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

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString = <empty>

    AdditionalInput = <empty>

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

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

  Update

    provided_data is
```

                                                    00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000

      V is
                                              00000000 00000001

Block #1
Blockin   00000000 00000001
Blockout 166B40B4 4ABA4BD6

      output_block is
                                              166B40B4 4ABA4BD6

      temp is
                                              166B40B4 4ABA4BD6

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000

      V is
                                              00000000 00000002

Block #1
Blockin   00000000 00000002
Blockout 06E7EA22 CE92708F

      output_block is
                                              06E7EA22 CE92708F

```
      temp is
                          166B40B4 4ABA4BD6 06E7EA22 CE92708F


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004


Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE
```

```
      output_block is
                                                D2FD8867 D50D2DFE


      temp is
                                                166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    16 6A42B74E
        BF4DD10E EEE029C2 9F7E805E A082DAB6 EF008BCA E4927CC9


    Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


    V is
                                                EF008BCA E4927CC9


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   EF008BCA E4927CCA
Blockout  077AF02D 5209B1A5

Block #1
Blockin   EF008BCA E4927CCB
Blockout  9086A90A F689863D

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

  Update
```

```
    provided_data is
                                                          00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCC


Block #1
Blockin   EF008BCA E4927CCC
Blockout  EAB6F0C7 2B1C15A6

      output_block is
                                              EAB6F0C7 2B1C15A6


      temp is
                                              EAB6F0C7 2B1C15A6


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

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCD


Block #1
Blockin   EF008BCA E4927CCD
Blockout  EE7244FC AB83AF9D

      output_block is
```

```
                                          EE7244FC AB83AF9D


      temp is
                          EAB6F0C7 2B1C15A6 EE7244FC AB83AF9D


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

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                          EF008BCA E4927CCE


Block #1
Blockin   EF008BCA E4927CCE
Blockout  17590CC9 C26E5A9F

      output_block is
                                          17590CC9 C26E5A9F


      temp is
        EAB6F0C7 2B1C15A6 EE7244FC AB83AF9D 17590CC9 C26E5A9F


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

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                          EF008BCA E4927CCF


Block #1
Blockin   EF008BCA E4927CCF
Blockout  4D86DE41 4EC7B6C5
```

```
      output_block is
                                              4D86DE41 4EC7B6C5


      temp is
                                              EAB6F0C7 2B1C15A6
        EE7244FC AB83AF9D 17590CC9 C26E5A9F 4D86DE41 4EC7B6C5


    temp XOR provided_data is
                                                    EA B6F0C72B
        1C15A6EE 7244FCAB 83AF9D17 590CC9C2 6E5A9F4D 86DE414E


    Key is
              EA B6F0C72B 1C15A6EE 7244FCAB 83AF9D17 590CC9C2


    V is
                                              6E5A9F4D 86DE414E


rnd_val is
                          077AF02D 5209B1A5 9086A90A F689863D


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   6E5A9F4D 86DE414F
Blockout  C78CC305 D0D238C9

Block #1
Blockin   6E5A9F4D 86DE4150
Blockout  AA647225 6FFFD0F9
```

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

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
              EA B6F0C72B 1C15A6EE 7244FCAB 83AF9D17 590CC9C2


      V is
                                            6E5A9F4D 86DE4151


Block #1
Blockin   6E5A9F4D 86DE4151
Blockout  CE5FE609 AF2D3242

      output_block is
                                            CE5FE609 AF2D3242


      temp is
                                            CE5FE609 AF2D3242


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

      While loop

      Key is
              EA B6F0C72B 1C15A6EE 7244FCAB 83AF9D17 590CC9C2


      V is
                                            6E5A9F4D 86DE4152
```

```
Block #1
Blockin   6E5A9F4D 86DE4152
Blockout  7442F203 B9DDC978

      output_block is
                                            7442F203 B9DDC978


      temp is
                          CE5FE609 AF2D3242 7442F203 B9DDC978


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

      While loop

      Key is
              EA B6F0C72B 1C15A6EE 7244FCAB 83AF9D17 590CC9C2


      V is
                                            6E5A9F4D 86DE4153


Block #1
Blockin   6E5A9F4D 86DE4153
Blockout  9B716E25 1D1AB17F

      output_block is
                                            9B716E25 1D1AB17F


      temp is
        CE5FE609 AF2D3242 7442F203 B9DDC978 9B716E25 1D1AB17F


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

      While loop

      Key is
              EA B6F0C72B 1C15A6EE 7244FCAB 83AF9D17 590CC9C2


      V is
                                            6E5A9F4D 86DE4154
```

```
Block #1
Blockin   6E5A9F4D 86DE4154
Blockout  BF160986 91AD7250

      output_block is
                                              BF160986 91AD7250


      temp is
                                              CE5FE609 AF2D3242
        7442F203 B9DDC978 9B716E25 1D1AB17F BF160986 91AD7250


    temp XOR provided_data is
                                                    CE 5FE609AF
        2D324274 42F203B9 DDC9789B 716E251D 1AB17FBF 16098691


    Key is
              CE 5FE609AF 2D324274 42F203B9 DDC9789B 716E251D


    V is
                                              1AB17FBF 16098691


rnd_val is
                          C78CC305 D0D238C9 AA647225 6FFFD0F9


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

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                    00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                    80 81828384
```

```
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    AdditionalInput2 =
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

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

  Update

    provided_data is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


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

```
      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                              166B40B4 4ABA4BD6


      temp is
                                              166B40B4 4ABA4BD6


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000002


Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F

      output_block is
                                              06E7EA22 CE92708F


      temp is
                           166B40B4 4ABA4BD6 06E7EA22 CE92708F
```

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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004


Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                              D2FD8867 D50D2DFE


      temp is
                                              166B40B4 4ABA4BD6
```

```
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    16 6A42B74E
        BF4DD10E EEE029C2 9F7E805E A082DAB6 EF008BCA E4927CC9


    Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


    V is
                                               EF008BCA E4927CC9


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                    60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                                                    60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


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

      While loop

      Key is
```

```
               16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCA


Block #1
Blockin   EF008BCA E4927CCA
Blockout  077AF02D 5209B1A5

      output_block is
                                              077AF02D 5209B1A5


      temp is
                                              077AF02D 5209B1A5


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

      While loop

      Key is
               16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCB


Block #1
Blockin   EF008BCA E4927CCB
Blockout  9086A90A F689863D

      output_block is
                                              9086A90A F689863D


      temp is
                           077AF02D 5209B1A5 9086A90A F689863D


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

      While loop
```

```
      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCC


Block #1
Blockin   EF008BCA E4927CCC
Blockout  EAB6F0C7 2B1C15A6

      output_block is
                                              EAB6F0C7 2B1C15A6


      temp is
        077AF02D 5209B1A5 9086A90A F689863D EAB6F0C7 2B1C15A6


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

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCD


Block #1
Blockin   EF008BCA E4927CCD
Blockout  EE7244FC AB83AF9D

      output_block is
                                              EE7244FC AB83AF9D


      temp is
                                              077AF02D 5209B1A5
        9086A90A F689863D EAB6F0C7 2B1C15A6 EE7244FC AB83AF9D
```

```
    temp XOR provided_data is
                                                        67 1B924E36
        6CD7C2F8 EFC3619A E4E8529A C782B45F 6963D196 0B3E87D7


    Key is
              67 1B924E36 6CD7C2F8 EFC3619A E4E8529A C782B45F


    V is
                                            6963D196 0B3E87D7


Block #1
Blockin   6963D196 0B3E87D8
Blockout  D3A44CA8 439CAC8D

Block #1
Blockin   6963D196 0B3E87D9
Blockout  9C7F4B1D B7977D4B

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

  Update

    provided_data is
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


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

      While loop

      Key is
              67 1B924E36 6CD7C2F8 EFC3619A E4E8529A C782B45F


      V is
                                            6963D196 0B3E87DA


Block #1
Blockin   6963D196 0B3E87DA
Blockout  B3A95F1C 6EC4A19F
```

```
      output_block is
                                              B3A95F1C 6EC4A19F

      temp is
                                              B3A95F1C 6EC4A19F

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

      While loop

      Key is
              67 1B924E36 6CD7C2F8 EFC3619A E4E8529A C782B45F

      V is
                                              6963D196 0B3E87DB

Block #1
Blockin   6963D196 0B3E87DB
Blockout  59A27ECD AD663B97

      output_block is
                                              59A27ECD AD663B97

      temp is
                           B3A95F1C 6EC4A19F 59A27ECD AD663B97

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

      While loop

      Key is
              67 1B924E36 6CD7C2F8 EFC3619A E4E8529A C782B45F

      V is
                                              6963D196 0B3E87DC

Block #1
Blockin   6963D196 0B3E87DC
```

```
Blockout  685B44F5 AD20D28D

      output_block is
                                              685B44F5 AD20D28D


      temp is
        B3A95F1C 6EC4A19F 59A27ECD AD663B97 685B44F5 AD20D28D


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

      While loop

      Key is
              67 1B924E36 6CD7C2F8 EFC3619A E4E8529A C782B45F


      V is
                                              6963D196 0B3E87DD


Block #1
Blockin   6963D196 0B3E87DD
Blockout  7E4FCAB4 F9C8AA63

      output_block is
                                              7E4FCAB4 F9C8AA63


      temp is
                                              B3A95F1C 6EC4A19F
        59A27ECD AD663B97 685B44F5 AD20D28D 7E4FCAB4 F9C8AA63


    temp XOR provided_data is
                                                    D3 C83D7F0A
        A1C7F831 CB14A6C1 0B55F818 2A3686D9 55A4FA06 36B0CF85


    Key is
              D3 C83D7F0A A1C7F831 CB14A6C1 0B55F818 2A3686D9


    V is
                                              55A4FA06 36B0CF85
```

```
rnd_val is
                          D3A44CA8 439CAC8D 9C7F4B1D B7977D4B


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


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

      While loop

      Key is
              D3 C83D7F0A A1C7F831 CB14A6C1 0B55F818 2A3686D9


      V is
                                           55A4FA06 36B0CF86


Block #1
Blockin   55A4FA06 36B0CF86
Blockout  5B50FA3E 59CE4714
```

```
      output_block is
                                              5B50FA3E 59CE4714

      temp is
                                              5B50FA3E 59CE4714

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

      While loop

      Key is
              D3 C83D7F0A A1C7F831 CB14A6C1 0B55F818 2A3686D9

      V is
                                              55A4FA06 36B0CF87

Block #1
Blockin   55A4FA06 36B0CF87
Blockout  2CE9013E B8892D71

      output_block is
                                              2CE9013E B8892D71

      temp is
                           5B50FA3E 59CE4714 2CE9013E B8892D71

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

      While loop

      Key is
              D3 C83D7F0A A1C7F831 CB14A6C1 0B55F818 2A3686D9

      V is
                                              55A4FA06 36B0CF88

Block #1
```

```
Blockin   55A4FA06 36B0CF88
Blockout  B756CBA9 99789C53

      output_block is
                                              B756CBA9 99789C53


      temp is
        5B50FA3E 59CE4714 2CE9013E B8892D71 B756CBA9 99789C53


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

      While loop

      Key is
              D3 C83D7F0A A1C7F831 CB14A6C1 0B55F818 2A3686D9


      V is
                                              55A4FA06 36B0CF89


Block #1
Blockin   55A4FA06 36B0CF89
Blockout  BD263872 5913FAC6

      output_block is
                                              BD263872 5913FAC6


      temp is
                                              5B50FA3E 59CE4714
        2CE9013E B8892D71 B756CBA9 99789C53 BD263872 5913FAC6


    temp XOR provided_data is
                                                    FB F1589DFD
        6BE1B384 40AB9514 2483DE07 E7791A2D CD2AE405 9F82C9E5


    Key is
              FB F1589DFD 6BE1B384 40AB9514 2483DE07 E7791A2D


    V is
```

```
                                                CD2AE405 9F82C9E5


Block #1
Blockin   CD2AE405 9F82C9E6
Blockout  E2810D58 E9457F8E

Block #1
Blockin   CD2AE405 9F82C9E7
Blockout  A0CA4C31 C4F5FB9B

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

  Update

    provided_data is
                                                          A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


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

      While loop

      Key is
              FB F1589DFD 6BE1B384 40AB9514 2483DE07 E7791A2D


      V is
                                                CD2AE405 9F82C9E8


Block #1
Blockin   CD2AE405 9F82C9E8
Blockout  E48D768A DC9C8A48

      output_block is
                                                E48D768A DC9C8A48


      temp is
                                                E48D768A DC9C8A48


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

```
      While loop

      Key is
              FB F1589DFD 6BE1B384 40AB9514 2483DE07 E7791A2D


      V is
                                           CD2AE405 9F82C9E9


Block #1
Blockin   CD2AE405 9F82C9E9
Blockout  EAC5967B B723FAE2

      output_block is
                                           EAC5967B B723FAE2


      temp is
                          E48D768A DC9C8A48 EAC5967B B723FAE2


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

      While loop

      Key is
              FB F1589DFD 6BE1B384 40AB9514 2483DE07 E7791A2D


      V is
                                           CD2AE405 9F82C9EA


Block #1
Blockin   CD2AE405 9F82C9EA
Blockout  E53CC977 3188535E

      output_block is
                                           E53CC977 3188535E


      temp is
        E48D768A DC9C8A48 EAC5967B B723FAE2 E53CC977 3188535E
```

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

      While loop

      Key is
              FB F1589DFD 6BE1B384 40AB9514 2483DE07 E7791A2D


      V is
                                            CD2AE405 9F82C9EB


Block #1
Blockin   CD2AE405 9F82C9EB
Blockout  C25E1469 F39D4938

      output_block is
                                            C25E1469 F39D4938


      temp is
                                            E48D768A DC9C8A48
        EAC5967B B723FAE2 E53CC977 3188535E C25E1469 F39D4938


    temp XOR provided_data is
                                                  44 2CD42978
        392CEF42 6C3CD01B 8E544D55 8D7BC485 3DE5E97A E7AED24F


    Key is
              44 2CD42978 392CEF42 6C3CD01B 8E544D55 8D7BC485


    V is
                                            3DE5E97A E7AED24F


rnd_val is
                          E2810D58 E9457F8E A0CA4C31 C4F5FB9B


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

CTR_DRBG
```

```
    Requested Security Strength = 112

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString =
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    AdditionalInput = <empty>

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    prediction_resistance_flag = "No PredictionResistance"

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

  Update
```

```
    provided_data is
                                                        40 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                              166B40B4 4ABA4BD6


      temp is
                                              166B40B4 4ABA4BD6


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000002


Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F
```

```
      output_block is
                                              06E7EA22 CE92708F


      temp is
                           166B40B4 4ABA4BD6 06E7EA22 CE92708F


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004


Block #1
Blockin   00000000 00000004
```

```
Blockout  D2FD8867 D50D2DFE

      output_block is
                                              D2FD8867 D50D2DFE


      temp is
                                              166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    56 2B00F40A
        FA0B9646 A7AA628E D230CF0E F1D089E2 BA56DC92 BDC82795


    Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


    V is
                                              BA56DC92 BDC82795


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   BA56DC92 BDC82796
Blockout  9E0082B6 B55E3596

Block #1
Blockin   BA56DC92 BDC82797
Blockout  F1A82251 90390124

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

```
  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                            BA56DC92 BDC82798


Block #1
Blockin   BA56DC92 BDC82798
Blockout  24C9B2C0 8D487353

      output_block is
                                            24C9B2C0 8D487353


      temp is
                                            24C9B2C0 8D487353


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

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                            BA56DC92 BDC82799


Block #1
Blockin   BA56DC92 BDC82799
Blockout  32269D08 E3F6F53A
```

```
      output_block is
                                              32269D08 E3F6F53A


      temp is
                           24C9B2C0 8D487353 32269D08 E3F6F53A


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

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                              BA56DC92 BDC8279A


Block #1
Blockin   BA56DC92 BDC8279A
Blockout  D10536CA 74513299

      output_block is
                                              D10536CA 74513299


      temp is
        24C9B2C0 8D487353 32269D08 E3F6F53A D10536CA 74513299


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

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                              BA56DC92 BDC8279B


Block #1
```

```
Blockin   BA56DC92 BDC8279B
Blockout  632447C4 C43BCD57

      output_block is
                                              632447C4 C43BCD57


      temp is
                                              24C9B2C0 8D487353
        32269D08 E3F6F53A D10536CA 74513299 632447C4 C43BCD57


    temp XOR provided_data is
                                                    24 C9B2C08D
        48735332 269D08E3 F6F53AD1 0536CA74 51329963 2447C4C4


    Key is
              24 C9B2C08D 48735332 269D08E3 F6F53AD1 0536CA74


    V is
                                              51329963 2447C4C4


rnd_val is
                          9E0082B6 B55E3596 F1A82251 90390124


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   51329963 2447C4C5
Blockout  BA17E856 88D12FDB

Block #1
```

```
Blockin   51329963 2447C4C6
Blockout  B9296F01 C7F97982

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

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
              24 C9B2C08D 48735332 269D08E3 F6F53AD1 0536CA74


      V is
                                            51329963 2447C4C7


Block #1
Blockin   51329963 2447C4C7
Blockout  C526F53C CC8E279E

      output_block is
                                            C526F53C CC8E279E


      temp is
                                            C526F53C CC8E279E


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

      While loop

      Key is
              24 C9B2C08D 48735332 269D08E3 F6F53AD1 0536CA74


      V is
                                            51329963 2447C4C8
```

```
Block #1
Blockin   51329963 2447C4C8
Blockout  9D51CA87 116B0930

      output_block is
                                              9D51CA87 116B0930


      temp is
                           C526F53C CC8E279E 9D51CA87 116B0930


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

      While loop

      Key is
              24 C9B2C08D 48735332 269D08E3 F6F53AD1 0536CA74


      V is
                                              51329963 2447C4C9


Block #1
Blockin   51329963 2447C4C9
Blockout  1001A638 3943F879

      output_block is
                                              1001A638 3943F879


      temp is
        C526F53C CC8E279E 9D51CA87 116B0930 1001A638 3943F879


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

      While loop

      Key is
              24 C9B2C08D 48735332 269D08E3 F6F53AD1 0536CA74
```

```
      V is
                                                51329963 2447C4CA


Block #1
Blockin   51329963 2447C4CA
Blockout  BCAC8FEB CDCF0E5C

      output_block is
                                                BCAC8FEB CDCF0E5C


      temp is
                                                C526F53C CC8E279E
        9D51CA87 116B0930 1001A638 3943F879 BCAC8FEB CDCF0E5C


    temp XOR provided_data is
                                                        C5 26F53CCC
        8E279E9D 51CA8711 6B093010 01A63839 43F879BC AC8FEBCD


    Key is
              C5 26F53CCC 8E279E9D 51CA8711 6B093010 01A63839


    V is
                                                43F879BC AC8FEBCD


rnd_val is
                          BA17E856 88D12FDB B9296F01 C7F97982


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

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C
```

```
    EntropyInput1 (for Reseed1) =
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString =
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    AdditionalInput1 =
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    AdditionalInput2 =
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    prediction_resistance_flag = "No PredictionResistance"

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

  Update
```

```
    provided_data is
                                                        40 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                              166B40B4 4ABA4BD6


      temp is
                                              166B40B4 4ABA4BD6


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000002


Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F
```

```
      output_block is
                                              06E7EA22 CE92708F


      temp is
                           166B40B4 4ABA4BD6 06E7EA22 CE92708F


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004


Block #1
Blockin   00000000 00000004
```

```
Blockout  D2FD8867 D50D2DFE

      output_block is
                                                D2FD8867 D50D2DFE


      temp is
                                                166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                        56 2B00F40A
        FA0B9646 A7AA628E D230CF0E F1D089E2 BA56DC92 BDC82795


    Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


    V is
                                                BA56DC92 BDC82795


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                                                        60 61626364
```

```
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


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

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                            BA56DC92 BDC82796


Block #1
Blockin   BA56DC92 BDC82796
Blockout  9E0082B6 B55E3596

      output_block is
                                            9E0082B6 B55E3596


      temp is
                                            9E0082B6 B55E3596


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

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                            BA56DC92 BDC82797


Block #1
Blockin   BA56DC92 BDC82797
Blockout  F1A82251 90390124

      output_block is
                                            F1A82251 90390124
```

```
      temp is
                          9E0082B6 B55E3596 F1A82251 90390124


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

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                              BA56DC92 BDC82798


Block #1
Blockin   BA56DC92 BDC82798
Blockout  24C9B2C0 8D487353

      output_block is
                                              24C9B2C0 8D487353


      temp is
        9E0082B6 B55E3596 F1A82251 90390124 24C9B2C0 8D487353


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

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                              BA56DC92 BDC82799


Block #1
Blockin   BA56DC92 BDC82799
Blockout  32269D08 E3F6F53A

      output_block is
```

```
                                                32269D08 E3F6F53A


      temp is
                                                9E0082B6 B55E3596
        F1A82251 90390124 24C9B2C0 8D487353 32269D08 E3F6F53A


    temp XOR provided_data is
                                                      FE 61E0D5D1
        3B53F199 C1483AFC 546F4B54 B8C0B3F9 3D05244A 5FE7739F


    Key is
              FE 61E0D5D1 3B53F199 C1483AFC 546F4B54 B8C0B3F9


    V is
                                                3D05244A 5FE7739F


Block #1
Blockin   3D05244A 5FE773A0
Blockout  5921C494 636A6CED

Block #1
Blockin   3D05244A 5FE773A1
Blockout  D3079514 F23B4A5B

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

  Update

    provided_data is
                                                      60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


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

      While loop

      Key is
              FE 61E0D5D1 3B53F199 C1483AFC 546F4B54 B8C0B3F9
```

```
      V is
                                              3D05244A 5FE773A2


Block #1
Blockin   3D05244A 5FE773A2
Blockout  49F68905 3BC4B2CE

      output_block is
                                              49F68905 3BC4B2CE


      temp is
                                              49F68905 3BC4B2CE


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

      While loop

      Key is
              FE 61E0D5D1 3B53F199 C1483AFC 546F4B54 B8C0B3F9


      V is
                                              3D05244A 5FE773A3


Block #1
Blockin   3D05244A 5FE773A3
Blockout  68B8303E 421FD382

      output_block is
                                              68B8303E 421FD382


      temp is
                           49F68905 3BC4B2CE 68B8303E 421FD382


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

      While loop

      Key is
              FE 61E0D5D1 3B53F199 C1483AFC 546F4B54 B8C0B3F9
```

```
      V is
                                              3D05244A 5FE773A4


Block #1
Blockin   3D05244A 5FE773A4
Blockout  CD61931B F8341BBB

      output_block is
                                              CD61931B F8341BBB


      temp is
        49F68905 3BC4B2CE 68B8303E 421FD382 CD61931B F8341BBB


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

      While loop

      Key is
              FE 61E0D5D1 3B53F199 C1483AFC 546F4B54 B8C0B3F9


      V is
                                              3D05244A 5FE773A5


Block #1
Blockin   3D05244A 5FE773A5
Blockout  F4341AF3 BC9D9757

      output_block is
                                              F4341AF3 BC9D9757


      temp is
                                              49F68905 3BC4B2CE
        68B8303E 421FD382 CD61931B F8341BBB F4341AF3 BC9D9757


    temp XOR provided_data is
                                                    29 97EB665F
        A1D4A900 D15A552E 72BDEDBD 10E1688C 416DCC8C 4D6088C0
```

```
    Key is
              29 97EB665F A1D4A900 D15A552E 72BDEDBD 10E1688C

    V is
                                           416DCC8C 4D6088C0

rnd_val is
                          5921C494 636A6CED D3079514 F23B4A5B

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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


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

      While loop

      Key is
              29 97EB665F A1D4A900 D15A552E 72BDEDBD 10E1688C
```

```
      V is
                                              416DCC8C 4D6088C1


Block #1
Blockin   416DCC8C 4D6088C1
Blockout  96BEB0B1 4A625631

      output_block is
                                              96BEB0B1 4A625631


      temp is
                                              96BEB0B1 4A625631


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

      While loop

      Key is
              29 97EB665F A1D4A900 D15A552E 72BDEDBD 10E1688C


      V is
                                              416DCC8C 4D6088C2


Block #1
Blockin   416DCC8C 4D6088C2
Blockout  77B10223 8E2FAAB7

      output_block is
                                              77B10223 8E2FAAB7


      temp is
                           96BEB0B1 4A625631 77B10223 8E2FAAB7


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

      While loop

      Key is
```

```
              29 97EB665F A1D4A900 D15A552E 72BDEDBD 10E1688C


      V is
                                              416DCC8C 4D6088C3


Block #1
Blockin   416DCC8C 4D6088C3
Blockout  4D4069A0 F468844C

      output_block is
                                              4D4069A0 F468844C


      temp is
        96BEB0B1 4A625631 77B10223 8E2FAAB7 4D4069A0 F468844C


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

      While loop

      Key is
              29 97EB665F A1D4A900 D15A552E 72BDEDBD 10E1688C


      V is
                                              416DCC8C 4D6088C4


Block #1
Blockin   416DCC8C 4D6088C4
Blockout  6DC395B6 353CC34E

      output_block is
                                              6DC395B6 353CC34E


      temp is
                                              96BEB0B1 4A625631
        77B10223 8E2FAAB7 4D4069A0 F468844C 6DC395B6 353CC34E


    temp XOR provided_data is
                                                    36 1F1212EE
```

```
        C7F096DF 18A88822 820418FD F1DB1340 DD32FBD5 7A2F0D89


    Key is
              36 1F1212EE C7F096DF 18A88822 820418FD F1DB1340


    V is
                                              DD32FBD5 7A2F0D89


Block #1
Blockin   DD32FBD5 7A2F0D8A
Blockout  D29F87DD 6FB87281

Block #1
Blockin   DD32FBD5 7A2F0D8B
Blockout  458BADBF 4BDB0F7E

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

  Update

    provided_data is
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


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

      While loop

      Key is
              36 1F1212EE C7F096DF 18A88822 820418FD F1DB1340


      V is
                                              DD32FBD5 7A2F0D8C


Block #1
Blockin   DD32FBD5 7A2F0D8C
Blockout  44F1F033 77093092

      output_block is
                                              44F1F033 77093092
```

```
      temp is
                                              44F1F033 77093092


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

      While loop

      Key is
              36 1F1212EE C7F096DF 18A88822 820418FD F1DB1340


      V is
                                              DD32FBD5 7A2F0D8D


Block #1
Blockin   DD32FBD5 7A2F0D8D
Blockout  284D9C6D 8FEC404D

      output_block is
                                              284D9C6D 8FEC404D


      temp is
                           44F1F033 77093092 284D9C6D 8FEC404D


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

      While loop

      Key is
              36 1F1212EE C7F096DF 18A88822 820418FD F1DB1340


      V is
                                              DD32FBD5 7A2F0D8E


Block #1
Blockin   DD32FBD5 7A2F0D8E
Blockout  067FF694 A9067966
```

```
      output_block is
                                              067FF694 A9067966

      temp is
        44F1F033 77093092 284D9C6D 8FEC404D 067FF694 A9067966

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

      While loop

      Key is
              36 1F1212EE C7F096DF 18A88822 820418FD F1DB1340

      V is
                                              DD32FBD5 7A2F0D8F


Block #1
Blockin   DD32FBD5 7A2F0D8F
Blockout  612A3FC4 914148F2

      output_block is
                                              612A3FC4 914148F2

      temp is
                                              44F1F033 77093092
        284D9C6D 8FEC404D 067FF694 A9067966 612A3FC4 914148F2

    temp XOR provided_data is
                                                    E4 505290D3
        AC963580 E436C623 41EEE2B6 CE44271D B3CFD1D9 93857F2D

    Key is
              E4 505290D3 AC963580 E436C623 41EEE2B6 CE44271D

    V is
                                              B3CFD1D9 93857F2D
```

```
rnd_val is
                          D29F87DD 6FB87281 458BADBF 4BDB0F7E


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

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                      00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                      80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                      C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString = <empty>

    AdditionalInput = <empty>

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                      00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

