FB CEE68CAD 773CD5B1


---------------------------

  returned_bits is
                                              129FF6D3 1A23FFBC
        870632B3 5EE477C2 280DDD2E CDABEDB9 00C78418 BE2D243B
        B9D8E509 3ECE7B6B F48638D8 F704D134 ADDEB7F4 E9D5C142
        CD05683E 72B51648 6AF24AEC 15D61E81 E270DD4E BED91B62
        12EB8896 A6250D5C 8BC3A4A1 2F7E3068 FBDF856F 47EB23D3
        79F82C1E BCD1585F B260B9C0 C42625FB CEE68CAD 773CD5B1


  call Update(additional_input, K, V)
---------------------------
```

```
  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                        6A F24AEC15 D61E81E2 70DD4EBE D91B6212
        EB8896A6 250D5C8B C3A4A12F 7E3068FB DF856F47 EB23D379
        F82C1EBC D1585FB2 60B9C0C4 2625FBCE E68CAD77 3CD5B100


    K = HMAC(K, V || 0x00 || provided_data) is
                           8AB868CE E3786F24 9731B824 583C54BE
        FBA2FC02 D3783FEB 2026E6AF 9583FF3D 4475EF98 FEEB3D7F
        8E22218B EFFD3A0D 11D81E86 4F902A39 27B0A677 B166EAA7


    V = HMAC(K, V) is
                           C4511D5E 80B125CF AF306267 21A25E01
        000E1711 077EBFE3 4EA6E58C 5F00775E 83DC13DD E2D86849
        4F3D6858 04C61BEC 70974A29 911E7C31 ACC5AA43 5AACFC0F


rnd_val is
                                              129FF6D3 1A23FFBC
        870632B3 5EE477C2 280DDD2E CDABEDB9 00C78418 BE2D243B
        B9D8E509 3ECE7B6B F48638D8 F704D134 ADDEB7F4 E9D5C142
        CD05683E 72B51648 6AF24AEC 15D61E81 E270DD4E BED91B62
        12EB8896 A6250D5C 8BC3A4A1 2F7E3068 FBDF856F 47EB23D3
        79F82C1E BCD1585F B260B9C0 C42625FB CEE68CAD 773CD5B1


##############################################################

HMAC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
```

```
    3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
    5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


EntropyInput1 (for Reseed1) =
                         808182 83848586 8788898A 8B8C8D8E
    8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
    A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
    BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
    D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


EntropyInput2 (for Reseed2) =
                         C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
    CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
    E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
    FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
    1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E


Nonce =
                       20212223 24252627 28292A2B 2C2D2E2F


PersonalizationString =
                         404142 43444546 4748494A 4B4C4D4E
    4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
    6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
    7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
    9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


AdditionalInput1 =
                         606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


AdditionalInput2 =
                         A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E
```

```
################################################################

****************************************************************

HMAC_DRBG_Instantiate_algorithm

    entropy_input is
                             000102 03040506 0708090A 0B0C0D0E
        0F101112 13141516 1718191A 1B1C1D1E 1F202122 23242526
        2728292A 2B2C2D2E 2F303132 33343536 3738393A 3B3C3D3E
        3F404142 43444546 4748494A 4B4C4D4E 4F505152 53545556
        5758595A 5B5C5D5E 5F606162 63646566 6768696A 6B6C6D6E


    nonce is
                           20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                             404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    prediction_resistance_flag = "PredictionResistance"

  Seed_Material is
             0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


  Key is
                           00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
```

```
        00000000 00000000 00000000 00000000 00000000 00000000


  V is
                         01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101


---------------------------

  Update

    provided_data
            0001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    ------------

    V || 0x00 || provided_data is
                           010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01010101 01010101 01010101 01010101 01010101 01010101
        01000001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x00 || provided_data) is
                           8FE3241B 7CEC3C91 831FEBC5 664A324E
```

```
        CE7885EC 0CFB79F0 A110CDDA 5C25FBDF 2724481F E501C813
        656BAC39 9CE61ABA DA1D0D75 7B2AB666 F4C98216 C1482F59


    V = HMAC(K, V) is
                           496DABED 7FE15C71 16E221B4 30EE825C
        72A53FC3 49091FBF 5060584F CF9BAA56 70592E2F BB7E0E5A
        AD170616 E98B6DC8 BC4D77A2 EA17DFDE 4E64B0DF 260D9DCB


