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

  Digital Signature Algorithm
    L = 1024
    N = 160

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

================================================================

Domain Parameter Generation
    L = 1024
    N = 160
    seedlen = 0
    hashlen = 160

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

domain_parameter_seed is
                ED8BEE8D 1CB89229 D2903CBF 0E51EE73 77F48698


Q-poss is
                E950511E AB424B9A 19A2AEB4 E159B784 4C589C4F


Found Q:
                E950511E AB424B9A 19A2AEB4 E159B784 4C589C4F


counter is <0>
P-poss is
                                           C4A26742 EB7D6535
        026D26DA 200B6D94 80BEA446 8DBD691F 35BB7BE5 E9135130
        B800D184 0D81D1E3 098B3F8A E2B9A2F4 D50787CD 016D9DBD
        F423924A A33C9C30 2DAC3CF5 DA4524D0 A3B03022 B5B56980
        F196EAD3 B1568763 EC5CD0B2 40AA8780 4B03332E F8055714
        78751CA7 C8897008 C1940022 85314B62 AAE3E8CA 2ABCD7F5


counter is <1>
P-poss is
                                           FB7BCA8A 6B3D640A
        0D77AFF5 57DB9168 E511C84D 705622A1 2948899A E4377118
        BDE73D8A 9FA0965A 265D20FF EA6414C1 8244237D 99B2AF67
        D1753A78 D9126601 D7238818 FB12F840 81C55C7F 6CA980AA
```

```
        FE2D0ACC 30529462 0E1851AB F67224AF D2717D9C 672ACB18
        4F5D3B3E 97FD3F60 E6432D29 9F6E6D77 9E6041E7 6B68A79F


counter is <2>
P-poss is
                                            8166A95B F6F14259
        FE16584A 0AC822EC 1DB358A8 C514C699 A1327E96 B308DCA8
        6A09C2F5 9A1F46CF CBD169B9 23386E3E CE027BDC A3302BD6
        81B15B9B 27EBB910 E383287A 4D8D2EC8 7F57DC8E CB7ADE92
        52333662 78EBB8E7 733FDAD4 1D43BD01 4226ABF2 72E3D6AE
        09696FB6 EA931FF5 F433C730 8E25AD1D 58E8EFCC DF8666AB


counter is <3>
P-poss is
                                            FDEC7B47 C968EF86
        85BFB90A 364A0332 5758401B 55758F4F 90952034 5E37B6AF
        F9551940 B1D0A458 2014030A B03BC1E2 D0C6BCAA B28F17ED
        46802DE5 4DBD0DB1 69D9BBAA 0433811A 1B11B667 336EFFA0
        067B2C13 56DDEC5A DC5E71B7 C59B8F35 7E66A2FC 1D84C88F
        07929E3C 760EB019 287722B6 78E661E4 3724743A 312C58CF


counter is <4>
P-poss is
                                            E63A75AB 610D65E0
        C5616649 44C40C7C A817DEFF 751BF602 ECE7F989 0E5651C1
        E93DAEAF 4C2A8090 8BBF4F58 165F23E0 2075A7A9 497ACA4A
        6F3DFE6B 12B5D796 F0DDA8B0 DA394BBC EAA9B549 BC93A008
        D1496519 EE6185EF E383227C E518DA85 E4D296CE 961735F4
        DA223A65 D66D2D96 03C559E7 F31D9917 B198C646 CD9C2585


counter is <5>
P-poss is
                                            E0A67598 CD1B763B
        C98C8ABB 333E5DDA 0CD3AA0E 5E1FB5BA 8A7B4EAB C10BA338
        FAE06DD4 B90FDA70 D7CF0CB0 C638BE33 41BEC0AF 8A7330A3
        307DED22 99A0EE60 6DF03517 7A239C34 A912C202 AA5F83B9
        C4A7CF02 35B5316B FC6EFB9A 24841125 8B30B839 AF172440
        F3256305 6CB67A86 1158DDD9 0E6A894C 72A5BBEF 9E286C6B


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

```
P is
                                                E0A67598 CD1B763B
        C98C8ABB 333E5DDA 0CD3AA0E 5E1FB5BA 8A7B4EAB C10BA338
        FAE06DD4 B90FDA70 D7CF0CB0 C638BE33 41BEC0AF 8A7330A3
        307DED22 99A0EE60 6DF03517 7A239C34 A912C202 AA5F83B9
        C4A7CF02 35B5316B FC6EFB9A 24841125 8B30B839 AF172440
        F3256305 6CB67A86 1158DDD9 0E6A894C 72A5BBEF 9E286C6B


Q is
                E950511E AB424B9A 19A2AEB4 E159B784 4C589C4F


Seed is
                ED8BEE8D 1CB89229 D2903CBF 0E51EE73 77F48698


counter is <5>

G is
                                                D29D5121 B0423C27
        69AB2184 3E5A3240 FF19CACC 792264E3 BB6BE4F7 8EDD1B15
        C4DFF7F1 D905431F 0AB16790 E1F773B5 CE01C804 E509066A
        9919F519 5F4ABC58 189FD9FF 987389CB 5BEDF21B 4DAB4F8B
        76A055FF E2770988 FE2EC2DE 11AD9221 9F0B3518 69AC24DA
        3D7BA870 11A701CE 8EE7BFE4 9486ED45 27B7186C A4610A75


H is
                                                              0002


============================================================

Domain Parameter Validation
    P is
                                                E0A67598 CD1B763B
        C98C8ABB 333E5DDA 0CD3AA0E 5E1FB5BA 8A7B4EAB C10BA338
        FAE06DD4 B90FDA70 D7CF0CB0 C638BE33 41BEC0AF 8A7330A3
        307DED22 99A0EE60 6DF03517 7A239C34 A912C202 AA5F83B9
        C4A7CF02 35B5316B FC6EFB9A 24841125 8B30B839 AF172440
        F3256305 6CB67A86 1158DDD9 0E6A894C 72A5BBEF 9E286C6B


    Q is
                E950511E AB424B9A 19A2AEB4 E159B784 4C589C4F
```

```
    domain_parameter_seed is
                ED8BEE8D 1CB89229 D2903CBF 0E51EE73 77F48698


    counter = 5
    hashlen = 160

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

Qtest is
                E950511E AB424B9A 19A2AEB4 E159B784 4C589C4F


Q-prime:
                E950511E AB424B9A 19A2AEB4 E159B784 4C589C4F


i is <0>
Ptest is
                                                C4A26742 EB7D6535
        026D26DA 200B6D94 80BEA446 8DBD691F 35BB7BE5 E9135130
        B800D184 0D81D1E3 098B3F8A E2B9A2F4 D50787CD 016D9DBD
        F423924A A33C9C30 2DAC3CF5 DA4524D0 A3B03022 B5B56980
        F196EAD3 B1568763 EC5CD0B2 40AA8780 4B03332E F8055714
        78751CA7 C8897008 C1940022 85314B62 AAE3E8CA 2ABCD7F5


i is <1>
Ptest is
                                                FB7BCA8A 6B3D640A
        0D77AFF5 57DB9168 E511C84D 705622A1 2948899A E4377118
        BDE73D8A 9FA0965A 265D20FF EA6414C1 8244237D 99B2AF67
        D1753A78 D9126601 D7238818 FB12F840 81C55C7F 6CA980AA
        FE2D0ACC 30529462 0E1851AB F67224AF D2717D9C 672ACB18
        4F5D3B3E 97FD3F60 E6432D29 9F6E6D77 9E6041E7 6B68A79F


i is <2>
Ptest is
                                                8166A95B F6F14259
        FE16584A 0AC822EC 1DB358A8 C514C699 A1327E96 B308DCA8
        6A09C2F5 9A1F46CF CBD169B9 23386E3E CE027BDC A3302BD6
        81B15B9B 27EBB910 E383287A 4D8D2EC8 7F57DC8E CB7ADE92
        52333662 78EBB8E7 733FDAD4 1D43BD01 4226ABF2 72E3D6AE
```

```
        09696FB6 EA931FF5 F433C730 8E25AD1D 58E8EFCC DF8666AB


i is <3>
Ptest is
                                            FDEC7B47 C968EF86
        85BFB90A 364A0332 5758401B 55758F4F 90952034 5E37B6AF
        F9551940 B1D0A458 2014030A B03BC1E2 D0C6BCAA B28F17ED
        46802DE5 4DBD0DB1 69D9BBAA 0433811A 1B11B667 336EFFA0
        067B2C13 56DDEC5A DC5E71B7 C59B8F35 7E66A2FC 1D84C88F
        07929E3C 760EB019 287722B6 78E661E4 3724743A 312C58CF


i is <4>
Ptest is
                                            E63A75AB 610D65E0
        C5616649 44C40C7C A817DEFF 751BF602 ECE7F989 0E5651C1
        E93DAEAF 4C2A8090 8BBF4F58 165F23E0 2075A7A9 497ACA4A
        6F3DFE6B 12B5D796 F0DDA8B0 DA394BBC EAA9B549 BC93A008
        D1496519 EE6185EF E383227C E518DA85 E4D296CE 961735F4
        DA223A65 D66D2D96 03C559E7 F31D9917 B198C646 CD9C2585


i is <5>
Ptest is
                                            E0A67598 CD1B763B
        C98C8ABB 333E5DDA 0CD3AA0E 5E1FB5BA 8A7B4EAB C10BA338
        FAE06DD4 B90FDA70 D7CF0CB0 C638BE33 41BEC0AF 8A7330A3
        307DED22 99A0EE60 6DF03517 7A239C34 A912C202 AA5F83B9
        C4A7CF02 35B5316B FC6EFB9A 24841125 8B30B839 AF172440
        F3256305 6CB67A86 1158DDD9 0E6A894C 72A5BBEF 9E286C6B


Ptest is probably prime
----------------------------------------------------------------

Parameters are VALID


================================================================

Key Pair Generation

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

C is
```

```
                                                          F3B4C192
        385620FE EC46CB7F 5D55FE0C 231B0404 A6153972 9EA1291C


X is
                D0EC4E50 BB290A42 E9E355C7 3D880934 5DE2E139


Y is
                                                 25282217 F5730501
        DD8DBA3E DFCF349A AFFEC209 21128D70 FAC44110 332201BB
        A3F10986 140CBB97 C7269380 60473C8E C97B4731 DB004293
        B5E73036 3609DF97 80F8D883 D8C4D41D ED6A2F1E 1BBBDC97
        9E1B9D6D 3C940301 F4E978D6 5B19041F CF1E8B51 8F5C0576
        C770FE5A 7A485D83 29EE2914 A2DE1B5D A4A6128C EAB70F79


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

================================================================

Per-Message Secret Number Generation

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

C is
                                                          798893FB
        FA6DE3D5 FAEC66A3 3E646BAF 25DF4ACF 5E0D94BC 1ACCD726


K is
                349C5564 8DCF992F 3F33E802 6CFAC87C 1D2BA075


Kinv is
                D557A1B4 E7346C4A 55427A28 D4719138 1C269BDE


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

================================================================

Signature Generation

    hashlen = 160
    Msg is 616263
```

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

K is
                349C5564 8DCF992F 3F33E802 6CFAC87C 1D2BA075


Kinv is
                D557A1B4 E7346C4A 55427A28 D4719138 1C269BDE


R is
                636155AC 9A4633B4 665D179F 9E4117DF 68601F34


Z = Hash(msg) is
                A9993E36 4706816A BA3E2571 7850C26C 9CD0D89D


S is
                6C540B02 D9D4852F 89DF8CFC 99963204 F4347704


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

Signature:
  R is
                636155AC 9A4633B4 665D179F 9E4117DF 68601F34


  S is
                6C540B02 D9D4852F 89DF8CFC 99963204 F4347704


===========================================================

Signature Verification

    hashlen = 160
    Msg is 616263

    R is
                636155AC 9A4633B4 665D179F 9E4117DF 68601F34


    S is
```

```
                6C540B02 D9D4852F 89DF8CFC 99963204 F4347704

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

W is
                7E4F353B 71D1A3DC 2946F6BA E3B9285E F736CE34

Z = Hash(msg) is
                A9993E36 4706816A BA3E2571 7850C26C 9CD0D89D

U1 is
                00ABFD27 8373EDF8 CE08347D 49CD8130 8880103E

U2 is
                0DA3AB84 AE3FF412 D703A63B 41D1EC61 D64B061C

V1 is
                                          9C26B549 69E24166
        D89B06F5 BEC3B0DF 8179E4F9 CF7606F6 7162EDD1 50F73A1F
        9E09E49D 21AB0D04 B4A02E24 46C47BC9 311E38C8 0EFFD862
        FB69FE39 EAB9FC27 0B494A57 5E0D0862 BEF45DF1 A826A448
        8BAC5B37 57E9C351 3DD4D965 E6B0EE18 811BC711 013CF4EA
        BEB57887 8C133783 F80342CA FA147B0C 1CC6E51E 937C8D11

V2 is
                                          841232C0 AA641D81
        74AA4619 826357F6 6FDF66E9 A9B2A7C8 32E901D0 4B07B0E3
        7C35596F E9E873E7 888AF879 AA4795F5 58D9BE9A A6CC302C
        B29B9CCB 03D72C5E BCFDA30E 03F3AB57 4D3C31C1 61B2FA41
        D31F49F9 D2DF72A5 A9137845 5B0A8526 14B6E40B 3C4D1CFE
        81E28EA6 CE9D563B 7506413C D29BFB7B DE64E2F1 4828A631

V is
                636155AC 9A4633B4 665D179F 9E4117DF 68601F34

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

Signature is verified
```

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

  Digital Signature Algorithm
    L = 2048
    N = 224

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

================================================================

Domain Parameter Generation
    L = 2048
    N = 224
    seedlen = 0
    hashlen = 224

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

domain_parameter_seed is
                                                        5AFCC1EF
        FC079A9C CA6ECA86 D6E3CC3B 18642D9B E1CC6207 C84002A9


Q-poss is
                                                        90EAF4D1
        AF0708B1 B612FF35 E0A2997E B9E9D263 C9CE6595 28945C0D


Found Q:
                                                        90EAF4D1
        AF0708B1 B612FF35 E0A2997E B9E9D263 C9CE6595 28945C0D


counter is <0>
P-poss is
                         DAD4DEC5 48623EF9 54F05EB9 AFA6EBFC
        1B9EF28F 63F32B11 45EDC037 452E247F 06AEBD83 8CAC61A4
        F601E3BC EF2873BF 1B778DCA FC9840F8 47D56A90 67F4CC0C
        A8F31688 4746954B 25301094 FB3BC0D0 BFAD71D8 F15BA253
        EF86F171 5683F35E 63BE2F04 BCBE4E34 2999CA30 EF471303
        FDF688F0 0F077940 CCA12E65 C7C558F2 83B2CC76 5E638176
        1371E4FA 0B19A9EF 55A18D5B 00F04EDB EA7C37AD 42C3F4AC
        47719BB1 45A2457C 3CD4CBD8 62B6C619 421213D3 B8F45FEC
        00C21764 C2B31735 155C7669 6ACE207E 5577FAE2 CD6BEFD2
        2B1DABD2 CF72E3A4 9EE3BC37 18CB3383 250B0BB8 979E86DB
        8A4BF167 F99BFCBB 51851143 4AF9A676 0F4BAFE1 6CF20C4F
```

counter is <1>
P-poss is
                        84962FC3 3168614A 09E349E8 3C45F937
        9F06ED8D DA1BA3D3 6F34A17B 2A01D720 D5C0B06E 3E70F32E
        558A98E6 252C9D3D 669C9007 342F47C2 EAF4AECE EE2782AC
        46CE754A 8CBFE939 D6ADD727 273AA621 C36BB10A 64BFCAC7
        E145E165 B7260EE1 F42B13B6 E1D7B0DC 9538A0C0 5ADA4EE7
        38561667 50E11271 2F5B09A2 D0A3B425 31AF1651 572285F3
        11EDDE72 6C056F37 6199CB5D FDEB8806 BAED41BE A5BEB59C
        F308FBFB 2CF953AD E3F1FED8 4D573883 B8119AC5 A9768D16
        D4EB7623 546BBB92 AC66A423 614ED54D 9094ED4A B6560585
        80017085 0E4788B1 8A458567 9DB42026 C26C38B4 F060BF1A
        28F5FB4D 8198082D 3EE20086 44A5D6F7 C2606F43 026EC5C5

counter is <2>
P-poss is
                        D9F3AAAC 71BB4199 5E7C5A91 6762B6F6
        84753659 31B82F69 819CBCE0 D056E15D F3BC76B5 6EA6A0E4
        13480F26 EF737CB5 2F36BFBD CD5E0D93 D99CA7CA D2EBB48D
        F16F1D89 30B0205C 765D867E B29B0880 27B18B89 83EDFD96
        2AE39490 CDFE12FC 036938D6 6351EAC0 62FEEB85 13D18FE0
        AFDB99A8 626FF9CA 90253342 ECD9AE8C C1B62757 D831D3FC
        F973F8DD 1A511BC2 6AA25A9F 5A9AC58A F22695FF C3F8BBB4
        DE0EDE22 8D5AFFE4 C83004DB B84C856A 840E0072 AA023404
        AD307895 D558A089 A679FA54 6620909B C6A374FA 9107681E
        CD1EDE92 E6897356 63D678FD D02FF111 806A8636 4500076B
        59633B2B 1CFDCE4B CA546881 9DCDBBF2 A458A5BF 476BCA75