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

```
  Update

    provided_data is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                              166B40B4 4ABA4BD6


      temp is
                                              166B40B4 4ABA4BD6


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000002


Block #1
Blockin   00000000 00000002
```

```
Blockout  06E7EA22 CE92708F

      output_block is
                                              06E7EA22 CE92708F


      temp is
                           166B40B4 4ABA4BD6 06E7EA22 CE92708F


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004
```

```
Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                              D2FD8867 D50D2DFE


      temp is
                                              166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    16 6A42B74E
        BF4DD10E EEE029C2 9F7E805E A082DAB6 EF008BCA E4927CC9


    Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


    V is
                                              EF008BCA E4927CC9


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

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

CTR_DRBG_Reseed

    entropy_input is
                                                    80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C
```

```
    additional_input is  <empty>

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

  Update

    provided_data is
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


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

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                            EF008BCA E4927CCA


Block #1
Blockin   EF008BCA E4927CCA
Blockout  077AF02D 5209B1A5

      output_block is
                                            077AF02D 5209B1A5


      temp is
                                            077AF02D 5209B1A5


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

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
```

```
                                            EF008BCA E4927CCB


Block #1
Blockin   EF008BCA E4927CCB
Blockout  9086A90A F689863D

      output_block is
                                            9086A90A F689863D


      temp is
                          077AF02D 5209B1A5 9086A90A F689863D


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

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                            EF008BCA E4927CCC


Block #1
Blockin   EF008BCA E4927CCC
Blockout  EAB6F0C7 2B1C15A6

      output_block is
                                            EAB6F0C7 2B1C15A6


      temp is
        077AF02D 5209B1A5 9086A90A F689863D EAB6F0C7 2B1C15A6


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

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6
```

```
      V is
                                              EF008BCA E4927CCD


Block #1
Blockin   EF008BCA E4927CCD
Blockout  EE7244FC AB83AF9D

      output_block is
                                              EE7244FC AB83AF9D


      temp is
                                              077AF02D 5209B1A5
        9086A90A F689863D EAB6F0C7 2B1C15A6 EE7244FC AB83AF9D


    temp XOR provided_data is
                                                    87 FB72AED6
        8C372218 0F23817A 0408B27A 276254BF 89833176 EBDE6737


    Key is
              87 FB72AED6 8C372218 0F23817A 0408B27A 276254BF


    V is
                                              89833176 EBDE6737


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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   89833176 EBDE6738
Blockout  76FFEB64 F39FD9DC

Block #1
Blockin   89833176 EBDE6739
Blockout  F407C209 7083158B
```

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

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
              87 FB72AED6 8C372218 0F23817A 0408B27A 276254BF


      V is
                                            89833176 EBDE673A


Block #1
Blockin   89833176 EBDE673A
Blockout  3C51738A 731CB88E

      output_block is
                                            3C51738A 731CB88E


      temp is
                                            3C51738A 731CB88E


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

      While loop

      Key is
              87 FB72AED6 8C372218 0F23817A 0408B27A 276254BF


      V is
                                            89833176 EBDE673B
```

```
Block #1
Blockin   89833176 EBDE673B
Blockout  C38C7074 F18E0A77

      output_block is
                                            C38C7074 F18E0A77


      temp is
                          3C51738A 731CB88E C38C7074 F18E0A77


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

      While loop

      Key is
              87 FB72AED6 8C372218 0F23817A 0408B27A 276254BF


      V is
                                            89833176 EBDE673C


Block #1
Blockin   89833176 EBDE673C
Blockout  56212CE3 D47B1446

      output_block is
                                            56212CE3 D47B1446


      temp is
        3C51738A 731CB88E C38C7074 F18E0A77 56212CE3 D47B1446


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

      While loop

      Key is
              87 FB72AED6 8C372218 0F23817A 0408B27A 276254BF


      V is
                                            89833176 EBDE673D
```

```
Block #1
Blockin   89833176 EBDE673D
Blockout  1A276E83 72B83722

      output_block is
                                            1A276E83 72B83722


      temp is
                                            3C51738A 731CB88E
        C38C7074 F18E0A77 56212CE3 D47B1446 1A276E83 72B83722


    temp XOR provided_data is
                                                  3C 51738A73
        1CB88EC3 8C7074F1 8E0A7756 212CE3D4 7B14461A 276E8372


    Key is
              3C 51738A73 1CB88EC3 8C7074F1 8E0A7756 212CE3D4


    V is
                                            7B14461A 276E8372


rnd_val is
                          76FFEB64 F39FD9DC F407C209 7083158B


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

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

```
CTR_DRBG_Reseed

    entropy_input is
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    additional_input is  <empty>

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

  Update

    provided_data is
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


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

      While loop

      Key is
              3C 51738A73 1CB88EC3 8C7074F1 8E0A7756 212CE3D4


      V is
                                              7B14461A 276E8373


Block #1
Blockin   7B14461A 276E8373
Blockout  D866B305 601C7577

      output_block is
                                              D866B305 601C7577


      temp is
                                              D866B305 601C7577


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

      While loop
```

```
      Key is
              3C 51738A73 1CB88EC3 8C7074F1 8E0A7756 212CE3D4


      V is
                                              7B14461A 276E8374


Block #1
Blockin   7B14461A 276E8374
Blockout  7ECE1C31 57A5271C

      output_block is
                                              7ECE1C31 57A5271C


      temp is
                           D866B305 601C7577 7ECE1C31 57A5271C


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

      While loop

      Key is
              3C 51738A73 1CB88EC3 8C7074F1 8E0A7756 212CE3D4


      V is
                                              7B14461A 276E8375


Block #1
Blockin   7B14461A 276E8375
Blockout  B2AB9F80 619B7DE9

      output_block is
                                              B2AB9F80 619B7DE9


      temp is
        D866B305 601C7577 7ECE1C31 57A5271C B2AB9F80 619B7DE9


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

```
      While loop

      Key is
              3C 51738A73 1CB88EC3 8C7074F1 8E0A7756 212CE3D4


      V is
                                             7B14461A 276E8376


Block #1
Blockin   7B14461A 276E8376
Blockout  89E3EDC9 23E5FAC0

      output_block is
                                             89E3EDC9 23E5FAC0


      temp is
                                             D866B305 601C7577
        7ECE1C31 57A5271C B2AB9F80 619B7DE9 89E3EDC9 23E5FAC0


    temp XOR provided_data is
                                                   18 A771C6A4
        D9B3B0B6 07D6FA9B 68E9D362 7A4D53B5 4EAB3E51 3A3712FF


    Key is
              18 A771C6A4 D9B3B0B6 07D6FA9B 68E9D362 7A4D53B5


    V is
                                             4EAB3E51 3A3712FF


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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
```

```
Blockin   4EAB3E51 3A371300
Blockout  D7A5955B 81F4EDA1

Block #1
Blockin   4EAB3E51 3A371301
Blockout  E1AE62DF 158FD0BC

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

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
              18 A771C6A4 D9B3B0B6 07D6FA9B 68E9D362 7A4D53B5


      V is
                                            4EAB3E51 3A371302


Block #1
Blockin   4EAB3E51 3A371302
Blockout  3D186644 E6B3E3B2

      output_block is
                                            3D186644 E6B3E3B2


      temp is
                                            3D186644 E6B3E3B2


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

      While loop

      Key is
              18 A771C6A4 D9B3B0B6 07D6FA9B 68E9D362 7A4D53B5
```

```
      V is
                                              4EAB3E51 3A371303


Block #1
Blockin   4EAB3E51 3A371303
Blockout  28A3A858 BE01177A

      output_block is
                                              28A3A858 BE01177A


      temp is
                           3D186644 E6B3E3B2 28A3A858 BE01177A


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

      While loop

      Key is
              18 A771C6A4 D9B3B0B6 07D6FA9B 68E9D362 7A4D53B5


      V is
                                              4EAB3E51 3A371304


Block #1
Blockin   4EAB3E51 3A371304
Blockout  2EB41D40 2C767A9D

      output_block is
                                              2EB41D40 2C767A9D


      temp is
        3D186644 E6B3E3B2 28A3A858 BE01177A 2EB41D40 2C767A9D


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

      While loop
```

```
      Key is
              18 A771C6A4 D9B3B0B6 07D6FA9B 68E9D362 7A4D53B5


      V is
                                             4EAB3E51 3A371305


Block #1
Blockin   4EAB3E51 3A371305
Blockout  A1D4FCFD 276AB6F8

      output_block is
                                             A1D4FCFD 276AB6F8


      temp is
                                             3D186644 E6B3E3B2
        28A3A858 BE01177A 2EB41D40 2C767A9D A1D4FCFD 276AB6F8


    temp XOR provided_data is
                                                   3D 186644E6
        B3E3B228 A3A858BE 01177A2E B41D402C 767A9DA1 D4FCFD27


    Key is
              3D 186644E6 B3E3B228 A3A858BE 01177A2E B41D402C


    V is
                                             767A9DA1 D4FCFD27


rnd_val is
                          D7A5955B 81F4EDA1 E1AE62DF 158FD0BC


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

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
```

```
                                                    00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                    80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                    C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                    60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    AdditionalInput2 =
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                    00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

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

  Update

    provided_data is
```

                                                    00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000

      V is
                                              00000000 00000001

Block #1
Blockin   00000000 00000001
Blockout 166B40B4 4ABA4BD6

      output_block is
                                              166B40B4 4ABA4BD6

      temp is
                                              166B40B4 4ABA4BD6

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000

      V is
                                              00000000 00000002

Block #1
Blockin   00000000 00000002
Blockout 06E7EA22 CE92708F

      output_block is
                                              06E7EA22 CE92708F

```
      temp is
                          166B40B4 4ABA4BD6 06E7EA22 CE92708F


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                              4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000004


Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE
```

```
      output_block is
                                                D2FD8867 D50D2DFE


      temp is
                                                166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    16 6A42B74E
        BF4DD10E EEE029C2 9F7E805E A082DAB6 EF008BCA E4927CC9


    Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


    V is
                                                EF008BCA E4927CC9


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                    60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


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

CTR_DRBG_Reseed

    entropy_input is
                                                    80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C
```

```
    additional_input is
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


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

  Update

    provided_data is
                                                        E0 E0E0E0E0
        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0

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

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCA


Block #1
Blockin   EF008BCA E4927CCA
Blockout  077AF02D 5209B1A5

      output_block is
                                              077AF02D 5209B1A5


      temp is
                                              077AF02D 5209B1A5


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

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6
```

```
      V is
                                              EF008BCA E4927CCB


Block #1
Blockin   EF008BCA E4927CCB
Blockout  9086A90A F689863D

      output_block is
                                              9086A90A F689863D


      temp is
                           077AF02D 5209B1A5 9086A90A F689863D


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

      While loop

      Key is
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCC


Block #1
Blockin   EF008BCA E4927CCC
Blockout  EAB6F0C7 2B1C15A6

      output_block is
                                              EAB6F0C7 2B1C15A6


      temp is
        077AF02D 5209B1A5 9086A90A F689863D EAB6F0C7 2B1C15A6


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

      While loop

      Key is
```

```
              16 6A42B74E BF4DD10E EEE029C2 9F7E805E A082DAB6


      V is
                                              EF008BCA E4927CCD


Block #1
Blockin   EF008BCA E4927CCD
Blockout  EE7244FC AB83AF9D

      output_block is
                                              EE7244FC AB83AF9D


      temp is
                                              077AF02D 5209B1A5
        9086A90A F689863D EAB6F0C7 2B1C15A6 EE7244FC AB83AF9D


    temp XOR provided_data is
                                                    E7 9A10CDB2
        E9514570 6649EA16 6966DD0A 561027CB FCF5460E 92A41C4B


    Key is
              E7 9A10CDB2 E9514570 6649EA16 6966DD0A 561027CB


    V is
                                              FCF5460E 92A41C4B


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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   FCF5460E 92A41C4C
Blockout  BA52044F 83558BC5

Block #1
```

```
Blockin   FCF5460E 92A41C4D
Blockout  2030A10E 475131CF

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

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
              E7 9A10CDB2 E9514570 6649EA16 6966DD0A 561027CB


      V is
                                            FCF5460E 92A41C4E


Block #1
Blockin   FCF5460E 92A41C4E
Blockout  2BE9E28C 8DC30D13

      output_block is
                                            2BE9E28C 8DC30D13


      temp is
                                            2BE9E28C 8DC30D13


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

      While loop

      Key is
              E7 9A10CDB2 E9514570 6649EA16 6966DD0A 561027CB


      V is
                                            FCF5460E 92A41C4F
```

```
Block #1
Blockin   FCF5460E 92A41C4F
Blockout  2259089D 9A42987D

      output_block is
                                              2259089D 9A42987D


      temp is
                           2BE9E28C 8DC30D13 2259089D 9A42987D


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

      While loop

      Key is
              E7 9A10CDB2 E9514570 6649EA16 6966DD0A 561027CB


      V is
                                              FCF5460E 92A41C50


Block #1
Blockin   FCF5460E 92A41C50
Blockout  FCAE2830 99B4966B

      output_block is
                                              FCAE2830 99B4966B


      temp is
        2BE9E28C 8DC30D13 2259089D 9A42987D FCAE2830 99B4966B


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

      While loop

      Key is
              E7 9A10CDB2 E9514570 6649EA16 6966DD0A 561027CB
```

```
      V is
                                                FCF5460E 92A41C51


Block #1
Blockin   FCF5460E 92A41C51
Blockout  4072AF99 75399510

      output_block is
                                                4072AF99 75399510


      temp is
                                                2BE9E28C 8DC30D13
        2259089D 9A42987D FCAE2830 99B4966B 4072AF99 75399510


    temp XOR provided_data is
                                                      2B E9E28C8D
        C30D1322 59089D9A 42987DFC AE283099 B4966B40 72AF9975


    Key is
              2B E9E28C8D C30D1322 59089D9A 42987DFC AE283099


    V is
                                                B4966B40 72AF9975


rnd_val is
                           BA52044F 83558BC5 2030A10E 475131CF


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                      A0 A1A2A3A4
```

```
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


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

CTR_DRBG_Reseed

    entropy_input is
                                                    C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    additional_input is
                                                    A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


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

  Update

    provided_data is
                                                    60 60606060
        60606060 60606060 60606060 60606060 60606060 60606060


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

      While loop

      Key is
              2B E9E28C8D C30D1322 59089D9A 42987DFC AE283099


      V is
                                            B4966B40 72AF9976


Block #1
Blockin   B4966B40 72AF9976
Blockout  EB82D768 1174B314

      output_block is
                                            EB82D768 1174B314
```

```
      temp is
                                              EB82D768 1174B314


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

      While loop

      Key is
              2B E9E28C8D C30D1322 59089D9A 42987DFC AE283099


      V is
                                              B4966B40 72AF9977


Block #1
Blockin   B4966B40 72AF9977
Blockout  298A9A80 7F7BBBE0

      output_block is
                                              298A9A80 7F7BBBE0


      temp is
                           EB82D768 1174B314 298A9A80 7F7BBBE0


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

      While loop

      Key is
              2B E9E28C8D C30D1322 59089D9A 42987DFC AE283099


      V is
                                              B4966B40 72AF9978


Block #1
Blockin   B4966B40 72AF9978
Blockout  B670F4C1 C1EB4DD0

      output_block is
```

```
                                              B670F4C1 C1EB4DD0


      temp is
        EB82D768 1174B314 298A9A80 7F7BBBE0 B670F4C1 C1EB4DD0


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

      While loop

      Key is
              2B E9E28C8D C30D1322 59089D9A 42987DFC AE283099


      V is
                                              B4966B40 72AF9979


Block #1
Blockin   B4966B40 72AF9979
Blockout  3EDD8281 FD1FCA15

      output_block is
                                              3EDD8281 FD1FCA15


      temp is
                                              EB82D768 1174B314
        298A9A80 7F7BBBE0 B670F4C1 C1EB4DD0 3EDD8281 FD1FCA15


    temp XOR provided_data is
                                                    8B E2B70871
        14D37449 EAFAE01F 1BDB80D6 1094A1A1 8B2DB05E BDE2E19D


    Key is
              8B E2B70871 14D37449 EAFAE01F 1BDB80D6 1094A1A1


    V is
                                              8B2DB05E BDE2E19D


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

```
CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   8B2DB05E BDE2E19E
Blockout  D6EC2A7F B7375E40

Block #1
Blockin   8B2DB05E BDE2E19F
Blockout  C3E6B5C3 6484B2DF

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

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
              8B E2B70871 14D37449 EAFAE01F 1BDB80D6 1094A1A1


      V is
                                            8B2DB05E BDE2E1A0


Block #1
Blockin   8B2DB05E BDE2E1A0
Blockout  687373F9 F19EB7FE

      output_block is
                                            687373F9 F19EB7FE


      temp is
                                            687373F9 F19EB7FE
```

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

      While loop

      Key is
              8B E2B70871 14D37449 EAFAE01F 1BDB80D6 1094A1A1


      V is
                                              8B2DB05E BDE2E1A1


Block #1
Blockin   8B2DB05E BDE2E1A1
Blockout  08960325 F0D6C998

      output_block is
                                              08960325 F0D6C998


      temp is
                           687373F9 F19EB7FE 08960325 F0D6C998


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

      While loop

      Key is
              8B E2B70871 14D37449 EAFAE01F 1BDB80D6 1094A1A1


      V is
                                              8B2DB05E BDE2E1A2


Block #1
Blockin   8B2DB05E BDE2E1A2
Blockout  08AAEFEB 487B3B15

      output_block is
                                              08AAEFEB 487B3B15
```

```
      temp is
        687373F9 F19EB7FE 08960325 F0D6C998 08AAEFEB 487B3B15


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

      While loop

      Key is
              8B E2B70871 14D37449 EAFAE01F 1BDB80D6 1094A1A1


      V is
                                            8B2DB05E BDE2E1A3


Block #1
Blockin   8B2DB05E BDE2E1A3
Blockout  12A4EE6F 2A6B5AC9

      output_block is
                                            12A4EE6F 2A6B5AC9


      temp is
                                            687373F9 F19EB7FE
        08960325 F0D6C998 08AAEFEB 487B3B15 12A4EE6F 2A6B5AC9


    temp XOR provided_data is
                                                  68 7373F9F1
        9EB7FE08 960325F0 D6C99808 AAEFEB48 7B3B1512 A4EE6F2A


    Key is
              68 7373F9F1 9EB7FE08 960325F0 D6C99808 AAEFEB48


    V is
                                            7B3B1512 A4EE6F2A


rnd_val is
                         D6EC2A7F B7375E40 C3E6B5C3 6484B2DF
```

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

CTR_DRBG

    Requested Security Strength = 112

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString =
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    AdditionalInput = <empty>

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                        00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is
                                                        40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    prediction_resistance_flag = "PredictionResistance"
```

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

  Update

    provided_data is
                                                        40 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                              166B40B4 4ABA4BD6


      temp is
                                              166B40B4 4ABA4BD6


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000002
```

```
Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F

      output_block is
                                            06E7EA22 CE92708F


      temp is
                          166B40B4 4ABA4BD6 06E7EA22 CE92708F


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                            00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                            4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                            00000000 00000004
```

```
Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                              D2FD8867 D50D2DFE


      temp is
                                              166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                    56 2B00F40A
        FA0B9646 A7AA628E D230CF0E F1D089E2 BA56DC92 BDC82795


    Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


    V is
                                              BA56DC92 BDC82795


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

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

CTR_DRBG_Reseed

    entropy_input is
```

```
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    additional_input is  <empty>

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

  Update

    provided_data is
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


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

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                            BA56DC92 BDC82796


Block #1
Blockin   BA56DC92 BDC82796
Blockout  9E0082B6 B55E3596

      output_block is
                                            9E0082B6 B55E3596


      temp is
                                            9E0082B6 B55E3596


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

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2
```

```
      V is
                                              BA56DC92 BDC82797


Block #1
Blockin   BA56DC92 BDC82797
Blockout  F1A82251 90390124

      output_block is
                                              F1A82251 90390124


      temp is
                           9E0082B6 B55E3596 F1A82251 90390124


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

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                              BA56DC92 BDC82798


Block #1
Blockin   BA56DC92 BDC82798
Blockout  24C9B2C0 8D487353

      output_block is
                                              24C9B2C0 8D487353


      temp is
        9E0082B6 B55E3596 F1A82251 90390124 24C9B2C0 8D487353


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

      While loop

      Key is
```

```
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                              BA56DC92 BDC82799


Block #1
Blockin   BA56DC92 BDC82799
Blockout  32269D08 E3F6F53A

      output_block is
                                              32269D08 E3F6F53A


      temp is
                                              9E0082B6 B55E3596
        F1A82251 90390124 24C9B2C0 8D487353 32269D08 E3F6F53A


    temp XOR provided_data is
                                                    1E 81003531
        DBB31179 21A8DA1C B48FABB4 58205319 DDE5C4AA BF07937F


    Key is
              1E 81003531 DBB31179 21A8DA1C B48FABB4 58205319


    V is
                                              DDE5C4AA BF07937F


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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   DDE5C4AA BF079380
Blockout  9AF00447 842ADA5C

Block #1
```

```
Blockin   DDE5C4AA BF079381
Blockout  26AAE321 F0707EAB

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

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
              1E 81003531 DBB31179 21A8DA1C B48FABB4 58205319


      V is
                                            DDE5C4AA BF079382


Block #1
Blockin   DDE5C4AA BF079382
Blockout  910C6503 F2C38D10

      output_block is
                                            910C6503 F2C38D10


      temp is
                                            910C6503 F2C38D10


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

      While loop

      Key is
              1E 81003531 DBB31179 21A8DA1C B48FABB4 58205319


      V is
                                            DDE5C4AA BF079383
```

```
Block #1
Blockin   DDE5C4AA BF079383
Blockout  11C9D57A D32E1393

      output_block is
                                            11C9D57A D32E1393


      temp is
                          910C6503 F2C38D10 11C9D57A D32E1393


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

      While loop

      Key is
              1E 81003531 DBB31179 21A8DA1C B48FABB4 58205319


      V is
                                            DDE5C4AA BF079384


Block #1
Blockin   DDE5C4AA BF079384
Blockout  8B4223C3 EB3DA759

      output_block is
                                            8B4223C3 EB3DA759


      temp is
        910C6503 F2C38D10 11C9D57A D32E1393 8B4223C3 EB3DA759


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

      While loop

      Key is
              1E 81003531 DBB31179 21A8DA1C B48FABB4 58205319
```

```
      V is
                                              DDE5C4AA BF079385


Block #1
Blockin   DDE5C4AA BF079385
Blockout  B37E305E 79F946EF

      output_block is
                                              B37E305E 79F946EF


      temp is
                                              910C6503 F2C38D10
        11C9D57A D32E1393 8B4223C3 EB3DA759 B37E305E 79F946EF


    temp XOR provided_data is
                                                    91 0C6503F2
        C38D1011 C9D57AD3 2E13938B 4223C3EB 3DA759B3 7E305E79


    Key is
              91 0C6503F2 C38D1011 C9D57AD3 2E13938B 4223C3EB


    V is
                                              3DA759B3 7E305E79


rnd_val is
                          9AF00447 842ADA5C 26AAE321 F0707EAB


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>
```

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

CTR_DRBG_Reseed

    entropy_input is
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    additional_input is  <empty>

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

  Update

    provided_data is
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


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

      While loop

      Key is
              91 0C6503F2 C38D1011 C9D57AD3 2E13938B 4223C3EB


      V is
                                            3DA759B3 7E305E7A


Block #1
Blockin   3DA759B3 7E305E7A
Blockout  81A533D1 D557C36F

      output_block is
                                            81A533D1 D557C36F


      temp is
                                            81A533D1 D557C36F


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

```
      While loop

      Key is
              91 0C6503F2 C38D1011 C9D57AD3 2E13938B 4223C3EB


      V is
                                             3DA759B3 7E305E7B


Block #1
Blockin   3DA759B3 7E305E7B
Blockout  CB17A484 D1AA94ED

      output_block is
                                             CB17A484 D1AA94ED


      temp is
                           81A533D1 D557C36F CB17A484 D1AA94ED


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

      While loop

      Key is
              91 0C6503F2 C38D1011 C9D57AD3 2E13938B 4223C3EB


      V is
                                             3DA759B3 7E305E7C


Block #1
Blockin   3DA759B3 7E305E7C
Blockout  6E226341 0E9181B2

      output_block is
                                             6E226341 0E9181B2


      temp is
        81A533D1 D557C36F CB17A484 D1AA94ED 6E226341 0E9181B2
```

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

      While loop

      Key is
              91 0C6503F2 C38D1011 C9D57AD3 2E13938B 4223C3EB


      V is
                                            3DA759B3 7E305E7D


Block #1
Blockin   3DA759B3 7E305E7D
Blockout  94D47C0A 5C1EA253

      output_block is
                                            94D47C0A 5C1EA253


      temp is
                                            81A533D1 D557C36F
        CB17A484 D1AA94ED 6E226341 0E9181B2 94D47C0A 5C1EA253


    temp XOR provided_data is
                                                  41 64F11211
        9205A803 DE6E4F1D 675A22BE F3B192DA 4457654C 0DA6D180


    Key is
              41 64F11211 9205A803 DE6E4F1D 675A22BE F3B192DA


    V is
                                            4457654C 0DA6D180


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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>
```

```
Block #1
Blockin   4457654C 0DA6D181
Blockout  B1C2B79F 8D857055

Block #1
Blockin   4457654C 0DA6D182
Blockout  7B650EE3 B1F3A674

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

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
              41 64F11211 9205A803 DE6E4F1D 675A22BE F3B192DA


      V is
                                              4457654C 0DA6D183


Block #1
Blockin   4457654C 0DA6D183
Blockout  81AD00BD 39189E1D

      output_block is
                                              81AD00BD 39189E1D


      temp is
                                              81AD00BD 39189E1D


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

      While loop
```

```
      Key is
              41 64F11211 9205A803 DE6E4F1D 675A22BE F3B192DA


      V is
                                              4457654C 0DA6D184


Block #1
Blockin   4457654C 0DA6D184
Blockout  250F9C5C 79DFDAC3

      output_block is
                                              250F9C5C 79DFDAC3


      temp is
                           81AD00BD 39189E1D 250F9C5C 79DFDAC3


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

      While loop

      Key is
              41 64F11211 9205A803 DE6E4F1D 675A22BE F3B192DA


      V is
                                              4457654C 0DA6D185


Block #1
Blockin   4457654C 0DA6D185
Blockout  9AFB6A1D 0C2928D1

      output_block is
                                              9AFB6A1D 0C2928D1


      temp is
        81AD00BD 39189E1D 250F9C5C 79DFDAC3 9AFB6A1D 0C2928D1


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

```
      While loop

      Key is
              41 64F11211 9205A803 DE6E4F1D 675A22BE F3B192DA


      V is
                                            4457654C 0DA6D186


Block #1
Blockin   4457654C 0DA6D186
Blockout  E6EB7429 1551530A

      output_block is
                                            E6EB7429 1551530A


      temp is
                                            81AD00BD 39189E1D
        250F9C5C 79DFDAC3 9AFB6A1D 0C2928D1 E6EB7429 1551530A


    temp XOR provided_data is
                                                  81 AD00BD39
        189E1D25 0F9C5C79 DFDAC39A FB6A1D0C 2928D1E6 EB742915


    Key is
              81 AD00BD39 189E1D25 0F9C5C79 DFDAC39A FB6A1D0C


    V is
                                            2928D1E6 EB742915


rnd_val is
                         B1C2B79F 8D857055 7B650EE3 B1F3A674


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

CTR_DRBG

    Requested Security Strength = 112
```

```
    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                      00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    EntropyInput1 (for Reseed1) =
                                                      80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    EntropyInput2 (for Reseed2) =
                                                      C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    PersonalizationString =
                                                      40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C


    AdditionalInput1 =
                                                      60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


    AdditionalInput2 =
                                                      A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                      00 01020304
        05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C


    personal_str is
                                                      40 41424344
        45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C
```

```
    prediction_resistance_flag = "PredictionResistance"

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

  Update

    provided_data is
                                                        40 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000001


Block #1
Blockin   00000000 00000001
Blockout  166B40B4 4ABA4BD6

      output_block is
                                              166B40B4 4ABA4BD6


      temp is
                                              166B40B4 4ABA4BD6


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                              00000000 00000002
```

```
Block #1
Blockin   00000000 00000002
Blockout  06E7EA22 CE92708F

      output_block is
                                            06E7EA22 CE92708F


      temp is
                          166B40B4 4ABA4BD6 06E7EA22 CE92708F


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000


      V is
                                            00000000 00000003


Block #1
Blockin   00000000 00000003
Blockout  4EB190C9 A2FA169C

      output_block is
                                            4EB190C9 A2FA169C


      temp is
        166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C


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

      While loop

      Key is
              00 00000000 00000000 00000000 00000000 00000000
```

```
      V is
                                                00000000 00000004


Block #1
Blockin   00000000 00000004
Blockout  D2FD8867 D50D2DFE

      output_block is
                                                D2FD8867 D50D2DFE


      temp is
                                                166B40B4 4ABA4BD6
        06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE


    temp XOR provided_data is
                                                        56 2B00F40A
        FA0B9646 A7AA628E D230CF0E F1D089E2 BA56DC92 BDC82795


    Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


    V is
                                                BA56DC92 BDC82795


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


Generate FAILED: Reseed is required
```

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

CTR_DRBG_Reseed

    entropy_input is
                                                        80 81828384
        85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C


    additional_input is
                                                        60 61626364
        65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C


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

  Update

    provided_data is
                                                        E0 E0E0E0E0
        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0


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

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                              BA56DC92 BDC82796


Block #1
Blockin   BA56DC92 BDC82796
Blockout  9E0082B6 B55E3596

      output_block is
                                              9E0082B6 B55E3596


      temp is
                                              9E0082B6 B55E3596
```

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

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                           BA56DC92 BDC82797


Block #1
Blockin   BA56DC92 BDC82797
Blockout  F1A82251 90390124

      output_block is
                                           F1A82251 90390124


      temp is
                           9E0082B6 B55E3596 F1A82251 90390124


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

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                           BA56DC92 BDC82798


Block #1
Blockin   BA56DC92 BDC82798
Blockout  24C9B2C0 8D487353

      output_block is
                                           24C9B2C0 8D487353


      temp is
```

```
        9E0082B6 B55E3596 F1A82251 90390124 24C9B2C0 8D487353


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

      While loop

      Key is
              56 2B00F40A FA0B9646 A7AA628E D230CF0E F1D089E2


      V is
                                            BA56DC92 BDC82799


Block #1
Blockin   BA56DC92 BDC82799
Blockout  32269D08 E3F6F53A

      output_block is
                                            32269D08 E3F6F53A


      temp is
                                            9E0082B6 B55E3596
        F1A82251 90390124 24C9B2C0 8D487353 32269D08 E3F6F53A


    temp XOR provided_data is
                                                  7E E0625655
        BED57611 48C2B170 D9E1C4C4 2952206D A893B3D2 C67DE803


    Key is
              7E E0625655 BED57611 48C2B170 D9E1C4C4 2952206D


    V is
                                            A893B3D2 C67DE803


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

CTR_DRBG_Generate

  requested_number_of_bits = 128
```

```
    additional_input is  <empty>

Block #1
Blockin   A893B3D2 C67DE804
Blockout  58674F0B CD88A4F5

Block #1
Blockin   A893B3D2 C67DE805
Blockout  107F6E91 FCFC477C

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

  Update

    provided_data is
                                                        00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
              7E E0625655 BED57611 48C2B170 D9E1C4C4 2952206D


      V is
                                            A893B3D2 C67DE806


Block #1
Blockin   A893B3D2 C67DE806
Blockout  65697455 25220EB7

      output_block is
                                            65697455 25220EB7


      temp is
                                            65697455 25220EB7


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

```
      While loop

      Key is
              7E E0625655 BED57611 48C2B170 D9E1C4C4 2952206D


      V is
                                            A893B3D2 C67DE807


Block #1
Blockin   A893B3D2 C67DE807
Blockout  F4F55A13 656ADFDF

      output_block is
                                            F4F55A13 656ADFDF


      temp is
                           65697455 25220EB7 F4F55A13 656ADFDF


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

      While loop

      Key is
              7E E0625655 BED57611 48C2B170 D9E1C4C4 2952206D


      V is
                                            A893B3D2 C67DE808


Block #1
Blockin   A893B3D2 C67DE808
Blockout  8C5A56BA 299916BC

      output_block is
                                            8C5A56BA 299916BC


      temp is
        65697455 25220EB7 F4F55A13 656ADFDF 8C5A56BA 299916BC
```

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

      While loop

      Key is
              7E E0625655 BED57611 48C2B170 D9E1C4C4 2952206D


      V is
                                            A893B3D2 C67DE809


Block #1
Blockin   A893B3D2 C67DE809
Blockout  6D65AF83 8CC02CDA

      output_block is
                                            6D65AF83 8CC02CDA


      temp is
                                            65697455 25220EB7
        F4F55A13 656ADFDF 8C5A56BA 299916BC 6D65AF83 8CC02CDA


    temp XOR provided_data is
                                                   65 69745525
        220EB7F4 F55A1365 6ADFDF8C 5A56BA29 9916BC6D 65AF838C


    Key is
              65 69745525 220EB7F4 F55A1365 6ADFDF8C 5A56BA29


    V is
                                            9916BC6D 65AF838C


rnd_val is
                          58674F0B CD88A4F5 107F6E91 FCFC477C


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

Second call to Generate
```

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


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

CTR_DRBG_Reseed

    entropy_input is
                                                        C0 C1C2C3C4
        C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC


    additional_input is
                                                        A0 A1A2A3A4
        A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC


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

  Update

    provided_data is
                                                        60 60606060
        60606060 60606060 60606060 60606060 60606060 60606060


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

      While loop

      Key is
              65 69745525 220EB7F4 F55A1365 6ADFDF8C 5A56BA29


      V is
                                              9916BC6D 65AF838D
```

```
Block #1
Blockin   9916BC6D 65AF838D
Blockout  43055D6A DBC6F3D9

      output_block is
                                              43055D6A DBC6F3D9


      temp is
                                              43055D6A DBC6F3D9


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

      While loop

      Key is
              65 69745525 220EB7F4 F55A1365 6ADFDF8C 5A56BA29


      V is
                                              9916BC6D 65AF838E


Block #1
Blockin   9916BC6D 65AF838E
Blockout  54F1A12F 32EFF9EA

      output_block is
                                              54F1A12F 32EFF9EA


      temp is
                           43055D6A DBC6F3D9 54F1A12F 32EFF9EA


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

      While loop

      Key is
              65 69745525 220EB7F4 F55A1365 6ADFDF8C 5A56BA29


      V is
```

```
                                                9916BC6D 65AF838F


Block #1
Blockin   9916BC6D 65AF838F
Blockout  586C4927 579F889F

      output_block is
                                                586C4927 579F889F


      temp is
        43055D6A DBC6F3D9 54F1A12F 32EFF9EA 586C4927 579F889F


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

      While loop

      Key is
              65 69745525 220EB7F4 F55A1365 6ADFDF8C 5A56BA29


      V is
                                                9916BC6D 65AF8390


Block #1
Blockin   9916BC6D 65AF8390
Blockout  5526CF26 D53D3D01

      output_block is
                                                5526CF26 D53D3D01


      temp is
                                                43055D6A DBC6F3D9
        54F1A12F 32EFF9EA 586C4927 579F889F 5526CF26 D53D3D01


    temp XOR provided_data is
                                                       23 653D0ABB
        A693B934 91C14F52 8F998A38 0C294737 FFE8FF35 46AF46B5


    Key is
```

```
              23 653D0ABB A693B934 91C14F52 8F998A38 0C294737


    V is
                                            FFE8FF35 46AF46B5

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

CTR_DRBG_Generate

  requested_number_of_bits = 128

    additional_input is  <empty>

Block #1
Blockin   FFE8FF35 46AF46B6
Blockout  65DD535E 768645BF

Block #1
Blockin   FFE8FF35 46AF46B7
Blockout  23701A88 93BA9AFB

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

  Update

    provided_data is
                                                    00 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
              23 653D0ABB A693B934 91C14F52 8F998A38 0C294737


      V is
                                            FFE8FF35 46AF46B8


Block #1
Blockin   FFE8FF35 46AF46B8
```

```
Blockout  3957588B 002DE9AC

      output_block is
                                              3957588B 002DE9AC


      temp is
                                              3957588B 002DE9AC


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

      While loop

      Key is
              23 653D0ABB A693B934 91C14F52 8F998A38 0C294737


      V is
                                              FFE8FF35 46AF46B9


Block #1
Blockin   FFE8FF35 46AF46B9
Blockout  0A9737D8 D1F906D4

      output_block is
                                              0A9737D8 D1F906D4


      temp is
                           3957588B 002DE9AC 0A9737D8 D1F906D4


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

      While loop

      Key is
              23 653D0ABB A693B934 91C14F52 8F998A38 0C294737


      V is
                                              FFE8FF35 46AF46BA
```

```
Block #1
Blockin   FFE8FF35 46AF46BA
Blockout  D6362C4D 53DB11D2

      output_block is
                                              D6362C4D 53DB11D2


      temp is
        3957588B 002DE9AC 0A9737D8 D1F906D4 D6362C4D 53DB11D2


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

      While loop

      Key is
              23 653D0ABB A693B934 91C14F52 8F998A38 0C294737


      V is
                                              FFE8FF35 46AF46BB


Block #1
Blockin   FFE8FF35 46AF46BB
Blockout  A0CC9C70 49FA167F

      output_block is
                                              A0CC9C70 49FA167F


      temp is
                                              3957588B 002DE9AC
        0A9737D8 D1F906D4 D6362C4D 53DB11D2 A0CC9C70 49FA167F


    temp XOR provided_data is
                                                    39 57588B00
        2DE9AC0A 9737D8D1 F906D4D6 362C4D53 DB11D2A0 CC9C7049


    Key is
              39 57588B00 2DE9AC0A 9737D8D1 F906D4D6 362C4D53
```

```
    V is
                                                DB11D2A0 CC9C7049


rnd_val is
                           65DD535E 768645BF 23701A88 93BA9AFB


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

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    PersonalizationString = <empty>

    AdditionalInput = <empty>

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is  <empty>
```

```
    prediction_resistance_flag = "No PredictionResistance"

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

  Update

    provided_data is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


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

      While loop

      Key is
                          00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000001


      output_block is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A


      temp is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A


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

      While loop

      Key is
                          00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000002


      output_block is
                          0388DACE 60B6A392 F328C2B9 71B2FE78
```

```
      temp is
                                                58E2FCCE FA7E3061
        367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78


    temp XOR provided_data is
                                                58E3FECD FE7B3666
        3E76175C A8EA4B55 1399C8DD 74A3B585 EB31D8A2 6DAFE067


    Key is
                           58E3FECD FE7B3666 3E76175C A8EA4B55


    V is
                           1399C8DD 74A3B585 EB31D8A2 6DAFE067


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
```

```
                    58E3FECD FE7B3666 3E76175C A8EA4B55

  V is
                    1399C8DD 74A3B585 EB31D8A2 6DAFE06A

  output_block is
                    14810C15 D85DA566 5C2518B4 553FB155

  temp is
                    14810C15 D85DA566 5C2518B4 553FB155

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

  While loop

  Key is
                    58E3FECD FE7B3666 3E76175C A8EA4B55

  V is
                    1399C8DD 74A3B585 EB31D8A2 6DAFE06B

  output_block is
                    B85442C7 900E7D82 7A11C60D 18F424E5

  temp is
                                      14810C15 D85DA566
    5C2518B4 553FB155 B85442C7 900E7D82 7A11C60D 18F424E5

temp XOR provided_data is
                                      14810C15 D85DA566
    5C2518B4 553FB155 B85442C7 900E7D82 7A11C60D 18F424E5

Key is
                    14810C15 D85DA566 5C2518B4 553FB155

V is
```

```
                        B85442C7 900E7D82 7A11C60D 18F424E5


rnd_val is
                                                 1686FFCF 9F358BE7
        4452E647 BA156AAB 05135797 117FD1AB 317D318C 660E3D18


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                                                 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
                        14810C15 D85DA566 5C2518B4 553FB155


      V is
                        B85442C7 900E7D82 7A11C60D 18F424E8


      output_block is
                        F75ECD8C D778C71E F4DC13AC 0779723F


      temp is
```

F75ECD8C D778C71E F4DC13AC 0779723F

While loop

Key is
14810C15 D85DA566 5C2518B4 553FB155

V is
B85442C7 900E7D82 7A11C60D 18F424E9

output_block is
2AE70FAB CD77683C DC921607 9C291D5B

temp is
F75ECD8C D778C71E
F4DC13AC 0779723F 2AE70FAB CD77683C DC921607 9C291D5B

temp XOR provided_data is
F75ECD8C D778C71E
F4DC13AC 0779723F 2AE70FAB CD77683C DC921607 9C291D5B

Key is
F75ECD8C D778C71E F4DC13AC 0779723F

V is
2AE70FAB CD77683C DC921607 9C291D5B

rnd_val is
F89A638F 026010CF
B9DCC706 B34C789C 07B94FD4 6DAB90EC 866A523B D05EF2CA

##

CTR_DRBG

```
    Requested Security Strength = 128

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    AdditionalInput2 =
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

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

```
Update

  provided_data is
                                          00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


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

    While loop

    Key is
                        00000000 00000000 00000000 00000000


    V is
                        00000000 00000000 00000000 00000001


    output_block is
                        58E2FCCE FA7E3061 367F1D57 A4E7455A


    temp is
                        58E2FCCE FA7E3061 367F1D57 A4E7455A


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

    While loop

    Key is
                        00000000 00000000 00000000 00000000


    V is
                        00000000 00000000 00000000 00000002


    output_block is
                        0388DACE 60B6A392 F328C2B9 71B2FE78


    temp is
                                          58E2FCCE FA7E3061
```

```
        367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78


    temp XOR provided_data is
                                              58E3FECD FE7B3666
        3E76175C A8EA4B55 1399C8DD 74A3B585 EB31D8A2 6DAFE067


    Key is
                          58E3FECD FE7B3666 3E76175C A8EA4B55


    V is
                          1399C8DD 74A3B585 EB31D8A2 6DAFE067


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                              60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                                              60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


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

      While loop

      Key is
```

```
                    58E3FECD FE7B3666 3E76175C A8EA4B55

  V is
                    1399C8DD 74A3B585 EB31D8A2 6DAFE068

  output_block is
                    1686FFCF 9F358BE7 4452E647 BA156AAB

  temp is
                    1686FFCF 9F358BE7 4452E647 BA156AAB

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

  While loop

  Key is
                    58E3FECD FE7B3666 3E76175C A8EA4B55

  V is
                    1399C8DD 74A3B585 EB31D8A2 6DAFE069

  output_block is
                    05135797 117FD1AB 317D318C 660E3D18

  temp is
                                      1686FFCF 9F358BE7
    4452E647 BA156AAB 05135797 117FD1AB 317D318C 660E3D18

temp XOR provided_data is
                                      76E79DAC FB50ED80
    2C3B8C2C D67804C4 756225E4 650AA7DC 49044BF7 1A734367

Key is
                    76E79DAC FB50ED80 2C3B8C2C D67804C4

V is
```

```
                          756225E4 650AA7DC 49044BF7 1A734367


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

  Update

    provided_data is
                                                 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


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

      While loop

      Key is
                          76E79DAC FB50ED80 2C3B8C2C D67804C4


      V is
                          756225E4 650AA7DC 49044BF7 1A73436A


      output_block is
                          04E81A0B 49D43C63 DD088CA7 02467720


      temp is
                          04E81A0B 49D43C63 DD088CA7 02467720


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

      While loop

      Key is
                          76E79DAC FB50ED80 2C3B8C2C D67804C4


      V is
                          756225E4 650AA7DC 49044BF7 1A73436B


      output_block is
                          2929B2BC F2CFDA80 A358BBC8 543103C9
```

```
      temp is
                                                04E81A0B 49D43C63
        DD088CA7 02467720 2929B2BC F2CFDA80 A358BBC8 543103C9


    temp XOR provided_data is
                                                64897868 2DB15A04
        B561E6CC 6E2B194F 5958C0CF 86BAACF7 DB21C1B3 284C7DB6


    Key is
                           64897868 2DB15A04 B561E6CC 6E2B194F


    V is
                           5958C0CF 86BAACF7 DB21C1B3 284C7DB6


rnd_val is
                                                CBFD7872 46E49C1C
        98569F68 5B808D8B 916F747C 09D419BE 60AF0735 2C60274A


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
```

```
                                          A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

  While loop

  Key is
                      64897868 2DB15A04 B561E6CC 6E2B194F


  V is
                      5958C0CF 86BAACF7 DB21C1B3 284C7DB7


  output_block is
                      2B9AFD91 EF659E4D BBE23AF5 22244A27


  temp is
                      2B9AFD91 EF659E4D BBE23AF5 22244A27


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

  While loop

  Key is
                      64897868 2DB15A04 B561E6CC 6E2B194F


  V is
                      5958C0CF 86BAACF7 DB21C1B3 284C7DB8


  output_block is
                      AC0565F4 30E74EA4 A9FA4FBF 50B048F1


  temp is
                                          2B9AFD91 EF659E4D
    BBE23AF5 22244A27 AC0565F4 30E74EA4 A9FA4FBF 50B048F1


temp XOR provided_data is
```

```
                                                8B3B5F32 4BC038EA
        134B905E 8E89E488 1CB4D747 8452F813 1143F504 EC0DF64E


    Key is
                          8B3B5F32 4BC038EA 134B905E 8E89E488


    V is
                          1CB4D747 8452F813 1143F504 EC0DF64E


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

  Update

    provided_data is
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

      While loop

      Key is
                          8B3B5F32 4BC038EA 134B905E 8E89E488


      V is
                          1CB4D747 8452F813 1143F504 EC0DF651


      output_block is
                          924095AD 1828265A EFBCC516 A8BBFD25


      temp is
                          924095AD 1828265A EFBCC516 A8BBFD25


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

      While loop

      Key is
```

```
                        8B3B5F32 4BC038EA 134B905E 8E89E488

      V is
                        1CB4D747 8452F813 1143F504 EC0DF652

      output_block is
                        F9811209 0A5F536D E0FFEBD2 FDCFAE56

      temp is
                                                 924095AD 1828265A
        EFBCC516 A8BBFD25 F9811209 0A5F536D E0FFEBD2 FDCFAE56

    temp XOR provided_data is
                                                 32E1370E BC8D80FD
        47156FBD 0416538A 4930A0BA BEEAE5DA 58465169 417210E9

    Key is
                        32E1370E BC8D80FD 47156FBD 0416538A

    V is
                        4930A0BA BEEAE5DA 58465169 417210E9

rnd_val is
                                                 3911B096 E12EE1C9
        DF59DD91 73BA0A49 6C39B748 705891B8 E08C1F36 E039BCE1

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

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                                 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
```

```
    EntropyInput1 (for Reseed1) =
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    PersonalizationString =
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    AdditionalInput = <empty>

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    prediction_resistance_flag = "No PredictionResistance"

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

  Update

    provided_data is
                                                40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


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

```
  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000001

  output_block is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

  temp is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

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

  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      0388DACE 60B6A392 F328C2B9 71B2FE78

  temp is
                                        58E2FCCE FA7E3061
    367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is
                                        18A2BC8E BA3E7021
    763F5D17 E4A7051A 43C89A8E 20F6E3D2 B36882F9 31F2BE38

Key is
                      18A2BC8E BA3E7021 763F5D17 E4A7051A
```

```
    V is
                          43C89A8E 20F6E3D2 B36882F9 31F2BE38

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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                                                 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
                          18A2BC8E BA3E7021 763F5D17 E4A7051A


      V is
                          43C89A8E 20F6E3D2 B36882F9 31F2BE3B


      output_block is
                          FD9E5A45 0FBEACBA C48AE96E A7E0B6EB


      temp is
                          FD9E5A45 0FBEACBA C48AE96E A7E0B6EB
```

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

      While loop

      Key is
                           18A2BC8E BA3E7021 763F5D17 E4A7051A


      V is
                           43C89A8E 20F6E3D2 B36882F9 31F2BE3C


      output_block is
                           33CED475 402EF666 C064E09E A9FD86B7


      temp is
                                             FD9E5A45 0FBEACBA
        C48AE96E A7E0B6EB 33CED475 402EF666 C064E09E A9FD86B7


    temp XOR provided_data is
                                             FD9E5A45 0FBEACBA
        C48AE96E A7E0B6EB 33CED475 402EF666 C064E09E A9FD86B7


    Key is
                           FD9E5A45 0FBEACBA C48AE96E A7E0B6EB


    V is
                           33CED475 402EF666 C064E09E A9FD86B7


rnd_val is
                                             FA1DF743 5039C649
        3B14D8C8 F9715BA5 CE6EE312 20EEDEE3 65A4B6B7 2FD68554


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

Second call to Generate

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

```
CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
                          FD9E5A45 0FBEACBA C48AE96E A7E0B6EB


      V is
                          33CED475 402EF666 C064E09E A9FD86BA


      output_block is
                          C2A75EEC 1593F3C0 11831516 F32115D9


      temp is
                          C2A75EEC 1593F3C0 11831516 F32115D9


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

      While loop

      Key is
                          FD9E5A45 0FBEACBA C48AE96E A7E0B6EB


      V is
                          33CED475 402EF666 C064E09E A9FD86BB
```

```
      output_block is
                          FE3B7B8C 420F4BC7 9EAFC24A 4E4F54ED


      temp is
                                              C2A75EEC 1593F3C0
        11831516 F32115D9 FE3B7B8C 420F4BC7 9EAFC24A 4E4F54ED


    temp XOR provided_data is
                                              C2A75EEC 1593F3C0
        11831516 F32115D9 FE3B7B8C 420F4BC7 9EAFC24A 4E4F54ED


    Key is
                          C2A75EEC 1593F3C0 11831516 F32115D9


    V is
                          FE3B7B8C 420F4BC7 9EAFC24A 4E4F54ED


rnd_val is
                                              021F0DA0 6944CB4B
        20A5E7CD 3740B1E6 AB90B3AA 66638A03 5BAC12CC F29C148A


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

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                                              00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                              80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
```

```
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    PersonalizationString =
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    AdditionalInput1 =
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    AdditionalInput2 =
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    prediction_resistance_flag = "No PredictionResistance"

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

  Update

    provided_data is
                                                40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040
```

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

  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000001

  output_block is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

  temp is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

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

  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      0388DACE 60B6A392 F328C2B9 71B2FE78

  temp is
                                        58E2FCCE FA7E3061
    367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is
                                        18A2BC8E BA3E7021
    763F5D17 E4A7051A 43C89A8E 20F6E3D2 B36882F9 31F2BE38
```

```
    Key is
                          18A2BC8E BA3E7021 763F5D17 E4A7051A

    V is
                          43C89A8E 20F6E3D2 B36882F9 31F2BE38

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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                              60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                                              60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


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

      While loop

      Key is
                          18A2BC8E BA3E7021 763F5D17 E4A7051A


      V is
                          43C89A8E 20F6E3D2 B36882F9 31F2BE39


      output_block is
```

```
                        FA1DF743 5039C649 3B14D8C8 F9715BA5

      temp is
                        FA1DF743 5039C649 3B14D8C8 F9715BA5

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

      While loop

      Key is
                        18A2BC8E BA3E7021 763F5D17 E4A7051A

      V is
                        43C89A8E 20F6E3D2 B36882F9 31F2BE3A

      output_block is
                        CE6EE312 20EEDEE3 65A4B6B7 2FD68554

      temp is
                                          FA1DF743 5039C649
        3B14D8C8 F9715BA5 CE6EE312 20EEDEE3 65A4B6B7 2FD68554

    temp XOR provided_data is
                                          9A7C9520 345CA02E
        537DB2A3 951C35CA BE1F9161 549BA894 1DDDCCCC 53ABFB2B

    Key is
                        9A7C9520 345CA02E 537DB2A3 951C35CA

    V is
                        BE1F9161 549BA894 1DDDCCCC 53ABFB2B

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

  Update

    provided_data is
```

```
                                          60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F

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

  While loop

  Key is
                     9A7C9520 345CA02E 537DB2A3 951C35CA

  V is
                     BE1F9161 549BA894 1DDDCCCC 53ABFB2E

  output_block is
                     BB26AF64 4DFF74EF 86BE7D45 7D176B7D

  temp is
                     BB26AF64 4DFF74EF 86BE7D45 7D176B7D

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

  While loop

  Key is
                     9A7C9520 345CA02E 537DB2A3 951C35CA

  V is
                     BE1F9161 549BA894 1DDDCCCC 53ABFB2F

  output_block is
                     F463EBC4 F2456A66 28274CC5 1569216E

  temp is
                                          BB26AF64 4DFF74EF
    86BE7D45 7D176B7D F463EBC4 F2456A66 28274CC5 1569216E

temp XOR provided_data is
```

```
                                                DB47CD07 299A1288
        EED7172E 117A0512 841299B7 86301C11 505E36BE 69145F11


    Key is
                          DB47CD07 299A1288 EED7172E 117A0512


    V is
                          841299B7 86301C11 505E36BE 69145F11


rnd_val is
                                                CBCA7021 E6E00F5C
        E8F499CA 8E566B48 05094A95 91DEDA27 47191006 3A6DA790


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

      While loop
```

```
  Key is
                      DB47CD07 299A1288 EED7172E 117A0512

  V is
                      841299B7 86301C11 505E36BE 69145F12

  output_block is
                      8283CC8B 341C8A7F 6C4A7D82 477E7EA2

  temp is
                      8283CC8B 341C8A7F 6C4A7D82 477E7EA2

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

  While loop

  Key is
                      DB47CD07 299A1288 EED7172E 117A0512

  V is
                      841299B7 86301C11 505E36BE 69145F13

  output_block is
                      04E254CC 86E2E651 0D6F26C8 A2547E78

  temp is
                                        8283CC8B 341C8A7F
    6C4A7D82 477E7EA2 04E254CC 86E2E651 0D6F26C8 A2547E78

temp XOR provided_data is
                                        22226E28 90B92CD8
    C4E3D729 EBD3D00D B453E67F 325750E6 B5D69C73 1EE9C0C7

Key is
                      22226E28 90B92CD8 C4E3D729 EBD3D00D
```

```
    V is
                          B453E67F 325750E6 B5D69C73 1EE9C0C7


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

  Update

    provided_data is
                                                 A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

      While loop

      Key is
                          22226E28 90B92CD8 C4E3D729 EBD3D00D


      V is
                          B453E67F 325750E6 B5D69C73 1EE9C0CA


      output_block is
                          328F23F8 54E627F9 EB672EBC 79A7EA84


      temp is
                          328F23F8 54E627F9 EB672EBC 79A7EA84


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

      While loop

      Key is
                          22226E28 90B92CD8 C4E3D729 EBD3D00D


      V is
                          B453E67F 325750E6 B5D69C73 1EE9C0CB


      output_block is
```

```
                        844E2773 02ED019C 212C2D7F 41A89738


      temp is
                                              328F23F8 54E627F9
        EB672EBC 79A7EA84 844E2773 02ED019C 212C2D7F 41A89738


    temp XOR provided_data is
                                              922E815B F043815E
        43CE8417 D50A442B 34FF95C0 B658B72B 999597C4 FD152987


    Key is
                        922E815B F043815E 43CE8417 D50A442B


    V is
                        34FF95C0 B658B72B 999597C4 FD152987


rnd_val is
                                              CB502773 1CCD0686
        04478567 64A3D2F1 909E1AB1 2FF39EF7 004390C3 F645ED70


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

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                              00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                              80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                              C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
```

```
    PersonalizationString = <empty>

    AdditionalInput = <empty>

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

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

  Update

    provided_data is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


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

      While loop

      Key is
                          00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000001


      output_block is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A
```

```
      temp is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A


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

      While loop

      Key is
                          00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000002


      output_block is
                          0388DACE 60B6A392 F328C2B9 71B2FE78


      temp is
                                            58E2FCCE FA7E3061
        367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78


    temp XOR provided_data is
                                            58E3FECD FE7B3666
        3E76175C A8EA4B55 1399C8DD 74A3B585 EB31D8A2 6DAFE067


    Key is
                          58E3FECD FE7B3666 3E76175C A8EA4B55


    V is
                          1399C8DD 74A3B585 EB31D8A2 6DAFE067


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

First call to Generate

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

CTR_DRBG_Generate
```

```
  requested_number_of_bits = 256

    additional_input is  <empty>

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

CTR_DRBG_Reseed

    entropy_input is
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    additional_input is  <empty>