    ------------

    V || 0x01 || provided_data is
                             496DAB ED7FE15C 7116E221 B430EE82
        5C72A53F C349091F BF506058 4FCF9BAA 5670592E 2FBB7E0E
        5AAD1706 16E98B6D C8BC4D77 A2EA17DF DE4E64B0 DF260D9D
        CB010001 02030405 06070809 0A0B0C0D 0E0F1011 12131415
        16171819 1A1B1C1D 1E1F2021 22232425 26272829 2A2B2C2D
        2E2F3031 32333435 36373839 3A3B3C3D 3E3F4041 42434445
        46474849 4A4B4C4D 4E4F5051 52535455 56575859 5A5B5C5D
        5E5F6061 62636465 66676869 6A6B6C6D 6E202122 23242526
        2728292A 2B2C2D2E 2F404142 43444546 4748494A 4B4C4D4E
        4F505152 53545556 5758595A 5B5C5D5E 5F606162 63646566
        6768696A 6B6C6D6E 6F707172 73747576 7778797A 7B7C7D7E
        7F808182 83848586 8788898A 8B8C8D8E 8F909192 93949596
        9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE


    K = HMAC(K, V || 0x01 || provided_data) is
                           96477F38 6DC67E91 FBE26228 31E00384
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1


    V = HMAC(K, V) is
                           FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


Update (Key, V):

    Key is
                           96477F38 6DC67E91 FBE26228 31E00384
        E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
        EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1
```

```
    V is
                          FAE68E0C ED06928D 3D6EC078 2D3FF3ED
        D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
        8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E


---------------------------------------------------------------

First call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                            808182 83848586 8788898A 8B8C8D8E
        8F909192 93949596 9798999A 9B9C9D9E 9FA0A1A2 A3A4A5A6
        A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE
        BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6
        D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE


    additional_input is
                            606162 63646566 6768696A 6B6C6D6E
        6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
        8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
        9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
        B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

Seed_Material is

```
                                                  8081 82838485
      86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
      9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
      B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
      CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
      E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

Key is

```
                       96477F38 6DC67E91 FBE26228 31E00384
      E017C17F 654AD9B7 1B2395A1 870D0BC2 48378809 87061D81
      EE39A9B2 EC5E9F65 98193BB8 43F3EFA8 D82C0CA7 F5543BF1
```

V is

```
                       FAE68E0C ED06928D 3D6EC078 2D3FF3ED
      D3E6D364 B11EF22B 715D26C4 4850F01D 7074E6C8 13109CD4
      8BD91FC8 678E972C 205511E4 3622F079 72ADB6BC 61BE4F7E
```

Update

provided_data

```
                                                  8081 82838485
      86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
      9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
      B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
      CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
      E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
      6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
      8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
      9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
      B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
```

V || 0x00 || provided_data is

```
      FAE68E 0CED0692 8D3D6EC0 782D3FF3 EDD3E6D3 64B11EF2
    2B715D26 C44850F0 1D7074E6 C813109C D48BD91F C8678E97
    2C205511 E43622F0 7972ADB6 BC61BE4F 7E008081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x00 || provided_data) is
                       1722866C 917C3B67 E5F99D7E A91045F8
    4193D957 7907CCD3 5550E52D A06D6754 0358C63B E94919BB
    C34BB792 E482A71C CECA46F3 163812E6 A66630AB 296B4C8E


V = HMAC(K, V) is
                       278B759C 8E0DA59A 0940CA85 E15715D2
    892F99C3 67D75B8C 2F990D01 1A51EB4D 18CA88EF 87CD6056
    3A92BD0C 4B43645D B79184FE FD492017 A0F57B77 7E71D53F


------------

V || 0x01 || provided_data is
      278B75 9C8E0DA5 9A0940CA 85E15715 D2892F99 C367D75B
    8C2F990D 011A51EB 4D18CA88 EF87CD60 563A92BD 0C4B4364
    5DB79184 FEFD4920 17A0F57B 777E71D5 3F018081 82838485
    86878889 8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C9D
    9E9FA0A1 A2A3A4A5 A6A7A8A9 AAABACAD AEAFB0B1 B2B3B4B5
    B6B7B8B9 BABBBCBD BEBFC0C1 C2C3C4C5 C6C7C8C9 CACBCCCD
    CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD DEDFE0E1 E2E3E4E5
    E6E7E8E9 EAEBECED EE606162 63646566 6768696A 6B6C6D6E
    6F707172 73747576 7778797A 7B7C7D7E 7F808182 83848586
    8788898A 8B8C8D8E 8F909192 93949596 9798999A 9B9C9D9E
    9FA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE AFB0B1B2 B3B4B5B6
    B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE


K = HMAC(K, V || 0x01 || provided_data) is
                       220DC427 79664520 EA800878 E8337D04
    C138AE48 59D68A72 11F03A22 E9602D6E 2277FCFF 6EE81581
```

```
        FDD7A710 ABC57629 369D42A0 47713DCE 221B2267 2C911CB4


    V = HMAC(K, V) is
                         FFC9E91F D3F965DD 153465B5 F91FBD55
        40F08248 882C7100 3BC48BEC D4E1EB5F 4F14428D 4237F160
        58329A64 4E80418C F6B5800D 9AD66B93 C9BC8725 A6A16053


  Update (Key, V):

    Key is
                         220DC427 79664520 EA800878 E8337D04
        C138AE48 59D68A72 11F03A22 E9602D6E 2277FCFF 6EE81581
        FDD7A710 ABC57629 369D42A0 47713DCE 221B2267 2C911CB4


    V is
                         FFC9E91F D3F965DD 153465B5 F91FBD55
        40F08248 882C7100 3BC48BEC D4E1EB5F 4F14428D 4237F160
        58329A64 4E80418C F6B5800D 9AD66B93 C9BC8725 A6A16053


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                         B8E82765 2175E6E0 6E513C7B E94B5810
        C14ED94A D9036479 40CAEB7E E014C848 8DCBBE6D 4D6616D0
        6656A3DC 707CDAC4 F02EE6D8 408C065F CB068C07 60DA47C5


    temp is
                         B8E82765 2175E6E0 6E513C7B E94B5810
        C14ED94A D9036479 40CAEB7E E014C848 8DCBBE6D 4D6616D0
        6656A3DC 707CDAC4 F02EE6D8 408C065F CB068C07 60DA47C5


  ------------
```

```
    V = HMAC(K, V) is
                           D60E5D70 D09DC392 9B697961 5D117F7B
        EDCC661A 98514B3A 1F55B2CB ABDCA59F 11823E48 38065F1F
        8431CBF2 8A577738 234AF3F1 88C7190C C19739E7 2E9BBFFF


    temp is
                                               B8E82765 2175E6E0
        6E513C7B E94B5810 C14ED94A D9036479 40CAEB7E E014C848
        8DCBBE6D 4D6616D0 6656A3DC 707CDAC4 F02EE6D8 408C065F
        CB068C07 60DA47C5 D60E5D70 D09DC392 9B697961 5D117F7B
        EDCC661A 98514B3A 1F55B2CB ABDCA59F 11823E48 38065F1F
        8431CBF2 8A577738 234AF3F1 88C7190C C19739E7 2E9BBFFF


----------------------------

  returned_bits is
                                               B8E82765 2175E6E0
        6E513C7B E94B5810 C14ED94A D9036479 40CAEB7E E014C848
        8DCBBE6D 4D6616D0 6656A3DC 707CDAC4 F02EE6D8 408C065F
        CB068C07 60DA47C5 D60E5D70 D09DC392 9B697961 5D117F7B
        EDCC661A 98514B3A 1F55B2CB ABDCA59F 11823E48 38065F1F
        8431CBF2 8A577738 234AF3F1 88C7190C C19739E7 2E9BBFFF


  call Update(additional_input, K, V)
----------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
                         D6 0E5D70D0 9DC3929B 6979615D 117F7BED
        CC661A98 514B3A1F 55B2CBAB DCA59F11 823E4838 065F1F84
        31CBF28A 57773823 4AF3F188 C7190CC1 9739E72E 9BBFFF00


    K = HMAC(K, V || 0x00 || provided_data) is
                           C0102CD0 756E55D2 FD8EA8B6 5C85B802
        C71BB175 DB898D58 B3180B1A F9DAC854 62DF83D8 127F751E
        7DBBD9C0 A1258636 B03A0886 726D9B36 B1E96414 10C3669E
```

```
    V = HMAC(K, V) is
                          44118780 B54B2EDB 5FA8B8B4 6A5BBF51
        1683D0A8 EDEF1FD0 4AA87BAB 28B3E07E FDAA0CC8 646A8830
        82500A00 33097142 75C0C8DB 1DDAF207 DA4F355B B1108AEE


rnd_val is
                                                B8E82765 2175E6E0
        6E513C7B E94B5810 C14ED94A D9036479 40CAEB7E E014C848
        8DCBBE6D 4D6616D0 6656A3DC 707CDAC4 F02EE6D8 408C065F
        CB068C07 60DA47C5 D60E5D70 D09DC392 9B697961 5D117F7B
        EDCC661A 98514B3A 1F55B2CB ABDCA59F 11823E48 38065F1F
        8431CBF2 8A577738 234AF3F1 88C7190C C19739E7 2E9BBFFF