counter is <3>
P-poss is
                        A2DC575B D7AE7F65 CEB6DE30 6347619B
        E83B9E0E AD85F862 1FF80806 120244B6 8A798BA7 CC7D7721
        CED0246E D6AE0855 3B628605 8F54A63B 0F4BF995 C858C759
        0DD5755A D16F4877 666E7012 8A75E288 622F0282 3778D094
        E0757FDA 5D972FC5 DD29BB0D 8660D0BD 217C1A65 971392DA
        6860A7FC 0D21DD92 E6212222 08B3FA12 E33B21C7 7541FA7E
        201B1669 2CD32581 BACF0786 A7113B8F 68975ABA A6BFFEDA
        A3E38999 4441C84E 876E0463 B2D656D6 A352E6D0 3A031966
        F74A81DA 32B0BF38 E8881B12 C762D5FB 93925B7D 58D0296B
        BD7A1E2A 7459539D 8C0756E8 8E936E03 D93F7BB9 0F5186D3
        A015D010 D360239B C2E65228 898FE511 23072CAF A96BB979

counter is <4>
P-poss is

EB3249DD 4822E012 93DA22F3 60422D6E
B94EA15B EAE3DC5A 30C91A3B B8B50740 C8DA1D3E 73FAB774
3E23253F CF5BE492 DD990E4C A0AACF73 04CA5FD5 80AA1227
2A3D831F B07A638D C30F953A 4DA34D41 C06DD82D FF9303A4
F17B5E4C C8A09C83 D9A66DA3 1D41CFB1 0DB854FD DE4E71F2
FEF8E59A E0B94E71 54B29C43 33F1F02F ECE54B1F 71BBD7E9
C093870E E75B8D57 B79C588A BAF704B2 E7D508A6 6AD120B2
BEBEDADC 2E404F91 4CE29FD1 FAB24E46 F3540452 83DCAC75
4BAA7A8E 45019C44 D8580537 17A4CF52 F1E895CE 2C5D36CA
6ADF5180 D1FC29A3 34A38B96 240F706C 100E4025 132A9E21
194ED2F1 E0EA56D1 3432F60A BBC3AFF9 8726B9E4 88FA4C7D

counter is <5>
P-poss is

F2DE3979 C3E34C5D EF779AAF FFF49C4C
9B05A305 6E354AB8 F70CE3F7 43D979B6 95B8F1A5 FE56BC41
FB524A1B FDFE8AF8 61128860 7A760351 16BF306F B3D0405A
D0B73947 81A1465E 1DF7EEA4 08639382 047E5859 89BC3884
7FAB9722 EA978054 71C84DD7 194CC485 50D1E3FA BED391C7
0CC5D1F5 AA54A6D0 165E30CB 93D559F3 B1AB9658 792A1690
0A055BA8 80C8A341 5192DC52 D991627D 68901530 36148EC7
47432DD5 8950EBFE B19269EC EBA27427 00E7ADE5 1420F941
74DF7666 FF3CF504 C954B286 4D3ADD0C 6AAEE467 AE60C363
BB3084E4 00E13B01 DB7D63EC 8FBE1CC1 6BCFEB3F CFA668AD
B8D6FB06 E389FB82 3E99D158 907C224B E03A3003 41F3163F

counter is <6>
P-poss is

D101A3D4 32CCDA58 5AB7A6D0 587E2047
184AA86A E302CE11 C0C4363F 35CDF3B1 A3BDEAF5 9EE8943E
68CFA7A6 1C53ECAA BC345A22 D064E5FE 8DB8E9C2 9B8DBE9C
811A820C ED437321 4D18871A 132816F9 72D82374 F800E4FA
4AC9E73D F59F15BC 44E80269 313E49CC 0EB44954 0F8E7650
DBAB5B54 E7C597ED 34E5001B 10CDD95A D79641AE D0522EC8
CDC2599F 507B4569 8693D9C0 697774DD E3634F32 BBC3B223
FD47BF52 ED7E6DE0 92898520 C88385D2 AC989AC1 D28387CA
DD52417F F56B384F 36BA2437 F63973B2 5BC4ADB2 6391D794
8FBC0F5C 964CA7D9 846ACCDD C31AEE14 5B5A411A 5949B58A
9819A56D B5ED3320 E1CDFBA2 948E24DE C5BCACF9 2A65917D

counter is <7>
P-poss is
                        F3A2F1D8 ADB73DC6 42731C8F 906AB704
        E6D80BBD 6D314FBC E9F4E327 6D04A62D 675E2C47 4AEF634F
        FBBD4878 2CB88DD1 C81BFC61 214E563E 950E5294 54CA4C75
        79407A78 D4092F72 7271647C E3D17CE0 9494FABF 3F2D502B
        9AB23A15 5588B089 84A98880 4B73A472 EADFBFB3 085D1590
        4BE0E881 65ACD46C 2984B1AB 8C6303D5 E5A6C6B9 96FF6107
        DFFAD776 F8985151 9A02009A 62599D89 0DE819C1 EFC00CBD
        E3F1EE1B C5BF1E08 43D647A8 41187BB2 E76040D7 F45DAB0E
        1B394C98 EE27E651 89949B7A B385506E C8B82E1F 32AC7C90
        E2FD1962 BB9F33B5 9F563564 8FD0AA3B 9898C341 1B041BA6
        1D540193 90392F31 EE0C9F52 90EEE378 37ACA75F 2ADD0F73

counter is <8>
P-poss is
                        A93266CD ACD72FC0 E66EBD4E EDEE5722
        5163612C 3EF4307C 7949AA13 32424F01 042BF07F D9175200
        26B4D554 EC892DC2 F6584EDE F3159D56 D1CDA745 728D637A
        2A5285D5 4E7CC5E7 3E85566C A9BB5B18 67DB9AB2 CCB4FB21
        83AB7922 21C12066 91BFB758 6135E611 B311FAB8 8C95BA2C
        DB5037C9 902B4BE3 BA746EBB 6A600E67 3012D351 825A793E
        A1EF820A 56201B0F 775B5B23 A04D185C 8A7EDAAB 4D7C9AC5
        973646A9 DC583DB2 DA0F5429 617AB3EF 8B0F41CE 3A3637F7
        F84E8076 A1EDFD49 C9EBC9A4 3EF6CC7D E15E717B D4E74845
        165D3612 2F72683D 29627801 37AE493C 42D3D9E8 BDE2A0D9
        FEC17C24 1271F43C F7500B1C 83CDA3A4 609FF9C2 A944B7FF

counter is <9>
P-poss is
                        896AF6DE 45A74FD8 6F4B1CAC 3436BB84
        D4A018FE 3701AB38 A8E7DE8F 9314C8FB C70CF83F 35A1B028
        BFEC4ADC 09CF0DB8 FF829A83 623D0B6D F0B644A7 5DA463F8
        535A8BCA 5E59ADBC E284AC8E 4F40C7DC 727894F9 CAA26B47
        0B74D4D9 95A4D305 F8109089 0AF0DCB3 0F95450A 2A47B597
        66EE3DFB B530D1E1 B312DD54 8D8519C4 63ACC4B0 CE203EF0
        F201F3C1 F3552844 94C01C25 EA4C6CE8 5758583C D9C163C3
        A2DFA0A8 55C46C71 F05B33C5 97071C36 3D2AF558 3D63DE87
        F45F1C93 1E8AA795 66C8CD68 D6438566 1E5567A2 11826A86
        54ADFC5D 8F75D2CF 66869342 F9620CBC 4E714677 9975A324
        C19702FD FB1DE1E2 608C90BE 301DD91A DA8EC2B5 AC3BC023

counter is <10>

P-poss is
                        CB947D03 A50A45AC E324BAE2 3D928042
        EE591836 90D0189B 7AF1F1C2 AA872936 FA5EDBE6 B2886084
        C0127162 B5091783 E5CFECBF F8D14843 60E5B7EF 0CA653FA
        97E7CE4F 40BFB1AA E0DB7446 44E5CF4A 0D7CE572 15175A15
        4A28B291 C46FDAF1 575D84FE 291CAFBD 1250C1D8 0BCCEC37
        231D51BA E131026D 4D06B81B 4DB982A7 5058714D 806214EA
        38FEE6CF 5AF2788F 8F630653 1ED7397D 95DA1663 D3AB09B2
        AB40EBA0 ACF37FAA 64C4E1CF 0F7A62F3 4AE5A5C2 8B018D57
        EB029938 66003362 A2334776 0AB14202 7824BC9E D8C5ED6F
        43725B77 E3D26436 B62A98B6 E7F365EE 0086ECDA 84045004
        4978D8F7 E7344DF9 23BE3186 0C196CE1 9E30B184 C4F41631

counter is <11>
P-poss is
                        9D3413BE AC97DB5A 031F4F77 23754A27
        AF55BF8A CFD43131 FF780F6B E77A7442 444BE4B6 00666D4E
        2AE98AAC F41062DD 97454E52 1A4A99F4 076E1FC1 690A9779
        0E288B97 952A2B49 587D7FAC 4889DED0 3F577FDC 1314FAA0
        85A0069B 375FB4BF DB9B1161 EB434B8A 7711CA84 A0A5EACA
        91B08DC9 BF3AED6A 14284B99 4B145E27 5AE3BA25 7E35884E
        47988201 19DEB54F 86741972 3D7E70B1 E234EC8B 283FE9C6
        1171CBD7 359F087E 93535D0A 60225D54 ECA0FD96 0345FE04
        E26A1096 2F0EC676 596BE92C 23D8BFF4 A75E488D 45689EB1
        8A41409F C0EAD32D 3E9C34C4 0D9C19B8 74216FB1 4063D07B
        041CE3D2 1E9437D5 806ADDC1 3AE28873 8881D69D 62908351

counter is <12>
P-poss is
                        BCA161ED CAA327F2 A2E0FD28 DD4C3BC3
        380D366C A1EF5D53 F7268F74 5CE25EC0 D40A4E7A 78A72882
        D2CDF371 51E1A2B1 CC514F6A 5A62AB8F 4E7B3E40 C6BE594C
        1946B1C0 772DC611 89607BFF 046C1745 CEDA4401 CEFE79AD
        5F22748D 05052B1A F1F6263F C7A14CE0 02DB70E0 A4E0453C
        A345296E 3E54358A 2C401F38 6FA90D81 D10F990E A90416C9
        625A6846 2B942257 2ADFE6C2 8BAF3C73 3A5503A1 61D44694
        9AAEB38F 0FA62EF4 E6CC58A0 CB262F2B 6904D94B 73EFE92D
        5E7BBFC5 EBF549FE 7D3BDB94 35750F62 100226A1 F50951B9
        232BBBA6 42CA8BE6 1902A116 EA62D7A2 8082B5CA 78DEF9E6
        E206FA3C 81A92FD7 DE4D81DE 5A43E1D8 5E45BD48 F0206007

counter is <13>
P-poss is

```
                        AA586728 87000602 F8CB465B 2923FC78
        9AE095B1 38C09B13 4B5F45FA 390221FF AB055E5C D64ACEDA
        0B278E69 096F4EAF 8567E3CE D98C134D A4469262 1E547576
        2AC1549B 56D03C8A 13EC114F D788F614 9707683C F82FE019
        4A79BEA0 B10BE567 264C50B5 BBA18DF3 5E21C0A0 2038D836
        BA636EE4 A88D8787 EC98462C 17E39016 DF4DB8AC A404BC93
        8CFD7CC3 16CC746A 0EC66C13 CD45A7B5 17C51942 5915DA93
        4B0DE6D2 2651B5E1 67A1B5B2 6D410659 606A23A0 5520FCC5
        3F50BF3F 48EFA6F6 C69571EF A4C376E4 540AD989 A7D027DD
        DA2DEC48 0655D187 94AE1C79 58683AE4 8216685A 50A0D719
        35A0F950 BBE54658 7C132581 3375DF2F 5DF0916E 7BF51DA5


counter is <14>
P-poss is
                        A686A32B D97B26B2 0C816E79 85D8DF3D
        E7C59C37 575AC8B9 EB7B7C44 09CD304D D303479E C07C1BA0
        1706C0FE F4D6AFBE 1D754569 E34080D6 49BE71AE 0E863607
        70707D21 FCD37E3D 47534EC5 FFF363B6 2AFE10F6 F382BB6C
        97297848 EA425902 383546FB AAC5FAB4 94D60155 47ED2304
        7D0D9C35 E49DC063 58E5EAA4 999F5500 65173C48 79A9D9A3
        761708AF 91B29ACB 07E199EB E785A969 4EB2BC4A 3C9898EB
        49AE26E8 BF092E0E 5E0CA2AC C778769B 19E580EF 4D3A5264
        18C56481 46F97DC8 087BA998 55729300 B3760C08 D9A00BDD
        43844DD4 1DA2BF22 3F2DFBC9 553AFDA1 513AD31C 1B57FF67
        7B422B7E 15EB99E9 14F86651 4B6DBDAD BD38A28A E783B71F


counter is <15>
P-poss is
                        8C081A8F 7C64708F 99DFD252 FC3E78D7
        220DD107 2E739A8C 49422C6A 8167EF35 CC13D77B E476A469
        B56E3469 16B40E92 68A9CFE4 0ECA902C 719642A7 8513A79F
        FB4D14CE B1F9552A 5E6E77F6 6601791B E47BC480 97A1AADC
        803BFACD 05D5A2C2 ABD593A2 0D93B12F 87D3B357 B5282B27
        022D66D1 71E3412A 6D90595A 906AEAB4 8ADED6C5 79CDCEC1
        3BEBFB17 3C1D534A 58866A6D 0BB82517 6FD40E5C D88E9922
        3C8B3039 E81EFE55 0EBE9044 F83E2BE8 4B762897 71B04856
        32021599 1F23CA2D A2D49941 7258968B B538CE56 EBD0EB0E
        E66DAFDB 06BEA558 31E2C25A 3FB4619E F734C95A 6CA83896
        0B012DA5 86741D09 2DD80896 2C0BE001 EE03155F C9CB1D6B


counter is <16>
P-poss is
                        EF55BDFE BBA46CEF AB887BCD 7A1BDCE9
```

4421C148 B59F37B9 3A0A2D86 749E5B81 FC03B6FA E7904E86
0DE36BFB 6CD28B62 7EA61B5C B8E548BB 30009158 9F2922F2
0C57837E 7A242B6E 91F0517D 49587F33 9C7ACEDA D672BA4F
C4908C9F 269BFE71 3F7E11DC 870C6FDC B65D86F1 866A17E3
E6E91C68 6E432B5D A85E7A58 8DAAF926 A8BD8F49 6C0A72AF
3B46E2C8 BA4C7FE3 1CC07400 7C899940 CABEAEED A3E8CDC3
00E967DD 1518ED1B 941F265C 76840D51 7024E547 DE31B736
68E5C625 8E9D527D 05A2CD9D C9594EBE 5E7FBD49 DFDD6E37
58F12E35 E3743FFB C28BBEE3 20BACA7C 3FD567D0 2D0EE00B
A8C0456D CA64198F 43374E2A 45C4F94D 4E0E0F47 8039ABDF

counter is <17>
P-poss is
EB68569B 4CE8E818 4952F9B3 5B097196
1437A0D8 96402D0F CD918DBF 1C4A2CC6 122FACBB 7D49D003
C79AB430 F1616EE1 CE954577 ADA564E1 96EB96C6 FC8BFC03
5A11C33C 59F74957 F6D0387A DB8CC220 664472B3 37566FFC
1AE880A7 3882659B 3A2F1B23 C21DD310 3C5E2DBB 11BA503A
BB5CCF90 D09BC891 BB95E8A2 F29FE078 97D83611 E77F1950
6AF8B7BF A6998AFE D4C12256 5B578D50 9742003C 593CA08A
D3C96C3B 479BD491 2DEECB16 96D1416B 5E084AF1 7CA674DF
062D775C 550BA9B8 0CC57552 44FB49AB 506BECEF 36F2CE65
D42FF1B1 53A70F5A 571703D2 6460C5DD 6839AFC5 A23E6A3D
9F334FCE C8341A91 32A188DE 7163DBEA D9A31F28 A6644607

counter is <18>
P-poss is
E6C69159 150D3B16 3AFC4FA2 27893F5B
089A1F16 9B06947A B29D96C5 15CC8F5C 512D7817 C9AEE4CD
03477100 946F1655 8C02C24D AFF6D768 8B9E88DB FC4E5BF2
04A853C6 E3877D95 AC424759 770DAF92 EFF53660 EB397CAB
36D2CD83 6AB396D3 22035D94 8335010F B7544676 DEC18424
CC0CB8DC 67576924 CC974206 4A4A79BE D5DBA713 50216D1C
C443C59E BFB23E80 8B8C1363 80236559 2EF0AA30 A5AE732F
5494473F 326CDE1E B4003A3A 061CD80A 8163A46B C940FB0F
6DC5049D D0CA92A3 2E6F29ED 6A1DDB47 B73F668F 47B1C5AA
69DF21DC AE0CB35B 828D6C77 9877BD49 3467D0E1 B60E287D
BB1E3DBB 769DC29A 4120519F 97BCB75E 3DF887EA 051AA62B