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

  Update

    provided_data is
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


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

      While loop

      Key is
                          58E3FECD FE7B3666 3E76175C A8EA4B55


      V is
                          1399C8DD 74A3B585 EB31D8A2 6DAFE068


      output_block is
                          1686FFCF 9F358BE7 4452E647 BA156AAB


      temp is
                          1686FFCF 9F358BE7 4452E647 BA156AAB


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

```
      While loop

      Key is
                           58E3FECD FE7B3666 3E76175C A8EA4B55

      V is
                           1399C8DD 74A3B585 EB31D8A2 6DAFE069

      output_block is
                           05135797 117FD1AB 317D318C 660E3D18

      temp is
                                                 1686FFCF 9F358BE7
        4452E647 BA156AAB 05135797 117FD1AB 317D318C 660E3D18

    temp XOR provided_data is
                                                 96077D4C 1BB00D60
       CCDB6CCC 3698E424 9582C504 85EA473C A9E4AB17 FA93A387

    Key is
                           96077D4C 1BB00D60 CCDB6CCC 3698E424

    V is
                           9582C504 85EA473C A9E4AB17 FA93A387

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
```

```
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


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

  While loop

  Key is
                      96077D4C 1BB00D60 CCDB6CCC 3698E424


  V is
                      9582C504 85EA473C A9E4AB17 FA93A38A


  output_block is
                      D816A3CD B36E3A01 AF11BA58 76F49516


  temp is
                      D816A3CD B36E3A01 AF11BA58 76F49516


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

  While loop

  Key is
                      96077D4C 1BB00D60 CCDB6CCC 3698E424


  V is
                      9582C504 85EA473C A9E4AB17 FA93A38B


  output_block is
                      8017C913 B23F851E 24425356 1474D074


  temp is
                                          D816A3CD B36E3A01
    AF11BA58 76F49516 8017C913 B23F851E 24425356 1474D074


temp XOR provided_data is
```

```
                                                D816A3CD B36E3A01
        AF11BA58 76F49516 8017C913 B23F851E 24425356 1474D074


    Key is
                          D816A3CD B36E3A01 AF11BA58 76F49516


    V is
                          8017C913 B23F851E 24425356 1474D074


rnd_val is
                                                89935DB7 5FC4ED67
        7F166E49 CAEDB105 48BB5B5E 7F8B32D6 44DFD3B7 CCDE3B60


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

CTR_DRBG_Reseed

    entropy_input is
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is  <empty>

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

  Update

    provided_data is
```

```
                                          C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


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

  While loop

  Key is
                     D816A3CD B36E3A01 AF11BA58 76F49516


  V is
                     8017C913 B23F851E 24425356 1474D075


  output_block is
                     C1660382 61B1D710 80C0CD6A 769A810B


  temp is
                     C1660382 61B1D710 80C0CD6A 769A810B


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

  While loop

  Key is
                     D816A3CD B36E3A01 AF11BA58 76F49516


  V is
                     8017C913 B23F851E 24425356 1474D076


  output_block is
                     5ADEAAA6 72E03BDC BFF96166 14BBBEDC


  temp is
                                          C1660382 61B1D710
    80C0CD6A 769A810B 5ADEAAA6 72E03BDC BFF96166 14BBBEDC


temp XOR provided_data is
```

```
                                                01A7C141 A57411D7
        480907A1 BA574FC4 8A0F7875 A635ED0B 6720BBBD C8666003


    Key is
                          01A7C141 A57411D7 480907A1 BA574FC4


    V is
                          8A0F7875 A635ED0B 6720BBBD C8666003


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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
                          01A7C141 A57411D7 480907A1 BA574FC4


      V is
                          8A0F7875 A635ED0B 6720BBBD C8666006


      output_block is
                          00B84831 ABFBE616 8FE6D0BD 4784ED4E


      temp is
```

```
                        00B84831 ABFBE616 8FE6D0BD 4784ED4E


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

      While loop

      Key is
                        01A7C141 A57411D7 480907A1 BA574FC4


      V is
                        8A0F7875 A635ED0B 6720BBBD C8666007


      output_block is
                        948ABF15 132F7F78 1ED83609 0ACA9F6E


      temp is
                                            00B84831 ABFBE616
        8FE6D0BD 4784ED4E 948ABF15 132F7F78 1ED83609 0ACA9F6E


    temp XOR provided_data is
                                            00B84831 ABFBE616
        8FE6D0BD 4784ED4E 948ABF15 132F7F78 1ED83609 0ACA9F6E


    Key is
                        00B84831 ABFBE616 8FE6D0BD 4784ED4E


    V is
                        948ABF15 132F7F78 1ED83609 0ACA9F6E


rnd_val is
                                            B5795CE0 AFADFBA6
        0C337129 8D105500 531853E4 65548878 9847E053 147D5C15


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

CTR_DRBG
```

```
    Requested Security Strength = 128

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    PersonalizationString = <empty>

    AdditionalInput1 =
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    AdditionalInput2 =
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

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

```
Update

  provided_data is
                                          00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


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

    While loop

    Key is
                        00000000 00000000 00000000 00000000


    V is
                        00000000 00000000 00000000 00000001


    output_block is
                        58E2FCCE FA7E3061 367F1D57 A4E7455A


    temp is
                        58E2FCCE FA7E3061 367F1D57 A4E7455A


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

    While loop

    Key is
                        00000000 00000000 00000000 00000000


    V is
                        00000000 00000000 00000000 00000002


    output_block is
                        0388DACE 60B6A392 F328C2B9 71B2FE78


    temp is
                                          58E2FCCE FA7E3061
```

```
        367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78


    temp XOR provided_data is
                                            58E3FECD FE7B3666
        3E76175C A8EA4B55 1399C8DD 74A3B585 EB31D8A2 6DAFE067


    Key is
                          58E3FECD FE7B3666 3E76175C A8EA4B55


    V is
                          1399C8DD 74A3B585 EB31D8A2 6DAFE067


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                            60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


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

CTR_DRBG_Reseed

    entropy_input is
                                            80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    additional_input is
                                            60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
```

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

  Update

    provided_data is
                                                E0E0E0E0 E0E0E0E0
        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0


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

      While loop

      Key is
                          58E3FECD FE7B3666 3E76175C A8EA4B55


      V is
                          1399C8DD 74A3B585 EB31D8A2 6DAFE068


      output_block is
                          1686FFCF 9F358BE7 4452E647 BA156AAB


      temp is
                          1686FFCF 9F358BE7 4452E647 BA156AAB


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

      While loop

      Key is
                          58E3FECD FE7B3666 3E76175C A8EA4B55


      V is
                          1399C8DD 74A3B585 EB31D8A2 6DAFE069


      output_block is
                          05135797 117FD1AB 317D318C 660E3D18


      temp is
```

```
                                                1686FFCF 9F358BE7
        4452E647 BA156AAB 05135797 117FD1AB 317D318C 660E3D18


    temp XOR provided_data is
                                                F6661F2F 7FD56B07
        A4B206A7 5AF58A4B E5F3B777 F19F314B D19DD16C 86EEDDF8


    Key is
                          F6661F2F 7FD56B07 A4B206A7 5AF58A4B


    V is
                          E5F3B777 F19F314B D19DD16C 86EEDDF8


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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
                          F6661F2F 7FD56B07 A4B206A7 5AF58A4B


      V is
                          E5F3B777 F19F314B D19DD16C 86EEDDFB
```

```
      output_block is
                          00D9D257 6D398E76 0057DAD3 6F462A0D

      temp is
                          00D9D257 6D398E76 0057DAD3 6F462A0D


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

      While loop

      Key is
                          F6661F2F 7FD56B07 A4B206A7 5AF58A4B

      V is
                          E5F3B777 F19F314B D19DD16C 86EEDDFC

      output_block is
                          A3C3633D 964C6D0B 148D435C 7EF870A4

      temp is
                                               00D9D257 6D398E76
        0057DAD3 6F462A0D A3C3633D 964C6D0B 148D435C 7EF870A4


    temp XOR provided_data is
                                               00D9D257 6D398E76
        0057DAD3 6F462A0D A3C3633D 964C6D0B 148D435C 7EF870A4


    Key is
                          00D9D257 6D398E76 0057DAD3 6F462A0D

    V is
                          A3C3633D 964C6D0B 148D435C 7EF870A4


rnd_val is
                                               7A95EE54 39D83828
        95B53929 3789D040 BAAF9751 C73B1F0E 66CE39AA 0E4DE0FC
```

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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                              A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

CTR_DRBG_Reseed

    entropy_input is
                                              C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is
                                              A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

  Update

    provided_data is
                                              60606060 60606060
        60606060 60606060 60606060 60606060 60606060 60606060


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

      While loop

      Key is
                           00D9D257 6D398E76 0057DAD3 6F462A0D
```

```
  V is
                      A3C3633D 964C6D0B 148D435C 7EF870A5

  output_block is
                      30A7280C 9DF010F7 C2876DA1 A7341E79

  temp is
                      30A7280C 9DF010F7 C2876DA1 A7341E79

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

  While loop

  Key is
                      00D9D257 6D398E76 0057DAD3 6F462A0D

  V is
                      A3C3633D 964C6D0B 148D435C 7EF870A6

  output_block is
                      49FCC388 3DF830EC 6667AB5D FB849096

  temp is
                                        30A7280C 9DF010F7
    C2876DA1 A7341E79 49FCC388 3DF830EC 6667AB5D FB849096

temp XOR provided_data is
                                        50C7486C FD907097
    A2E70DC1 C7547E19 299CA3E8 5D98508C 0607CB3D 9BE4F0F6

Key is
                      50C7486C FD907097 A2E70DC1 C7547E19

V is
                      299CA3E8 5D98508C 0607CB3D 9BE4F0F6
```

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
                          50C7486C FD907097 A2E70DC1 C7547E19


      V is
                          299CA3E8 5D98508C 0607CB3D 9BE4F0F9


      output_block is
                          9FD6CA5D C8B39E75 8ADCB5CF CB4012D1


      temp is
                          9FD6CA5D C8B39E75 8ADCB5CF CB4012D1


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

      While loop

      Key is
                          50C7486C FD907097 A2E70DC1 C7547E19
```

```
      V is
                          299CA3E8 5D98508C 0607CB3D 9BE4F0FA


      output_block is
                          81E4EA7A AFA955AA DB506F01 E3F27EAE


      temp is
                                                 9FD6CA5D C8B39E75
        8ADCB5CF CB4012D1 81E4EA7A AFA955AA DB506F01 E3F27EAE


    temp XOR provided_data is
                                                 9FD6CA5D C8B39E75
        8ADCB5CF CB4012D1 81E4EA7A AFA955AA DB506F01 E3F27EAE


    Key is
                          9FD6CA5D C8B39E75 8ADCB5CF CB4012D1


    V is
                          81E4EA7A AFA955AA DB506F01 E3F27EAE


rnd_val is
                                                 598F7694 08F56946
        EB720776 1263BABC 964F306B E99BBA5A E329E01C FA100EC2


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

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                 00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                                 80818283 84858687
```

```
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    PersonalizationString =
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    AdditionalInput = <empty>

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    prediction_resistance_flag = "PredictionResistance"

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

  Update

    provided_data is
                                                40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


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

      While loop
```

```
  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000001

  output_block is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

  temp is
                      58E2FCCE FA7E3061 367F1D57 A4E7455A

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

  While loop

  Key is
                      00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      0388DACE 60B6A392 F328C2B9 71B2FE78

  temp is
                                        58E2FCCE FA7E3061
    367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is
                                        18A2BC8E BA3E7021
    763F5D17 E4A7051A 43C89A8E 20F6E3D2 B36882F9 31F2BE38

Key is
                      18A2BC8E BA3E7021 763F5D17 E4A7051A
```

```
    V is
                          43C89A8E 20F6E3D2 B36882F9 31F2BE38


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

CTR_DRBG_Reseed

    entropy_input is
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    additional_input is  <empty>

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

  Update

    provided_data is
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


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

      While loop

      Key is
                          18A2BC8E BA3E7021 763F5D17 E4A7051A


      V is
```

```
                        43C89A8E 20F6E3D2 B36882F9 31F2BE39

      output_block is
                        FA1DF743 5039C649 3B14D8C8 F9715BA5

      temp is
                        FA1DF743 5039C649 3B14D8C8 F9715BA5

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

      While loop

      Key is
                        18A2BC8E BA3E7021 763F5D17 E4A7051A

      V is
                        43C89A8E 20F6E3D2 B36882F9 31F2BE3A

      output_block is
                        CE6EE312 20EEDEE3 65A4B6B7 2FD68554

      temp is
                                             FA1DF743 5039C649
        3B14D8C8 F9715BA5 CE6EE312 20EEDEE3 65A4B6B7 2FD68554

    temp XOR provided_data is
                                             7A9C75C0 D4BC40CE
        B39D5243 75FCD52A 5EFF7181 B47B4874 FD3D2C2C B34B1BCB

    Key is
                        7A9C75C0 D4BC40CE B39D5243 75FCD52A

    V is
                        5EFF7181 B47B4874 FD3D2C2C B34B1BCB

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

```
CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
                          7A9C75C0 D4BC40CE B39D5243 75FCD52A


      V is
                          5EFF7181 B47B4874 FD3D2C2C B34B1BCE


      output_block is
                          0B983A61 CA075354 1C9BC0C6 6AB5CE59


      temp is
                          0B983A61 CA075354 1C9BC0C6 6AB5CE59


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

      While loop

      Key is
                          7A9C75C0 D4BC40CE B39D5243 75FCD52A


      V is
                          5EFF7181 B47B4874 FD3D2C2C B34B1BCF
```

```
      output_block is
                           A6E4E62F 7A9B71B8 194B3BC2 475AF1B1


      temp is
                                              0B983A61 CA075354
        1C9BC0C6 6AB5CE59 A6E4E62F 7A9B71B8 194B3BC2 475AF1B1


    temp XOR provided_data is
                                              0B983A61 CA075354
        1C9BC0C6 6AB5CE59 A6E4E62F 7A9B71B8 194B3BC2 475AF1B1


    Key is
                           0B983A61 CA075354 1C9BC0C6 6AB5CE59


    V is
                           A6E4E62F 7A9B71B8 194B3BC2 475AF1B1


rnd_val is
                                              C7C914C1 AF21B9D0
        0002C9F2 11A9AB4A 3E7C3871 2779687A 03DFFD32 645CB4CD


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

CTR_DRBG_Reseed
```

```
    entropy_input is
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is  <empty>

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

  Update

    provided_data is
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


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

      While loop

      Key is
                          0B983A61 CA075354 1C9BC0C6 6AB5CE59


      V is
                          A6E4E62F 7A9B71B8 194B3BC2 475AF1B2


      output_block is
                          457D7BE0 6EC8D5F1 B712CFD2 5F1544F1


      temp is
                          457D7BE0 6EC8D5F1 B712CFD2 5F1544F1


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

      While loop

      Key is
                          0B983A61 CA075354 1C9BC0C6 6AB5CE59


      V is
                          A6E4E62F 7A9B71B8 194B3BC2 475AF1B3
```

```
      output_block is
                           F930608A 207776B5 A2B87C93 A513D3FC


      temp is
                                              457D7BE0 6EC8D5F1
        B712CFD2 5F1544F1 F930608A 207776B5 A2B87C93 A513D3FC


    temp XOR provided_data is
                                              85BCB923 AA0D1336
        7FDB0519 93D88A3E 29E1B259 F4A2A062 7A61A648 79CE0D23


    Key is
                           85BCB923 AA0D1336 7FDB0519 93D88A3E


    V is
                           29E1B259 F4A2A062 7A61A648 79CE0D23


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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                                              00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
```

```
                    85BCB923 AA0D1336 7FDB0519 93D88A3E

  V is
                    29E1B259 F4A2A062 7A61A648 79CE0D26

  output_block is
                    21F5F987 37C498DE F25C78C3 50447DAC

  temp is
                    21F5F987 37C498DE F25C78C3 50447DAC

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

  While loop

  Key is
                    85BCB923 AA0D1336 7FDB0519 93D88A3E

  V is
                    29E1B259 F4A2A062 7A61A648 79CE0D27

  output_block is
                    53D4BFA2 99CFBC0E 9D741ECA 610DAE5F

  temp is
                                      21F5F987 37C498DE
    F25C78C3 50447DAC 53D4BFA2 99CFBC0E 9D741ECA 610DAE5F

temp XOR provided_data is
                                      21F5F987 37C498DE
    F25C78C3 50447DAC 53D4BFA2 99CFBC0E 9D741ECA 610DAE5F

Key is
                    21F5F987 37C498DE F25C78C3 50447DAC

V is
```

```
                        53D4BFA2 99CFBC0E 9D741ECA 610DAE5F


rnd_val is
                                                35AF6092 8E3ED896
        20DE692D 9660289A 2D321CBC 0F1E0A58 724B393B 7735D445


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

CTR_DRBG

    Requested Security Strength = 128

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    EntropyInput1 (for Reseed1) =
                                                80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    EntropyInput2 (for Reseed2) =
                                                C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    PersonalizationString =
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    AdditionalInput1 =
                                                60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    AdditionalInput2 =
                                                A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                                                00010203 04050607
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F


    personal_str is
                                                40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    prediction_resistance_flag = "PredictionResistance"

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

  Update

    provided_data is
                                                40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


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

      While loop

      Key is
                          00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000001


      output_block is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A


      temp is
                          58E2FCCE FA7E3061 367F1D57 A4E7455A
```

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

      While loop

      Key is
                           00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000002


      output_block is
                           0388DACE 60B6A392 F328C2B9 71B2FE78


      temp is
                                               58E2FCCE FA7E3061
        367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78


    temp XOR provided_data is
                                               18A2BC8E BA3E7021
        763F5D17 E4A7051A 43C89A8E 20F6E3D2 B36882F9 31F2BE38


    Key is
                           18A2BC8E BA3E7021 763F5D17 E4A7051A


    V is
                           43C89A8E 20F6E3D2 B36882F9 31F2BE38


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                               60616263 64656667
```

```
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


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

CTR_DRBG_Reseed

    entropy_input is
                                               80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    additional_input is
                                               60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


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

  Update

    provided_data is
                                               E0E0E0E0 E0E0E0E0
        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0


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

      While loop

      Key is
                          18A2BC8E BA3E7021 763F5D17 E4A7051A


      V is
                          43C89A8E 20F6E3D2 B36882F9 31F2BE39


      output_block is
                          FA1DF743 5039C649 3B14D8C8 F9715BA5


      temp is
                          FA1DF743 5039C649 3B14D8C8 F9715BA5
```

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

      While loop

      Key is
                           18A2BC8E BA3E7021 763F5D17 E4A7051A


      V is
                           43C89A8E 20F6E3D2 B36882F9 31F2BE3A


      output_block is
                           CE6EE312 20EEDEE3 65A4B6B7 2FD68554


      temp is
                                             FA1DF743 5039C649
        3B14D8C8 F9715BA5 CE6EE312 20EEDEE3 65A4B6B7 2FD68554


    temp XOR provided_data is
                                             1AFD17A3 B0D926A9
       DBF43828 1991BB45 2E8E03F2 C00E3E03 85445657 CF3665B4


    Key is
                           1AFD17A3 B0D926A9 DBF43828 1991BB45


    V is
                           2E8E03F2 C00E3E03 85445657 CF3665B4


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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update
```

```
provided_data is
                                                00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


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

  While loop

  Key is
                      1AFD17A3 B0D926A9 DBF43828 1991BB45


  V is
                      2E8E03F2 C00E3E03 85445657 CF3665B7


  output_block is
                      47B3433E 78449967 B66DE6DD 5212883D


  temp is
                      47B3433E 78449967 B66DE6DD 5212883D


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

  While loop

  Key is
                      1AFD17A3 B0D926A9 DBF43828 1991BB45


  V is
                      2E8E03F2 C00E3E03 85445657 CF3665B8


  output_block is
                      561936F4 ADBD65A6 43E50E2F D753F120


  temp is
                                                47B3433E 78449967
    B66DE6DD 5212883D 561936F4 ADBD65A6 43E50E2F D753F120
```

```
    temp XOR provided_data is
                                            47B3433E 78449967
        B66DE6DD 5212883D 561936F4 ADBD65A6 43E50E2F D753F120


    Key is
                         47B3433E 78449967 B66DE6DD 5212883D


    V is
                         561936F4 ADBD65A6 43E50E2F D753F120


rnd_val is
                                            DCC71C5D 851228E5
        EEF37E18 6AECBDAE A081040E 0EC04DBE 3328B5AB E3249D2D


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

CTR_DRBG_Reseed

    entropy_input is
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is
                                            A0A1A2A3 A4A5A6A7
```

```
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

  Update

    provided_data is
                                                 60606060 60606060
        60606060 60606060 60606060 60606060 60606060 60606060


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

      While loop

      Key is
                          47B3433E 78449967 B66DE6DD 5212883D


      V is
                          561936F4 ADBD65A6 43E50E2F D753F121


      output_block is
                          605C7D97 F28AAD7B E85763BC 91432D98


      temp is
                          605C7D97 F28AAD7B E85763BC 91432D98


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

      While loop

      Key is
                          47B3433E 78449967 B66DE6DD 5212883D


      V is
                          561936F4 ADBD65A6 43E50E2F D753F122


      output_block is
                          05E5B36D AD934227 DD99A526 76689DD2
```

```
      temp is
                                                605C7D97 F28AAD7B
        E85763BC 91432D98 05E5B36D AD934227 DD99A526 76689DD2


    temp XOR provided_data is
                                                003C1DF7 92EACD1B
        883703DC F1234DF8 6585D30D CDF32247 BDF9C546 1608FDB2


    Key is
                          003C1DF7 92EACD1B 883703DC F1234DF8


    V is
                          6585D30D CDF32247 BDF9C546 1608FDB2

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
                          003C1DF7 92EACD1B 883703DC F1234DF8


      V is
```

```
                        6585D30D CDF32247 BDF9C546 1608FDB5

      output_block is
                        2CECDB8B 151A48A7 6473908D F85FFFB2

      temp is
                        2CECDB8B 151A48A7 6473908D F85FFFB2

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

      While loop

      Key is
                        003C1DF7 92EACD1B 883703DC F1234DF8

      V is
                        6585D30D CDF32247 BDF9C546 1608FDB6

      output_block is
                        3CD321D9 6DA4981F AEFC26D2 B9DEC7FC

      temp is
                                            2CECDB8B 151A48A7
        6473908D F85FFFB2 3CD321D9 6DA4981F AEFC26D2 B9DEC7FC

    temp XOR provided_data is
                                            2CECDB8B 151A48A7
        6473908D F85FFFB2 3CD321D9 6DA4981F AEFC26D2 B9DEC7FC

    Key is
                        2CECDB8B 151A48A7 6473908D F85FFFB2

    V is
                        3CD321D9 6DA4981F AEFC26D2 B9DEC7FC

rnd_val is
```

```
                                                15800389 9C6FCB09
        97B58522 B0AE5071 97CFE7B7 1B2D4CF0 F2E3334D 00491C12


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

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    PersonalizationString = <empty>

    AdditionalInput = <empty>

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

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

```
Update

  provided_data is
                         00010203 04050607 08090A0B 0C0D0E0F
      10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


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

    While loop

    Key is
      00000000 00000000 00000000 00000000 00000000 00000000


    V is
                         00000000 00000000 00000000 00000001


    output_block is
                         CD33B28A C773F74B A00ED1F3 12572435


    temp is
                         CD33B28A C773F74B A00ED1F3 12572435


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

    While loop

    Key is
      00000000 00000000 00000000 00000000 00000000 00000000


    V is
                         00000000 00000000 00000000 00000002


    output_block is
                         98E7247C 07F0FE41 1C267E43 84B0F600


    temp is
                                              CD33B28A C773F74B
```

```
        A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


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

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000003


      output_block is
                           2A3493E6 6235EE67 DEECCD2F 3B393BD8


      temp is
        CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
        1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


    temp XOR provided_data is
                           CD32B089 C376F14C A807DBF8 1E5A2A3A
        88F6366F 13E5E856 043F6458 98ADE81F 0A15B1C5 4610C840


    Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


    V is
                           043F6458 98ADE81F 0A15B1C5 4610C840


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256
```

```
    additional_input is  <empty>

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

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                          043F6458 98ADE81F 0A15B1C5 4610C843


      output_block is
                          685C8679 5A13E060 4CA155CA 4D9BF978


      temp is
                          685C8679 5A13E060 4CA155CA 4D9BF978


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

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                          043F6458 98ADE81F 0A15B1C5 4610C844


      output_block is
                          2D689829 7F86953C A13FD9F3 D499D39C
```

```
      temp is
                                              685C8679 5A13E060
        4CA155CA 4D9BF978 2D689829 7F86953C A13FD9F3 D499D39C


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

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                           043F6458 98ADE81F 0A15B1C5 4610C845


      output_block is
                           04C3FDEF A12684E0 F4DE317D DCA8DA26


      temp is
        685C8679 5A13E060 4CA155CA 4D9BF978 2D689829 7F86953C
        A13FD9F3 D499D39C 04C3FDEF A12684E0 F4DE317D DCA8DA26


    temp XOR provided_data is
                           685C8679 5A13E060 4CA155CA 4D9BF978
        2D689829 7F86953C A13FD9F3 D499D39C 04C3FDEF A12684E0


    Key is
        685C8679 5A13E060 4CA155CA 4D9BF978 2D689829 7F86953C


    V is
                           A13FD9F3 D499D39C 04C3FDEF A12684E0


rnd_val is
                                              01E0793E 6C7464FA
        FE1F6CF9 B7466A8A C4841737 9CBAA104 13DBCD98 E1977019
```

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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
        685C8679 5A13E060 4CA155CA 4D9BF978 2D689829 7F86953C


      V is
                          A13FD9F3 D499D39C 04C3FDEF A12684E3


      output_block is
                          8190E9BB FDFDDE79 E5264E86 6871234C


      temp is
                          8190E9BB FDFDDE79 E5264E86 6871234C


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

      While loop

      Key is
```

```
    685C8679 5A13E060 4CA155CA 4D9BF978 2D689829 7F86953C


  V is
                     A13FD9F3 D499D39C 04C3FDEF A12684E4


  output_block is
                     3CE8504E 14EF7C8A F4DE516E 7DB043D1


  temp is
                                          8190E9BB FDFDDE79
    E5264E86 6871234C 3CE8504E 14EF7C8A F4DE516E 7DB043D1


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

  While loop

  Key is
    685C8679 5A13E060 4CA155CA 4D9BF978 2D689829 7F86953C


  V is
                     A13FD9F3 D499D39C 04C3FDEF A12684E5


  output_block is
                     9A487B3A F1909DC3 169D374E C0B0D991


  temp is
    8190E9BB FDFDDE79 E5264E86 6871234C 3CE8504E 14EF7C8A
    F4DE516E 7DB043D1 9A487B3A F1909DC3 169D374E C0B0D991


temp XOR provided_data is
                     8190E9BB FDFDDE79 E5264E86 6871234C
    3CE8504E 14EF7C8A F4DE516E 7DB043D1 9A487B3A F1909DC3


Key is
    8190E9BB FDFDDE79 E5264E86 6871234C 3CE8504E 14EF7C8A
```

```
    V is
                          F4DE516E 7DB043D1 9A487B3A F1909DC3


rnd_val is
                                                 88CE7B6C 16365EEA
        6FEE02BF BAE2DF4D 93AB03B9 CF8807E5 BEAD31D4 FB721DC9


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

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    PersonalizationString = <empty>

    AdditionalInput1 =
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    AdditionalInput2 =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