---------------------------------------------------------------

Second call to Generate

***************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is
                             A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


Generate FAILED: Reseed is required
***************************************************************

HMAC_DRBG_Reseed_algorithm

    entropy_input is
                             C0C1C2 C3C4C5C6 C7C8C9CA CBCCCDCE
        CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE DFE0E1E2 E3E4E5E6
        E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6 F7F8F9FA FBFCFDFE
        FF000102 03040506 0708090A 0B0C0D0E 0F101112 13141516
        1718191A 1B1C1D1E 1F202122 23242526 2728292A 2B2C2D2E
```

```
  additional_input is
                          A0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  Seed_Material is
                                                 C0C1 C2C3C4C5
      C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
      DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
      F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
      0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
      26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
      AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
      C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
      DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
      F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


  Key is
                          C0102CD0 756E55D2 FD8EA8B6 5C85B802
      C71BB175 DB898D58 B3180B1A F9DAC854 62DF83D8 127F751E
      7DBBD9C0 A1258636 B03A0886 726D9B36 B1E96414 10C3669E


  V is
                          44118780 B54B2EDB 5FA8B8B4 6A5BBF51
      1683D0A8 EDEF1FD0 4AA87BAB 28B3E07E FDAA0CC8 646A8830
      82500A00 33097142 75C0C8DB 1DDAF207 DA4F355B B1108AEE


----------------------------

  Update

    provided_data
                                                 C0C1 C2C3C4C5
      C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
      DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
      F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
      0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
      26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


------------

V || 0x00 || provided_data is
      441187 80B54B2E DB5FA8B8 B46A5BBF 511683D0 A8EDEF1F
    D04AA87B AB28B3E0 7EFDAA0C C8646A88 3082500A 00330971
    4275C0C8 DB1DDAF2 07DA4F35 5BB1108A EE00C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
    AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
    C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
    DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
    F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


K = HMAC(K, V || 0x00 || provided_data) is
                        5E30CFA7 88DB0C81 95DE4152 3E9E19B8
    EE9BE2FB 43C318C3 09E2E68E 5157EBA5 878E1A78 A8C54423
    0062F627 34689232 ED28FC94 703294F1 BAA42834 BF7600A6


V = HMAC(K, V) is
                        60C3B3D9 63C283E4 673A221D 75F5B03F
    AD549A93 B89A86BD AD4A6326 B004CFB0 25890A60 F4037155
    689B3B51 E0DDCCBC E7FA6605 5200D88B 58F61C44 604C21B1


------------

V || 0x01 || provided_data is
      60C3B3 D963C283 E4673A22 1D75F5B0 3FAD549A 93B89A86
    BDAD4A63 26B004CF B025890A 60F40371 55689B3B 51E0DDCC
    BCE7FA66 055200D8 8B58F61C 44604C21 B101C0C1 C2C3C4C5
    C6C7C8C9 CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCDD
    DEDFE0E1 E2E3E4E5 E6E7E8E9 EAEBECED EEEFF0F1 F2F3F4F5
    F6F7F8F9 FAFBFCFD FEFF0001 02030405 06070809 0A0B0C0D
    0E0F1011 12131415 16171819 1A1B1C1D 1E1F2021 22232425
    26272829 2A2B2C2D 2EA0A1A2 A3A4A5A6 A7A8A9AA ABACADAE
```

```
        AFB0B1B2 B3B4B5B6 B7B8B9BA BBBCBDBE BFC0C1C2 C3C4C5C6
        C7C8C9CA CBCCCDCE CFD0D1D2 D3D4D5D6 D7D8D9DA DBDCDDDE
        DFE0E1E2 E3E4E5E6 E7E8E9EA EBECEDEE EFF0F1F2 F3F4F5F6
        F7F8F9FA FBFCFDFE FF000102 03040506 0708090A 0B0C0D0E


    K = HMAC(K, V || 0x01 || provided_data) is
                            0DF49D5D E3A4A75F 3A4FD7E9 7338C252
        8DC83097 EE71926B 3DE86274 DA87D828 9A68F570 4D1D018E
        61D15233 D2A17C62 5A063A4A 0FF62A1E 192AFA8A BC6BA6FE