counter is <19>
P-poss is
AC0FCE95 D3F89369 CF700543 0EC944EF
9416DD4B A62F9A78 27BDA7A9 FDFC1FF8 209F83C6 38BA7051

```
        B79989F7 4861D081 B5B46749 2B338F03 9B6A94B7 0D8BEAD0
        1B78C945 F18BDD77 4ED8EB95 EFEA2DF2 9E10EA8A 8BFD007B
        D0E923BA 9D78AC7F 78FE873A 117FAAA5 2E118572 63A1E357
        3F9DDAF7 B209D2C2 1B4553ED 655D988D 94F33EB6 03B05EDC
        CDAACE8F 4A8E3D92 09DF4268 65055858 EB66C77E 12D4A979
        6FA54227 0BE5294E 7980BDCF 70CE4103 ECD5BA29 2F1A72D3
        F4D000B1 DCFAAAAF 50DECA2F BB5AE476 C627740C 5D463145
        AAD4CC1B 59FF33A8 9643D1CA 6F7D3774 FBFC00BF 08C22865
        B0032CD5 48160034 54DF0B58 843DB481 28F1B925 B857E1EF


counter is <20>
P-poss is
                        B134E07C 599985AC 1074716A 63E1ED76
        E89D60D7 57BA36AF 9FC194C4 6C433F27 A5D9A935 BEB96905
        2D6E3362 ADD00126 CC06C410 6FE6F125 37F54212 51D03061
        C5625300 C4A7A032 54C58A58 A5A3EE3C 88513CD7 8CA969DD
        98EAE4C1 C21A65C4 614CB474 C6BACA6E 89FD2B37 FDB1B6E5
        2F816858 2F6CBD0A 7A6A55BE 619DE265 8F40080F D62FD0F1
        3DBDF548 A0330127 40AE5C4F CD46A4ED 89C49BC0 85476C5E
        5F92A2B1 E5E0DA0F B084A32B 5E360929 136E55BC AC73896F
        5F19B4EB 1C3661E8 4F1D6D1A E2D010F1 6040E6D9 0DC2EEB1
        3EEF5333 C59F5275 725CB9F5 BD00B2A6 6AC21C06 E8C66191
        2C5DB8A0 5EFDC15B 1AE71723 14F17E94 E07F9427 008F857B


counter is <21>
P-poss is
                        C196BA05 AC29E1F9 C3C72D56 DFFC6154
        A033F147 7AC88EC3 7F09BE6C 5BB95F51 C296DD20 D1A28A06
        7CCC4D43 16A4BD1D CA55ED10 66D438C3 5AEBAABF 57E7DAE4
        28782A95 ECA1C143 DB701FD4 8533A3C1 8F0FE235 57EA7AE6
        19ECACC7 E0B51652 A8776D02 A425567D ED36EABD 90CA33A1
        E8D988F0 BBB92D02 D1D20290 113BB562 CE1FC856 EEB7CDD9
        2D33EEA6 F410859B 179E7E78 9A8F75F6 45FAE2E1 36D252BF
        FAFF8952 8945C1AB E705A38D BC2D364A ADE99BE0 D0AAD82E
        53201214 96DC65B3 930E3804 7294FF87 7831A16D 5228418D
        E8AB275D 7D75651C EFED65F7 8AFC3EA7 FE4D79B3 5F62A040
        2A111759 9ADAC7B2 69A59F35 3CF450E6 982D3B17 02D9CA83


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

P is
                        C196BA05 AC29E1F9 C3C72D56 DFFC6154
        A033F147 7AC88EC3 7F09BE6C 5BB95F51 C296DD20 D1A28A06
```

```
        7CCC4D43 16A4BD1D CA55ED10 66D438C3 5AEBAABF 57E7DAE4
        28782A95 ECA1C143 DB701FD4 8533A3C1 8F0FE235 57EA7AE6
        19ECACC7 E0B51652 A8776D02 A425567D ED36EABD 90CA33A1
        E8D988F0 BBB92D02 D1D20290 113BB562 CE1FC856 EEB7CDD9
        2D33EEA6 F410859B 179E7E78 9A8F75F6 45FAE2E1 36D252BF
        FAFF8952 8945C1AB E705A38D BC2D364A ADE99BE0 D0AAD82E
        53201214 96DC65B3 930E3804 7294FF87 7831A16D 5228418D
        E8AB275D 7D75651C EFED65F7 8AFC3EA7 FE4D79B3 5F62A040
        2A111759 9ADAC7B2 69A59F35 3CF450E6 982D3B17 02D9CA83


Q is
                                                    90EAF4D1
        AF0708B1 B612FF35 E0A2997E B9E9D263 C9CE6595 28945C0D


Seed is
                                                    5AFCC1EF
        FC079A9C CA6ECA86 D6E3CC3B 18642D9B E1CC6207 C84002A9


counter is <21>

G is
                         A59A749A 11242C58 C894E9E5 A91804E8
        FA0AC64B 56288F8D 47D51B1E DC4D6544 4FECA011 1D78F35F
        C9FDD4CB 1F1B79A3 BA9CBEE8 3A3F8110 12503C81 17F98E50
        48B089E3 87AF6949 BF8784EB D9EF4587 6F2E6A5A 495BE64B
        6E770409 494B7FEE 1DBB1E4B 2BC2A53D 4F893D41 8B715959
        2E4FFFDF 6969E91D 770DAEBD 0B5CB14C 00AD68EC 7DC1E574
        5EA55C70 6C4A1C5C 88964E34 D09DEB75 3AD418C1 AD0F4FDF
        D049A955 E5D78491 C0B7A2F1 575A008C CD727AB3 76DB6E69
        5515B05B D412F5B8 C2F4C77E E10DA48A BD53F5DD 498927EE
        7B692BBB CDA2FB23 A516C5B4 533D7398 0B2A3B60 E384ED20
        0AE21B40 D273651A D6060C13 D97FD69A A13C5611 A51B9085


H is
                                                        0002


============================================================

Domain Parameter Validation
    P is
                         C196BA05 AC29E1F9 C3C72D56 DFFC6154
```

```
        A033F147 7AC88EC3 7F09BE6C 5BB95F51 C296DD20 D1A28A06
        7CCC4D43 16A4BD1D CA55ED10 66D438C3 5AEBAABF 57E7DAE4
        28782A95 ECA1C143 DB701FD4 8533A3C1 8F0FE235 57EA7AE6
        19ECACC7 E0B51652 A8776D02 A425567D ED36EABD 90CA33A1
        E8D988F0 BBB92D02 D1D20290 113BB562 CE1FC856 EEB7CDD9
        2D33EEA6 F410859B 179E7E78 9A8F75F6 45FAE2E1 36D252BF
        FAFF8952 8945C1AB E705A38D BC2D364A ADE99BE0 D0AAD82E
        53201214 96DC65B3 930E3804 7294FF87 7831A16D 5228418D
        E8AB275D 7D75651C EFED65F7 8AFC3EA7 FE4D79B3 5F62A040
        2A111759 9ADAC7B2 69A59F35 3CF450E6 982D3B17 02D9CA83


    Q is
                                                        90EAF4D1
        AF0708B1 B612FF35 E0A2997E B9E9D263 C9CE6595 28945C0D


    domain_parameter_seed is
                                                        5AFCC1EF
        FC079A9C CA6ECA86 D6E3CC3B 18642D9B E1CC6207 C84002A9


    counter = 21
    hashlen = 224

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

Qtest is
                                                        90EAF4D1
        AF0708B1 B612FF35 E0A2997E B9E9D263 C9CE6595 28945C0D


Q-prime:
                                                        90EAF4D1
        AF0708B1 B612FF35 E0A2997E B9E9D263 C9CE6595 28945C0D


i is <0>
Ptest is
                        DAD4DEC5 48623EF9 54F05EB9 AFA6EBFC
        1B9EF28F 63F32B11 45EDC037 452E247F 06AEBD83 8CAC61A4
        F601E3BC EF2873BF 1B778DCA FC9840F8 47D56A90 67F4CC0C
        A8F31688 4746954B 25301094 FB3BC0D0 BFAD71D8 F15BA253
        EF86F171 5683F35E 63BE2F04 BCBE4E34 2999CA30 EF471303
        FDF688F0 0F077940 CCA12E65 C7C558F2 83B2CC76 5E638176
        1371E4FA 0B19A9EF 55A18D5B 00F04EDB EA7C37AD 42C3F4AC
```

47719BB1 45A2457C 3CD4CBD8 62B6C619 421213D3 B8F45FEC
00C21764 C2B31735 155C7669 6ACE207E 5577FAE2 CD6BEFD2
2B1DABD2 CF72E3A4 9EE3BC37 18CB3383 250B0BB8 979E86DB
8A4BF167 F99BFCBB 51851143 4AF9A676 0F4BAFE1 6CF20C4F

i is <1>
Ptest is
84962FC3 3168614A 09E349E8 3C45F937
9F06ED8D DA1BA3D3 6F34A17B 2A01D720 D5C0B06E 3E70F32E
558A98E6 252C9D3D 669C9007 342F47C2 EAF4AECE EE2782AC
46CE754A 8CBFE939 D6ADD727 273AA621 C36BB10A 64BFCAC7
E145E165 B7260EE1 F42B13B6 E1D7B0DC 9538A0C0 5ADA4EE7
38561667 50E11271 2F5B09A2 D0A3B425 31AF1651 572285F3
11EDDE72 6C056F37 6199CB5D FDEB8806 BAED41BE A5BEB59C
F308FBFB 2CF953AD E3F1FED8 4D573883 B8119AC5 A9768D16
D4EB7623 546BBB92 AC66A423 614ED54D 9094ED4A B6560585
80017085 0E4788B1 8A458567 9DB42026 C26C38B4 F060BF1A
28F5FB4D 8198082D 3EE20086 44A5D6F7 C2606F43 026EC5C5

i is <2>
Ptest is
D9F3AAAC 71BB4199 5E7C5A91 6762B6F6
84753659 31B82F69 819CBCE0 D056E15D F3BC76B5 6EA6A0E4
13480F26 EF737CB5 2F36BFBD CD5E0D93 D99CA7CA D2EBB48D
F16F1D89 30B0205C 765D867E B29B0880 27B18B89 83EDFD96
2AE39490 CDFE12FC 036938D6 6351EAC0 62FEEB85 13D18FE0
AFDB99A8 626FF9CA 90253342 ECD9AE8C C1B62757 D831D3FC
F973F8DD 1A511BC2 6AA25A9F 5A9AC58A F22695FF C3F8BBB4
DE0EDE22 8D5AFFE4 C83004DB B84C856A 840E0072 AA023404
AD307895 D558A089 A679FA54 6620909B C6A374FA 9107681E
CD1EDE92 E6897356 63D678FD D02FF111 806A8636 4500076B
59633B2B 1CFDCE4B CA546881 9DCDBBF2 A458A5BF 476BCA75

i is <3>
Ptest is
A2DC575B D7AE7F65 CEB6DE30 6347619B
E83B9E0E AD85F862 1FF80806 120244B6 8A798BA7 CC7D7721
CED0246E D6AE0855 3B628605 8F54A63B 0F4BF995 C858C759
0DD5755A D16F4877 666E7012 8A75E288 622F0282 3778D094
E0757FDA 5D972FC5 DD29BB0D 8660D0BD 217C1A65 971392DA
6860A7FC 0D21DD92 E6212222 08B3FA12 E33B21C7 7541FA7E
201B1669 2CD32581 BACF0786 A7113B8F 68975ABA A6BFFEDA
A3E38999 4441C84E 876E0463 B2D656D6 A352E6D0 3A031966

```
        F74A81DA 32B0BF38 E8881B12 C762D5FB 93925B7D 58D0296B
        BD7A1E2A 7459539D 8C0756E8 8E936E03 D93F7BB9 0F5186D3
        A015D010 D360239B C2E65228 898FE511 23072CAF A96BB979


i is <4>
Ptest is
                        EB3249DD 4822E012 93DA22F3 60422D6E
        B94EA15B EAE3DC5A 30C91A3B B8B50740 C8DA1D3E 73FAB774
        3E23253F CF5BE492 DD990E4C A0AACF73 04CA5FD5 80AA1227
        2A3D831F B07A638D C30F953A 4DA34D41 C06DD82D FF9303A4
        F17B5E4C C8A09C83 D9A66DA3 1D41CFB1 0DB854FD DE4E71F2
        FEF8E59A E0B94E71 54B29C43 33F1F02F ECE54B1F 71BBD7E9
        C093870E E75B8D57 B79C588A BAF704B2 E7D508A6 6AD120B2
        BEBEDADC 2E404F91 4CE29FD1 FAB24E46 F3540452 83DCAC75
        4BAA7A8E 45019C44 D8580537 17A4CF52 F1E895CE 2C5D36CA
        6ADF5180 D1FC29A3 34A38B96 240F706C 100E4025 132A9E21
        194ED2F1 E0EA56D1 3432F60A BBC3AFF9 8726B9E4 88FA4C7D


i is <5>
Ptest is
                        F2DE3979 C3E34C5D EF779AAF FFF49C4C
        9B05A305 6E354AB8 F70CE3F7 43D979B6 95B8F1A5 FE56BC41
        FB524A1B FDFE8AF8 61128860 7A760351 16BF306F B3D0405A
        D0B73947 81A1465E 1DF7EEA4 08639382 047E5859 89BC3884
        7FAB9722 EA978054 71C84DD7 194CC485 50D1E3FA BED391C7
        0CC5D1F5 AA54A6D0 165E30CB 93D559F3 B1AB9658 792A1690
        0A055BA8 80C8A341 5192DC52 D991627D 68901530 36148EC7
        47432DD5 8950EBFE B19269EC EBA27427 00E7ADE5 1420F941
        74DF7666 FF3CF504 C954B286 4D3ADD0C 6AAEE467 AE60C363
        BB3084E4 00E13B01 DB7D63EC 8FBE1CC1 6BCFEB3F CFA668AD
        B8D6FB06 E389FB82 3E99D158 907C224B E03A3003 41F3163F


i is <6>
Ptest is
                        D101A3D4 32CCDA58 5AB7A6D0 587E2047
        184AA86A E302CE11 C0C4363F 35CDF3B1 A3BDEAF5 9EE8943E
        68CFA7A6 1C53ECAA BC345A22 D064E5FE 8DB8E9C2 9B8DBE9C
        811A820C ED437321 4D18871A 132816F9 72D82374 F800E4FA
        4AC9E73D F59F15BC 44E80269 313E49CC 0EB44954 0F8E7650
        DBAB5B54 E7C597ED 34E5001B 10CDD95A D79641AE D0522EC8
        CDC2599F 507B4569 8693D9C0 697774DD E3634F32 BBC3B223
        FD47BF52 ED7E6DE0 92898520 C88385D2 AC989AC1 D28387CA
        DD52417F F56B384F 36BA2437 F63973B2 5BC4ADB2 6391D794
```

```
        8FBC0F5C 964CA7D9 846ACCDD C31AEE14 5B5A411A 5949B58A
        9819A56D B5ED3320 E1CDFBA2 948E24DE C5BCACF9 2A65917D


i is <7>
Ptest is
                         F3A2F1D8 ADB73DC6 42731C8F 906AB704
        E6D80BBD 6D314FBC E9F4E327 6D04A62D 675E2C47 4AEF634F
        FBBD4878 2CB88DD1 C81BFC61 214E563E 950E5294 54CA4C75
        79407A78 D4092F72 7271647C E3D17CE0 9494FABF 3F2D502B
        9AB23A15 5588B089 84A98880 4B73A472 EADFBFB3 085D1590
        4BE0E881 65ACD46C 2984B1AB 8C6303D5 E5A6C6B9 96FF6107
        DFFAD776 F8985151 9A02009A 62599D89 0DE819C1 EFC00CBD
        E3F1EE1B C5BF1E08 43D647A8 41187BB2 E76040D7 F45DAB0E
        1B394C98 EE27E651 89949B7A B385506E C8B82E1F 32AC7C90
        E2FD1962 BB9F33B5 9F563564 8FD0AA3B 9898C341 1B041BA6
        1D540193 90392F31 EE0C9F52 90EEE378 37ACA75F 2ADD0F73


i is <8>
Ptest is
                         A93266CD ACD72FC0 E66EBD4E EDEE5722
        5163612C 3EF4307C 7949AA13 32424F01 042BF07F D9175200
        26B4D554 EC892DC2 F6584EDE F3159D56 D1CDA745 728D637A
        2A5285D5 4E7CC5E7 3E85566C A9BB5B18 67DB9AB2 CCB4FB21
        83AB7922 21C12066 91BFB758 6135E611 B311FAB8 8C95BA2C
        DB5037C9 902B4BE3 BA746EBB 6A600E67 3012D351 825A793E
        A1EF820A 56201B0F 775B5B23 A04D185C 8A7EDAAB 4D7C9AC5
        973646A9 DC583DB2 DA0F5429 617AB3EF 8B0F41CE 3A3637F7
        F84E8076 A1EDFD49 C9EBC9A4 3EF6CC7D E15E717B D4E74845
        165D3612 2F72683D 29627801 37AE493C 42D3D9E8 BDE2A0D9
        FEC17C24 1271F43C F7500B1C 83CDA3A4 609FF9C2 A944B7FF


i is <9>
Ptest is
                         896AF6DE 45A74FD8 6F4B1CAC 3436BB84
        D4A018FE 3701AB38 A8E7DE8F 9314C8FB C70CF83F 35A1B028
        BFEC4ADC 09CF0DB8 FF829A83 623D0B6D F0B644A7 5DA463F8
        535A8BCA 5E59ADBC E284AC8E 4F40C7DC 727894F9 CAA26B47
        0B74D4D9 95A4D305 F8109089 0AF0DCB3 0F95450A 2A47B597
        66EE3DFB B530D1E1 B312DD54 8D8519C4 63ACC4B0 CE203EF0
        F201F3C1 F3552844 94C01C25 EA4C6CE8 5758583C D9C163C3
        A2DFA0A8 55C46C71 F05B33C5 97071C36 3D2AF558 3D63DE87
        F45F1C93 1E8AA795 66C8CD68 D6438566 1E5567A2 11826A86
        54ADFC5D 8F75D2CF 66869342 F9620CBC 4E714677 9975A324
```