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

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

```
CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                            00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

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

  Update

    provided_data is
                            00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


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

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                            00000000 00000000 00000000 00000001


      output_block is
                            CD33B28A C773F74B A00ED1F3 12572435


      temp is
                            CD33B28A C773F74B A00ED1F3 12572435


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

      While loop

      Key is
```

```
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                           CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


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

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      2A3493E6 6235EE67 DEECCD2F 3B393BD8


  temp is
    CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
    1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


temp XOR provided_data is
                      CD32B089 C376F14C A807DBF8 1E5A2A3A
    88F6366F 13E5E856 043F6458 98ADE81F 0A15B1C5 4610C840


Key is
    CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856
```

```
    V is
                          043F6458 98ADE81F 0A15B1C5 4610C840


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


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

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                          043F6458 98ADE81F 0A15B1C5 4610C841


      output_block is
                          01E0793E 6C7464FA FE1F6CF9 B7466A8A


      temp is
```

```
                    01E0793E 6C7464FA FE1F6CF9 B7466A8A


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

  While loop

  Key is
    CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


  V is
                    043F6458 98ADE81F 0A15B1C5 4610C842


  output_block is
                    C4841737 9CBAA104 13DBCD98 E1977019


  temp is
                                       01E0793E 6C7464FA
    FE1F6CF9 B7466A8A C4841737 9CBAA104 13DBCD98 E1977019


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

  While loop

  Key is
    CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


  V is
                    043F6458 98ADE81F 0A15B1C5 4610C843


  output_block is
                    685C8679 5A13E060 4CA155CA 4D9BF978


  temp is
    01E0793E 6C7464FA FE1F6CF9 B7466A8A C4841737 9CBAA104
    13DBCD98 E1977019 685C8679 5A13E060 4CA155CA 4D9BF978


temp XOR provided_data is
```

```
                        61811B5D 0811029D 96760692 DB2B04E5
        B4F56544 E8CFD773 6BA2B7E3 9DEA0E66 E8DD04FA DE9666E7


    Key is
        61811B5D 0811029D 96760692 DB2B04E5 B4F56544 E8CFD773


    V is
                        6BA2B7E3 9DEA0E66 E8DD04FA DE9666E7


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

  Update

    provided_data is
                        60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


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

      While loop

      Key is
        61811B5D 0811029D 96760692 DB2B04E5 B4F56544 E8CFD773


      V is
                        6BA2B7E3 9DEA0E66 E8DD04FA DE9666EA


      output_block is
                        C6FB2B83 812E5D99 7087CA64 E19A1ACD


      temp is
                        C6FB2B83 812E5D99 7087CA64 E19A1ACD


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

      While loop

      Key is
```

```
    61811B5D 0811029D 96760692 DB2B04E5 B4F56544 E8CFD773


  V is
                     6BA2B7E3 9DEA0E66 E8DD04FA DE9666EB


  output_block is
                     48AAF49B 9E8359A3 35B3B157 05F7C99E


  temp is
                                       C6FB2B83 812E5D99
    7087CA64 E19A1ACD 48AAF49B 9E8359A3 35B3B157 05F7C99E


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

  While loop

  Key is
    61811B5D 0811029D 96760692 DB2B04E5 B4F56544 E8CFD773


  V is
                     6BA2B7E3 9DEA0E66 E8DD04FA DE9666EC


  output_block is
                     C7F5365C 0BFF94EA 87BE9358 FDC201BA


  temp is
    C6FB2B83 812E5D99 7087CA64 E19A1ACD 48AAF49B 9E8359A3
    35B3B157 05F7C99E C7F5365C 0BFF94EA 87BE9358 FDC201BA


temp XOR provided_data is
                     A69A49E0 E54B3BFE 18EEA00F 8DF774A2
    38DB86E8 EAF62FD4 4DCACB2C 798AB7E1 4774B4DF 8F7A126D


Key is
    A69A49E0 E54B3BFE 18EEA00F 8DF774A2 38DB86E8 EAF62FD4
```

```
    V is
                          4DCACB2C 798AB7E1 4774B4DF 8F7A126D


rnd_val is
                                               3A298716 7FF43CD7
        94A9778F 3932A2E9 AA7C9518 24C82924 C7324560 4B0BEFA5


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


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

      While loop

      Key is
        A69A49E0 E54B3BFE 18EEA00F 8DF774A2 38DB86E8 EAF62FD4


      V is
                          4DCACB2C 798AB7E1 4774B4DF 8F7A126E
```

```
  output_block is
                      433A5A5C ECFD33CD FA67D7D6 5607CD48

  temp is
                      433A5A5C ECFD33CD FA67D7D6 5607CD48

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

  While loop

  Key is
    A69A49E0 E54B3BFE 18EEA00F 8DF774A2 38DB86E8 EAF62FD4

  V is
                      4DCACB2C 798AB7E1 4774B4DF 8F7A126F

  output_block is
                      BECC799D AAF47F22 CFD9EEF1 AD8B178D

  temp is
                                        433A5A5C ECFD33CD
    FA67D7D6 5607CD48 BECC799D AAF47F22 CFD9EEF1 AD8B178D

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

  While loop

  Key is
    A69A49E0 E54B3BFE 18EEA00F 8DF774A2 38DB86E8 EAF62FD4

  V is
                      4DCACB2C 798AB7E1 4774B4DF 8F7A1270

  output_block is
                      2D368884 3376F6BD D14EE304 9FA8BFEB

  temp is
```

```
        433A5A5C ECFD33CD FA67D7D6 5607CD48 BECC799D AAF47F22
        CFD9EEF1 AD8B178D 2D368884 3376F6BD D14EE304 9FA8BFEB


    temp XOR provided_data is
                          E39BF8FF 4858956A 52CE7D7D FAAA63E7
        0E7DCB2E 1E41C995 7760544A 1136A932 EDF74A47 F7B3307A


    Key is
        E39BF8FF 4858956A 52CE7D7D FAAA63E7 0E7DCB2E 1E41C995


    V is
                          7760544A 1136A932 EDF74A47 F7B3307A


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

  Update

    provided_data is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


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

      While loop

      Key is
        E39BF8FF 4858956A 52CE7D7D FAAA63E7 0E7DCB2E 1E41C995


      V is
                          7760544A 1136A932 EDF74A47 F7B3307D


      output_block is
                          76216733 654CD5AA 4F1756AB 4683568B


      temp is
                          76216733 654CD5AA 4F1756AB 4683568B
```

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

  While loop

  Key is
    E39BF8FF 4858956A 52CE7D7D FAAA63E7 0E7DCB2E 1E41C995


  V is
                      7760544A 1136A932 EDF74A47 F7B3307E


  output_block is
                      0D8A7249 375AA6BE 0EDC3CBD 26FF8E9C


  temp is
                                           76216733 654CD5AA
    4F1756AB 4683568B 0D8A7249 375AA6BE 0EDC3CBD 26FF8E9C


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

  While loop

  Key is
    E39BF8FF 4858956A 52CE7D7D FAAA63E7 0E7DCB2E 1E41C995


  V is
                      7760544A 1136A932 EDF74A47 F7B3307F


  output_block is
                      9413F800 3CC5FF4D 852CA338 AB836A1C


  temp is
    76216733 654CD5AA 4F1756AB 4683568B 0D8A7249 375AA6BE
    0EDC3CBD 26FF8E9C 9413F800 3CC5FF4D 852CA338 AB836A1C


temp XOR provided_data is
                      D680C590 C1E9730D E7BEFC00 EA2EF824
    BD3BC0FA 83EF1009 B6658606 9A423023 54D23AC3 F800398A
```

```
    Key is
        D680C590 C1E9730D E7BEFC00 EA2EF824 BD3BC0FA 83EF1009


    V is
                            B6658606 9A423023 54D23AC3 F800398A


rnd_val is
                                                 A963857B 976F18FD
        1F1B3301 DA08E8E8 4694AAFB 55EA2B10 196BEE84 77570853


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

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                            00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                            80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                            C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    PersonalizationString =
                            40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    AdditionalInput = <empty>

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

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

```
CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                           00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is
                           40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    prediction_resistance_flag = "No PredictionResistance"

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

  Update

    provided_data is
                           40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


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

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           CD33B28A C773F74B A00ED1F3 12572435


      temp is
                           CD33B28A C773F74B A00ED1F3 12572435


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

```
  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000002


  output_block is
                       98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                         CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


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

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000003


  output_block is
                       2A3493E6 6235EE67 DEECCD2F 3B393BD8


  temp is
    CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
    1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


temp XOR provided_data is
                       8D73F2CA 8733B70B E04E91B3 52176475
    D8A7643C 47B0BE01 5C663E03 C4F0B640 6A74D3A6 2275AE27


Key is
```

```
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


    V is
                        5C663E03 C4F0B640 6A74D3A6 2275AE27

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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                        00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


      V is
                        5C663E03 C4F0B640 6A74D3A6 2275AE2A


      output_block is
                        2D882249 1114B01B 2208E492 F0F35C54


      temp is
                        2D882249 1114B01B 2208E492 F0F35C54
```

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

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                      5C663E03 C4F0B640 6A74D3A6 2275AE2B


  output_block is
                      86555AB1 87E3784E 74F52A4A B2A563EE


  temp is
                                        2D882249 1114B01B
    2208E492 F0F35C54 86555AB1 87E3784E 74F52A4A B2A563EE


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

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                      5C663E03 C4F0B640 6A74D3A6 2275AE2C


  output_block is
                      005240DE 5857A85A 45E4B451 D42DAF2D


  temp is
    2D882249 1114B01B 2208E492 F0F35C54 86555AB1 87E3784E
    74F52A4A B2A563EE 005240DE 5857A85A 45E4B451 D42DAF2D


temp XOR provided_data is
                      2D882249 1114B01B 2208E492 F0F35C54
```

```
        86555AB1 87E3784E 74F52A4A B2A563EE 005240DE 5857A85A


    Key is
        2D882249 1114B01B 2208E492 F0F35C54 86555AB1 87E3784E


    V is
                         74F52A4A B2A563EE 005240DE 5857A85A


rnd_val is
                                           517150FF D52BD344
        DE78992B A224930C 98FC9FAC 541236E8 D199A476 B960B301


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                         00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
        2D882249 1114B01B 2208E492 F0F35C54 86555AB1 87E3784E


      V is
```

```
                    74F52A4A B2A563EE 005240DE 5857A85D

  output_block is
                    7EEB7C54 20128FEA C6BA2019 E6BBBEFC

  temp is
                    7EEB7C54 20128FEA C6BA2019 E6BBBEFC

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

  While loop

  Key is
    2D882249 1114B01B 2208E492 F0F35C54 86555AB1 87E3784E

  V is
                    74F52A4A B2A563EE 005240DE 5857A85E

  output_block is
                    54E9AE9E 6DF3C90C E1D395C3 E87F03BD

  temp is
                                        7EEB7C54 20128FEA
    C6BA2019 E6BBBEFC 54E9AE9E 6DF3C90C E1D395C3 E87F03BD

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

  While loop

  Key is
    2D882249 1114B01B 2208E492 F0F35C54 86555AB1 87E3784E

  V is
                    74F52A4A B2A563EE 005240DE 5857A85F

  output_block is
                    000D5096 45D19E8E 40EE54D9 A2D151B4
```

```
      temp is
        7EEB7C54 20128FEA C6BA2019 E6BBBEFC 54E9AE9E 6DF3C90C
        E1D395C3 E87F03BD 000D5096 45D19E8E 40EE54D9 A2D151B4


    temp XOR provided_data is
                         7EEB7C54 20128FEA C6BA2019 E6BBBEFC
        54E9AE9E 6DF3C90C E1D395C3 E87F03BD 000D5096 45D19E8E


    Key is
        7EEB7C54 20128FEA C6BA2019 E6BBBEFC 54E9AE9E 6DF3C90C


    V is
                         E1D395C3 E87F03BD 000D5096 45D19E8E


rnd_val is
                                            1F46912D 4DEA17B8
        6500AA70 836A5076 24C090C5 C440EB07 D46A05AE 4822113D


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

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                         00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                         80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                         C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7
```

```
    PersonalizationString =
                          40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    AdditionalInput1 =
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    AdditionalInput2 =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is
                          40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    prediction_resistance_flag = "No PredictionResistance"

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

  Update

    provided_data is
                          40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


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

      While loop
```

```
  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000001


  output_block is
                       CD33B28A C773F74B A00ED1F3 12572435


  temp is
                       CD33B28A C773F74B A00ED1F3 12572435


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

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000002


  output_block is
                       98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                          CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


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

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000
```

```
      V is
                          00000000 00000000 00000000 00000003


      output_block is
                          2A3493E6 6235EE67 DEECCD2F 3B393BD8


      temp is
        CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
        1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


    temp XOR provided_data is
                          8D73F2CA 8733B70B E04E91B3 52176475
        D8A7643C 47B0BE01 5C663E03 C4F0B640 6A74D3A6 2275AE27


    Key is
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


    V is
                          5C663E03 C4F0B640 6A74D3A6 2275AE27


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


  additional_input <> NULL, process appropriately
---------------------------

  Update
```

```
provided_data is
                      60616263 64656667 68696A6B 6C6D6E6F
    70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


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

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                      5C663E03 C4F0B640 6A74D3A6 2275AE28


  output_block is
                      517150FF D52BD344 DE78992B A224930C


  temp is
                      517150FF D52BD344 DE78992B A224930C


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

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                      5C663E03 C4F0B640 6A74D3A6 2275AE29


  output_block is
                      98FC9FAC 541236E8 D199A476 B960B301


  temp is
                                        517150FF D52BD344
    DE78992B A224930C 98FC9FAC 541236E8 D199A476 B960B301
```

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

      While loop

      Key is
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


      V is
                           5C663E03 C4F0B640 6A74D3A6 2275AE2A


      output_block is
                           2D882249 1114B01B 2208E492 F0F35C54


      temp is
        517150FF D52BD344 DE78992B A224930C 98FC9FAC 541236E8
        D199A476 B960B301 2D882249 1114B01B 2208E492 F0F35C54


    temp XOR provided_data is
                           3110329C B14EB523 B611F340 CE49FD63
        E88DEDDF 2067409F A9E0DE0D C51DCD7E AD09A0CA 9591369C


    Key is
        3110329C B14EB523 B611F340 CE49FD63 E88DEDDF 2067409F


    V is
                           A9E0DE0D C51DCD7E AD09A0CA 9591369C


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

  Update

    provided_data is
                           60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


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

      While loop
```

```
  Key is
    3110329C B14EB523 B611F340 CE49FD63 E88DEDDF 2067409F


  V is
                      A9E0DE0D C51DCD7E AD09A0CA 9591369F


  output_block is
                      5DD0E3F8 4FBC38F3 B20AE469 CE505605


  temp is
                      5DD0E3F8 4FBC38F3 B20AE469 CE505605


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

  While loop

  Key is
    3110329C B14EB523 B611F340 CE49FD63 E88DEDDF 2067409F


  V is
                      A9E0DE0D C51DCD7E AD09A0CA 959136A0


  output_block is
                      54EDA5FB 1641935C 6E667BDA 293E7ED9


  temp is
                                        5DD0E3F8 4FBC38F3
    B20AE469 CE505605 54EDA5FB 1641935C 6E667BDA 293E7ED9


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

  While loop

  Key is
    3110329C B14EB523 B611F340 CE49FD63 E88DEDDF 2067409F
```

```
      V is
                          A9E0DE0D C51DCD7E AD09A0CA 959136A1


      output_block is
                          E7A75AA5 60343055 4D6FB178 58794471


      temp is
        5DD0E3F8 4FBC38F3 B20AE469 CE505605 54EDA5FB 1641935C
        6E667BDA 293E7ED9 E7A75AA5 60343055 4D6FB178 58794471


    temp XOR provided_data is
                          3DB1819B 2BD95E94 DA638E02 A23D386A
        249CD788 6234E52B 161F01A1 554300A6 6726D826 E4B1B6D2


    Key is
        3DB1819B 2BD95E94 DA638E02 A23D386A 249CD788 6234E52B


    V is
                          161F01A1 554300A6 6726D826 E4B1B6D2


rnd_val is
                                             ABB31FC6 61357CEB
        BCAE1E1C AEAA2E20 2F391044 9C5033B4 8FD3A23B DB7EA158


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7
```

```
  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


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

      While loop

      Key is
        3DB1819B 2BD95E94 DA638E02 A23D386A 249CD788 6234E52B


      V is
                          161F01A1 554300A6 6726D826 E4B1B6D3


      output_block is
                          BF216E90 8D69EC04 9E25BAB5 738BA1B4


      temp is
                          BF216E90 8D69EC04 9E25BAB5 738BA1B4


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

      While loop

      Key is
        3DB1819B 2BD95E94 DA638E02 A23D386A 249CD788 6234E52B


      V is
                          161F01A1 554300A6 6726D826 E4B1B6D4


      output_block is
                          830F8CC5 6B61D025 DE9BEC72 D8631655
```

```
      temp is
                                                BF216E90 8D69EC04
        9E25BAB5 738BA1B4 830F8CC5 6B61D025 DE9BEC72 D8631655


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

      While loop

      Key is
        3DB1819B 2BD95E94 DA638E02 A23D386A 249CD788 6234E52B


      V is
                           161F01A1 554300A6 6726D826 E4B1B6D5


      output_block is
                           C7D7EA9B A10168F8 AAC66626 259B5C4F


      temp is
        BF216E90 8D69EC04 9E25BAB5 738BA1B4 830F8CC5 6B61D025
        DE9BEC72 D8631655 C7D7EA9B A10168F8 AAC66626 259B5C4F


    temp XOR provided_data is
                           1F80CC33 29CC4AA3 368C101E DF260F1B
        33BE3E76 DFD46692 662256C9 64DEA8EA 07162858 65C4AE3F


    Key is
        1F80CC33 29CC4AA3 368C101E DF260F1B 33BE3E76 DFD46692


    V is
                           662256C9 64DEA8EA 07162858 65C4AE3F


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

  Update

    provided_data is
                           A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7
```

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

  While loop

  Key is
    1F80CC33 29CC4AA3 368C101E DF260F1B 33BE3E76 DFD46692


  V is
                       662256C9 64DEA8EA 07162858 65C4AE42


  output_block is
                       19F7F6A1 528CBEE6 3F9CBF4F 1AB3408F


  temp is
                       19F7F6A1 528CBEE6 3F9CBF4F 1AB3408F


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

  While loop

  Key is
    1F80CC33 29CC4AA3 368C101E DF260F1B 33BE3E76 DFD46692


  V is
                       662256C9 64DEA8EA 07162858 65C4AE43


  output_block is
                       F239F9F4 A8AFC42D D4A50A9D 3DE4C243


  temp is
                                          19F7F6A1 528CBEE6
    3F9CBF4F 1AB3408F F239F9F4 A8AFC42D D4A50A9D 3DE4C243


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

  While loop
```

```
      Key is
        1F80CC33 29CC4AA3 368C101E DF260F1B 33BE3E76 DFD46692


      V is
                           662256C9 64DEA8EA 07162858 65C4AE44


      output_block is
                           4B4E6879 44DCF4AB ACACB343 D6B9EB4D


      temp is
        19F7F6A1 528CBEE6 3F9CBF4F 1AB3408F F239F9F4 A8AFC42D
        D4A50A9D 3DE4C243 4B4E6879 44DCF4AB ACACB343 D6B9EB4D


    temp XOR provided_data is
                           B9565402 F6291841 973515E4 B61EEE20
        42884B47 1C1A729A 6C1CB026 81597CFC 8B8FAABA 8019326C


    Key is
        B9565402 F6291841 973515E4 B61EEE20 42884B47 1C1A729A


    V is
                           6C1CB026 81597CFC 8B8FAABA 8019326C


rnd_val is
                                              08C0521E BC9871E9
        DC055DA1 B79E2FF0 DCE28C18 9E83156F F3D71586 21F5675A


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

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                           00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
```

```
    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    PersonalizationString = <empty>

    AdditionalInput = <empty>

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

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

  Update

    provided_data is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


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

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000
```

```
  V is
                      00000000 00000000 00000000 00000001


  output_block is
                      CD33B28A C773F74B A00ED1F3 12572435


  temp is
                      CD33B28A C773F74B A00ED1F3 12572435


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

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                          CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


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

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003
```

```
      output_block is
                          2A3493E6 6235EE67 DEECCD2F 3B393BD8


      temp is
        CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
        1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


    temp XOR provided_data is
                          CD32B089 C376F14C A807DBF8 1E5A2A3A
        88F6366F 13E5E856 043F6458 98ADE81F 0A15B1C5 4610C840


    Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


    V is
                          043F6458 98ADE81F 0A15B1C5 4610C840


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

CTR_DRBG_Reseed

    entropy_input is
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    additional_input is  <empty>
```

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

  Update

    provided_data is
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


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

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                          043F6458 98ADE81F 0A15B1C5 4610C841


      output_block is
                          01E0793E 6C7464FA FE1F6CF9 B7466A8A


      temp is
                          01E0793E 6C7464FA FE1F6CF9 B7466A8A


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

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                          043F6458 98ADE81F 0A15B1C5 4610C842


      output_block is
                          C4841737 9CBAA104 13DBCD98 E1977019
```

```
      temp is
                                                01E0793E 6C7464FA
        FE1F6CF9 B7466A8A C4841737 9CBAA104 13DBCD98 E1977019


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

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                           043F6458 98ADE81F 0A15B1C5 4610C843


      output_block is
                           685C8679 5A13E060 4CA155CA 4D9BF978


      temp is
        01E0793E 6C7464FA FE1F6CF9 B7466A8A C4841737 9CBAA104
        13DBCD98 E1977019 685C8679 5A13E060 4CA155CA 4D9BF978


    temp XOR provided_data is
                           8161FBBD E8F1E27D 7696E672 3BCBE405
        541585A4 082F3793 8B425703 7D0AEE86 C8FD24DA FEB646C7


    Key is
        8161FBBD E8F1E27D 7696E672 3BCBE405 541585A4 082F3793


    V is
                           8B425703 7D0AEE86 C8FD24DA FEB646C7


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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>
```

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

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
        8161FBBD E8F1E27D 7696E672 3BCBE405 541585A4 082F3793


      V is
                          8B425703 7D0AEE86 C8FD24DA FEB646CA


      output_block is
                          D22454A5 C69A88BB 9F794ECD BE269F00


      temp is
                          D22454A5 C69A88BB 9F794ECD BE269F00


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

      While loop

      Key is
        8161FBBD E8F1E27D 7696E672 3BCBE405 541585A4 082F3793


      V is
                          8B425703 7D0AEE86 C8FD24DA FEB646CB


      output_block is
                          A5A864D8 F73455B5 AF08CFCB 5A692D38
```

```
      temp is
                                              D22454A5 C69A88BB
        9F794ECD BE269F00 A5A864D8 F73455B5 AF08CFCB 5A692D38


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

      While loop

      Key is
        8161FBBD E8F1E27D 7696E672 3BCBE405 541585A4 082F3793


      V is
                           8B425703 7D0AEE86 C8FD24DA FEB646CC


      output_block is
                           E7E12D86 FC49BC02 8EC6F12C CD5D8AEB


      temp is
        D22454A5 C69A88BB 9F794ECD BE269F00 A5A864D8 F73455B5
        AF08CFCB 5A692D38 E7E12D86 FC49BC02 8EC6F12C CD5D8AEB


    temp XOR provided_data is
                           D22454A5 C69A88BB 9F794ECD BE269F00
        A5A864D8 F73455B5 AF08CFCB 5A692D38 E7E12D86 FC49BC02


    Key is
        D22454A5 C69A88BB 9F794ECD BE269F00 A5A864D8 F73455B5


    V is
                           AF08CFCB 5A692D38 E7E12D86 FC49BC02


rnd_val is
                                              2A63138E AC6C8BD5
        AFDBEA16 C751A239 24A5C5C3 63452EF1 8259D96F EA6D6334


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

```
Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

CTR_DRBG_Reseed

    entropy_input is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    additional_input is  <empty>

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

  Update

    provided_data is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


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

      While loop

      Key is
        D22454A5 C69A88BB 9F794ECD BE269F00 A5A864D8 F73455B5


      V is
                          AF08CFCB 5A692D38 E7E12D86 FC49BC03


      output_block is
                          B361741A 22BDF0A6 B4FC7A25 36750B6D
```

```
  temp is
                      B361741A 22BDF0A6 B4FC7A25 36750B6D


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

  While loop

  Key is
    D22454A5 C69A88BB 9F794ECD BE269F00 A5A864D8 F73455B5


  V is
                      AF08CFCB 5A692D38 E7E12D86 FC49BC04


  output_block is
                      CD76540C 799278F1 511ACBAD F835DFAF


  temp is
                                        B361741A 22BDF0A6
    B4FC7A25 36750B6D CD76540C 799278F1 511ACBAD F835DFAF


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

  While loop

  Key is
    D22454A5 C69A88BB 9F794ECD BE269F00 A5A864D8 F73455B5


  V is
                      AF08CFCB 5A692D38 E7E12D86 FC49BC05


  output_block is
                      33D4CE1B C9CE5AE7 572F5244 41F61501


  temp is
    B361741A 22BDF0A6 B4FC7A25 36750B6D CD76540C 799278F1
    511ACBAD F835DFAF 33D4CE1B C9CE5AE7 572F5244 41F61501
```

```
    temp XOR provided_data is
                          73A0B6D9 E6783661 7C35B0EE FAB8C5A2
        1DA786DF AD47AE26 89C31176 24E80170 D3352CF8 2D2BBC00


    Key is
        73A0B6D9 E6783661 7C35B0EE FAB8C5A2 1DA786DF AD47AE26


    V is
                          89C31176 24E80170 D3352CF8 2D2BBC00


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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
        73A0B6D9 E6783661 7C35B0EE FAB8C5A2 1DA786DF AD47AE26


      V is
                          89C31176 24E80170 D3352CF8 2D2BBC03


      output_block is
                          29BC0399 0071959E 1B1883BE 6CFB8491
```

```
  temp is
                      29BC0399 0071959E 1B1883BE 6CFB8491


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

  While loop

  Key is
    73A0B6D9 E6783661 7C35B0EE FAB8C5A2 1DA786DF AD47AE26


  V is
                      89C31176 24E80170 D3352CF8 2D2BBC04


  output_block is
                      137879F8 D65054CA FE54B28E D4893A5F


  temp is
                                        29BC0399 0071959E
    1B1883BE 6CFB8491 137879F8 D65054CA FE54B28E D4893A5F


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

  While loop

  Key is
    73A0B6D9 E6783661 7C35B0EE FAB8C5A2 1DA786DF AD47AE26


  V is
                      89C31176 24E80170 D3352CF8 2D2BBC05


  output_block is
                      4A792EC9 5BAE9624 D529E396 88DE671D


  temp is
    29BC0399 0071959E 1B1883BE 6CFB8491 137879F8 D65054CA
    FE54B28E D4893A5F 4A792EC9 5BAE9624 D529E396 88DE671D
```

```
    temp XOR provided_data is
                          29BC0399 0071959E 1B1883BE 6CFB8491
        137879F8 D65054CA FE54B28E D4893A5F 4A792EC9 5BAE9624


    Key is
        29BC0399 0071959E 1B1883BE 6CFB8491 137879F8 D65054CA


    V is
                          FE54B28E D4893A5F 4A792EC9 5BAE9624


rnd_val is
                                            7B737A56 AD339224
        EA513F69 F7D4253E 832B6B48 A82AFA53 28C8E061 7F55AB54


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

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    PersonalizationString = <empty>

    AdditionalInput1 =
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687
```

```
    AdditionalInput2 =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

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

  Update

    provided_data is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


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

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000001


      output_block is
                          CD33B28A C773F74B A00ED1F3 12572435
```

```
  temp is
                      CD33B28A C773F74B A00ED1F3 12572435


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

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                        CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


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

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      2A3493E6 6235EE67 DEECCD2F 3B393BD8


  temp is
    CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
    1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8
```

```
    temp XOR provided_data is
                          CD32B089 C376F14C A807DBF8 1E5A2A3A
        88F6366F 13E5E856 043F6458 98ADE81F 0A15B1C5 4610C840


    Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


    V is
                          043F6458 98ADE81F 0A15B1C5 4610C840


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


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

CTR_DRBG_Reseed

    entropy_input is
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


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

```
Update

  provided_data is
                        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0
      E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 20202020 20202020


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

    While loop

    Key is
      CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


    V is
                        043F6458 98ADE81F 0A15B1C5 4610C841


    output_block is
                        01E0793E 6C7464FA FE1F6CF9 B7466A8A


    temp is
                        01E0793E 6C7464FA FE1F6CF9 B7466A8A


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

    While loop

    Key is
      CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


    V is
                        043F6458 98ADE81F 0A15B1C5 4610C842


    output_block is
                        C4841737 9CBAA104 13DBCD98 E1977019


    temp is
                                             01E0793E 6C7464FA
      FE1F6CF9 B7466A8A C4841737 9CBAA104 13DBCD98 E1977019
```

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

      While loop

      Key is
        CD32B089 C376F14C A807DBF8 1E5A2A3A 88F6366F 13E5E856


      V is
                           043F6458 98ADE81F 0A15B1C5 4610C843


      output_block is
                           685C8679 5A13E060 4CA155CA 4D9BF978


      temp is
        01E0793E 6C7464FA FE1F6CF9 B7466A8A C4841737 9CBAA104
        13DBCD98 E1977019 685C8679 5A13E060 4CA155CA 4D9BF978


    temp XOR provided_data is
                           E10099DE 8C94841A 1EFF8C19 57A68A6A
        2464F7D7 7C5A41E4 F33B2D78 017790F9 487CA659 7A33C040