    V = HMAC(K, V) is
                            AB725F55 F27890A4 8194D008 FFC961F5
        14AF792D F52A1B9D CF840FC7 FB528058 9537CC05 6797523F
        70670C9D F0AA161B B735C3D0 3ECF4A52 60FB9775 AA1D69BA


  Update (Key, V):

    Key is
                            0DF49D5D E3A4A75F 3A4FD7E9 7338C252
        8DC83097 EE71926B 3DE86274 DA87D828 9A68F570 4D1D018E
        61D15233 D2A17C62 5A063A4A 0FF62A1E 192AFA8A BC6BA6FE


    V is
                            AB725F55 F27890A4 8194D008 FFC961F5
        14AF792D F52A1B9D CF840FC7 FB528058 9537CC05 6797523F
        70670C9D F0AA161B B735C3D0 3ECF4A52 60FB9775 AA1D69BA


**************************************************************

HMAC_DRBG_Generate

  requested_number_of_bits = 1024

    additional_input is  <empty>

  ------------

    V = HMAC(K, V) is
                            7ED41B9C FDC8C256 83BBB4C5 53CC2DC6
        1F690E62 ABC9F038 A16B8C51 9690CABE BD1B5C19 6C57CF75
        9BB9871B E0C163A5 7315EA96 F615136D 064572F0 9F26D659
```

```
    temp is
                          7ED41B9C FDC8C256 83BBB4C5 53CC2DC6
        1F690E62 ABC9F038 A16B8C51 9690CABE BD1B5C19 6C57CF75
        9BB9871B E0C163A5 7315EA96 F615136D 064572F0 9F26D659


  ------------

    V = HMAC(K, V) is
                          D24211F9 610FFCDF FDA8CE23 FFA96735
        75951826 60877766 035EED80 0B05364C E324A75E B63FD9B3
        EED956D1 47480B1D 0A42DF8A A990BB62 8666F6F6 1D60CBE2


    temp is
                                                 7ED41B9C FDC8C256
        83BBB4C5 53CC2DC6 1F690E62 ABC9F038 A16B8C51 9690CABE
        BD1B5C19 6C57CF75 9BB9871B E0C163A5 7315EA96 F615136D
        064572F0 9F26D659 D24211F9 610FFCDF FDA8CE23 FFA96735
        75951826 60877766 035EED80 0B05364C E324A75E B63FD9B3
        EED956D1 47480B1D 0A42DF8A A990BB62 8666F6F6 1D60CBE2


---------------------------

  returned_bits is
                                                 7ED41B9C FDC8C256
        83BBB4C5 53CC2DC6 1F690E62 ABC9F038 A16B8C51 9690CABE
        BD1B5C19 6C57CF75 9BB9871B E0C163A5 7315EA96 F615136D
        064572F0 9F26D659 D24211F9 610FFCDF FDA8CE23 FFA96735
        75951826 60877766 035EED80 0B05364C E324A75E B63FD9B3
        EED956D1 47480B1D 0A42DF8A A990BB62 8666F6F6 1D60CBE2


  call Update(additional_input, K, V)
---------------------------

  Update

    provided_data <empty>

    ------------

    V || 0x00 || provided_data is
```

```
                    D2 4211F961 0FFCDFFD A8CE23FF A9673575
        95182660 87776603 5EED800B 05364CE3 24A75EB6 3FD9B3EE
        D956D147 480B1D0A 42DF8AA9 90BB6286 66F6F61D 60CBE200


    K = HMAC(K, V || 0x00 || provided_data) is
                        0F5F718A 5EA08533 1A00665B 781DD9CC
        0A57758A 99FD23D9 3DA2728E 714E13B7 9FB414AF AED8385D
        A5AEDF23 5B67A398 E68D15C9 76FE1083 8A672844 C1CF01FF


    V = HMAC(K, V) is
                        6DF16C1A 6B6ADD93 725F4D0E F83559CE
        0CB0EFE2 20298503 160A3AC1 16F6FCF6 79B5FF05 B6331D81
        F48796CC 5B937577 360A64F1 404DE16F D02913C6 AB7AEC44


rnd_val is
                                            7ED41B9C FDC8C256
        83BBB4C5 53CC2DC6 1F690E62 ABC9F038 A16B8C51 9690CABE
        BD1B5C19 6C57CF75 9BB9871B E0C163A5 7315EA96 F615136D
        064572F0 9F26D659 D24211F9 610FFCDF FDA8CE23 FFA96735
        75951826 60877766 035EED80 0B05364C E324A75E B63FD9B3
        EED956D1 47480B1D 0A42DF8A A990BB62 8666F6F6 1D60CBE2
```