C19702FD FB1DE1E2 608C90BE 301DD91A DA8EC2B5 AC3BC023

i is <10>
Ptest is
CB947D03 A50A45AC E324BAE2 3D928042
EE591836 90D0189B 7AF1F1C2 AA872936 FA5EDBE6 B2886084
C0127162 B5091783 E5CFECBF F8D14843 60E5B7EF 0CA653FA
97E7CE4F 40BFB1AA E0DB7446 44E5CF4A 0D7CE572 15175A15
4A28B291 C46FDAF1 575D84FE 291CAFBD 1250C1D8 0BCCEC37
231D51BA E131026D 4D06B81B 4DB982A7 5058714D 806214EA
38FEE6CF 5AF2788F 8F630653 1ED7397D 95DA1663 D3AB09B2
AB40EBA0 ACF37FAA 64C4E1CF 0F7A62F3 4AE5A5C2 8B018D57
EB029938 66003362 A2334776 0AB14202 7824BC9E D8C5ED6F
43725B77 E3D26436 B62A98B6 E7F365EE 0086ECDA 84045004
4978D8F7 E7344DF9 23BE3186 0C196CE1 9E30B184 C4F41631

i is <11>
Ptest is
9D3413BE AC97DB5A 031F4F77 23754A27
AF55BF8A CFD43131 FF780F6B E77A7442 444BE4B6 00666D4E
2AE98AAC F41062DD 97454E52 1A4A99F4 076E1FC1 690A9779
0E288B97 952A2B49 587D7FAC 4889DED0 3F577FDC 1314FAA0
85A0069B 375FB4BF DB9B1161 EB434B8A 7711CA84 A0A5EACA
91B08DC9 BF3AED6A 14284B99 4B145E27 5AE3BA25 7E35884E
47988201 19DEB54F 86741972 3D7E70B1 E234EC8B 283FE9C6
1171CBD7 359F087E 93535D0A 60225D54 ECA0FD96 0345FE04
E26A1096 2F0EC676 596BE92C 23D8BFF4 A75E488D 45689EB1
8A41409F C0EAD32D 3E9C34C4 0D9C19B8 74216FB1 4063D07B
041CE3D2 1E9437D5 806ADDC1 3AE28873 8881D69D 62908351

i is <12>
Ptest is
BCA161ED CAA327F2 A2E0FD28 DD4C3BC3
380D366C A1EF5D53 F7268F74 5CE25EC0 D40A4E7A 78A72882
D2CDF371 51E1A2B1 CC514F6A 5A62AB8F 4E7B3E40 C6BE594C
1946B1C0 772DC611 89607BFF 046C1745 CEDA4401 CEFE79AD
5F22748D 05052B1A F1F6263F C7A14CE0 02DB70E0 A4E0453C
A345296E 3E54358A 2C401F38 6FA90D81 D10F990E A90416C9
625A6846 2B942257 2ADFE6C2 8BAF3C73 3A5503A1 61D44694
9AAEB38F 0FA62EF4 E6CC58A0 CB262F2B 6904D94B 73EFE92D
5E7BBFC5 EBF549FE 7D3BDB94 35750F62 100226A1 F50951B9
232BBBA6 42CA8BE6 1902A116 EA62D7A2 8082B5CA 78DEF9E6
E206FA3C 81A92FD7 DE4D81DE 5A43E1D8 5E45BD48 F0206007

```
i is <13>
Ptest is
                        AA586728 87000602 F8CB465B 2923FC78
        9AE095B1 38C09B13 4B5F45FA 390221FF AB055E5C D64ACEDA
        0B278E69 096F4EAF 8567E3CE D98C134D A4469262 1E547576
        2AC1549B 56D03C8A 13EC114F D788F614 9707683C F82FE019
        4A79BEA0 B10BE567 264C50B5 BBA18DF3 5E21C0A0 2038D836
        BA636EE4 A88D8787 EC98462C 17E39016 DF4DB8AC A404BC93
        8CFD7CC3 16CC746A 0EC66C13 CD45A7B5 17C51942 5915DA93
        4B0DE6D2 2651B5E1 67A1B5B2 6D410659 606A23A0 5520FCC5
        3F50BF3F 48EFA6F6 C69571EF A4C376E4 540AD989 A7D027DD
        DA2DEC48 0655D187 94AE1C79 58683AE4 8216685A 50A0D719
        35A0F950 BBE54658 7C132581 3375DF2F 5DF0916E 7BF51DA5


i is <14>
Ptest is
                        A686A32B D97B26B2 0C816E79 85D8DF3D
        E7C59C37 575AC8B9 EB7B7C44 09CD304D D303479E C07C1BA0
        1706C0FE F4D6AFBE 1D754569 E34080D6 49BE71AE 0E863607
        70707D21 FCD37E3D 47534EC5 FFF363B6 2AFE10F6 F382BB6C
        97297848 EA425902 383546FB AAC5FAB4 94D60155 47ED2304
        7D0D9C35 E49DC063 58E5EAA4 999F5500 65173C48 79A9D9A3
        761708AF 91B29ACB 07E199EB E785A969 4EB2BC4A 3C9898EB
        49AE26E8 BF092E0E 5E0CA2AC C778769B 19E580EF 4D3A5264
        18C56481 46F97DC8 087BA998 55729300 B3760C08 D9A00BDD
        43844DD4 1DA2BF22 3F2DFBC9 553AFDA1 513AD31C 1B57FF67
        7B422B7E 15EB99E9 14F86651 4B6DBDAD BD38A28A E783B71F


i is <15>
Ptest is
                        8C081A8F 7C64708F 99DFD252 FC3E78D7
        220DD107 2E739A8C 49422C6A 8167EF35 CC13D77B E476A469
        B56E3469 16B40E92 68A9CFE4 0ECA902C 719642A7 8513A79F
        FB4D14CE B1F9552A 5E6E77F6 6601791B E47BC480 97A1AADC
        803BFACD 05D5A2C2 ABD593A2 0D93B12F 87D3B357 B5282B27
        022D66D1 71E3412A 6D90595A 906AEAB4 8ADED6C5 79CDCEC1
        3BEBFB17 3C1D534A 58866A6D 0BB82517 6FD40E5C D88E9922
        3C8B3039 E81EFE55 0EBE9044 F83E2BE8 4B762897 71B04856
        32021599 1F23CA2D A2D49941 7258968B B538CE56 EBD0EB0E
        E66DAFDB 06BEA558 31E2C25A 3FB4619E F734C95A 6CA83896
        0B012DA5 86741D09 2DD80896 2C0BE001 EE03155F C9CB1D6B
```

```
i is <16>
Ptest is
                        EF55BDFE BBA46CEF AB887BCD 7A1BDCE9
        4421C148 B59F37B9 3A0A2D86 749E5B81 FC03B6FA E7904E86
        0DE36BFB 6CD28B62 7EA61B5C B8E548BB 30009158 9F2922F2
        0C57837E 7A242B6E 91F0517D 49587F33 9C7ACEDA D672BA4F
        C4908C9F 269BFE71 3F7E11DC 870C6FDC B65D86F1 866A17E3
        E6E91C68 6E432B5D A85E7A58 8DAAF926 A8BD8F49 6C0A72AF
        3B46E2C8 BA4C7FE3 1CC07400 7C899940 CABEAEED A3E8CDC3
        00E967DD 1518ED1B 941F265C 76840D51 7024E547 DE31B736
        68E5C625 8E9D527D 05A2CD9D C9594EBE 5E7FBD49 DFDD6E37
        58F12E35 E3743FFB C28BBEE3 20BACA7C 3FD567D0 2D0EE00B
        A8C0456D CA64198F 43374E2A 45C4F94D 4E0E0F47 8039ABDF


i is <17>
Ptest is
                        EB68569B 4CE8E818 4952F9B3 5B097196
        1437A0D8 96402D0F CD918DBF 1C4A2CC6 122FACBB 7D49D003
        C79AB430 F1616EE1 CE954577 ADA564E1 96EB96C6 FC8BFC03
        5A11C33C 59F74957 F6D0387A DB8CC220 664472B3 37566FFC
        1AE880A7 3882659B 3A2F1B23 C21DD310 3C5E2DBB 11BA503A
        BB5CCF90 D09BC891 BB95E8A2 F29FE078 97D83611 E77F1950
        6AF8B7BF A6998AFE D4C12256 5B578D50 9742003C 593CA08A
        D3C96C3B 479BD491 2DEECB16 96D1416B 5E084AF1 7CA674DF
        062D775C 550BA9B8 0CC57552 44FB49AB 506BECEF 36F2CE65
        D42FF1B1 53A70F5A 571703D2 6460C5DD 6839AFC5 A23E6A3D
        9F334FCE C8341A91 32A188DE 7163DBEA D9A31F28 A6644607


i is <18>
Ptest is
                        E6C69159 150D3B16 3AFC4FA2 27893F5B
        089A1F16 9B06947A B29D96C5 15CC8F5C 512D7817 C9AEE4CD
        03477100 946F1655 8C02C24D AFF6D768 8B9E88DB FC4E5BF2
        04A853C6 E3877D95 AC424759 770DAF92 EFF53660 EB397CAB
        36D2CD83 6AB396D3 22035D94 8335010F B7544676 DEC18424
        CC0CB8DC 67576924 CC974206 4A4A79BE D5DBA713 50216D1C
        C443C59E BFB23E80 8B8C1363 80236559 2EF0AA30 A5AE732F
        5494473F 326CDE1E B4003A3A 061CD80A 8163A46B C940FB0F
        6DC5049D D0CA92A3 2E6F29ED 6A1DDB47 B73F668F 47B1C5AA
        69DF21DC AE0CB35B 828D6C77 9877BD49 3467D0E1 B60E287D
        BB1E3DBB 769DC29A 4120519F 97BCB75E 3DF887EA 051AA62B
```

```
i is <19>
Ptest is
                        AC0FCE95 D3F89369 CF700543 0EC944EF
        9416DD4B A62F9A78 27BDA7A9 FDFC1FF8 209F83C6 38BA7051
        B79989F7 4861D081 B5B46749 2B338F03 9B6A94B7 0D8BEAD0
        1B78C945 F18BDD77 4ED8EB95 EFEA2DF2 9E10EA8A 8BFD007B
        D0E923BA 9D78AC7F 78FE873A 117FAAA5 2E118572 63A1E357
        3F9DDAF7 B209D2C2 1B4553ED 655D988D 94F33EB6 03B05EDC
        CDAACE8F 4A8E3D92 09DF4268 65055858 EB66C77E 12D4A979
        6FA54227 0BE5294E 7980BDCF 70CE4103 ECD5BA29 2F1A72D3
        F4D000B1 DCFAAAAF 50DECA2F BB5AE476 C627740C 5D463145
        AAD4CC1B 59FF33A8 9643D1CA 6F7D3774 FBFC00BF 08C22865
        B0032CD5 48160034 54DF0B58 843DB481 28F1B925 B857E1EF


i is <20>
Ptest is
                        B134E07C 599985AC 1074716A 63E1ED76
        E89D60D7 57BA36AF 9FC194C4 6C433F27 A5D9A935 BEB96905
        2D6E3362 ADD00126 CC06C410 6FE6F125 37F54212 51D03061
        C5625300 C4A7A032 54C58A58 A5A3EE3C 88513CD7 8CA969DD
        98EAE4C1 C21A65C4 614CB474 C6BACA6E 89FD2B37 FDB1B6E5
        2F816858 2F6CBD0A 7A6A55BE 619DE265 8F40080F D62FD0F1
        3DBDF548 A0330127 40AE5C4F CD46A4ED 89C49BC0 85476C5E
        5F92A2B1 E5E0DA0F B084A32B 5E360929 136E55BC AC73896F
        5F19B4EB 1C3661E8 4F1D6D1A E2D010F1 6040E6D9 0DC2EEB1
        3EEF5333 C59F5275 725CB9F5 BD00B2A6 6AC21C06 E8C66191
        2C5DB8A0 5EFDC15B 1AE71723 14F17E94 E07F9427 008F857B


i is <21>
Ptest is
                        C196BA05 AC29E1F9 C3C72D56 DFFC6154
        A033F147 7AC88EC3 7F09BE6C 5BB95F51 C296DD20 D1A28A06
        7CCC4D43 16A4BD1D CA55ED10 66D438C3 5AEBAABF 57E7DAE4
        28782A95 ECA1C143 DB701FD4 8533A3C1 8F0FE235 57EA7AE6
        19ECACC7 E0B51652 A8776D02 A425567D ED36EABD 90CA33A1
        E8D988F0 BBB92D02 D1D20290 113BB562 CE1FC856 EEB7CDD9
        2D33EEA6 F410859B 179E7E78 9A8F75F6 45FAE2E1 36D252BF
        FAFF8952 8945C1AB E705A38D BC2D364A ADE99BE0 D0AAD82E
        53201214 96DC65B3 930E3804 7294FF87 7831A16D 5228418D
        E8AB275D 7D75651C EFED65F7 8AFC3EA7 FE4D79B3 5F62A040
        2A111759 9ADAC7B2 69A59F35 3CF450E6 982D3B17 02D9CA83


Ptest is probably prime
```

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

Parameters are VALID

============================================================

Key Pair Generation

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

C is
                                    1AB8E747 21242705 F05EF642
        8B9F43DB 620DFA42 3A81D561 17AF5E51 446C92CD 321866C2


X is
                                                      00D0F09E
        D3E2568F 6CADF922 4117DA2A EC5A4300 E009DE13 66023E17


Y is
                          70035C9A 3B225B25 8F16741F 3941FBF0
        6F3D056C D7BD8646 04CBB5EE 9DD85304 EE8E8E4A BD5E9032
        11DDF25C E1490755 10ACE166 970AFDC7 DF552B72 44F342FA
        02F7A621 405B7549 09D757F9 7290E1FE 5036E904 CF593446
        0C046D95 659821E1 597ED9F2 B1F0E208 63A6BBD0 CE74DACB
        A5D8C68A 90B29C21 57CDEDB8 2EC12B81 EE3068F9 BF5F7F34
        6ECA41ED 174CCCD7 D154FA4F 42F80FFE 1BF46AE9 D8125DEB
        5B4BA08A 72BDD865 96DBEDDC 9550FDD6 50C58F5A E5133509
        A702F79A 31ECB490 F7A3C558 1631F7C5 BE4FF7F9 E9F27FA3
        90E47347 AD118350 9FED6FCF 198BA9A7 1AB3335B 4F38BE8D
        15496A00 B6DC2263 E20A5F6B 662320A3 A1EC033A A61E3B68


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

============================================================

Per-Message Secret Number Generation

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

C is
                                    0DA161C1 E4BEA190 BB83E277
        763C4D7C C159787D 9E8A2622 552BF51D 0313AAE1 F1D7349C
```

K is
                                                        735959CC
        4463B8B4 40E407EE CA8A473B F6A6D1FE 657546F6 7D401F05

Kinv is
                                                        711B7835
        403AD69B C8CD7AAD 4E73FC88 4485216F C2CA6744 4391864A

==========

Signature Generation

    hashlen = 224
    Msg is 616263

K is
                                                        735959CC
        4463B8B4 40E407EE CA8A473B F6A6D1FE 657546F6 7D401F05

Kinv is
                                                        711B7835
        403AD69B C8CD7AAD 4E73FC88 4485216F C2CA6744 4391864A

R is
                                                        4400138D
        05F9639C AF54A583 CAAF25D2 B76D0C3E AD752CE1 7DBC85FE

Z = Hash(msg) is
                                                        23097D22
        3405D822 8642A477 BDA255B3 2AADBCE4 BDA0B3F7 E36C9DA7

S is
                                                        874D4F12
        CB13B617 32D39844 5698CFA9 D92381D9 38AA57EE 2C9327B3

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

Signature:
  R is
                                                        4400138D
        05F9639C AF54A583 CAAF25D2 B76D0C3E AD752CE1 7DBC85FE


  S is
                                                        874D4F12
        CB13B617 32D39844 5698CFA9 D92381D9 38AA57EE 2C9327B3


===============================================================

Signature Verification

    hashlen = 224
    Msg is 616263

    R is
                                                        4400138D
        05F9639C AF54A583 CAAF25D2 B76D0C3E AD752CE1 7DBC85FE


    S is
                                                        874D4F12
        CB13B617 32D39844 5698CFA9 D92381D9 38AA57EE 2C9327B3


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

W is
                                                        4EB5DF8B
        0D117B3C 74EC2282 44C1EF9D 38D89D0B EDD73FD7 881365F5


Z = Hash(msg) is
                                                        23097D22
        3405D822 8642A477 BDA255B3 2AADBCE4 BDA0B3F7 E36C9DA7


U1 is
                                                        6E3D0963
```

```
        DE96EC4F 57F32ED9 364D7EFC 04C7342F 6AFEECC3 6A1188A3


U2 is
                                                          5C0EA8DB
        62A5A02D 58B88771 AC555232 17C48519 37BD1C73 7504CD96


V1 is
                          B5DDEF02 014F3B7E 3486C6B5 DC40C5DC
        506BD370 5EBB09ED 8C3411A3 F22074F2 E66E7495 BE496ECC
        3F8C215F E8013790 10BBA789 8EB2047E 5FE2989D 6B64CC28
        C42C1F8D 3032F8F0 1A3774E7 9654908D 21650476 AB56923D
        032D4993 DA770697 EFDDBEA9 1BAF9933 F3EC7ED2 19FC3E2A
        42A500B6 F2FD08A2 A06B8D7A 0A9CDF77 89C902EE 7726CFA6
        5ECD5360 46E150FC 2ECAD78C 749D4B20 CAFEEAAA 287B7480
        CAF9E230 E3F1C5B4 CE692604 03BF1D1F DC678834 7349CF71
        4E272C7D 0C387402 6BD04D00 8EC52F9C D53915A6 ECE42C02
        886D5E26 681D8AF1 0F6845A0 70391B3F 871E6D33 018AAA2E
        2324D8DD 85F5716F F313EF40 2A42906A 1628539D AA8464C0


V2 is
                          30000A38 16401209 B0E6777D F294B5DA
        98FF4DDC 59D8E45F 68D08769 FC8D128A 1F16DEE6 7E5C4A6C
        1CA4E332 1527EDD3 0A2BE407 92D8F91D E821C40F 37B68A43
        08601B7E 34C21D8B E119943C 5AA1DDD4 EE893066 0EA5CCAB
        960A7AE3 81E5129C 0EB8AF8F 7A20C411 B0F8EEA2 F0751FA5
        9737ACB5 0FB5A7CF 76C3BFCB 39124F1C EBC26AC4 DF87D4E9
        215DDF87 49B0D49F 2AA4B631 2B3B3D80 25CA3A49 ABE58C34
        4DB4889A 9E61B0DF D9AB9865 A4F662AA 9573680C 7A866D9B
        019E2F64 C14B7859 52A72697 8E0A9830 CC90307C 0746DCA0
        21021807 8377CA9C 3F52A659 055E4528 60C7F35A B50212B9
        AE33510E C447A137 BE42B63F B9830C49 BF50A304 2B6CA4FF


V is
                                                          4400138D
        05F9639C AF54A583 CAAF25D2 B76D0C3E AD752CE1 7DBC85FE


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

Signature is verified
```