    Key is
        E10099DE 8C94841A 1EFF8C19 57A68A6A 2464F7D7 7C5A41E4


    V is
                           F33B2D78 017790F9 487CA659 7A33C040


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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

```
Update

  provided_data is
                        00000000 00000000 00000000 00000000
      00000000 00000000 00000000 00000000 00000000 00000000


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

    While loop

    Key is
      E10099DE 8C94841A 1EFF8C19 57A68A6A 2464F7D7 7C5A41E4


    V is
                        F33B2D78 017790F9 487CA659 7A33C043


    output_block is
                        8634F673 A82114CB 4A44F2FE A27931AC


    temp is
                        8634F673 A82114CB 4A44F2FE A27931AC


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

    While loop

    Key is
      E10099DE 8C94841A 1EFF8C19 57A68A6A 2464F7D7 7C5A41E4


    V is
                        F33B2D78 017790F9 487CA659 7A33C044


    output_block is
                        A63249E0 C3BC126A 9EA4A87C 1E175989


    temp is
                                            8634F673 A82114CB
      4A44F2FE A27931AC A63249E0 C3BC126A 9EA4A87C 1E175989
```

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

      While loop

      Key is
        E10099DE 8C94841A 1EFF8C19 57A68A6A 2464F7D7 7C5A41E4


      V is
                           F33B2D78 017790F9 487CA659 7A33C045


      output_block is
                           DA056F63 F4FDE170 DC496497 1DEB4607


      temp is
        8634F673 A82114CB 4A44F2FE A27931AC A63249E0 C3BC126A
        9EA4A87C 1E175989 DA056F63 F4FDE170 DC496497 1DEB4607


    temp XOR provided_data is
                           8634F673 A82114CB 4A44F2FE A27931AC
        A63249E0 C3BC126A 9EA4A87C 1E175989 DA056F63 F4FDE170


    Key is
        8634F673 A82114CB 4A44F2FE A27931AC A63249E0 C3BC126A


    V is
                           9EA4A87C 1E175989 DA056F63 F4FDE170


rnd_val is
                                              771B1F40 BFCE49D0
        9CFF56F8 9B171066 B07B6F07 BDFEAD61 04A5DCDA 011F2C68


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

Second call to Generate

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

```
CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


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

CTR_DRBG_Reseed

    entropy_input is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


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

  Update

    provided_data is
                          60606060 60606060 60606060 60606060
        60606060 60606060 60606060 60606060 20202020 20202020


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

      While loop

      Key is
        8634F673 A82114CB 4A44F2FE A27931AC A63249E0 C3BC126A


      V is
                          9EA4A87C 1E175989 DA056F63 F4FDE171
```

```
  output_block is
                      ECAAFA28 34FD5CD0 1CBBE049 55247EE9

  temp is
                      ECAAFA28 34FD5CD0 1CBBE049 55247EE9

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

  While loop

  Key is
    8634F673 A82114CB 4A44F2FE A27931AC A63249E0 C3BC126A

  V is
                      9EA4A87C 1E175989 DA056F63 F4FDE172

  output_block is
                      A167A122 6E3FAB97 76DDA1B2 BEC2CC85

  temp is
                                        ECAAFA28 34FD5CD0
    1CBBE049 55247EE9 A167A122 6E3FAB97 76DDA1B2 BEC2CC85

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

  While loop

  Key is
    8634F673 A82114CB 4A44F2FE A27931AC A63249E0 C3BC126A

  V is
                      9EA4A87C 1E175989 DA056F63 F4FDE173

  output_block is
                      26683FD2 A0E12C4C 11AE83C9 69EA69C6

  temp is
```

```
        ECAAFA28 34FD5CD0 1CBBE049 55247EE9 A167A122 6E3FAB97
        76DDA1B2 BEC2CC85 26683FD2 A0E12C4C 11AE83C9 69EA69C6


    temp XOR provided_data is
                         8CCA9A48 549D3CB0 7CDB8029 35441E89
        C107C142 0E5FCBF7 16BDC1D2 DEA2ACE5 06481FF2 80C10C6C


    Key is
        8CCA9A48 549D3CB0 7CDB8029 35441E89 C107C142 0E5FCBF7


    V is
                         16BDC1D2 DEA2ACE5 06481FF2 80C10C6C


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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                         00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
        8CCA9A48 549D3CB0 7CDB8029 35441E89 C107C142 0E5FCBF7


      V is
                         16BDC1D2 DEA2ACE5 06481FF2 80C10C6F
```

```
  output_block is
                      298EC2BE BC7DAE53 F88D67DE 7125CB97

  temp is
                      298EC2BE BC7DAE53 F88D67DE 7125CB97

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

  While loop

  Key is
    8CCA9A48 549D3CB0 7CDB8029 35441E89 C107C142 0E5FCBF7

  V is
                      16BDC1D2 DEA2ACE5 06481FF2 80C10C70

  output_block is
                      E06FA0E8 A20A15A1 FC155364 07F4A3E9

  temp is
                                        298EC2BE BC7DAE53
    F88D67DE 7125CB97 E06FA0E8 A20A15A1 FC155364 07F4A3E9

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

  While loop

  Key is
    8CCA9A48 549D3CB0 7CDB8029 35441E89 C107C142 0E5FCBF7

  V is
                      16BDC1D2 DEA2ACE5 06481FF2 80C10C71

  output_block is
                      9036A585 5D5D1DA7 5D0BE6B0 404CA1B9

  temp is
```

```
        298EC2BE BC7DAE53 F88D67DE 7125CB97 E06FA0E8 A20A15A1
        FC155364 07F4A3E9 9036A585 5D5D1DA7 5D0BE6B0 404CA1B9


    temp XOR provided_data is
                         298EC2BE BC7DAE53 F88D67DE 7125CB97
        E06FA0E8 A20A15A1 FC155364 07F4A3E9 9036A585 5D5D1DA7


    Key is
        298EC2BE BC7DAE53 F88D67DE 7125CB97 E06FA0E8 A20A15A1


    V is
                         FC155364 07F4A3E9 9036A585 5D5D1DA7


rnd_val is
                                            E2F2D79B 95699645
        125E327B 6E277ADE 061CA509 70E25CD3 7F42347E 371D3A24


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

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                         00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                         80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                         C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    PersonalizationString =
                         40414243 44454647 48494A4B 4C4D4E4F
```

```
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    AdditionalInput = <empty>

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                         00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is
                         40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    prediction_resistance_flag = "PredictionResistance"

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

  Update

    provided_data is
                         40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


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

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                         00000000 00000000 00000000 00000001


      output_block is
                         CD33B28A C773F74B A00ED1F3 12572435
```

```
  temp is
                      CD33B28A C773F74B A00ED1F3 12572435


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

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                        CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


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

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      2A3493E6 6235EE67 DEECCD2F 3B393BD8


  temp is
    CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
    1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8
```

```
    temp XOR provided_data is
                          8D73F2CA 8733B70B E04E91B3 52176475
        D8A7643C 47B0BE01 5C663E03 C4F0B640 6A74D3A6 2275AE27


    Key is
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


    V is
                          5C663E03 C4F0B640 6A74D3A6 2275AE27


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

CTR_DRBG_Reseed

    entropy_input is
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    additional_input is  <empty>

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

  Update

    provided_data is
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
```

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

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                       5C663E03 C4F0B640 6A74D3A6 2275AE28


  output_block is
                       517150FF D52BD344 DE78992B A224930C


  temp is
                       517150FF D52BD344 DE78992B A224930C


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

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                       5C663E03 C4F0B640 6A74D3A6 2275AE29


  output_block is
                       98FC9FAC 541236E8 D199A476 B960B301


  temp is
                                          517150FF D52BD344
    DE78992B A224930C 98FC9FAC 541236E8 D199A476 B960B301


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

  While loop
```

```
      Key is
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


      V is
                           5C663E03 C4F0B640 6A74D3A6 2275AE2A


      output_block is
                           2D882249 1114B01B 2208E492 F0F35C54


      temp is
        517150FF D52BD344 DE78992B A224930C 98FC9FAC 541236E8
        D199A476 B960B301 2D882249 1114B01B 2208E492 F0F35C54


    temp XOR provided_data is
                           D1F0D27C 51AE55C3 56F113A0 2EA91D83
        086D0D3F C087A07F 49003EED 25FD2D9E 8D2980EA B5B116BC


    Key is
        D1F0D27C 51AE55C3 56F113A0 2EA91D83 086D0D3F C087A07F


    V is
                           49003EED 25FD2D9E 8D2980EA B5B116BC


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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                           00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
```

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

  While loop

  Key is
    D1F0D27C 51AE55C3 56F113A0 2EA91D83 086D0D3F C087A07F


  V is
                       49003EED 25FD2D9E 8D2980EA B5B116BF


  output_block is
                       A56D4CE9 FD170AE7 82685E09 9032604C


  temp is
                       A56D4CE9 FD170AE7 82685E09 9032604C


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

  While loop

  Key is
    D1F0D27C 51AE55C3 56F113A0 2EA91D83 086D0D3F C087A07F


  V is
                       49003EED 25FD2D9E 8D2980EA B5B116C0


  output_block is
                       6E29C59B 2273C047 5F34F3BF 7703D618


  temp is
                                            A56D4CE9 FD170AE7
    82685E09 9032604C 6E29C59B 2273C047 5F34F3BF 7703D618


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

  While loop
```

```
      Key is
        D1F0D27C 51AE55C3 56F113A0 2EA91D83 086D0D3F C087A07F


      V is
                           49003EED 25FD2D9E 8D2980EA B5B116C1


      output_block is
                           2A65FBCB E232DB6C 99F15760 4D61C485


      temp is
        A56D4CE9 FD170AE7 82685E09 9032604C 6E29C59B 2273C047
        5F34F3BF 7703D618 2A65FBCB E232DB6C 99F15760 4D61C485


    temp XOR provided_data is
                           A56D4CE9 FD170AE7 82685E09 9032604C
        6E29C59B 2273C047 5F34F3BF 7703D618 2A65FBCB E232DB6C


    Key is
        A56D4CE9 FD170AE7 82685E09 9032604C 6E29C59B 2273C047


    V is
                           5F34F3BF 7703D618 2A65FBCB E232DB6C


rnd_val is
                                              77562EBE 8EECDF9E
        DB9A2E88 640D8DFF 9F2A5E99 20B30313 DC33D3A8 CE3BAB41


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256
```

```
    additional_input is  <empty>

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

CTR_DRBG_Reseed

    entropy_input is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    additional_input is  <empty>

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

  Update

    provided_data is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


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

      While loop

      Key is
        A56D4CE9 FD170AE7 82685E09 9032604C 6E29C59B 2273C047


      V is
                          5F34F3BF 7703D618 2A65FBCB E232DB6D


      output_block is
                          05A1EDE5 719ACDE6 47A89FB9 87921D0E


      temp is
                          05A1EDE5 719ACDE6 47A89FB9 87921D0E


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

      While loop
```

```
  Key is
    A56D4CE9 FD170AE7 82685E09 9032604C 6E29C59B 2273C047


  V is
                       5F34F3BF 7703D618 2A65FBCB E232DB6E


  output_block is
                       325735D9 1CCAA935 6DCA4C7E B58663A3


  temp is
                                         05A1EDE5 719ACDE6
    47A89FB9 87921D0E 325735D9 1CCAA935 6DCA4C7E B58663A3


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

  While loop

  Key is
    A56D4CE9 FD170AE7 82685E09 9032604C 6E29C59B 2273C047


  V is
                       5F34F3BF 7703D618 2A65FBCB E232DB6F


  output_block is
                       763ECAA0 2113F3A2 7A47C858 C9A54596


  temp is
    05A1EDE5 719ACDE6 47A89FB9 87921D0E 325735D9 1CCAA935
    6DCA4C7E B58663A3 763ECAA0 2113F3A2 7A47C858 C9A54596


temp XOR provided_data is
                       C5602F26 B55F0B21 8F615572 4B5FD3C1
    E286E70A C81F7FE2 B51396A5 695BBD7C 96DF2843 C5F61545


Key is
    C5602F26 B55F0B21 8F615572 4B5FD3C1 E286E70A C81F7FE2
```

```
    V is
                          B51396A5 695BBD7C 96DF2843 C5F61545

***************************************************************
CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
        C5602F26 B55F0B21 8F615572 4B5FD3C1 E286E70A C81F7FE2


      V is
                          B51396A5 695BBD7C 96DF2843 C5F61548


      output_block is
                          602034D1 338F663B 0C0D138A D6C6901E


      temp is
                          602034D1 338F663B 0C0D138A D6C6901E


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

      While loop
```

```
  Key is
    C5602F26 B55F0B21 8F615572 4B5FD3C1 E286E70A C81F7FE2


  V is
                      B51396A5 695BBD7C 96DF2843 C5F61549


  output_block is
                      E54548F7 E8C639EE 17A732EB 53C51B24


  temp is
                                          602034D1 338F663B
    0C0D138A D6C6901E E54548F7 E8C639EE 17A732EB 53C51B24


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

  While loop

  Key is
    C5602F26 B55F0B21 8F615572 4B5FD3C1 E286E70A C81F7FE2


  V is
                      B51396A5 695BBD7C 96DF2843 C5F6154A


  output_block is
                      8C2513B5 1E0959B7 8B678503 5C1C486D


  temp is
    602034D1 338F663B 0C0D138A D6C6901E E54548F7 E8C639EE
    17A732EB 53C51B24 8C2513B5 1E0959B7 8B678503 5C1C486D


temp XOR provided_data is
                      602034D1 338F663B 0C0D138A D6C6901E
    E54548F7 E8C639EE 17A732EB 53C51B24 8C2513B5 1E0959B7


Key is
    602034D1 338F663B 0C0D138A D6C6901E E54548F7 E8C639EE
```

```
    V is
                          17A732EB 53C51B24 8C2513B5 1E0959B7


rnd_val is
                                                1BB94DB5 81E84F96
        37933BE7 81749070 62F0E95F 7AA30739 EC6FB059 6B74CFFD


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

CTR_DRBG

    Requested Security Strength = 192

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    PersonalizationString =
                          40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    AdditionalInput1 =
                          60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


    AdditionalInput2 =
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7
```

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627


    personal_str is
                          40414243 44454647 48494A4B 4C4D4E4F
        50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667


    prediction_resistance_flag = "PredictionResistance"

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

  Update

    provided_data is
                          40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


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

      While loop

      Key is
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                          00000000 00000000 00000000 00000001


      output_block is
                          CD33B28A C773F74B A00ED1F3 12572435


      temp is
```

```
                     CD33B28A C773F74B A00ED1F3 12572435


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

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                     00000000 00000000 00000000 00000002


  output_block is
                     98E7247C 07F0FE41 1C267E43 84B0F600


  temp is
                                        CD33B28A C773F74B
    A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600


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

  While loop

  Key is
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                     00000000 00000000 00000000 00000003


  output_block is
                     2A3493E6 6235EE67 DEECCD2F 3B393BD8


  temp is
    CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
    1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8


temp XOR provided_data is
```

```
                        8D73F2CA 8733B70B E04E91B3 52176475
        D8A7643C 47B0BE01 5C663E03 C4F0B640 6A74D3A6 2275AE27


    Key is
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


    V is
                        5C663E03 C4F0B640 6A74D3A6 2275AE27


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
                        60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


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

CTR_DRBG_Reseed

    entropy_input is
                        80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7


    additional_input is
                        60616263 64656667 68696A6B 6C6D6E6F
        70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687


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

  Update
```

```
provided_data is
                        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0
    E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 20202020 20202020


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

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                        5C663E03 C4F0B640 6A74D3A6 2275AE28


  output_block is
                        517150FF D52BD344 DE78992B A224930C


  temp is
                        517150FF D52BD344 DE78992B A224930C


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

  While loop

  Key is
    8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


  V is
                        5C663E03 C4F0B640 6A74D3A6 2275AE29


  output_block is
                        98FC9FAC 541236E8 D199A476 B960B301


  temp is
                                            517150FF D52BD344
    DE78992B A224930C 98FC9FAC 541236E8 D199A476 B960B301
```

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

      While loop

      Key is
        8D73F2CA 8733B70B E04E91B3 52176475 D8A7643C 47B0BE01


      V is
                           5C663E03 C4F0B640 6A74D3A6 2275AE2A


      output_block is
                           2D882249 1114B01B 2208E492 F0F35C54


      temp is
        517150FF D52BD344 DE78992B A224930C 98FC9FAC 541236E8
        D199A476 B960B301 2D882249 1114B01B 2208E492 F0F35C54


    temp XOR provided_data is
                           B191B01F 35CB33A4 3E9879CB 42C473EC
        781C7F4C B4F2D608 31794496 598053E1 0DA80269 3134903B


    Key is
        B191B01F 35CB33A4 3E9879CB 42C473EC 781C7F4C B4F2D608


    V is
                           31794496 598053E1 0DA80269 3134903B


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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update
```

```
provided_data is
                      00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


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

  While loop

  Key is
    B191B01F 35CB33A4 3E9879CB 42C473EC 781C7F4C B4F2D608


  V is
                      31794496 598053E1 0DA80269 3134903E


  output_block is
                      912734C5 1650B758 E174DF45 FE78D27C


  temp is
                      912734C5 1650B758 E174DF45 FE78D27C


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

  While loop

  Key is
    B191B01F 35CB33A4 3E9879CB 42C473EC 781C7F4C B4F2D608


  V is
                      31794496 598053E1 0DA80269 3134903F


  output_block is
                      607F2F46 44BA4BDE E94EA700 CFA1A761


  temp is
                                        912734C5 1650B758
    E174DF45 FE78D27C 607F2F46 44BA4BDE E94EA700 CFA1A761
```

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

      While loop

      Key is
        B191B01F 35CB33A4 3E9879CB 42C473EC 781C7F4C B4F2D608


      V is
                           31794496 598053E1 0DA80269 31349040


      output_block is
                           407918E1 DE591203 5D647E0E DD62AE0B


      temp is
        912734C5 1650B758 E174DF45 FE78D27C 607F2F46 44BA4BDE
        E94EA700 CFA1A761 407918E1 DE591203 5D647E0E DD62AE0B


    temp XOR provided_data is
                           912734C5 1650B758 E174DF45 FE78D27C
        607F2F46 44BA4BDE E94EA700 CFA1A761 407918E1 DE591203


    Key is
        912734C5 1650B758 E174DF45 FE78D27C 607F2F46 44BA4BDE


    V is
                           E94EA700 CFA1A761 407918E1 DE591203


rnd_val is
                                               4C36423F DDD11096
        DB6A62DA B872B607 F51ACB6E AA1A8FAD BA9A955E 08C2C136


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

Second call to Generate

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

CTR_DRBG_Generate
```

```
  requested_number_of_bits = 256

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


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

CTR_DRBG_Reseed

    entropy_input is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7


    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
        B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7


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

  Update

    provided_data is
                          60606060 60606060 60606060 60606060
        60606060 60606060 60606060 60606060 20202020 20202020


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

      While loop

      Key is
        912734C5 1650B758 E174DF45 FE78D27C 607F2F46 44BA4BDE


      V is
                          E94EA700 CFA1A761 407918E1 DE591204


      output_block is
                          27CF86C6 8CC59F31 B56D6AEF C5E39991
```

```
  temp is
                      27CF86C6 8CC59F31 B56D6AEF C5E39991


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

  While loop

  Key is
    912734C5 1650B758 E174DF45 FE78D27C 607F2F46 44BA4BDE


  V is
                      E94EA700 CFA1A761 407918E1 DE591205


  output_block is
                      5464349A 2D386DD7 8C680950 896580CB


  temp is
                                        27CF86C6 8CC59F31
    B56D6AEF C5E39991 5464349A 2D386DD7 8C680950 896580CB


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

  While loop

  Key is
    912734C5 1650B758 E174DF45 FE78D27C 607F2F46 44BA4BDE


  V is
                      E94EA700 CFA1A761 407918E1 DE591206


  output_block is
                      90002416 13E390C0 BF953D14 A880A2C4


  temp is
    27CF86C6 8CC59F31 B56D6AEF C5E39991 5464349A 2D386DD7
    8C680950 896580CB 90002416 13E390C0 BF953D14 A880A2C4
```

```
    temp XOR provided_data is
                          47AFE6A6 ECA5FF51 D50D0A8F A583F9F1
        340454FA 4D580DB7 EC086930 E905E0AB B0200436 33C3B0E0


    Key is
        47AFE6A6 ECA5FF51 D50D0A8F A583F9F1 340454FA 4D580DB7


    V is
                          EC086930 E905E0AB B0200436 33C3B0E0


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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
                          00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
        47AFE6A6 ECA5FF51 D50D0A8F A583F9F1 340454FA 4D580DB7


      V is
                          EC086930 E905E0AB B0200436 33C3B0E3


      output_block is
                          EAC7E6F8 4AC4F0FF 1740CEF4 EE88EF73
```

```
  temp is
                      EAC7E6F8 4AC4F0FF 1740CEF4 EE88EF73


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

  While loop

  Key is
    47AFE6A6 ECA5FF51 D50D0A8F A583F9F1 340454FA 4D580DB7


  V is
                      EC086930 E905E0AB B0200436 33C3B0E4


  output_block is
                      C16D1FBC 4061AEE2 4702F9A7 81EB43A2


  temp is
                                          EAC7E6F8 4AC4F0FF
    1740CEF4 EE88EF73 C16D1FBC 4061AEE2 4702F9A7 81EB43A2


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

  While loop

  Key is
    47AFE6A6 ECA5FF51 D50D0A8F A583F9F1 340454FA 4D580DB7


  V is
                      EC086930 E905E0AB B0200436 33C3B0E5


  output_block is
                      274483A2 FC3B21EB B267557C 42C6AB80


  temp is
    EAC7E6F8 4AC4F0FF 1740CEF4 EE88EF73 C16D1FBC 4061AEE2
    4702F9A7 81EB43A2 274483A2 FC3B21EB B267557C 42C6AB80
```

```
    temp XOR provided_data is
                          EAC7E6F8 4AC4F0FF 1740CEF4 EE88EF73
        C16D1FBC 4061AEE2 4702F9A7 81EB43A2 274483A2 FC3B21EB


    Key is
        EAC7E6F8 4AC4F0FF 1740CEF4 EE88EF73 C16D1FBC 4061AEE2


    V is
                          4702F9A7 81EB43A2 274483A2 FC3B21EB


rnd_val is
                                             D859C7BF 0D15D50D
        81A65FEA B7D34605 1123E19F 64141105 43EA6D6F EE50EDEB


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

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    PersonalizationString = <empty>

    AdditionalInput = <empty>
```

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

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

  Update

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


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

      While loop

      Key is
                                              00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


      temp is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


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

```
  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      CEA7403D 4D606B6E 074EC5D3 BAF39D18


  temp is
                                              530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


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

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      726003CA 37A62A74 D1A2F58E 7506358E


  temp is
    530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
    074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


temp XOR provided_data is
    530E88F8 C34030BE A16ABEFA C8C67D84 DEB6522E 59757D79
    1F57DFC8 A6EE8307 524121E9 13830C53 F98BDFA5 592B1BA1
```

```
    Key is
                                            530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


    V is
                          524121E9 13830C53 F98BDFA5 592B1BA1


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
                                            530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


      V is
                          524121E9 13830C53 F98BDFA5 592B1BA4


      output_block is
```

```
                    056A8C26 6F9EF97E D08541DB D2E1FFA1

  temp is
                    056A8C26 6F9EF97E D08541DB D2E1FFA1

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

  While loop

  Key is
                                        530E88F8 C34030BE
    A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307

  V is
                    524121E9 13830C53 F98BDFA5 592B1BA5

  output_block is
                    9810F539 2D076276 EF41277C 3AB6E94A

  temp is
                                        056A8C26 6F9EF97E
    D08541DB D2E1FFA1 9810F539 2D076276 EF41277C 3AB6E94A

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

  While loop

  Key is
                                        530E88F8 C34030BE
    A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307

  V is
                    524121E9 13830C53 F98BDFA5 592B1BA6

  output_block is
                    4E3B7DCC 104A05BB 089D338B F55C72CA
```

```
      temp is
        056A8C26 6F9EF97E D08541DB D2E1FFA1 9810F539 2D076276
        EF41277C 3AB6E94A 4E3B7DCC 104A05BB 089D338B F55C72CA


    temp XOR provided_data is
        056A8C26 6F9EF97E D08541DB D2E1FFA1 9810F539 2D076276
        EF41277C 3AB6E94A 4E3B7DCC 104A05BB 089D338B F55C72CA


    Key is
                                            056A8C26 6F9EF97E
        D08541DB D2E1FFA1 9810F539 2D076276 EF41277C 3AB6E94A


    V is
                           4E3B7DCC 104A05BB 089D338B F55C72CA


rnd_val is
                                            06155023 4D158C5E
        C95595FE 04EF7A25 767F2E24 CC2BC479 D09D86DC 9ABCFDE7


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

```
  While loop

  Key is
                                          056A8C26 6F9EF97E
    D08541DB D2E1FFA1 9810F539 2D076276 EF41277C 3AB6E94A


  V is
                      4E3B7DCC 104A05BB 089D338B F55C72CD


  output_block is
                      18FB8B4B 5DAC63E5 B479E085 C28B4073


  temp is
                      18FB8B4B 5DAC63E5 B479E085 C28B4073


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

  While loop

  Key is
                                          056A8C26 6F9EF97E
    D08541DB D2E1FFA1 9810F539 2D076276 EF41277C 3AB6E94A


  V is
                      4E3B7DCC 104A05BB 089D338B F55C72CE


  output_block is
                      A6D7A24A 4E880BCE 3CFE4D7F B9DFABE1


  temp is
                                          18FB8B4B 5DAC63E5
    B479E085 C28B4073 A6D7A24A 4E880BCE 3CFE4D7F B9DFABE1


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

  While loop
```

```
      Key is
                                              056A8C26 6F9EF97E
        D08541DB D2E1FFA1 9810F539 2D076276 EF41277C 3AB6E94A


      V is
                           4E3B7DCC 104A05BB 089D338B F55C72CF


      output_block is
                           AFDD5272 2A0D37B5 17F7B959 2D4E755D


      temp is
        18FB8B4B 5DAC63E5 B479E085 C28B4073 A6D7A24A 4E880BCE
        3CFE4D7F B9DFABE1 AFDD5272 2A0D37B5 17F7B959 2D4E755D


    temp XOR provided_data is
        18FB8B4B 5DAC63E5 B479E085 C28B4073 A6D7A24A 4E880BCE
        3CFE4D7F B9DFABE1 AFDD5272 2A0D37B5 17F7B959 2D4E755D


    Key is
                                              18FB8B4B 5DAC63E5
        B479E085 C28B4073 A6D7A24A 4E880BCE 3CFE4D7F B9DFABE1


    V is
                           AFDD5272 2A0D37B5 17F7B959 2D4E755D


rnd_val is
                                              1A9FBCBC 8DA36DFF
        2ABE2032 96170FDB 97C3297F 67FCB679 AC719C9F D00253B0


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

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
```

```
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    PersonalizationString = <empty>

    AdditionalInput1 =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


    AdditionalInput2 =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

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

  Update

    provided_data is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
```

```
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


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

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000001


  output_block is
                       530F8AFB C74536B9 A963B4F1 C4CB738B


  temp is
                       530F8AFB C74536B9 A963B4F1 C4CB738B


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

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000002


  output_block is
                       CEA7403D 4D606B6E 074EC5D3 BAF39D18


  temp is
                                              530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18
```

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

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000003


      output_block is
                           726003CA 37A62A74 D1A2F58E 7506358E


      temp is
        530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
        074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


    temp XOR provided_data is
        530E88F8 C34030BE A16ABEFA C8C67D84 DEB6522E 59757D79
        1F57DFC8 A6EE8307 524121E9 13830C53 F98BDFA5 592B1BA1


    Key is
                                                530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


    V is
                           524121E9 13830C53 F98BDFA5 592B1BA1


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256
```

```
    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


  additional_input <> NULL, process appropriately
--------------------------

  Update

    provided_data is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


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

      While loop

      Key is
                                              530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


      V is
                          524121E9 13830C53 F98BDFA5 592B1BA2


      output_block is
                          06155023 4D158C5E C95595FE 04EF7A25


      temp is
                          06155023 4D158C5E C95595FE 04EF7A25


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

      While loop

      Key is
                                              530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


      V is
```

```
                      524121E9 13830C53 F98BDFA5 592B1BA3


  output_block is
                      767F2E24 CC2BC479 D09D86DC 9ABCFDE7


  temp is
                                        06155023 4D158C5E
    C95595FE 04EF7A25 767F2E24 CC2BC479 D09D86DC 9ABCFDE7


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

  While loop

  Key is
                                        530E88F8 C34030BE
    A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