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

  Digital Signature Algorithm
    L = 2048
    N = 256

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

================================================================

Domain Parameter Generation
    L = 2048
    N = 256
    seedlen = 0
    hashlen = 256

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

domain_parameter_seed is
                                                47830819 72865EA9
        5D43318A B2EAF9C6 1A2FC7BB F1B772A0 9017BDF5 A58F4FF0


Q-poss is
                                                C24ED361 870B61E0
        D367F008 F99F8A1F 75525889 C89DB1B6 73C45AF5 867CB467


Found Q:
                                                C24ED361 870B61E0
        D367F008 F99F8A1F 75525889 C89DB1B6 73C45AF5 867CB467


counter is <0>
P-poss is
                          E46D386A 8F65A4D9 928A2F87 C52E917C
        26346EF0 966D70E8 61ED94A9 F74BFC6A D35D5E9D A083C91C
        8E0FB7BF 337FA25A 828B3F60 5BB3AE95 5CED49F8 49524B87
        0A6403CB B1B8B2DA BA68AB29 611D7BFC 7A9CB4E1 D74A17A1
        A73DC750 FCD42CCA E7BDA622 9A470AA4 B4A8C3AF 26DB24E5
        01F87C5F 9556C92A D2E8D2CF E628DE0E 4887F778 48F9F173
        B915B6ED 366FA29F 317C60B4 9C4192F7 1EA8719B 21376CD8
        693B1AF9 57039CDC 6887F544 43DACB2C 9C6A9B20 BF74CB6E
        26300B71 4226512E 6A669091 780EC658 1FD250AE 28710989
        0A423A82 D4EB9E5F F80F6224 C9A8CD9D 0FC49896 AD91AA66
        9A8829A6 198F3BB0 B32116DC 644F67B5 4AC18A1D A25A217B
```

```
counter is <1>
P-poss is
                        F05D7CAA 10B69987 3EA51B8D 8C73B316
        1B7F1F2F CAE5CA5F 39464575 CDB128B2 C301BE91 C95A02E0
        A0AB1CC1 71B3BC16 DD63A1B9 ED266289 51E0BEEF AF16886B
        525EA5F5 EAAB566D DB36B379 193DA14B B5052D0C C387FBD1
        EE22FFAE 052F9262 0B77170D 6DEA84F0 CC14D572 3F2D7D47
        6DBACD15 82F23DB9 3CC02434 7CAED83C 3E113FE7 6DC3900D
        61D8183F 053366F8 FEEEBB89 4C5FF287 BF224B6D B91C978C
        0AD37E4B C9539D14 E5F922A1 8334CE24 094E3FBF 86DFC447
        FD52271E 2FB7078B E9636E7A E08D7097 032D0802 61F3EB62
        7E7BE0AC A7155D8A 5A0CA204 3AF89745 7041D8FB C0963445
        F3FF5F8A 658BC192 D8C849C4 26698DC8 BBE98F92 3CE27205


counter is <2>
P-poss is
                        DB52970B D1BD220E 7585EBB7 97E07564
        0B60CF50 895B0E36 D8145313 63FD6AD9 76E9DA43 B571B265
        7FBA2F24 6424628B 01C5C371 E02BB00F C8FD3031 8ED6DC6F
        B8DD1B06 FCF60A12 D6AA4D59 886CD557 16039F6F 074D2B80
        18C8158E 72DB8E83 F57B4DCB 12181396 0EF14C9E 18E0813E
        D87E4E20 C5D3222E BEB1D662 58187A30 FA9D6B77 273DFD83
        8D74E89A F2371B9A 12A8C428 5775FF1F DC3F826D D0FFD12D
        A7882A3C 8F82BC4A E6016537 04504DB0 86172020 F2FB343E
        FD431C5A 25E819A8 3809504A A122B6DF B62F4CCD F632B38E
        B83D975E A40C471B C4310CB9 2C2FB9F9 FBDCC2A2 492A5CCC
        4850595D 316BF98A 4734F4B3 6623D62D C6B8A9EC B5DDEE03


counter is <3>
P-poss is
                        EB2AD4CB F0F62EA9 E08FCB77 BED60FC9
        71F3B92C 2AD02390 1164582F CA206C00 B81C1E8B 7D0F4FA3
        77303CC0 3A1F9E84 9D1710E4 626108D9 46484AA0 50B8A484
        F004A76C FC8BA059 525B4605 7906A050 9B85D71F F3386102
        DBAADA98 6DE97AA7 EB06143B 0A6FF301 502C4177 838B4599
        B98CCFA8 4CF07B85 201CD2AA 25952545 C29C31B9 32C790E6
        F693B9D7 635EBB9B 646917E3 83389E39 5CC72059 0C3E4EC5
        987BF2D0 4744814A 1A7B61F8 C73A7388 93D2420D B3ADE987
        E80F8E76 7C4B84EC 9764C5F6 C5DCDBDD 32B8AB61 1E0D7783
        A9B2D720 DC437A3E DD97857B 8F62D385 F3EDDFAD EFEBBD3D
        FE2B0981 9F799184 443E2F48 A6AAD37C F17D69B8 ED0A457B
```

counter is <4>
P-poss is

A8DA61F7 A1451157 CDBF46B8 3CDA35CA
0A50906B 2A111CC5 5356CD10 2E9FD84B 0568F146 DFADEC7E
2B55D103 77778E1B BEE3940E 2EFDE6A1 DB6239A6 52D172A1
18C8711C CB4054BC 6AB64991 84BC7B7A 59119A91 4045C1BC
0D40397A 66C9B2BE 588C0226 1F6A2720 2FA93A5A 004F0436
3EFF6721 69A47C57 2DE3DE13 B9A64C0C F9425FFF 0D77F088
4918A470 4653C5FF 97D129C7 3A3F0B84 AB50935D D7ED1F30
F901A66D 8CDDFF8A F8DF2B71 03ED42FF 0F6D815B 0073C4CC
3000B4CE E0BE3936 5303D315 742CA385 8E9248A1 83838F84
3BEEB03F 452B48B6 68EC46D6 2C656F97 E19E1741 B9C63BA4
7FD94613 502AC603 E011C20F 8D638FA1 5B092CBE F3227A55

counter is <5>
P-poss is

B0C94960 1F57DD97 492DBDAE AE4C809E
4A69128A EBB039F6 DF61AEF9 AD2D587E 8FB8D468 6014A5F9
DA545245 40AE88E8 D1325F7D 5D1E64A2 D5AB1F38 3125CF75
BA1ADE75 3819A093 1DDA9407 9B348E4A 0E7FDC1B 821ECC29
7E139D7C 6D97FFA7 D201199D AD30CDE4 5788626E 5EB1C771
4AD8F5A4 0C38C1E9 2DF0DABF 7092DA84 A7C5A8D8 57AF1664
E90EB028 B57E498E A1DC8458 076A717D F18E4A04 FADD70D0
32FC2162 FEA05BA9 432508CC 7FC174A2 E94CA1B9 8A6BA8A1
DC8E8D6E FD88441D 7593A94D 160F89E5 7931ABD7 C2A259F9
77BE6FD4 00DB9AC2 055E016A F7B893C8 63A9EBFD CE1FD936
472FA896 20E0EB7A A426E47B 565AC9BE CFE17937 D953FE79

counter is <6>
P-poss is

E6144A89 95A5B3BC 683F0824 67CD595B
93489B34 C97F1FD5 C873C1CC 4A52D85D 47B0C174 5B54C68B
F0B91734 17626970 71DCF62F 1FFEC6F9 A0A90A62 095E9446
C1E9FE05 F09A84AA 0CDCCEBA D2F09CF2 5C7ADC0E 084199AD
E60CCA87 F2B2AE6F DE47CE20 5FA908CF 05505EFC F6944FCE
98CDF1E3 9FF7920C E0C3FDEE 1B9C0C87 8A4932EC AC8A2B52
308B7044 2BC57BAE D1C1631D F2AEE986 C32DAD99 7744DC81
269C0923 4295A18F EAF7054E 9EF20FA0 630573AC 522AAB84
1924DA15 20E62773 365EAA09 9B177813 B21A582B 06B58EEF
0311934C 6797238E 674465AD 9BD3A580 5D887D1B 9BD6F8B2
67DD4A43 F8DAE9A5 D6B79949 A05A92B3 5B3205F2 08DE7A7F

counter is <7>
P-poss is

		BC91BA6C	B5501C18	581ACBF4	4D49DCE2
4C3C54A8	7E57C780	318962C5	1E90CC25	0BFF08DD	D40F3B1E
04AED147	5704D697	22176F68	A44BBFB1	359D76E1	A2D8B223
B907E03C	1E17A615	537FC9F0	1FA4ED9C	9AC890D7	F15B1726
4D9B630C	7BEDEBD0	2D865CAD	7DBDA106	CF106738	3ECAD42B
CB3DA297	B123A27E	18CB9C16	D0ECFC91	B4AFECEB	69FE5DC0
70E97A6F	F5E26310	3E871AA1	CDFC0106	1C107E18	07AF8F8C
EB1F362A	4FBCEEA1	C50D7960	14189E59	597665ED	35BCFC9A
819D0A5F	A4DFB9FE	F20FC0C8	5B2DBCF0	4D74CA44	6C7133B5
CFEAE794	648FCE50	BBC9259D	00C2A529	9D6ABA07	DFE1E384
3A4FB389	F1E3EF8A	06AAF060	77BD6D06	511AA5D2	B8B6690F

counter is <8>
P-poss is

		A6B117EB	EE793BBE	92D9433A	DD39AE30
00574373	4596E5DC	CA3F70A5	3E23F101	92C49D60	5A68B16A
F3D2CAF9	EA97603F	AF6EE055	F0D29D81	DEDDFDBA	1934BE89
3DFD73CC	7D177E6D	B00FF7F7	72FA22ED	DF902F47	4B52BE9A
2A85352C	3F95E020	CA5A6A54	A0C67B26	0D874C02	C2DF5936
4886845A	E9CED9F8	EFB098B7	F486C8DA	C9B9B921	5389A7E5
800D21DF	889864C0	E85CD5B7	8D4FD7A8	B1FDB9A5	6658F5B2
F5CF5E83	5563C93A	8136F8D2	EBF3E505	22428791	28AAB667
3231B469	375D4547	78C0F5E3	3423EBE6	681D97B3	8882571C
8EE673D4	1E92178B	DC1FDA8D	B8BAC225	D33ED82C	AEABC7C4
E8872379	335AFC9F	1636CB0C	A209F2A0	35ADB246	218CA299

counter is <9>
P-poss is

		958809A4	A45295A2	E9917E4D	01DE35D7
B6E0A3C9	A9E3A8DC	9081B4C1	6BF60691	D992B189	C821B96B
C57B02B2	461BFC3B	0BADE772	D37D77EB	9F8D8D73	8B0983B9
DC0A9104	02B2BA7E	B697DADA	E6B1250F	3D8C4CD5	349AD82B
917EE697	83FED60D	2DEB005D	7F455A7A	91A29CCC	8744ECF1
82D62163	48F2922D	BEF5FC72	F2E29D4F	6BFE337B	CDE3DA4C
A9372759	253EF5CA	4F5A5DE1	E594D963	43511340	EDC99E66
BF3A6B6C	459217AA	12D0ED34	6AD28CF0	D1A1ABEB	FEB2820F
DD4AC538	B018FC32	844FE4CC	A35334E7	43A30F0C	C951B004
07BC5679	62EE43D9	CA44C951	EAF8A020	87B0470D	D26B5980
BC5F35CE	725FB926	03A7716E	EF5B349F	8E38A13B	683A684D

counter is <10>

```
P-poss is
                        BF54D59D ECB2CB0A B53C337D D34B5C2F
        0B86D277 585E1178 E4A12E15 020BB2B7 3460DB7F 5821F787
        99165841 BB643F2D 30BC4FD4 1AABCDCD BE374F85 832E7C0F
        18866F16 9B407D42 83AA8411 435D197C 3432FBDD 8296A5C2
        161853D1 4E254C8D BB9CF427 D4687D2E E8D5DBC0 F718E60B
        587CA596 4B231C0C A8BC742F F54552CA C0B2B4B3 1D0ED4F1
        C0D71C0B CBCA8B3D C741EBB9 3D622D14 00412A12 D55A8E94
        E7EC616B 92981640 B7C67C14 509CAE0A B5F9725C BAEFF41D
        6FBFDB7E 5BE068ED 0B32500F 53F371EE BB85B032 601F53BB
        2A9FEACC 24377A54 5CEE88F1 6E018716 EC14F557 5D035D30
        2DE55549 63A8FC88 6C7F82D5 253912FE 14E73EA8 A14573DB


counter is <11>
P-poss is
                        C8A35411 13B512A2 609089A7 7F3CFA13
        54F2E14F 681CF409 D1EA2B77 C06281AF CBBC2D7A E8BD756E
        18E57608 250C437F A1E4BD9D 2CB8F4B0 2CBA9C29 E8EF0091
        226FBB5F CFCFA305 3D3990DB B5797DA0 A22D2E68 660DD112
        53A27603 EBA3B8BE 9CFD5C2A EFF025E8 DBB04A38 108E6B52
        C47830EA 777A4E26 8CE05095 63C33D7D CE787022 6697AD06
        AF8D3458 26BF9CC3 ACF7725A DF0F534A B6CE7192 B1DF4A5F
        DF5A7E5A 8E65572F 75932C8B AB8A7209 B97C789D 6E1F57D9
        13420061 DBD599FE 2B833E38 BF05F1F3 8F4CA333 10FE199E
        09D54F30 DF62E59D 5E0D52A6 266BB732 48BC8B43 C4A939B9
        D30333AD 99FEFEAB 378A2C67 2885076B 1A045A72 8C3DCE1F


counter is <12>
P-poss is
                        F56C2A7D 366E3EBD EAA1891F D2A0D099
        436438A6 73FED4D7 5F594959 CFFEBCA7 BE0FC72E 4FE67D91
        D801CBA0 693AC4ED 9E411B41 D19E2FD1 699C4390 AD27D94C
        69C0B143 F1DC8893 2CFE2310 C8864120 47BD9B1C 7A67F8A2
        59091326 27F51A0C 866877E6 72E55534 2BDF9355 347DBD43
        B47156B2 C20BAD9D 2B071BC2 FDCF9757 F75C168C 5D9FC431
        31BE162A 0756D1BD EC2CA0EB 0E3B018A 8B38D3EF 2487782A
        EB9FBF99 D8B30499 C55E4F61 E5C7DCEE 2A2BB55B D7F75FCD
        F00E48F2 E8356BDB 59D86114 028F67B8 E07B1277 44778AFF
        1CF1399A 4D679D92 FDE7D941 C5C85C5D 7BFF91BA 69F9489D
        531D1EBF A727CFDA 651390F8 021719FA 9F7216CE B177BD75