  V is
                      524121E9 13830C53 F98BDFA5 592B1BA4


  output_block is
                      056A8C26 6F9EF97E D08541DB D2E1FFA1


  temp is
    06155023 4D158C5E C95595FE 04EF7A25 767F2E24 CC2BC479
    D09D86DC 9ABCFDE7 056A8C26 6F9EF97E D08541DB D2E1FFA1


temp XOR provided_data is
    66743240 2970EA39 A13CFF95 6882144A 060E5C57 B85EB20E
    A8E4FCA7 E6C18398 85EB0EA5 EB1B7FF9 580CCB50 5E6C712E


Key is
                                        66743240 2970EA39
    A13CFF95 6882144A 060E5C57 B85EB20E A8E4FCA7 E6C18398


V is
                      85EB0EA5 EB1B7FF9 580CCB50 5E6C712E
```

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

  Update

    provided_data is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


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

      While loop

      Key is
                                              66743240 2970EA39
        A13CFF95 6882144A 060E5C57 B85EB20E A8E4FCA7 E6C18398


      V is
                           85EB0EA5 EB1B7FF9 580CCB50 5E6C7131


      output_block is
                           346800DF CE6D40F5 0FCB89CD EE82941B


      temp is
                           346800DF CE6D40F5 0FCB89CD EE82941B


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

      While loop

      Key is
                                              66743240 2970EA39
        A13CFF95 6882144A 060E5C57 B85EB20E A8E4FCA7 E6C18398


      V is
                           85EB0EA5 EB1B7FF9 580CCB50 5E6C7132


      output_block is
```

```
                        7E6C7BA8 4CFACC6A 0D721810 81DD5C32


      temp is
                                              346800DF CE6D40F5
        0FCB89CD EE82941B 7E6C7BA8 4CFACC6A 0D721810 81DD5C32


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

      While loop

      Key is
                                              66743240 2970EA39
        A13CFF95 6882144A 060E5C57 B85EB20E A8E4FCA7 E6C18398


      V is
                        85EB0EA5 EB1B7FF9 580CCB50 5E6C7133


      output_block is
                        877534D9 08545CFD 9CAEAB8B 7A239397


      temp is
        346800DF CE6D40F5 0FCB89CD EE82941B 7E6C7BA8 4CFACC6A
        0D721810 81DD5C32 877534D9 08545CFD 9CAEAB8B 7A239397


    temp XOR provided_data is
        540962BC AA082692 67A2E3A6 82EFFA74 0E1D09DB 388FBA1D
        750B626B FDA0224D 07F4B65A 8CD1DA7A 14272100 F6AE1D18


    Key is
                                              540962BC AA082692
        67A2E3A6 82EFFA74 0E1D09DB 388FBA1D 750B626B FDA0224D


    V is
                        07F4B65A 8CD1DA7A 14272100 F6AE1D18


rnd_val is
                                              93A8EF3A C44E4A3D
```

```
        587DF216 EB6FE3B7 75EE3E94 4CAAC70F 35B56004 AE24B7B8


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


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

      While loop

      Key is
                                            540962BC AA082692
        67A2E3A6 82EFFA74 0E1D09DB 388FBA1D 750B626B FDA0224D


      V is
                           07F4B65A 8CD1DA7A 14272100 F6AE1D19


      output_block is
                           BCF91363 DA114FBB 6251B840 B0132E6C


      temp is
```

```
                    BCF91363 DA114FBB 6251B840 B0132E6C


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

  While loop

  Key is
                                        540962BC AA082692
    67A2E3A6 82EFFA74 0E1D09DB 388FBA1D 750B626B FDA0224D


  V is
                    07F4B65A 8CD1DA7A 14272100 F6AE1D1A


  output_block is
                    F4B50026 055E61C5 B89CB4C2 3D8C1F6A


  temp is
                                        BCF91363 DA114FBB
    6251B840 B0132E6C F4B50026 055E61C5 B89CB4C2 3D8C1F6A


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

  While loop

  Key is
                                        540962BC AA082692
    67A2E3A6 82EFFA74 0E1D09DB 388FBA1D 750B626B FDA0224D


  V is
                    07F4B65A 8CD1DA7A 14272100 F6AE1D1B


  output_block is
                    F50B710D 4167CE53 0C1463B0 A361FBB0


  temp is
    BCF91363 DA114FBB 6251B840 B0132E6C F4B50026 055E61C5
    B89CB4C2 3D8C1F6A F50B710D 4167CE53 0C1463B0 A361FBB0
```

```
    temp XOR provided_data is
        1C58B1C0 7EB4E91C CAF812EB 1CBE80C3 4404B295 B1EBD772
        00250E79 8131A1D5 35CAB3CE 85A20894 C4DDA97B 6FAC357F


    Key is
                                            1C58B1C0 7EB4E91C
        CAF812EB 1CBE80C3 4404B295 B1EBD772 00250E79 8131A1D5


    V is
                         35CAB3CE 85A20894 C4DDA97B 6FAC357F


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

  Update

    provided_data is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


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

      While loop

      Key is
                                            1C58B1C0 7EB4E91C
        CAF812EB 1CBE80C3 4404B295 B1EBD772 00250E79 8131A1D5


      V is
                         35CAB3CE 85A20894 C4DDA97B 6FAC3582


      output_block is
                         EECEE3A0 69F7653D 4A96AE43 7172EE2C


      temp is
                         EECEE3A0 69F7653D 4A96AE43 7172EE2C


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

```
  While loop

  Key is
                                          1C58B1C0 7EB4E91C
    CAF812EB 1CBE80C3 4404B295 B1EBD772 00250E79 8131A1D5


  V is
                      35CAB3CE 85A20894 C4DDA97B 6FAC3583


  output_block is
                      848A92C9 E1E71461 E48D403E E6893AB0


  temp is
                                          EECEE3A0 69F7653D
    4A96AE43 7172EE2C 848A92C9 E1E71461 E48D403E E6893AB0


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

  While loop

  Key is
                                          1C58B1C0 7EB4E91C
    CAF812EB 1CBE80C3 4404B295 B1EBD772 00250E79 8131A1D5


  V is
                      35CAB3CE 85A20894 C4DDA97B 6FAC3584


  output_block is
                      2393599C 9F15A18C A4F18BCE E25FDBD3


  temp is
    EECEE3A0 69F7653D 4A96AE43 7172EE2C 848A92C9 E1E71461
    E48D403E E6893AB0 2393599C 9F15A18C A4F18BCE E25FDBD3


temp XOR provided_data is
    4E6F4103 CD52C39A E23F04E8 DDDF4083 343B207A 5552A2D6
    5C34FA85 5A34840F E3529B5F 5BD0674B 6C384105 2E92151C
```

```
    Key is
                                            4E6F4103 CD52C39A
        E23F04E8 DDDF4083 343B207A 5552A2D6 5C34FA85 5A34840F


    V is
                         E3529B5F 5BD0674B 6C384105 2E92151C


rnd_val is
                                            8911B73C 1EC1626F
        37F221B1 2929BD5D 20B67373 768048E8 A1E0737E DF0F22D6


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

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput = <empty>

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    prediction_resistance_flag = "No PredictionResistance"

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

  Update

    provided_data is
        40404040 40404040 40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


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

      While loop

      Key is
                                              00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


      temp is
                           530F8AFB C74536B9 A963B4F1 C4CB738B
```

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

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000002


  output_block is
                       CEA7403D 4D606B6E 074EC5D3 BAF39D18


  temp is
                                              530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


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

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                       00000000 00000000 00000000 00000003


  output_block is
                       726003CA 37A62A74 D1A2F58E 7506358E


  temp is
    530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
    074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


temp XOR provided_data is
```

```
        134FCABB 870576F9 E923F4B1 848B33CB 8EE7007D 0D202B2E
        470E8593 FAB3DD58 3220438A 77E66A34 91E2B5CE 354675CE


    Key is
                                           134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


    V is
                         3220438A 77E66A34 91E2B5CE 354675CE


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
                                           134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


      V is
                         3220438A 77E66A34 91E2B5CE 354675D1
```

```
  output_block is
                      79B18865 9E08DC83 10050D9A 2EB958DF

  temp is
                      79B18865 9E08DC83 10050D9A 2EB958DF

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

  While loop

  Key is
                                        134FCABB 870576F9
    E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58

  V is
                      3220438A 77E66A34 91E2B5CE 354675D2

  output_block is
                      87730C9A E9461189 C5EF7300 DE0F752C

  temp is
                                        79B18865 9E08DC83
    10050D9A 2EB958DF 87730C9A E9461189 C5EF7300 DE0F752C

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

  While loop

  Key is
                                        134FCABB 870576F9
    E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58

  V is
                      3220438A 77E66A34 91E2B5CE 354675D3

  output_block is
                      33AC1C7E FB7384A0 A4A267F4 9CC5DA4E
```

```
      temp is
        79B18865 9E08DC83 10050D9A 2EB958DF 87730C9A E9461189
        C5EF7300 DE0F752C 33AC1C7E FB7384A0 A4A267F4 9CC5DA4E


    temp XOR provided_data is
        79B18865 9E08DC83 10050D9A 2EB958DF 87730C9A E9461189
        C5EF7300 DE0F752C 33AC1C7E FB7384A0 A4A267F4 9CC5DA4E


    Key is
                                            79B18865 9E08DC83
        10050D9A 2EB958DF 87730C9A E9461189 C5EF7300 DE0F752C


    V is
                          33AC1C7E FB7384A0 A4A267F4 9CC5DA4E


rnd_val is
                                            5DE6AA50 022F01DF
        045B3FDA 58A2AD77 9132F66F B04CE0C2 B0FA0721 F686D3E4


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
```

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

  While loop

  Key is
                                          79B18865 9E08DC83
    10050D9A 2EB958DF 87730C9A E9461189 C5EF7300 DE0F752C


  V is
                      33AC1C7E FB7384A0 A4A267F4 9CC5DA51


  output_block is
                      CA8AFAEE 6CAFC480 16508AD9 1B8F9012


  temp is
                      CA8AFAEE 6CAFC480 16508AD9 1B8F9012


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

  While loop

  Key is
                                          79B18865 9E08DC83
    10050D9A 2EB958DF 87730C9A E9461189 C5EF7300 DE0F752C


  V is
                      33AC1C7E FB7384A0 A4A267F4 9CC5DA52


  output_block is
                      DFCAEBD4 7953986D E33FDCCB 3CD614DD


  temp is
                                          CA8AFAEE 6CAFC480
    16508AD9 1B8F9012 DFCAEBD4 7953986D E33FDCCB 3CD614DD


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

```
      While loop

      Key is
                                              79B18865 9E08DC83
        10050D9A 2EB958DF 87730C9A E9461189 C5EF7300 DE0F752C


      V is
                           33AC1C7E FB7384A0 A4A267F4 9CC5DA53


      output_block is
                           443B3D78 CCF212E4 9EFD4003 A3C33A05


      temp is
        CA8AFAEE 6CAFC480 16508AD9 1B8F9012 DFCAEBD4 7953986D
        E33FDCCB 3CD614DD 443B3D78 CCF212E4 9EFD4003 A3C33A05


    temp XOR provided_data is
        CA8AFAEE 6CAFC480 16508AD9 1B8F9012 DFCAEBD4 7953986D
        E33FDCCB 3CD614DD 443B3D78 CCF212E4 9EFD4003 A3C33A05


    Key is
                                              CA8AFAEE 6CAFC480
        16508AD9 1B8F9012 DFCAEBD4 7953986D E33FDCCB 3CD614DD


    V is
                           443B3D78 CCF212E4 9EFD4003 A3C33A05


rnd_val is
                                              1DD89F20 7997AE24
        C8EB7550 21A90AA1 3CA67FFC 6881D577 1A9745F8 0C7FD207


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

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "NOT ENABLED"
```

```
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput1 =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


    AdditionalInput2 =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F
```

```
    prediction_resistance_flag = "No PredictionResistance"

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

  Update

    provided_data is
        40404040 40404040 40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


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

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


      temp is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


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

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000002


      output_block is
```

```
                        CEA7403D 4D606B6E 074EC5D3 BAF39D18


      temp is
                                               530F8AFB C74536B9
        A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


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

      While loop

      Key is
                                               00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                        00000000 00000000 00000000 00000003


      output_block is
                        726003CA 37A62A74 D1A2F58E 7506358E


      temp is
        530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
        074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


    temp XOR provided_data is
        134FCABB 870576F9 E923F4B1 848B33CB 8EE7007D 0D202B2E
        470E8593 FAB3DD58 3220438A 77E66A34 91E2B5CE 354675CE


    Key is
                                               134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


    V is
                        3220438A 77E66A34 91E2B5CE 354675CE


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

```
First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


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

      While loop

      Key is
                                             134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


      V is
                           3220438A 77E66A34 91E2B5CE 354675CF


      output_block is
                           5DE6AA50 022F01DF 045B3FDA 58A2AD77


      temp is
                           5DE6AA50 022F01DF 045B3FDA 58A2AD77


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

```
  While loop

  Key is
                                          134FCABB 870576F9
    E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


  V is
                     3220438A 77E66A34 91E2B5CE 354675D0


  output_block is
                     9132F66F B04CE0C2 B0FA0721 F686D3E4


  temp is
                                          5DE6AA50 022F01DF
    045B3FDA 58A2AD77 9132F66F B04CE0C2 B0FA0721 F686D3E4


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

  While loop

  Key is
                                          134FCABB 870576F9
    E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


  V is
                     3220438A 77E66A34 91E2B5CE 354675D1


  output_block is
                     79B18865 9E08DC83 10050D9A 2EB958DF


  temp is
    5DE6AA50 022F01DF 045B3FDA 58A2AD77 9132F66F B04CE0C2
    B0FA0721 F686D3E4 79B18865 9E08DC83 10050D9A 2EB958DF


temp XOR provided_data is
    3D87C833 664A67B8 6C3255B1 34CFC318 E143841C C43996B5
    C8837D5A 8AFBAD9B F9300AE6 1A8D5A04 988C8711 A234D650
```

```
    Key is
                                            3D87C833 664A67B8
        6C3255B1 34CFC318 E143841C C43996B5 C8837D5A 8AFBAD9B


    V is
                         F9300AE6 1A8D5A04 988C8711 A234D650


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

  Update

    provided_data is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


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

      While loop

      Key is
                                            3D87C833 664A67B8
        6C3255B1 34CFC318 E143841C C43996B5 C8837D5A 8AFBAD9B


      V is
                         F9300AE6 1A8D5A04 988C8711 A234D653


      output_block is
                         FE4B16FC 3F12CD7C 9D681FEF BE37D72E


      temp is
                         FE4B16FC 3F12CD7C 9D681FEF BE37D72E


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

      While loop

      Key is
                                            3D87C833 664A67B8
```

```
    6C3255B1 34CFC318 E143841C C43996B5 C8837D5A 8AFBAD9B


  V is
                      F9300AE6 1A8D5A04 988C8711 A234D654


  output_block is
                      0793697D B707C0D0 D194BDB6 7A7C821D


  temp is
                                        FE4B16FC 3F12CD7C
    9D681FEF BE37D72E 0793697D B707C0D0 D194BDB6 7A7C821D


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

  While loop

  Key is
                                        3D87C833 664A67B8
    6C3255B1 34CFC318 E143841C C43996B5 C8837D5A 8AFBAD9B


  V is
                      F9300AE6 1A8D5A04 988C8711 A234D655


  output_block is
                      522AC4DF 59F07E9E 79359831 6150EFB3


  temp is
    FE4B16FC 3F12CD7C 9D681FEF BE37D72E 0793697D B707C0D0
    D194BDB6 7A7C821D 522AC4DF 59F07E9E 79359831 6150EFB3


temp XOR provided_data is
    9E2A749F 5B77AB1B F5017584 D25AB941 77E21B0E C372B6A7
    A9EDC7CD 0601FC62 D2AB465C DD75F819 F1BC12BA EDDD613C


Key is
                                        9E2A749F 5B77AB1B
    F5017584 D25AB941 77E21B0E C372B6A7 A9EDC7CD 0601FC62
```

```
    V is
                          D2AB465C DD75F819 F1BC12BA EDDD613C


rnd_val is
                                              35CE8218 C03B7592
        FAF29D19 72273983 6CEEF066 6E058ABF 8B837AB5 E5E743D9


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


  additional_input <> NULL, process appropriately
---------------------------

  Update

    provided_data is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


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

      While loop

      Key is
                                              9E2A749F 5B77AB1B
        F5017584 D25AB941 77E21B0E C372B6A7 A9EDC7CD 0601FC62


      V is
```

```
                      D2AB465C DD75F819 F1BC12BA EDDD613D

  output_block is
                      3E56FF9B 2E3BC503 12CDDC61 47A1511F

  temp is
                      3E56FF9B 2E3BC503 12CDDC61 47A1511F

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

  While loop

  Key is
                                          9E2A749F 5B77AB1B
    F5017584 D25AB941 77E21B0E C372B6A7 A9EDC7CD 0601FC62

  V is
                      D2AB465C DD75F819 F1BC12BA EDDD613E

  output_block is
                      FE3CCEA1 E661A3C3 9F75BF33 E6A50D11

  temp is
                                          3E56FF9B 2E3BC503
    12CDDC61 47A1511F FE3CCEA1 E661A3C3 9F75BF33 E6A50D11

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

  While loop

  Key is
                                          9E2A749F 5B77AB1B
    F5017584 D25AB941 77E21B0E C372B6A7 A9EDC7CD 0601FC62

  V is
                      D2AB465C DD75F819 F1BC12BA EDDD613F
```

```
      output_block is
                           BAFDFC5F E40E86DE BA48BFAE 8A16B1F5


      temp is
        3E56FF9B 2E3BC503 12CDDC61 47A1511F FE3CCEA1 E661A3C3
        9F75BF33 E6A50D11 BAFDFC5F E40E86DE BA48BFAE 8A16B1F5


    temp XOR provided_data is
        9EF75D38 8A9E63A4 BA6476CA EB0CFFB0 4E8D7C12 52D41574
        27CC0588 5A18B3AE 7A3C3E9C 20CB4019 72817565 46DB7F3A


    Key is
                                             9EF75D38 8A9E63A4
        BA6476CA EB0CFFB0 4E8D7C12 52D41574 27CC0588 5A18B3AE


    V is
                           7A3C3E9C 20CB4019 72817565 46DB7F3A


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

  Update

    provided_data is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


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

      While loop

      Key is
                                             9EF75D38 8A9E63A4
        BA6476CA EB0CFFB0 4E8D7C12 52D41574 27CC0588 5A18B3AE


      V is
                           7A3C3E9C 20CB4019 72817565 46DB7F3D


      output_block is
```

```
                    0D5AC3AD 225F868B 78ED4FD6 821E5C5E

  temp is
                    0D5AC3AD 225F868B 78ED4FD6 821E5C5E

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

  While loop

  Key is
                                       9EF75D38 8A9E63A4
    BA6476CA EB0CFFB0 4E8D7C12 52D41574 27CC0588 5A18B3AE

  V is
                    7A3C3E9C 20CB4019 72817565 46DB7F3E

  output_block is
                    61B988FC E1614A2E 85BC9BEA 4767F7F7

  temp is
                                       0D5AC3AD 225F868B
    78ED4FD6 821E5C5E 61B988FC E1614A2E 85BC9BEA 4767F7F7

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

  While loop

  Key is
                                       9EF75D38 8A9E63A4
    BA6476CA EB0CFFB0 4E8D7C12 52D41574 27CC0588 5A18B3AE

  V is
                    7A3C3E9C 20CB4019 72817565 46DB7F3F

  output_block is
                    29C2F084 866A22CF 1E447F3D 7A46C68B
```

```
      temp is
        0D5AC3AD 225F868B 78ED4FD6 821E5C5E 61B988FC E1614A2E
        85BC9BEA 4767F7F7 29C2F084 866A22CF 1E447F3D 7A46C68B


    temp XOR provided_data is
        ADFB610E 86FA202C D044E57D 2EB3F2F1 D1083A4F 55D4FC99
        3D052151 FBDA4948 E9033247 42AFE408 D68DB5F6 B68B0844


    Key is
                                            ADFB610E 86FA202C
        D044E57D 2EB3F2F1 D1083A4F 55D4FC99 3D052151 FBDA4948


    V is
                           E9033247 42AFE408 D68DB5F6 B68B0844


rnd_val is
                                            836CA0F7 75468B8A
        ABCD3129 FE2A2227 B2251DCC 22A0BFA0 175EAB7C A29892BA


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

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
```

```
    PersonalizationString = <empty>

    AdditionalInput = <empty>

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

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

  Update

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


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

      While loop

      Key is
                                              00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


      temp is
```

```
                    530F8AFB C74536B9 A963B4F1 C4CB738B


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

  While loop

  Key is
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                    00000000 00000000 00000000 00000002


  output_block is
                    CEA7403D 4D606B6E 074EC5D3 BAF39D18


  temp is
                                          530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


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

  While loop

  Key is
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                    00000000 00000000 00000000 00000003


  output_block is
                    726003CA 37A62A74 D1A2F58E 7506358E


  temp is
    530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
    074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E
```

```
    temp XOR provided_data is
        530E88F8 C34030BE A16ABEFA C8C67D84 DEB6522E 59757D79
        1F57DFC8 A6EE8307 524121E9 13830C53 F98BDFA5 592B1BA1


    Key is
                                            530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


    V is
                          524121E9 13830C53 F98BDFA5 592B1BA1


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

CTR_DRBG_Reseed

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    additional_input is  <empty>

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

  Update

    provided_data is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
```

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

  While loop

  Key is
                                          530E88F8 C34030BE
    A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


  V is
                      524121E9 13830C53 F98BDFA5 592B1BA2


  output_block is
                      06155023 4D158C5E C95595FE 04EF7A25


  temp is
                      06155023 4D158C5E C95595FE 04EF7A25


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

  While loop

  Key is
                                          530E88F8 C34030BE
    A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


  V is
                      524121E9 13830C53 F98BDFA5 592B1BA3


  output_block is
                      767F2E24 CC2BC479 D09D86DC 9ABCFDE7


  temp is
                                          06155023 4D158C5E
    C95595FE 04EF7A25 767F2E24 CC2BC479 D09D86DC 9ABCFDE7


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

```
      While loop

      Key is
                                              530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


      V is
                           524121E9 13830C53 F98BDFA5 592B1BA4


      output_block is
                           056A8C26 6F9EF97E D08541DB D2E1FFA1


      temp is
        06155023 4D158C5E C95595FE 04EF7A25 767F2E24 CC2BC479
        D09D86DC 9ABCFDE7 056A8C26 6F9EF97E D08541DB D2E1FFA1


    temp XOR provided_data is
        8694D2A0 C9900AD9 41DC1F75 8862F4AA E6EEBCB7 58BE52EE
        48041C47 06216378 A5CB2E85 CB3B5FD9 782CEB70 7E4C510E


    Key is
                                              8694D2A0 C9900AD9
        41DC1F75 8862F4AA E6EEBCB7 58BE52EE 48041C47 06216378


    V is
                           A5CB2E85 CB3B5FD9 782CEB70 7E4C510E


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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update
```

```
provided_data is
    00000000 00000000 00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


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

  While loop

  Key is
                                          8694D2A0 C9900AD9
    41DC1F75 8862F4AA E6EEBCB7 58BE52EE 48041C47 06216378


  V is
                     A5CB2E85 CB3B5FD9 782CEB70 7E4C5111


  output_block is
                     D38F59F3 0937A627 4AFFFC17 6FF04E6C


  temp is
                     D38F59F3 0937A627 4AFFFC17 6FF04E6C


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

  While loop

  Key is
                                          8694D2A0 C9900AD9
    41DC1F75 8862F4AA E6EEBCB7 58BE52EE 48041C47 06216378


  V is
                     A5CB2E85 CB3B5FD9 782CEB70 7E4C5112


  output_block is
                     6BCA6A95 33E7A5DB 8B946C2D 24271896


  temp is
                                          D38F59F3 0937A627
```

```
        4AFFFC17 6FF04E6C 6BCA6A95 33E7A5DB 8B946C2D 24271896


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

      While loop

      Key is
                                              8694D2A0 C9900AD9
        41DC1F75 8862F4AA E6EEBCB7 58BE52EE 48041C47 06216378


      V is
                           A5CB2E85 CB3B5FD9 782CEB70 7E4C5113


      output_block is
                           ED06041B 417EBE9F 071443C9 47A03552


      temp is
        D38F59F3 0937A627 4AFFFC17 6FF04E6C 6BCA6A95 33E7A5DB
        8B946C2D 24271896 ED06041B 417EBE9F 071443C9 47A03552


    temp XOR provided_data is
        D38F59F3 0937A627 4AFFFC17 6FF04E6C 6BCA6A95 33E7A5DB
        8B946C2D 24271896 ED06041B 417EBE9F 071443C9 47A03552


    Key is
                                              D38F59F3 0937A627
        4AFFFC17 6FF04E6C 6BCA6A95 33E7A5DB 8B946C2D 24271896


    V is
                           ED06041B 417EBE9F 071443C9 47A03552


rnd_val is
                                              893EB3AE 65F69FE3
        1D7EFC8E E1583348 C1723F25 9F66875A 213CD971 2706FBA1


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

```
Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

CTR_DRBG_Reseed

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    additional_input is  <empty>

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

  Update

    provided_data is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


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

      While loop

      Key is
                                              D38F59F3 0937A627
        4AFFFC17 6FF04E6C 6BCA6A95 33E7A5DB 8B946C2D 24271896


      V is
                           ED06041B 417EBE9F 071443C9 47A03553


      output_block is
                           9C7214B1 7A62F3FF 04208CE6 37FDE278
```

```
  temp is
                      9C7214B1 7A62F3FF 04208CE6 37FDE278


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

  While loop

  Key is
                                           D38F59F3 0937A627
    4AFFFC17 6FF04E6C 6BCA6A95 33E7A5DB 8B946C2D 24271896


  V is
                      ED06041B 417EBE9F 071443C9 47A03554


  output_block is
                      D15FE4BB 48ED41E1 7CD0BCB9 C3EC3734


  temp is
                                           9C7214B1 7A62F3FF
    04208CE6 37FDE278 D15FE4BB 48ED41E1 7CD0BCB9 C3EC3734


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

  While loop

  Key is
                                           D38F59F3 0937A627
    4AFFFC17 6FF04E6C 6BCA6A95 33E7A5DB 8B946C2D 24271896


  V is
                      ED06041B 417EBE9F 071443C9 47A03555


  output_block is
                      85E9A763 6B4BD924 6743708C B189CA43


  temp is
```

```
        9C7214B1 7A62F3FF 04208CE6 37FDE278 D15FE4BB 48ED41E1
        7CD0BCB9 C3EC3734 85E9A763 6B4BD924 6743708C B189CA43


    temp XOR provided_data is
        5CB3D672 BEA73538 CCE9462D FB302CB7 018E3668 9C389736
        A4096662 1F31E9EB 65084580 8FAE3FC3 8FAA9A67 5D6424AC


    Key is
                                            5CB3D672 BEA73538
        CCE9462D FB302CB7 018E3668 9C389736 A4096662 1F31E9EB


    V is
                           65084580 8FAE3FC3 8FAA9A67 5D6424AC


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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
                                            5CB3D672 BEA73538
        CCE9462D FB302CB7 018E3668 9C389736 A4096662 1F31E9EB


      V is
                           65084580 8FAE3FC3 8FAA9A67 5D6424AF
```

```
  output_block is
                      71A61373 72EB2FBE 90990C00 1B36E133

  temp is
                      71A61373 72EB2FBE 90990C00 1B36E133

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

  While loop

  Key is
                                          5CB3D672 BEA73538
    CCE9462D FB302CB7 018E3668 9C389736 A4096662 1F31E9EB

  V is
                      65084580 8FAE3FC3 8FAA9A67 5D6424B0

  output_block is
                      8CAECEDB 87EE5AC1 02796183 02CAEFDF

  temp is
                                          71A61373 72EB2FBE
    90990C00 1B36E133 8CAECEDB 87EE5AC1 02796183 02CAEFDF

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

  While loop

  Key is
                                          5CB3D672 BEA73538
    CCE9462D FB302CB7 018E3668 9C389736 A4096662 1F31E9EB

  V is
                      65084580 8FAE3FC3 8FAA9A67 5D6424B1

  output_block is
```

```
                          F58B83F4 A66CDE4D 30E913DC DF0F9501


      temp is
        71A61373 72EB2FBE 90990C00 1B36E133 8CAECEDB 87EE5AC1
        02796183 02CAEFDF F58B83F4 A66CDE4D 30E913DC DF0F9501


    temp XOR provided_data is
        71A61373 72EB2FBE 90990C00 1B36E133 8CAECEDB 87EE5AC1
        02796183 02CAEFDF F58B83F4 A66CDE4D 30E913DC DF0F9501