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

```
P is
                        F56C2A7D 366E3EBD EAA1891F D2A0D099
        436438A6 73FED4D7 5F594959 CFFEBCA7 BE0FC72E 4FE67D91
        D801CBA0 693AC4ED 9E411B41 D19E2FD1 699C4390 AD27D94C
        69C0B143 F1DC8893 2CFE2310 C8864120 47BD9B1C 7A67F8A2
        59091326 27F51A0C 866877E6 72E55534 2BDF9355 347DBD43
        B47156B2 C20BAD9D 2B071BC2 FDCF9757 F75C168C 5D9FC431
        31BE162A 0756D1BD EC2CA0EB 0E3B018A 8B38D3EF 2487782A
        EB9FBF99 D8B30499 C55E4F61 E5C7DCEE 2A2BB55B D7F75FCD
        F00E48F2 E8356BDB 59D86114 028F67B8 E07B1277 44778AFF
        1CF1399A 4D679D92 FDE7D941 C5C85C5D 7BFF91BA 69F9489D
        531D1EBF A727CFDA 651390F8 021719FA 9F7216CE B177BD75


Q is
                                            C24ED361 870B61E0
        D367F008 F99F8A1F 75525889 C89DB1B6 73C45AF5 867CB467


Seed is
                                            47830819 72865EA9
        5D43318A B2EAF9C6 1A2FC7BB F1B772A0 9017BDF5 A58F4FF0


counter is <12>

G is
                        8DC6CC81 4CAE4A1C 05A3E186 A6FE27EA
        BA8CDB13 3FDCE14A 963A92E8 09790CBA 096EAA26 140550C1
        29FA2B98 C16E8423 6AA33BF9 19CD6F58 7E048C52 666576DB
        6E925C6C BE9B9EC5 C16020F9 A44C9F1C 8F7A8E61 1C1F6EC2
        513EA6AA 0B8D0F72 FED73CA3 7DF240DB 57BBB274 31D61869
        7B9E771B 0B301D5D F0595542 5061A30D C6D33BB6 D2A32BD0
        A75A0A71 D2184F50 6372ABF8 4A56AEEE A8EB693B F29A6403
        45FA1298 A16E8542 1B2208D0 0068A5A4 2915F82C F0B858C8
        FA39D43D 704B6927 E0B2F916 304E86FB 6A1B487F 07D8139E
        428BB096 C6D67A76 EC0B8D4E F274B8A2 CF556D27 9AD267CC
        EF5AF477 AFED029F 485B5597 739F5D02 40F67C2D 948A6279


H is
                                                        0002


============================================================
```

```
Domain Parameter Validation
    P is
                          F56C2A7D 366E3EBD EAA1891F D2A0D099
        436438A6 73FED4D7 5F594959 CFFEBCA7 BE0FC72E 4FE67D91
        D801CBA0 693AC4ED 9E411B41 D19E2FD1 699C4390 AD27D94C
        69C0B143 F1DC8893 2CFE2310 C8864120 47BD9B1C 7A67F8A2
        59091326 27F51A0C 866877E6 72E55534 2BDF9355 347DBD43
        B47156B2 C20BAD9D 2B071BC2 FDCF9757 F75C168C 5D9FC431
        31BE162A 0756D1BD EC2CA0EB 0E3B018A 8B38D3EF 2487782A
        EB9FBF99 D8B30499 C55E4F61 E5C7DCEE 2A2BB55B D7F75FCD
        F00E48F2 E8356BDB 59D86114 028F67B8 E07B1277 44778AFF
        1CF1399A 4D679D92 FDE7D941 C5C85C5D 7BFF91BA 69F9489D
        531D1EBF A727CFDA 651390F8 021719FA 9F7216CE B177BD75


    Q is
                                            C24ED361 870B61E0
        D367F008 F99F8A1F 75525889 C89DB1B6 73C45AF5 867CB467


    domain_parameter_seed is
                                            47830819 72865EA9
        5D43318A B2EAF9C6 1A2FC7BB F1B772A0 9017BDF5 A58F4FF0


    counter = 12
    hashlen = 256

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

Qtest is
                                            C24ED361 870B61E0
        D367F008 F99F8A1F 75525889 C89DB1B6 73C45AF5 867CB467


Q-prime:
                                            C24ED361 870B61E0
        D367F008 F99F8A1F 75525889 C89DB1B6 73C45AF5 867CB467


i is <0>
Ptest is
                          E46D386A 8F65A4D9 928A2F87 C52E917C
        26346EF0 966D70E8 61ED94A9 F74BFC6A D35D5E9D A083C91C
        8E0FB7BF 337FA25A 828B3F60 5BB3AE95 5CED49F8 49524B87
        0A6403CB B1B8B2DA BA68AB29 611D7BFC 7A9CB4E1 D74A17A1
```

A73DC750 FCD42CCA E7BDA622 9A470AA4 B4A8C3AF 26DB24E5
01F87C5F 9556C92A D2E8D2CF E628DE0E 4887F778 48F9F173
B915B6ED 366FA29F 317C60B4 9C4192F7 1EA8719B 21376CD8
693B1AF9 57039CDC 6887F544 43DACB2C 9C6A9B20 BF74CB6E
26300B71 4226512E 6A669091 780EC658 1FD250AE 28710989
0A423A82 D4EB9E5F F80F6224 C9A8CD9D 0FC49896 AD91AA66
9A8829A6 198F3BB0 B32116DC 644F67B5 4AC18A1D A25A217B

i is <1>
Ptest is
F05D7CAA 10B69987 3EA51B8D 8C73B316
1B7F1F2F CAE5CA5F 39464575 CDB128B2 C301BE91 C95A02E0
A0AB1CC1 71B3BC16 DD63A1B9 ED266289 51E0BEEF AF16886B
525EA5F5 EAAB566D DB36B379 193DA14B B5052D0C C387FBD1
EE22FFAE 052F9262 0B77170D 6DEA84F0 CC14D572 3F2D7D47
6DBACD15 82F23DB9 3CC02434 7CAED83C 3E113FE7 6DC3900D
61D8183F 053366F8 FEEEBB89 4C5FF287 BF224B6D B91C978C
0AD37E4B C9539D14 E5F922A1 8334CE24 094E3FBF 86DFC447
FD52271E 2FB7078B E9636E7A E08D7097 032D0802 61F3EB62
7E7BE0AC A7155D8A 5A0CA204 3AF89745 7041D8FB C0963445
F3FF5F8A 658BC192 D8C849C4 26698DC8 BBE98F92 3CE27205

i is <2>
Ptest is
DB52970B D1BD220E 7585EBB7 97E07564
0B60CF50 895B0E36 D8145313 63FD6AD9 76E9DA43 B571B265
7FBA2F24 6424628B 01C5C371 E02BB00F C8FD3031 8ED6DC6F
B8DD1B06 FCF60A12 D6AA4D59 886CD557 16039F6F 074D2B80
18C8158E 72DB8E83 F57B4DCB 12181396 0EF14C9E 18E0813E
D87E4E20 C5D3222E BEB1D662 58187A30 FA9D6B77 273DFD83
8D74E89A F2371B9A 12A8C428 5775FF1F DC3F826D D0FFD12D
A7882A3C 8F82BC4A E6016537 04504DB0 86172020 F2FB343E
FD431C5A 25E819A8 3809504A A122B6DF B62F4CCD F632B38E
B83D975E A40C471B C4310CB9 2C2FB9F9 FBDCC2A2 492A5CCC
4850595D 316BF98A 4734F4B3 6623D62D C6B8A9EC B5DDEE03

i is <3>
Ptest is
EB2AD4CB F0F62EA9 E08FCB77 BED60FC9
71F3B92C 2AD02390 1164582F CA206C00 B81C1E8B 7D0F4FA3
77303CC0 3A1F9E84 9D1710E4 626108D9 46484AA0 50B8A484
F004A76C FC8BA059 525B4605 7906A050 9B85D71F F3386102
DBAADA98 6DE97AA7 EB06143B 0A6FF301 502C4177 838B4599

B98CCFA8 4CF07B85 201CD2AA 25952545 C29C31B9 32C790E6
F693B9D7 635EBB9B 646917E3 83389E39 5CC72059 0C3E4EC5
987BF2D0 4744814A 1A7B61F8 C73A7388 93D2420D B3ADE987
E80F8E76 7C4B84EC 9764C5F6 C5DCDBDD 32B8AB61 1E0D7783
A9B2D720 DC437A3E DD97857B 8F62D385 F3EDDFAD EFEBBD3D
FE2B0981 9F799184 443E2F48 A6AAD37C F17D69B8 ED0A457B

i is <4>
Ptest is
A8DA61F7 A1451157 CDBF46B8 3CDA35CA
0A50906B 2A111CC5 5356CD10 2E9FD84B 0568F146 DFADEC7E
2B55D103 77778E1B BEE3940E 2EFDE6A1 DB6239A6 52D172A1
18C8711C CB4054BC 6AB64991 84BC7B7A 59119A91 4045C1BC
0D40397A 66C9B2BE 588C0226 1F6A2720 2FA93A5A 004F0436
3EFF6721 69A47C57 2DE3DE13 B9A64C0C F9425FFF 0D77F088
4918A470 4653C5FF 97D129C7 3A3F0B84 AB50935D D7ED1F30
F901A66D 8CDDFF8A F8DF2B71 03ED42FF 0F6D815B 0073C4CC
3000B4CE E0BE3936 5303D315 742CA385 8E9248A1 83838F84
3BEEB03F 452B48B6 68EC46D6 2C656F97 E19E1741 B9C63BA4
7FD94613 502AC603 E011C20F 8D638FA1 5B092CBE F3227A55

i is <5>
Ptest is
B0C94960 1F57DD97 492DBDAE AE4C809E
4A69128A EBB039F6 DF61AEF9 AD2D587E 8FB8D468 6014A5F9
DA545245 40AE88E8 D1325F7D 5D1E64A2 D5AB1F38 3125CF75
BA1ADE75 3819A093 1DDA9407 9B348E4A 0E7FDC1B 821ECC29
7E139D7C 6D97FFA7 D201199D AD30CDE4 5788626E 5EB1C771
4AD8F5A4 0C38C1E9 2DF0DABF 7092DA84 A7C5A8D8 57AF1664
E90EB028 B57E498E A1DC8458 076A717D F18E4A04 FADD70D0
32FC2162 FEA05BA9 432508CC 7FC174A2 E94CA1B9 8A6BA8A1
DC8E8D6E FD88441D 7593A94D 160F89E5 7931ABD7 C2A259F9
77BE6FD4 00DB9AC2 055E016A F7B893C8 63A9EBFD CE1FD936
472FA896 20E0EB7A A426E47B 565AC9BE CFE17937 D953FE79

i is <6>
Ptest is
E6144A89 95A5B3BC 683F0824 67CD595B
93489B34 C97F1FD5 C873C1CC 4A52D85D 47B0C174 5B54C68B
F0B91734 17626970 71DCF62F 1FFEC6F9 A0A90A62 095E9446
C1E9FE05 F09A84AA 0CDCCEBA D2F09CF2 5C7ADC0E 084199AD
E60CCA87 F2B2AE6F DE47CE20 5FA908CF 05505EFC F6944FCE
98CDF1E3 9FF7920C E0C3FDEE 1B9C0C87 8A4932EC AC8A2B52

308B7044 2BC57BAE D1C1631D F2AEE986 C32DAD99 7744DC81
269C0923 4295A18F EAF7054E 9EF20FA0 630573AC 522AAB84
1924DA15 20E62773 365EAA09 9B177813 B21A582B 06B58EEF
0311934C 6797238E 674465AD 9BD3A580 5D887D1B 9BD6F8B2
67DD4A43 F8DAE9A5 D6B79949 A05A92B3 5B3205F2 08DE7A7F

i is <7>
Ptest is
BC91BA6C B5501C18 581ACBF4 4D49DCE2
4C3C54A8 7E57C780 318962C5 1E90CC25 0BFF08DD D40F3B1E
04AED147 5704D697 22176F68 A44BBFB1 359D76E1 A2D8B223
B907E03C 1E17A615 537FC9F0 1FA4ED9C 9AC890D7 F15B1726
4D9B630C 7BEDEBD0 2D865CAD 7DBDA106 CF106738 3ECAD42B
CB3DA297 B123A27E 18CB9C16 D0ECFC91 B4AFECEB 69FE5DC0
70E97A6F F5E26310 3E871AA1 CDFC0106 1C107E18 07AF8F8C
EB1F362A 4FBCEEA1 C50D7960 14189E59 597665ED 35BCFC9A
819D0A5F A4DFB9FE F20FC0C8 5B2DBCF0 4D74CA44 6C7133B5
CFEAE794 648FCE50 BBC9259D 00C2A529 9D6ABA07 DFE1E384
3A4FB389 F1E3EF8A 06AAF060 77BD6D06 511AA5D2 B8B6690F

i is <8>
Ptest is
A6B117EB EE793BBE 92D9433A DD39AE30
00574373 4596E5DC CA3F70A5 3E23F101 92C49D60 5A68B16A
F3D2CAF9 EA97603F AF6EE055 F0D29D81 DEDDFDBA 1934BE89
3DFD73CC 7D177E6D B00FF7F7 72FA22ED DF902F47 4B52BE9A
2A85352C 3F95E020 CA5A6A54 A0C67B26 0D874C02 C2DF5936
4886845A E9CED9F8 EFB098B7 F486C8DA C9B9B921 5389A7E5
800D21DF 889864C0 E85CD5B7 8D4FD7A8 B1FDB9A5 6658F5B2
F5CF5E83 5563C93A 8136F8D2 EBF3E505 22428791 28AAB667
3231B469 375D4547 78C0F5E3 3423EBE6 681D97B3 8882571C
8EE673D4 1E92178B DC1FDA8D B8BAC225 D33ED82C AEABC7C4
E8872379 335AFC9F 1636CB0C A209F2A0 35ADB246 218CA299

i is <9>
Ptest is
958809A4 A45295A2 E9917E4D 01DE35D7
B6E0A3C9 A9E3A8DC 9081B4C1 6BF60691 D992B189 C821B96B
C57B02B2 461BFC3B 0BADE772 D37D77EB 9F8D8D73 8B0983B9
DC0A9104 02B2BA7E B697DADA E6B1250F 3D8C4CD5 349AD82B
917EE697 83FED60D 2DEB005D 7F455A7A 91A29CCC 8744ECF1
82D62163 48F2922D BEF5FC72 F2E29D4F 6BFE337B CDE3DA4C
A9372759 253EF5CA 4F5A5DE1 E594D963 43511340 EDC99E66

BF3A6B6C 459217AA 12D0ED34 6AD28CF0 D1A1ABEB FEB2820F
DD4AC538 B018FC32 844FE4CC A35334E7 43A30F0C C951B004
07BC5679 62EE43D9 CA44C951 EAF8A020 87B0470D D26B5980
BC5F35CE 725FB926 03A7716E EF5B349F 8E38A13B 683A684D

i is <10>
Ptest is
BF54D59D ECB2CB0A B53C337D D34B5C2F
0B86D277 585E1178 E4A12E15 020BB2B7 3460DB7F 5821F787
99165841 BB643F2D 30BC4FD4 1AABCDCD BE374F85 832E7C0F
18866F16 9B407D42 83AA8411 435D197C 3432FBDD 8296A5C2
161853D1 4E254C8D BB9CF427 D4687D2E E8D5DBC0 F718E60B
587CA596 4B231C0C A8BC742F F54552CA C0B2B4B3 1D0ED4F1
C0D71C0B CBCA8B3D C741EBB9 3D622D14 00412A12 D55A8E94
E7EC616B 92981640 B7C67C14 509CAE0A B5F9725C BAEFF41D
6FBFDB7E 5BE068ED 0B32500F 53F371EE BB85B032 601F53BB
2A9FEACC 24377A54 5CEE88F1 6E018716 EC14F557 5D035D30
2DE55549 63A8FC88 6C7F82D5 253912FE 14E73EA8 A14573DB

i is <11>
Ptest is
C8A35411 13B512A2 609089A7 7F3CFA13
54F2E14F 681CF409 D1EA2B77 C06281AF CBBC2D7A E8BD756E
18E57608 250C437F A1E4BD9D 2CB8F4B0 2CBA9C29 E8EF0091
226FBB5F CFCFA305 3D3990DB B5797DA0 A22D2E68 660DD112
53A27603 EBA3B8BE 9CFD5C2A EFF025E8 DBB04A38 108E6B52
C47830EA 777A4E26 8CE05095 63C33D7D CE787022 6697AD06
AF8D3458 26BF9CC3 ACF7725A DF0F534A B6CE7192 B1DF4A5F
DF5A7E5A 8E65572F 75932C8B AB8A7209 B97C789D 6E1F57D9
13420061 DBD599FE 2B833E38 BF05F1F3 8F4CA333 10FE199E
09D54F30 DF62E59D 5E0D52A6 266BB732 48BC8B43 C4A939B9
D30333AD 99FEFEAB 378A2C67 2885076B 1A045A72 8C3DCE1F

i is <12>
Ptest is
F56C2A7D 366E3EBD EAA1891F D2A0D099
436438A6 73FED4D7 5F594959 CFFEBCA7 BE0FC72E 4FE67D91
D801CBA0 693AC4ED 9E411B41 D19E2FD1 699C4390 AD27D94C
69C0B143 F1DC8893 2CFE2310 C8864120 47BD9B1C 7A67F8A2
59091326 27F51A0C 866877E6 72E55534 2BDF9355 347DBD43
B47156B2 C20BAD9D 2B071BC2 FDCF9757 F75C168C 5D9FC431
31BE162A 0756D1BD EC2CA0EB 0E3B018A 8B38D3EF 2487782A
EB9FBF99 D8B30499 C55E4F61 E5C7DCEE 2A2BB55B D7F75FCD

```
        F00E48F2 E8356BDB 59D86114 028F67B8 E07B1277 44778AFF
        1CF1399A 4D679D92 FDE7D941 C5C85C5D 7BFF91BA 69F9489D
        531D1EBF A727CFDA 651390F8 021719FA 9F7216CE B177BD75


Ptest is probably prime
------------------------------------------------------------

Parameters are VALID


============================================================

Key Pair Generation

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

C is
                        786C42D4 667ED589 FEDB5206 99A4803C
        DE077E7A 3340D5F3 7AF625F3 E40239F8 A49F4EDE 9FA3683D


X is
                                           0CAF2EF5 47EC49C4
        F3A6FE6D F4223A17 4D01F2C1 15D49A6F 73437C29 A2A8458C


Y is
                        2828003D 7C747199 143C370F DD07A286
        1524514A CC57F63F 80C38C20 87C6B795 B62DE1C2 24BF8D1D
        1424E60C E3F5AE3F 76C754A2 464AF292 286D873A 7A30B7EA
        CBBC75AA FDE7191D 9157598C DB0B60E0 C5AA3F6E BE425500
        C611957D BF5ED354 90714A42 811FDCDE B19AF2AB 30BEADFF
        2907931C EE7F3B55 532CFFAE B371F84F 01347630 EB227A41
        9B1F3F55 8BC8A509 D64A765D 8987D493 B007C441 2C297CAF
        41566E26 FAEE4751 37EC781A 0DC088A2 6C8804A9 8C23140E
        7C936281 864B9957 1EE95C41 6AA38CEE BB41FDBF F1EB1D1D
        C97B63CE 13552576 27C8B0FD 840DDB20 ED35BE92 F08C49AE
        A5613957 D7E5C7A6 D5A5834B 4CB069E0 831753EC F65BA02B


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

============================================================

Per-Message Secret Number Generation
```

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

C is
                          786C42D4 667ED589 FEDB5206 99A4803C
        DE077E7A 3340D5F3 7AF625F3 E40239F8 A49F4EDE 9FA3683D


K is
                                            0CAF2EF5 47EC49C4
        F3A6FE6D F4223A17 4D01F2C1 15D49A6F 73437C29 A2A8458C


Kinv is
                                            2C42D852 886B0414
        DF7D7AF2 6E729CF8 2E7918F2 010CE876 FC5D0160 1381CCF4


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

===========================================================

Signature Generation

    hashlen = 256
    Msg is 616263

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

K is
                                            0CAF2EF5 47EC49C4
        F3A6FE6D F4223A17 4D01F2C1 15D49A6F 73437C29 A2A8458C


Kinv is
                                            2C42D852 886B0414
        DF7D7AF2 6E729CF8 2E7918F2 010CE876 FC5D0160 1381CCF4


R is
                                            315C875D CD4850E9
        48B8AC42 824E9483 A32D5BA5 ABE0681B 9B9448D4 44F2BE3C


Z = Hash(msg) is
                                            BA7816BF 8F01CFEA
```

```
        414140DE 5DAE2223 B00361A3 96177A9C B410FF61 F20015AD


S is
                                                  89718D12 E54A8D9E
        D066E4A5 5F7ED5A2 229CD23B 9A3CEE78 F83ED6AA 61F6BCB9


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

Signature:
  R is
                                                  315C875D CD4850E9
        48B8AC42 824E9483 A32D5BA5 ABE0681B 9B9448D4 44F2BE3C


  S is
                                                  89718D12 E54A8D9E
        D066E4A5 5F7ED5A2 229CD23B 9A3CEE78 F83ED6AA 61F6BCB9


============================================================

Signature Verification

    hashlen = 256
    Msg is 616263

    R is
                                                  315C875D CD4850E9
        48B8AC42 824E9483 A32D5BA5 ABE0681B 9B9448D4 44F2BE3C


    S is
                                                  89718D12 E54A8D9E
        D066E4A5 5F7ED5A2 229CD23B 9A3CEE78 F83ED6AA 61F6BCB9


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

W is
                                                  703DE1B5 4BAB6CFA
        F6CD5F4D 1EC4B00F 6E9835B3 A5458949 A0FFBBBB 155AD98A


Z = Hash(msg) is
```

```
                                          BA7816BF 8F01CFEA
        414140DE 5DAE2223 B00361A3 96177A9C B410FF61 F20015AD


U1 is
                                          524E6959 EF2DD879
        D9D398B7 5163244F 7F19F0FB 5DED07E9 6D6BF0D5 88B6F91F


U2 is
                                          5937AF40 AD7CAC85
        EEA247FB 3A38E126 285FAE37 0C971E99 262A840E 07DEE9C8


V1 is
                          489D9FAC 011AB08C 48760F38 DADEFFB0
        353FAC93 EEE39649 CB4D7FFA C47B05B7 B8BFDC7E 29272D38
        4727CCEC CDEF8D0D 444F980E E08246C0 74F9CFA3 6CC19750
        25C9244B 38FAD1E2 3CB28CF9 0350D8D7 D9249A83 12FBE888
        1142B640 C9FDB56B DD62B7E8 BC97579F B38E68C4 CD935C0D
        5A8A95A1 BD02D504 693A089F 1A69809E D0C8DB83 93A66AA2
        A545D3BE E0B831F2 BED601DE 51D851E1 7B33E71C 6F3D32E8
        B3192240 898B58B5 B9654DE3 9E4B6B95 2C073DFC 0F87E9A3
        93D0F272 1FA199E9 3B21D2E3 CDC22BF5 917A50C1 F62D374D
        3C3CF58D 40EDA7FA 9B1C8D7B 1805761C A90BBEEB B2C497D6
        2C231BA2 359C29CB C458D892 05303F9B 38A9AA7B 55BA1E86


V2 is
                          DC114F55 D14D25F1 36380812 423CD9A5
        1ED60A62 313B9276 67C49651 AE733EE8 7E1BDA00 0013EE93
        4100ECA6 7975AB1B 1B792413 7E341342 DA1E6658 BE1572DA
        9450A084 9AD6C3A3 F6232647 AC2DC667 8036F987 A13FD526
        E7F95158 78D3A3BB 02DC80F3 364794D7 98DEAD26 DE24CB4A
        BBD89D90 D779D8D4 0F3BBF39 08103F02 9D23AC7C 3104BA18
        739AFABD 032C614D B9DC6E30 430676A4 95BF9C52 E02F6F28
        0CD411E5 1A6669B7 70E6688C 696446F6 23EDB64B DA6AFAD2
        3F5606E6 F4D8A996 3E54A3EB 7E4E1FAB 8B81A7DD 0825DE4A
        DB2E696B BD9BE433 D091A862 AF9EA2BA A10713B7 3C6B69D1
        A4DA37E0 55099209 D05B5D99 364B47BA C736FB10 0B0792EA


V is
                                          315C875D CD4850E9
        48B8AC42 824E9483 A32D5BA5 ABE0681B 9B9448D4 44F2BE3C
```

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

Signature is verified
```

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

  Digital Signature Algorithm
    L = 3072
    N = 256

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

================================================================

Domain Parameter Generation
    L = 3072
    N = 256
    seedlen = 0
    hashlen = 256

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

domain_parameter_seed is
                                                193AFCA7 C1E77B3C
        1ECC618C 81322E47 B8B8B997 C9C83515 C59CC446 C2D9BD47


Q-poss is
                                                CFA0478A 54717B08
        CE64805B 76E5B142 49A77A48 38469DF7 F7DC987E FCCFB11D


Found Q:
                                                CFA0478A 54717B08
        CE64805B 76E5B142 49A77A48 38469DF7 F7DC987E FCCFB11D