    Key is
                                           71A61373 72EB2FBE
        90990C00 1B36E133 8CAECEDB 87EE5AC1 02796183 02CAEFDF


    V is
                          F58B83F4 A66CDE4D 30E913DC DF0F9501


rnd_val is
                                           67219E23 0FEF83C0
        DF3B2020 1C8F9B5D DFF62224 D9CEF23A 6C96474C 2D1A51CD


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

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
```

```
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    PersonalizationString = <empty>

    AdditionalInput1 =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


    AdditionalInput2 =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

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

  Update

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


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

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000
```

```
  V is
                      00000000 00000000 00000000 00000001

  output_block is
                      530F8AFB C74536B9 A963B4F1 C4CB738B

  temp is
                      530F8AFB C74536B9 A963B4F1 C4CB738B

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

  While loop

  Key is
                                            00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000

  V is
                      00000000 00000000 00000000 00000002

  output_block is
                      CEA7403D 4D606B6E 074EC5D3 BAF39D18

  temp is
                                            530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18

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

  While loop

  Key is
                                            00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000

  V is
```

```
                          00000000 00000000 00000000 00000003


      output_block is
                          726003CA 37A62A74 D1A2F58E 7506358E


      temp is
        530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
        074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


    temp XOR provided_data is
        530E88F8 C34030BE A16ABEFA C8C67D84 DEB6522E 59757D79
        1F57DFC8 A6EE8307 524121E9 13830C53 F98BDFA5 592B1BA1


    Key is
                                            530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


    V is
                          524121E9 13830C53 F98BDFA5 592B1BA1


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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


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

CTR_DRBG_Reseed
```

```
    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


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

  Update

    provided_data is
        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0
        E0E0E0E0 E0E0E0E0 20202020 20202020 20202020 20202020


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

      While loop

      Key is
                                              530E88F8 C34030BE
        A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


      V is
                           524121E9 13830C53 F98BDFA5 592B1BA2


      output_block is
                           06155023 4D158C5E C95595FE 04EF7A25


      temp is
                           06155023 4D158C5E C95595FE 04EF7A25


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

      While loop

      Key is
                                              530E88F8 C34030BE
```

```
    A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


  V is
                      524121E9 13830C53 F98BDFA5 592B1BA3


  output_block is
                      767F2E24 CC2BC479 D09D86DC 9ABCFDE7


  temp is
                                        06155023 4D158C5E
    C95595FE 04EF7A25 767F2E24 CC2BC479 D09D86DC 9ABCFDE7


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

  While loop

  Key is
                                        530E88F8 C34030BE
    A16ABEFA C8C67D84 DEB6522E 59757D79 1F57DFC8 A6EE8307


  V is
                      524121E9 13830C53 F98BDFA5 592B1BA4


  output_block is
                      056A8C26 6F9EF97E D08541DB D2E1FFA1


  temp is
    06155023 4D158C5E C95595FE 04EF7A25 767F2E24 CC2BC479
    D09D86DC 9ABCFDE7 056A8C26 6F9EF97E D08541DB D2E1FFA1


temp XOR provided_data is
    E6F5B0C3 ADF56CBE 29B5751E E40F9AC5 969FCEC4 2CCB2499
    307D663C 7A5C1D07 254AAC06 4FBED95E F0A561FB F2C1DF81


Key is
                                        E6F5B0C3 ADF56CBE
    29B5751E E40F9AC5 969FCEC4 2CCB2499 307D663C 7A5C1D07
```

```
    V is
                          254AAC06 4FBED95E F0A561FB F2C1DF81


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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
                                             E6F5B0C3 ADF56CBE
        29B5751E E40F9AC5 969FCEC4 2CCB2499 307D663C 7A5C1D07


      V is
                          254AAC06 4FBED95E F0A561FB F2C1DF84


      output_block is
                          DD63AE35 48ABB73F BF204A84 128DB2DB


      temp is
                          DD63AE35 48ABB73F BF204A84 128DB2DB


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

```
  While loop

  Key is
                                          E6F5B0C3 ADF56CBE
    29B5751E E40F9AC5 969FCEC4 2CCB2499 307D663C 7A5C1D07


  V is
                      254AAC06 4FBED95E F0A561FB F2C1DF85


  output_block is
                      6562237F 51697F0D 33E4E071 64FCF487


  temp is
                                          DD63AE35 48ABB73F
    BF204A84 128DB2DB 6562237F 51697F0D 33E4E071 64FCF487


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

  While loop

  Key is
                                          E6F5B0C3 ADF56CBE
    29B5751E E40F9AC5 969FCEC4 2CCB2499 307D663C 7A5C1D07


  V is
                      254AAC06 4FBED95E F0A561FB F2C1DF86


  output_block is
                      17E289C6 FFECF684 27E216B5 FE2907EC


  temp is
    DD63AE35 48ABB73F BF204A84 128DB2DB 6562237F 51697F0D
    33E4E071 64FCF487 17E289C6 FFECF684 27E216B5 FE2907EC


temp XOR provided_data is
    DD63AE35 48ABB73F BF204A84 128DB2DB 6562237F 51697F0D
    33E4E071 64FCF487 17E289C6 FFECF684 27E216B5 FE2907EC
```

```
    Key is
                                            DD63AE35 48ABB73F
        BF204A84 128DB2DB 6562237F 51697F0D 33E4E071 64FCF487


    V is
                          17E289C6 FFECF684 27E216B5 FE2907EC


rnd_val is
                                            499B4951 9CB0C1A7
        13CA0E5B 82DF4D11 6C370752 3D483563 BEBE9407 8C2A5E01


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

Second call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


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

CTR_DRBG_Reseed

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


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

```
Update

  provided_data is
      60606060 60606060 60606060 60606060 60606060 60606060
      60606060 60606060 20202020 20202020 20202020 20202020


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

    While loop

    Key is
                                              DD63AE35 48ABB73F
      BF204A84 128DB2DB 6562237F 51697F0D 33E4E071 64FCF487


    V is
                         17E289C6 FFECF684 27E216B5 FE2907ED


    output_block is
                         63262AB5 C764586B F1B3B575 1A872086


    temp is
                         63262AB5 C764586B F1B3B575 1A872086


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

    While loop

    Key is
                                              DD63AE35 48ABB73F
      BF204A84 128DB2DB 6562237F 51697F0D 33E4E071 64FCF487


    V is
                         17E289C6 FFECF684 27E216B5 FE2907EE


    output_block is
                         80A7C59D 38A25C34 9BEBA5A2 4AB4223D
```

```
      temp is
                                              63262AB5 C764586B
        F1B3B575 1A872086 80A7C59D 38A25C34 9BEBA5A2 4AB4223D


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

      While loop

      Key is
                                              DD63AE35 48ABB73F
        BF204A84 128DB2DB 6562237F 51697F0D 33E4E071 64FCF487


      V is
                           17E289C6 FFECF684 27E216B5 FE2907EF


      output_block is
                           6FB7EC4C 720DE4FB C66C81B2 719FDD90


      temp is
        63262AB5 C764586B F1B3B575 1A872086 80A7C59D 38A25C34
        9BEBA5A2 4AB4223D 6FB7EC4C 720DE4FB C66C81B2 719FDD90


    temp XOR provided_data is
        03464AD5 A704380B 91D3D515 7AE740E6 E0C7A5FD 58C23C54
        FB8BC5C2 2AD4425D 4F97CC6C 522DC4DB E64CA192 51BFFDB0


    Key is
                                              03464AD5 A704380B
        91D3D515 7AE740E6 E0C7A5FD 58C23C54 FB8BC5C2 2AD4425D


    V is
                           4F97CC6C 522DC4DB E64CA192 51BFFDB0

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

CTR_DRBG_Generate

  requested_number_of_bits = 256
```

```
    additional_input is  <empty>

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

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
                                              03464AD5 A704380B
        91D3D515 7AE740E6 E0C7A5FD 58C23C54 FB8BC5C2 2AD4425D


      V is
                           4F97CC6C 522DC4DB E64CA192 51BFFDB3


      output_block is
                           6F2CD028 10A911FF 62691817 C3A59DDD


      temp is
                           6F2CD028 10A911FF 62691817 C3A59DDD


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

      While loop

      Key is
                                              03464AD5 A704380B
        91D3D515 7AE740E6 E0C7A5FD 58C23C54 FB8BC5C2 2AD4425D


      V is
                           4F97CC6C 522DC4DB E64CA192 51BFFDB4
```

```
      output_block is
                          4EB1F43E 186B49EF B7C3024E A407151A

      temp is
                                               6F2CD028 10A911FF
        62691817 C3A59DDD 4EB1F43E 186B49EF B7C3024E A407151A

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

      While loop

      Key is
                                               03464AD5 A704380B
        91D3D515 7AE740E6 E0C7A5FD 58C23C54 FB8BC5C2 2AD4425D

      V is
                          4F97CC6C 522DC4DB E64CA192 51BFFDB5

      output_block is
                          8D075C41 42648381 376D27A8 8EE2760A

      temp is
        6F2CD028 10A911FF 62691817 C3A59DDD 4EB1F43E 186B49EF
        B7C3024E A407151A 8D075C41 42648381 376D27A8 8EE2760A

    temp XOR provided_data is
        6F2CD028 10A911FF 62691817 C3A59DDD 4EB1F43E 186B49EF
        B7C3024E A407151A 8D075C41 42648381 376D27A8 8EE2760A

    Key is
                                               6F2CD028 10A911FF
        62691817 C3A59DDD 4EB1F43E 186B49EF B7C3024E A407151A

    V is
                          8D075C41 42648381 376D27A8 8EE2760A

rnd_val is
```

```
                                                353B67AA E68C0CC6
        3C5567B4 86F2B27C 121469A2 757951E0 9429E33F 0758F3AD


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

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput = <empty>

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

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

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
```

```
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    prediction_resistance_flag = "PredictionResistance"

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

  Update

    provided_data is
        40404040 40404040 40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


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

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


      temp is
                           530F8AFB C74536B9 A963B4F1 C4CB738B


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

      While loop

      Key is
                                                00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000002
```

```
  output_block is
                      CEA7403D 4D606B6E 074EC5D3 BAF39D18


  temp is
                                          530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


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

  While loop

  Key is
                                          00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      726003CA 37A62A74 D1A2F58E 7506358E


  temp is
    530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
    074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


temp XOR provided_data is
    134FCABB 870576F9 E923F4B1 848B33CB 8EE7007D 0D202B2E
    470E8593 FAB3DD58 3220438A 77E66A34 91E2B5CE 354675CE


Key is
                                          134FCABB 870576F9
    E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


V is
                      3220438A 77E66A34 91E2B5CE 354675CE
```

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

First call to Generate

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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

CTR_DRBG_Reseed

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    additional_input is  <empty>

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

  Update

    provided_data is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


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

      While loop

      Key is
                                            134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


      V is
                          3220438A 77E66A34 91E2B5CE 354675CF
```

```
  output_block is
                      5DE6AA50 022F01DF 045B3FDA 58A2AD77

  temp is
                      5DE6AA50 022F01DF 045B3FDA 58A2AD77

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

  While loop

  Key is
                                          134FCABB 870576F9
    E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58

  V is
                      3220438A 77E66A34 91E2B5CE 354675D0

  output_block is
                      9132F66F B04CE0C2 B0FA0721 F686D3E4

  temp is
                                          5DE6AA50 022F01DF
    045B3FDA 58A2AD77 9132F66F B04CE0C2 B0FA0721 F686D3E4

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

  While loop

  Key is
                                          134FCABB 870576F9
    E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58

  V is
                      3220438A 77E66A34 91E2B5CE 354675D1

  output_block is
                      79B18865 9E08DC83 10050D9A 2EB958DF
```

```
      temp is
        5DE6AA50 022F01DF 045B3FDA 58A2AD77 9132F66F B04CE0C2
        B0FA0721 F686D3E4 79B18865 9E08DC83 10050D9A 2EB958DF


    temp XOR provided_data is
        DD6728D3 86AA8758 8CD2B551 D42F23F8 01A364FC 24D97655
        28639DBA 6A1B4D7B D9102AC6 3AAD7A24 B8ACA731 8214F670


    Key is
                                            DD6728D3 86AA8758
        8CD2B551 D42F23F8 01A364FC 24D97655 28639DBA 6A1B4D7B


    V is
                          D9102AC6 3AAD7A24 B8ACA731 8214F670


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

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

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

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


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

      While loop

      Key is
                                            DD6728D3 86AA8758
        8CD2B551 D42F23F8 01A364FC 24D97655 28639DBA 6A1B4D7B
```

```
  V is
                      D9102AC6 3AAD7A24 B8ACA731 8214F673

  output_block is
                      11B6D033 090305B8 189EC43F 14921586

  temp is
                      11B6D033 090305B8 189EC43F 14921586

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

  While loop

  Key is
                                          DD6728D3 86AA8758
    8CD2B551 D42F23F8 01A364FC 24D97655 28639DBA 6A1B4D7B

  V is
                      D9102AC6 3AAD7A24 B8ACA731 8214F674

  output_block is
                      B2430E0C 27B8117A 155C0F24 4FAFF785

  temp is
                                          11B6D033 090305B8
    189EC43F 14921586 B2430E0C 27B8117A 155C0F24 4FAFF785

------------

  While loop

  Key is
                                          DD6728D3 86AA8758
    8CD2B551 D42F23F8 01A364FC 24D97655 28639DBA 6A1B4D7B

  V is
                      D9102AC6 3AAD7A24 B8ACA731 8214F675
```

```
      output_block is
                           659E02E3 3674432B E02B26C7 CFC5F21E


      temp is
        11B6D033 090305B8 189EC43F 14921586 B2430E0C 27B8117A
        155C0F24 4FAFF785 659E02E3 3674432B E02B26C7 CFC5F21E


    temp XOR provided_data is
        11B6D033 090305B8 189EC43F 14921586 B2430E0C 27B8117A
        155C0F24 4FAFF785 659E02E3 3674432B E02B26C7 CFC5F21E


    Key is
                                              11B6D033 090305B8
        189EC43F 14921586 B2430E0C 27B8117A 155C0F24 4FAFF785


    V is
                           659E02E3 3674432B E02B26C7 CFC5F21E


rnd_val is
                                              1CD51D0A A03AA992
        782B53B5 96297930 DD0541DC 3B05C9AD 35998E53 DB960664


------------------------------------------------------------

Second call to Generate

**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

Generate FAILED: Reseed is required
**************************************************************

CTR_DRBG_Reseed
```

```
    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    ------------

      While loop

      Key is
                                              11B6D033 090305B8
        189EC43F 14921586 B2430E0C 27B8117A 155C0F24 4FAFF785


      V is
                           659E02E3 3674432B E02B26C7 CFC5F21F


      output_block is
                           08D669B0 3A7A8061 B04F770F E270384C


      temp is
                           08D669B0 3A7A8061 B04F770F E270384C


    ------------

      While loop

      Key is
                                              11B6D033 090305B8
        189EC43F 14921586 B2430E0C 27B8117A 155C0F24 4FAFF785
```

```
  V is
                      659E02E3 3674432B E02B26C7 CFC5F220


  output_block is
                      DD6A1359 4038AEC7 272E7C58 EA864D02


  temp is
                                           08D669B0 3A7A8061
    B04F770F E270384C DD6A1359 4038AEC7 272E7C58 EA864D02


------------

  While loop

  Key is
                                           11B6D033 090305B8
    189EC43F 14921586 B2430E0C 27B8117A 155C0F24 4FAFF785


  V is
                      659E02E3 3674432B E02B26C7 CFC5F221


  output_block is
                      D08EB2D1 33BF2A6E 1B19F017 F38518D3


  temp is
    08D669B0 3A7A8061 B04F770F E270384C DD6A1359 4038AEC7
    272E7C58 EA864D02 D08EB2D1 33BF2A6E 1B19F017 F38518D3


temp XOR provided_data is
    C817AB73 FEBF46A6 7886BDC4 2EBDF683 0DBBC18A 94ED7810
    FFF7A683 365B93DD 306F5032 D75ACC89 F3F01AFC 1F68F63C


Key is
                                           C817AB73 FEBF46A6
    7886BDC4 2EBDF683 0DBBC18A 94ED7810 FFF7A683 365B93DD
```

```
    V is
                          306F5032 D75ACC89 F3F01AFC 1F68F63C

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                              C817AB73 FEBF46A6
        7886BDC4 2EBDF683 0DBBC18A 94ED7810 FFF7A683 365B93DD


      V is
                          306F5032 D75ACC89 F3F01AFC 1F68F63F


      output_block is
                          3E94A310 16B2A5FE 650AA422 DB996CD9


      temp is
                          3E94A310 16B2A5FE 650AA422 DB996CD9


    ------------

      While loop
```

```
  Key is
                                          C817AB73 FEBF46A6
    7886BDC4 2EBDF683 0DBBC18A 94ED7810 FFF7A683 365B93DD


  V is
                      306F5032 D75ACC89 F3F01AFC 1F68F640


  output_block is
                      1E261052 E88E88C5 D7A9FC48 35597270


  temp is
                                          3E94A310 16B2A5FE
    650AA422 DB996CD9 1E261052 E88E88C5 D7A9FC48 35597270


------------

  While loop

  Key is
                                          C817AB73 FEBF46A6
    7886BDC4 2EBDF683 0DBBC18A 94ED7810 FFF7A683 365B93DD


  V is
                      306F5032 D75ACC89 F3F01AFC 1F68F641


  output_block is
                      BC908518 2245456E 639DA7BA BDD8723E


  temp is
    3E94A310 16B2A5FE 650AA422 DB996CD9 1E261052 E88E88C5
    D7A9FC48 35597270 BC908518 2245456E 639DA7BA BDD8723E


temp XOR provided_data is
    3E94A310 16B2A5FE 650AA422 DB996CD9 1E261052 E88E88C5
    D7A9FC48 35597270 BC908518 2245456E 639DA7BA BDD8723E


Key is
```

                                                3E94A310 16B2A5FE
        650AA422 DB996CD9 1E261052 E88E88C5 D7A9FC48 35597270

    V is
                            BC908518 2245456E 639DA7BA BDD8723E

rnd_val is
                                                3A4E58FC 06DD9AAB
        B85480E7 896AF882 0B43F969 FDC38628 EBA7F06C D9A063D8

##

CTR_DRBG

    Requested Security Strength = 256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F

    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF

    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF

    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F

    AdditionalInput1 =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F

    AdditionalInput2 =

```
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


###############################################################

***************************************************************

CTR_DRBG_Instantiate_algorithm - without derivation function

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
        58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F


    prediction_resistance_flag = "PredictionResistance"

---------------------------

  Update

    provided_data is
        40404040 40404040 40404040 40404040 40404040 40404040
        40404040 40404040 40404040 40404040 40404040 40404040


    ------------

      While loop

      Key is
                                              00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


      V is
                           00000000 00000000 00000000 00000001


      output_block is
                           530F8AFB C74536B9 A963B4F1 C4CB738B
```

```
  temp is
                      530F8AFB C74536B9 A963B4F1 C4CB738B


------------

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000002


  output_block is
                      CEA7403D 4D606B6E 074EC5D3 BAF39D18


  temp is
                                              530F8AFB C74536B9
    A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18


------------

  While loop

  Key is
                                              00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


  V is
                      00000000 00000000 00000000 00000003


  output_block is
                      726003CA 37A62A74 D1A2F58E 7506358E


  temp is
```

```
        530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
        074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E


    temp XOR provided_data is
        134FCABB 870576F9 E923F4B1 848B33CB 8EE7007D 0D202B2E
        470E8593 FAB3DD58 3220438A 77E66A34 91E2B5CE 354675CE


    Key is
                                           134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


    V is
                           3220438A 77E66A34 91E2B5CE 354675CE


-------------------------------------------------------------

First call to Generate

*************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F


Generate FAILED: Reseed is required
*************************************************************

CTR_DRBG_Reseed

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
        78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F
```

```
---------------------------

  Update

    provided_data is
        E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0 E0E0E0E0
        E0E0E0E0 E0E0E0E0 20202020 20202020 20202020 20202020


    ------------

      While loop

      Key is
                                              134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


      V is
                           3220438A 77E66A34 91E2B5CE 354675CF


      output_block is
                           5DE6AA50 022F01DF 045B3FDA 58A2AD77


      temp is
                           5DE6AA50 022F01DF 045B3FDA 58A2AD77


    ------------

      While loop

      Key is
                                              134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


      V is
                           3220438A 77E66A34 91E2B5CE 354675D0


      output_block is
```

```
                        9132F66F B04CE0C2 B0FA0721 F686D3E4


      temp is
                                              5DE6AA50 022F01DF
        045B3FDA 58A2AD77 9132F66F B04CE0C2 B0FA0721 F686D3E4


    ------------

      While loop

      Key is
                                              134FCABB 870576F9
        E923F4B1 848B33CB 8EE7007D 0D202B2E 470E8593 FAB3DD58


      V is
                        3220438A 77E66A34 91E2B5CE 354675D1


      output_block is
                        79B18865 9E08DC83 10050D9A 2EB958DF


      temp is
        5DE6AA50 022F01DF 045B3FDA 58A2AD77 9132F66F B04CE0C2
        B0FA0721 F686D3E4 79B18865 9E08DC83 10050D9A 2EB958DF


    temp XOR provided_data is
        BD064AB0 E2CFE13F E4BBDF3A B8424D97 71D2168F 50AC0022
        501AE7C1 16663304 5991A845 BE28FCA3 30252DBA 0E9978FF


    Key is
                                              BD064AB0 E2CFE13F
        E4BBDF3A B8424D97 71D2168F 50AC0022 501AE7C1 16663304


    V is
                        5991A845 BE28FCA3 30252DBA 0E9978FF

**************************************************************
```

```
CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

---------------------------

  Update

    provided_data is
        00000000 00000000 00000000 00000000 00000000 00000000
        00000000 00000000 00000000 00000000 00000000 00000000


    ------------

      While loop

      Key is
                                              BD064AB0 E2CFE13F
        E4BBDF3A B8424D97 71D2168F 50AC0022 501AE7C1 16663304


      V is
                           5991A845 BE28FCA3 30252DBA 0E997902


      output_block is
                           0D3F8C6B 2BE6683F 042281B8 78AA03F3


      temp is
                           0D3F8C6B 2BE6683F 042281B8 78AA03F3


    ------------

      While loop

      Key is
                                              BD064AB0 E2CFE13F
        E4BBDF3A B8424D97 71D2168F 50AC0022 501AE7C1 16663304


      V is
```

```
                    5991A845 BE28FCA3 30252DBA 0E997903


  output_block is
                    0778915B 5E4D27D4 D637F72A 8B3AD309


  temp is
                                      0D3F8C6B 2BE6683F
    042281B8 78AA03F3 0778915B 5E4D27D4 D637F72A 8B3AD309


------------

  While loop

  Key is
                                      BD064AB0 E2CFE13F
    E4BBDF3A B8424D97 71D2168F 50AC0022 501AE7C1 16663304


  V is
                    5991A845 BE28FCA3 30252DBA 0E997904


  output_block is
                    0B6551E1 680E4908 FEAF5E04 F71DABD4


  temp is
    0D3F8C6B 2BE6683F 042281B8 78AA03F3 0778915B 5E4D27D4
    D637F72A 8B3AD309 0B6551E1 680E4908 FEAF5E04 F71DABD4


temp XOR provided_data is
    0D3F8C6B 2BE6683F 042281B8 78AA03F3 0778915B 5E4D27D4
    D637F72A 8B3AD309 0B6551E1 680E4908 FEAF5E04 F71DABD4


Key is
                                      0D3F8C6B 2BE6683F
    042281B8 78AA03F3 0778915B 5E4D27D4 D637F72A 8B3AD309


V is
                    0B6551E1 680E4908 FEAF5E04 F71DABD4
```

```
rnd_val is
                                                DBAFEF48 988EF939
        5298F5E3 4CF7A6A4 FBD2256C 52A8C8C7 80B848BB B90EA521


---------------------------------------------------------------

Second call to Generate

***************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


Generate FAILED: Reseed is required
***************************************************************

CTR_DRBG_Reseed

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF


    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
        B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


---------------------------

  Update

    provided_data is
        60606060 60606060 60606060 60606060 60606060 60606060
        60606060 60606060 20202020 20202020 20202020 20202020
```

```
------------

  While loop

  Key is
                                          0D3F8C6B 2BE6683F
    042281B8 78AA03F3 0778915B 5E4D27D4 D637F72A 8B3AD309


  V is
                     0B6551E1 680E4908 FEAF5E04 F71DABD5


  output_block is
                     13E83086 24D57354 0A188423 C5CBFFBA


  temp is
                     13E83086 24D57354 0A188423 C5CBFFBA


------------

  While loop

  Key is
                                          0D3F8C6B 2BE6683F
    042281B8 78AA03F3 0778915B 5E4D27D4 D637F72A 8B3AD309


  V is
                     0B6551E1 680E4908 FEAF5E04 F71DABD6


  output_block is
                     901788F6 86854925 9ACC8A66 A8681F0C


  temp is
                                          13E83086 24D57354
    0A188423 C5CBFFBA 901788F6 86854925 9ACC8A66 A8681F0C


------------

  While loop
```

```
      Key is
                                            0D3F8C6B 2BE6683F
        042281B8 78AA03F3 0778915B 5E4D27D4 D637F72A 8B3AD309


      V is
                          0B6551E1 680E4908 FEAF5E04 F71DABD7


      output_block is
                          8DC5475B B6CC802F E14CD960 C78DCBF6


      temp is
        13E83086 24D57354 0A188423 C5CBFFBA 901788F6 86854925
        9ACC8A66 A8681F0C 8DC5475B B6CC802F E14CD960 C78DCBF6


    temp XOR provided_data is
        738850E6 44B51334 6A78E443 A5AB9FDA F077E896 E6E52945
        FAACEA06 C8087F6C ADE5677B 96ECA00F C16CF940 E7ADEBD6


    Key is
                                            738850E6 44B51334
        6A78E443 A5AB9FDA F077E896 E6E52945 FAACEA06 C8087F6C


    V is
                          ADE5677B 96ECA00F C16CF940 E7ADEBD6


**************************************************************

CTR_DRBG_Generate

  requested_number_of_bits = 256

    additional_input is  <empty>

----------------------------

  Update

    provided_data is
```

```
    00000000 00000000 00000000 00000000 00000000 00000000
    00000000 00000000 00000000 00000000 00000000 00000000


------------

  While loop

  Key is
                                          738850E6 44B51334
    6A78E443 A5AB9FDA F077E896 E6E52945 FAACEA06 C8087F6C


  V is
                      ADE5677B 96ECA00F C16CF940 E7ADEBD9


  output_block is
                      AA2DB253 D141A408 B1CF00B2 05C7FB66


  temp is
                      AA2DB253 D141A408 B1CF00B2 05C7FB66


------------

  While loop

  Key is
                                          738850E6 44B51334
    6A78E443 A5AB9FDA F077E896 E6E52945 FAACEA06 C8087F6C


  V is
                      ADE5677B 96ECA00F C16CF940 E7ADEBDA


  output_block is
                      E7AEF3D0 0C992E32 B2BB091A 1A6D90AA


  temp is
                                          AA2DB253 D141A408
    B1CF00B2 05C7FB66 E7AEF3D0 0C992E32 B2BB091A 1A6D90AA
```

```
    ------------

      While loop

      Key is
                                              738850E6 44B51334
        6A78E443 A5AB9FDA F077E896 E6E52945 FAACEA06 C8087F6C


      V is
                           ADE5677B 96ECA00F C16CF940 E7ADEBDB


      output_block is
                           B58E18F1 C55434A6 30E81E94 74855E7C


      temp is
        AA2DB253 D141A408 B1CF00B2 05C7FB66 E7AEF3D0 0C992E32
        B2BB091A 1A6D90AA B58E18F1 C55434A6 30E81E94 74855E7C


    temp XOR provided_data is
        AA2DB253 D141A408 B1CF00B2 05C7FB66 E7AEF3D0 0C992E32
        B2BB091A 1A6D90AA B58E18F1 C55434A6 30E81E94 74855E7C


    Key is
                                              AA2DB253 D141A408
        B1CF00B2 05C7FB66 E7AEF3D0 0C992E32 B2BB091A 1A6D90AA


    V is
                           B58E18F1 C55434A6 30E81E94 74855E7C


rnd_val is
                                              50A6509D 314E1C24
        26ADD435 2D1B3CF4 6C9896F5 7E4148A9 4DBCA894 63F22239
```