counter is <0>
P-poss is
        FAE86624 F049677F 74A3A82A 47172382 C4DDD6A0 30235767
        9C01D515 5237D1F8 D5C44771 32AF0CD1 07EAA68D F3533CAE
        7AC63141 00891ADB D38C0DC2 E98F4845 B9B55A56 E6E6CB60
        B0746082 546FA2D5 E0A7B1FF 343E9064 A2CED218 48E3F867
        D36C6EC9 114E8979 53D55E97 DEC4F275 B561BF48 874E86B8
        BC3D6239 FD578E1C F70D4AD7 57167EC5 6E2DD1ED A625C275
        2703D15A DF792D7D DE945C74 F959287B 90A93D06 839E2746
        6BC99EC8 17F04701 7314EAB4 D29EEEE7 BBA3FFDD F81D2F41
        BCE7AEC8 59D41B90 83680B8B 391BD5BB 8B7A1FB6 7ECC9966
        A809C6E2 BF7FE740 64C4B2A1 F6FD2DF4 12108196 919A8466
        BBFA160F FD587D86 0A57F501 73F4573C D52601FD AAFDCCDA
```

4A46360E 17815B7E F99D5638 F3CA77FE 7FC29D00 DA7658A1
B6328992 7EB57130 F5A930B7 6EC7BAAB 763BFAE1 D2EF3117
BA3BFFA0 4CE5032F 903F0F73 79D7585B 61B18A08 1AE530CE
215430AD B405E898 FB56DE0E BCDEC916 78550CE8 FE8A50CB
61865E32 07D0E850 211E6FFC 7BFAC761 0B4AC5A8 03ED16E3

counter is <1>
P-poss is
9B61EDFD 3799EBE0 51174E5E 2046D800 C7A707F1 09B06DD6
EB36CC12 928B654E 1DCE4F9C E1F6C470 5053A481 C8E1319C
662A5CD7 3F95CF14 602573FF 8854AF34 8E59C1D8 AEC3A810
E850642F 5C86AC78 6AB2FA56 3E8AF968 2A80CF51 AF301B81
C8F78D7E DCE68E35 BF515864 F1D9D1CA 369F9955 BC0B7E1A
7C15A02E EA39A618 B6B8052B 101F2205 ACB1AF6F 7A027BC2
C6C32C6E 0487C903 167ED829 804E91D0 23CEF7E2 F588B0D5
CF56706D 25363DF8 7183B64A 601E7E2E E70942F7 53DB7095
E8E46E98 6B0B51AC E0FFEFBD B68E8257 048DAAD3 1551DD59
B0C40D8F 16794607 857EE499 5C2EEC4A 7F6D03E9 3B603766
F17D34C2 DE37CD0F 1D1A46EE AB7CE002 D2306FC1 3EEE644F
C2ACC33F 339D5D84 C3E6E3A8 648AB9F2 4EF802B5 5FD5026D
568C863B 7A686E08 DF6AEB8C CFEC7035 6A7B5DCF D5A0DE11
BD19F353 A7544B2D C17D8E2C 04EA6820 54B83323 72B35690
033BFC85 E0F0FB4C 941395B9 DC957688 7AA890B8 89B188A1
AF97A904 71C49163 68A548FB DEFD1BD2 3431850B 4E79739F

counter is <2>
P-poss is
8AA72CF0 AC9F4E00 78BFA1B6 6DBB247F 5FDA1E1B 8E4BD619
21A0EB04 6F618C27 3B2AA65A 23DFBEDB 0E4F5A69 CEFB5B52
8FA0D7FA A5A105A2 1999313A 0B931A56 51952197 2EF1BDDC
B8BAB1BB E9B43404 F2CD4787 13ED971E 2CFF6D4D DD4183E5
3039639A 1C204E61 1E3E74DC 9C63B901 30DF2D75 9AB4DBD6
1D8C2680 1BD13DB2 4212C62C 1F47EB9B A92116AB E1F4A60C
D1FFC047 7859EBEC F201023D 9109D48F F8A108BA D627B647
9E8B8E82 3FD20B5B 5F7E248D A1A71675 D0D33A4E 68C2320B
687BE02F 1163FAF2 034CBAF9 D1B8FBD7 E1EC221A C90A3000
14C6F448 801DF31F 6883166C 02C3CD53 73E1E6E2 10339A55
3CDED645 1A1CFD21 4BC09CA4 2C45EB99 01A8A447 AFC7B193
B3FBC14D 7E880B54 DAADB4B2 E3E9B624 68CAC5CE C29B4485
43B79FE9 8AADAE9C 29D02E92 77248018 A9F645A5 00F71376
A1EEBE4E 5F185BE1 DE441789 BAC8B598 399B9E47 DBCC551D
0905337B D9F4790F 95FC23CE C0174D5F B72883FB EA2D7FF3
9FFBD161 387F417C 6F907A37 7D6BAB01 5A9FE93F 2A391F0F

counter is <3>
P-poss is
	B493FCBF 54DC2074 AADFC9E5 5FD009C5 7FBEA7E1 83F6AFA3
	E663B24E 14866BF0 E4B17955 3868DAFC DB39FCA3 98B7BD45
	128AA32E E1BAC2E9 8D6CCFD4 23CD8BEF 1430758E FD841F80
	A7981854 967344A5 8E750788 A84B9B8F 337B2237 46B16618
	10440FB0 CC9BE03E 017FB4F3 69D4EF13 3E1BFA49 D75C7EC2
	C2E9BA64 8794E412 FA303A31 E37C8F11 EA9F5E7B 147DE0BE
	CA6B415C F3F1DCF1 0C3434AC 6A317BD5 248C930D 25E55798
	17E2DDCD E1F80FCC 18DD5A7A CEB11A76 8133BE33 66F48047
	C0FA44D4 C4D09286 948813E6 C85DF209 0C9039E8 D411676C
	0B69E1AD 3AF68E01 164F070B 296C8CCD 1FE2932E A9F93248
	2644283A A5D6D13A B60F9C38 A3DED7D3 2A8420C0 799E877E
	E99FAD0B E6806B6C 5FFAE61B 76FA5A24 53053FE1 E837ADFC
	018AD3D6 E7132E1B B4054E95 3117F727 9D6B8FAF 4A2D21AB
	D53C213C BB87DC74 E565FA33 D99889F9 21634A9B 8C13B51F
	2123289B E361AD53 8E465A1A 7D5AEDB6 A48BCED0 A68BC075
	20D74472 D197E558 9001C983 CB64EB1C A2C6B455 5A35B691

counter is <4>
P-poss is
	ACD260BC 6960F75B 83F0FEA9 81E12830 47443A74 E8C9CA44
	6232EB2F C00647BF 7CEB5BF8 E4C87B25 1E8975D6 961ED1F9
	50832BFD 6A961067 D8F54399 CD16B8B7 AF2A5CA3 E55D04F7
	178F9463 B6535185 E56A062F 1B8E33E4 D66FD49F 0E957BC6
	DAB4ACEA 855A4F50 AD3ECD2A 36BBC949 ABB7ED63 037AC8D4
	04DE7B59 75A629C9 125222BE F3BAD80C D243CD4C 7982ADA5
	4BE34897 B76E88A9 68FA1A3F 745EEE54 A534CF6B B5D2491E
	9477E402 C9231A2D C3ABC49B 6CEDF902 F2F1AD08 E3BBFB60
	7199F805 899EC861 71C0D2E1 6CC8BDEE EA9C1ADA B9A5A8B5
	DB9D48AC F574302B 15EFA9EC 5D9EB399 1076C7FC FB00F3C2
	CFDBC5E1 C478ADD5 39D3A726 A21F9ED3 D6BC9F62 86FAC55B
	D6CBA195 E4C6B466 A0CBB0B4 FF1432C6 0C2EB1F1 748C05F8
	87AC2952 48E71077 06C1405A 8E4E625D E2CFCADE F11B3A8D
	681EEFD4 1D566C66 7810A939 E8AF0112 CDCC18F7 23F7F4C5
	895181FE CFC0F128 9F207F3B D401D185 7314F470 ED1F7653
	73364B2F 1FE65193 8CD504CE D41BA99F 4427A06E 1C8D60D9

counter is <5>
P-poss is
	93572BFA ACBA114D 782E3C6F 807BD096 F13BB98F 9E5D4220
	92302F74 F646AE60 2B443B72 DC7360FD 502B88CD BDA92F30
	6363E8EA 9AEDAC7D 9E3785F3 82D486BD 3B58C930 92FCC483

47A7845F FF312653 C2F8A88A A464A45A 0160E859 3F224009
5A172C7D B1119F51 135AF365 7D89E1CC FA6CCFAF 28020E6F
393D4A3B 535609D9 73E9C9FD B8B814D6 9CB871F3 12AB7A0C
802A0D30 FAF10C4D 0D7A79F5 3C49D832 C0B5C053 A8C4A70B
64B99EEE 126909AC 6F775F8D 5520115E BDEEEB9C C1CDACEF
4CB7312E 2A08F4CC 5F9055E6 454A360F 34CBDE30 DBDF172D
C80262AC 8C70586E 6020F49D 5E1EFFAB 2CF8926C A579338A
E19D0E28 F44CD3E9 F47ED9DE 427E9E02 8CAF1EFB 6801DEF2
942342BE 354275AA E4B2980C 9C1C1102 F2734341 64EDCA15
7318C78A A85F384A 15ED227A AB1857A1 76B493A2 FA604CAC
16E197FC 36F66A7D 7019A2F9 FCE5990E 3D696660 35DE9F6B
F550D7FA 9F2AA1FB 7E88C1CF EF6AA0E4 105E1409 3A8E44E0
E97EE3D8 0BC2F082 93C4BB11 DE2EB3EA 16BD2FCA 81DAEC9B

counter is <6>
P-poss is
E3C27D66 3B0222CC F7675856 5377F848 C05629B8 5D61B74A
CC579F2B AB058935 232A2152 02554CAB A23BF0F5 DFFAE105
C571662A 833D17C3 7E2FB38C A935E579 49C77B49 BE70C6BC
7092F5CB E252AC1A 236841C0 71F93C97 126EB19D 6F7D25EE
ACDCDDF6 C5927138 9D158725 C999DD7A 5962889E DC520BE7
A1ACBF01 FDF897EA E92A300E 91971994 9B6247AE 6DE46751
B86B7D6C 29F13E93 9E425FB5 ED3D149D 298AE3F3 644CE56D
EC9D2E40 37B74100 78C35B84 58065B2E 0DF30EF2 3E0E33AF
7DFA1488 E1FE53EF A3BA0457 055909D3 7DB30784 EC0103C6
B3D5EB80 7E92091B 6A8A7610 530F9CC4 B0C85119 3D63B39F
D93B7B7D B8AFE4FD 98C3B662 B8D9237A 278451B8 0A44FE6C
C4CDE302 4CFD1FA1 A0CF4E2D 4C13C54B 7E9CE188 E7BA6A5C
8B6E202F E4DB7561 F713A806 53E9070A 23634319 CBB5834D
147C282D F4B786B6 9431EFBE CDAA6141 E02F6785 4E2A80AA
DA3B3BC4 59AC10BF 42785E24 B12BDF9F EC84A490 86548C75
ED82B01A AD353915 100B26A6 0B15749E BDFCB37B C7AB36EF

counter is <7>
P-poss is
946930B2 A57FF80E 21CA4DF9 A8BAA2B5 665CDF1C D921640F
41EAA714 649287BD 517A8101 658C5B1A 0DB1B63A C243F212
A10A4F40 2F01ED0C C85C0AAE E0A6875D CCCAFED8 5CE902F2
CD2F947E 296DD24F 55EF1421 71390D0D 93450D83 0806D365
CEFA5865 4F544E34 0DEEA2D5 9E71C4D6 F468B9BE 4878FCEC
F4A67BEF 63DFFC26 F64137AF B1CDAF68 C08481D3 03FA2D5C
DD2D5E5B B9EE9AD9 8BB19932 B1709A41 EEC0AC86 E7335393
42ACF5E3 C1AEEB8D 865DA91D 774A6D1B C70C57EE EFAFF0F3
3ED3127B 0BC32309 206E8470 AE8FEC19 DFEB3164 D5CC34F9

06094751 137226E3 FA3C59BC 6258D0FB 2BC59A4D 8DC834BA
5C54C39F 3B4624EA 0D1115DE 4BBAC3FC AA2FEE15 ED63B829
9752B211 354D26CC 5291CC58 E02F058F E0206DBE 4EC3B740
263CA745 1F4A3327 8E992EA3 C38C5EB9 AB46D04B A38BA6A6
FCA35519 9E817A93 46F572DB 8A344C1A 68074229 7343AFC9
3831C7C0 356769EC 53B45852 C1A25F84 32D70E2E 8DB94AAA
D7B068C3 B637DB70 7E540D03 D9CB8A45 CA71C5D2 6D8D52B3

counter is <8>
P-poss is
AE7B5322 41894E21 D741E54B 32AFFEF8 1E89178D CAAEC33E
630E74B3 211B92A8 E4CF9082 F7ADACB1 BAB41DE4 A41B5D87
EECFDF8D CEFE53F2 FE279D1D 287CE9A1 0B7C8BB9 E04EACE6
F4A03DB1 B5D123F8 69E72D97 6225B2DB 4BE4DF75 FE707135
0EE35373 C70449DC 79D02448 6BDB35D0 21552FA9 26A33DBB
39BD90FB 8E490C9C C1A621C5 EBE37C47 CB3F5951 1C42F657
A25CEC1C 17808A8A 373BAA88 5D068310 1E4E69AF 6CA2A813
2B3000E8 B338BAD8 DA59C9B9 6892CC57 45A54C39 4A6CE562
63059EC9 7BEF13F3 D7E2B6BA 009AFC8B A26B5ABB BEDAD818
3F9292D8 A7F81DC3 A57BB82D 7F148A89 F7B6B29E A6BA0A59
AEF0313B 3226354B E5DA60FD A5A68094 95BB070F 4048B928
B03858C8 A7A53ED1 0B5E7D35 721EA20E E85D79B6 4DE59F8B
E6F53D98 F246AD14 77960717 6B365E01 5AD43CB3 5427257B
07A5C767 76633EBA E76F6775 35AAA282 3795A7DE 875029F5
61370D41 720D8624 3834E70E BD87D9C0 6FCEE6B4 CAEB8346
2507ADCD 1079AE37 2993604F 2BC22CA9 BBBE0348 2EB22B07

counter is <9>
P-poss is
EDD290F6 29FE3F62 4A804F66 03A67AAD 093E36BA B38B8E2B
5EA4F424 1E4790D1 C93F99FA DE79723F 8D4A1048 9252B87A
5D3A3591 672D8C70 FEB4A482 3669D839 D934051B 13EBA0C0
00BBE9ED 7B558ECB 0BDE4248 1C1CB415 84C04180 EBF113DD
D070CA58 82816BD9 E9462A7B EA33BC30 AB5DB257 FA13DB12
BC7DF4CB 9C277A17 12E59B8B E80187DC D0A4E599 9F3A534B
A033B0D1 EDDF520E 27C98024 34434EFC 35C00A44 9F7BA936
2C240261 CA2100A9 48F4B632 F79A01A2 703FE0EE 99F673E3
352D5694 ABA85A45 4DFEE1F1 13F01D3C E3ACA647 EFCA9ECB
C8F47786 2E4A1A24 E6D62B25 4516F48E 634F2B26 DA68B62C
B024824C 84912BB8 E9673B71 A34955C9 B0EDD9DF 263694DC
E3A2E535 27669F46 CBB694A3 B42D790C BFE3C026 6216513D
ABA878E1 6DA72D53 16C8CF98 4135D736 06F1D087 E227BD42
43C0F0F9 F0E17D0F A18DC5CA 3D8ACEC7 1B0135D1 CCE3875A
D6FC3F06 45ABAB03 FE864720 1962F58A 01F177CE 4764B952

76B8FE34 80375DDA F8D0A01C CE38E2F1 6C5A1D15 96E94DBD

counter is <10>
P-poss is
E5017E69 2365A37D 59DB01E2 DA3D2A75 4E66BA53 DA3F51A6
24980991 19E2FD74 E8E085E3 390ABE2A B119B90A 6640EE96
C7F5B47B A54D8E68 4467CDFE D9A43430 5559B0CC ED8530FD
B4AA581E BE179E98 B25EDAD2 C5670BFD 41FA4AFC 686E7613
8985F3D8 E2EEB17C AB5DFF5E 970F9262 054D493B FBD5E379
A6D9847E 4F59F77E 8467A3BE 44D0B242 1555EE54 7D8F7F6A
B147BAFB D59FCA60 3C4ABB67 D59E30C6 2F9673E6 61EF60FD
F96FB3A0 5AE8CD8A 8EDB64EF 7A8C0323 EB0531FA 171CA82C
42C5AF10 D151EC62 4A1B2864 86E9C36E AC93EA01 3A30BDAC
EF9305A6 76C877B1 1D8067A0 A1D7F7F2 14E69083 334DD3EF
F0B2B8FA F31235DC 0AEBFAA9 41EF8771 5DC4849A FC23BD83
C5915740 A0E980BF 9F98BF7C 62E541BD 7B562CBD C4740196
E8D4BC32 B3A6F427 EABABA21 F212E13B 3C6A5D36 B26B98CB
56AF706C 12BCCE97 737F2F8B 44292F1A 9F03F836 C59E7A52
DB0020D1 5F2C1035 C32976EB 88269535 569E2780 0CD01DA3
F189FE93 305B3558 BB6E7F0F 9ECA2941 CCF1F422 617D62E9

counter is <11>
P-poss is
80A6DFDE EAFC13F4 9235C4AB 5A8421BA C5E0DC85 D4E213DD
256BD092 EF59A901 C7E1C7C4 C9BD4E9F D3096B18 733C6F42
2D913852 30567257 3B28C76A 8945DE17 2880EB41 A64AF29D
F2F85B9D CFBBA13C 8EEC5EA4 5D163502 537139F3 505F9D54
6E341DB0 917D0523 F94FF2F9 39D5E2D3 65A3112E B14DBF04
1B8A0D03 E2739A9D 709AFAF5 8CD94597 B4998ADC 8B451226
B001BCF0 A85FF570 92C5BE8A DD2ACD67 6CD9EA11 65BC8AAC
9D90A630 DFFD0BF5 6ECC1865 C9995D0C 7D6947A6 A1B6593F
15B20238 0B328975 FB17A626 A40AF916 C30DB156 57E8233F
4A5E6EF7 51921CA3 74D991A9 61CE2836 7A19EC14 0B1986BA
045692E8 866026AB 10565D13 B92A0781 3A3B32EC D0FC7973
10FC6FA0 72C90A32 DAFCDAD4 2289930D 568ACF58 FC6B1E26
D3B8ECF4 56FCAE24 9EFF52E6 5C41111B 86A27FBC 8A5C1044
F7C0EA60 0EA26DE2 1D3E6B9D E98D55C6 87047822 CF33F63E
B550847A 3E21414F 6E6970DC 98E1D1FC 034FC04D AF4D8596
87747EC0 9F00A1C2 57AC03C5 4A0A5B3C 7D3E5714 B0CDA453

counter is <12>
P-poss is
D7D0622D 3E8CD92C 338AB6EC 4A7F4BDF 5492EDB7 D27A7ADB

B4A1094B 57D07E15 30B3F231 84BB5975 7DCE9AE8 0ABFE36E
9CE72CF9 6A9C0B70 931F6CBA F0EB0C7A 798222C2 0259FF54
8E6698F8 B18BACB9 A46DC963 93DA6C31 5BC6EC0A A3117766
DA2FD54F EAA09194 0A272948 F796F4BA 79138019 3C85CD89
AE9542B6 63A29C8D 785F38DC 4B191201 67ADF60E 45D58790
818B819E FA754CFE 449FD6EF F3202BEF 5BB086FE 23E59C06
E7B2242B B6609E0E D233D2F9 97B9DAB5 1ECF8EE3 938D9201
9A30B6A7 DC5AF615 C4425DDF CE6453AE FCDF4532 EEA1AF2C
B3D1D18E 952FB9FE 97184B49 658395E5 10A3B6F3 BD455940
88EA1390 2DA98F55 1EB2A8E9 21429CDE 03F6079F 4152C21A
EC98C041 E1E95EBD 7E30D7AD B5A2F274 A097B318 410F7D82
6D068B13 3A242149 9CCF24B0 C1E4655E 35F987D4 D62E4055
9B9F69D0 D726228A 50885D71 6F452114 AA3EFC7F E8BFB375
8954C38E FB7B0655 833ABFDE CBA1ECA7 3DC0E23E A32C8C5D
45ECA296 362E09CB 1AF51730 70DF6B97 27303417 06F9BAFB

counter is <13>
P-poss is
E5821965 6BA316E9 2EBE5F38 3C01742D 139399DF 199D5542
7A53897C 1ABE0847 370E02E7 AA63B64C D34030E5 F2D3A92E
09B872AD 8D4CB288 68C49B23 44F5927C AE608459 95022207
EF454E3B 915AD405 2E49B356 7E562A4E 72DE9CE4 4B938A2F
1ACFBB43 350062C1 A56626B7 FB346A6B C9DA4362 C7BDC1C0
CC7AFC35 185899BE 9E379059 33F911B6 29699F30 A25465D4
2198F9BF 88CC1F12 64A0252E 2A24CD9F BD7AA5A0 D41C357C
120A3062 553CF62D B773BEF9 DD1233B4 51906D6F 19EF82B7
8D5B2DD3 A2FC908F E52CEAD8 F957FE68 32611C33 665AE111
7C59253F 40140E77 B420D0B1 71EF8757 BDA1E835 79129E82
8DD4750D A3EE3547 D9D97C14 AADE4831 D8E8FDC4 9E1F4B57
B03EF191 588E875A 1FDC9A20 5088A739 CBA03432 00D76B6F
77748D8F BC4835BA 1FF4F593 AF4D4E38 40507710 728F6AF6
02208B8C 64BB29C5 D0B83B01 36A19847 C703C679 F6105CED
04ECC034 23E09852 9A8EEBBF F5806C98 D8B739AD 6C586267
36AB3C6A ABEF6438 F35FB4A4 BFD7080A 698A4556 A4D4B007

counter is <14>
P-poss is
F42A2499 E759967E 8567BAA3 6E129CAF 1BB645AF D2F6F783
4D70D329 E3C11EFB 99CFD23B 4A2074BB 15D418BE 8D3D5455
A707EA58 13C7A6B2 9E976DB8 10749C13 6058639E 4C5CDD70
7A2DA522 1C279DA3 24B1330E 8EB7FF7A F86599D3 5C935153
3DEEC55F 1966C0DA D18C8900 FDE7ADE9 C2198165 EE4AE016
5A7A1652 BE161570 13698E14 2F0C5B82 3A63E642 09D4B699
0B67D147 FFF12F45 FC63A729 4052B95D 589BB768 692D34C4

6BC3F53F 654FAB44 F94FD719 C4E126A2 4CD937B3 5199A118
D934090A 34332AE7 50CBB30C 72302C31 5F3EB334 606E01AE
7F1BAC85 484B6A32 F11FC1F8 ED16C307 D7810A32 0CA9159D
3F5551DB CF518EF4 527F4CF0 43EC949E 55C377F2 3F6B21EA
F569EF96 DD1B8D33 978856DC BE8D9759 7D3FCD81 B8DB5F35
24F498D7 1E2FE609 77886CE7 CACF6D51 5A3ABBD2 318220FE
72281232 4057E9AE 17ECA34B 0D54F5CD 738112F4 17A0D078
B359757C C8B8D1D5 281DC515 C4B7197B 36C0A14C 682C0C54
D387DFB2 946F5539 5EDA2AF3 69A9C01B FF1A7EE5 06EF37F1

counter is <15>
P-poss is
B33C3A30 A945012D 1EC49256 6CB862BE A2FC0A0C E92551C8
AD87058C 0C48F8DA 9083223B 08AEDF18 0AB46E7B 20ADEF02
C2037DAF 85483F51 4AA5FE35 14F45783 DBBD29F7 8E949C6A
14E4DD3A C21F006D 7FA2A698 3DBC5D8F 4FD4B2CF ECBCF3AD
51B9ADBE 88A0089D B5ECA1C4 43AC2CF8 91322ABA 0038DFB4
E8B8B96F 21CC0669 F90AA76C 524BB61C E5409009 707F02DF
A4C8D1FF F095F5D3 8B61060E 318CEA65 3A4EE63D 9B42C81C
A74E6F80 9CB44C06 BA9DD7E4 25FBFC24 B062CD7A 5E11593F
77147A1E 27A484BF 28A5A943 F10406F2 0D6B4128 235E1A52
51D41982 2641DC9F DEAFD2B8 D5602E6E 71E58191 E6C39E7D
E8C50476 1E5F99D2 6E32A9AC 8E623822 EF2DA15C D812502C
F036215F 316FDC7F 1F9F562A 44A2D344 3FA012B8 A6DC3649
A0EE6708 A11595C4 3943B535 4C52681C B99F5B62 FBD4E3F8
4540DFBC 6B4B658B EF7EF985 FCDF0607 12548E31 DCAC6B7C
A0872375 8CABFEF2 93D78374 79CE5D75 1FA76711 62834BF8
4A616E66 67F713DF 68ED6B50 BE442B3A 4DF24C45 1172DBC7

counter is <16>
P-poss is
CD43E22A 8CB85350 4668F95E EF9ACA30 2BEB6835 8A8544D8
881593AC EA0B28AE 117D4DD9 0A261D46 43888126 E15BD244
BD85FD00 6014B53D 415E8AF9 3388231A 161AEC4E 23CB4F9E
09D9A72E C84A90CF F59CB45E 17154523 B44423C0 AAEE9AA3
F3C2F0CE 963AB483 99E588B0 677BA217 DC350B60 49BB325A
E9BE0559 56C89B6A DC287641 EF3A9621 E17F3D6A 555BE901
029387F6 62C4B3E7 300098AF 9012C627 DC6324FA DBE64062
07D286CC C306257A A1F69304 4CFADE50 E47A2648 EEBD0962
5C68A7B2 9B0AEA7F 8B7965A0 15C34F0E 65293018 43C97CF2
EC7765EC 7A5E98F0 AA24689D BC4E45CF 3D88E316 4DB6118D
DCA1B9E8 8D7EB607 CA44A35B 2468EFCC 9674CF3B 7FD1ADD3
097FC243 7B23F611 920C52AF EB1586E8 AF0225DC 1256F6E7
5167DC35 C397A699 B47313F4 B766E10F CEE76061 7EB4AE45

```
        100D5A33 71584907 D4302636 D32B9CCC 5DC4DFC7 4E7B01B0
        4808BBBC C2712F89 DF86B40B 13D2F7D2 E910C611 F0EC2D32
        52098AF9 394E4DB5 C61528F9 6FB1F7E1 F74716F2 5B32EF81


counter is <17>
P-poss is
        CB971CF0 2E727719 593E9B86 4C5A196E 5B0438B3 F3D97824
        E67B6437 67561C84 DFAE8F36 4DF3E47E F7B26D10 00B28940
        7BB95ADB 6F5ADECD 7AB3607F CBE547D0 98F271FE 5066D82F
        01CC2B1F 8DF7EEB4 3B6A3A15 456D5055 AAF20F6F 8814615C
        3A694450 13B6A14A A8E324DE 8FA4754C 08E3D6F0 EC962967
        AFCC3CCE 509E7E82 C0F49061 A42485EE D65AA639 DA1841E8
        5816D9AA 9B305FFF 02FB6C2B AF741471 AB7F49B6 B9C04FB7
        D8D9D7CB 0C59BF68 4B78CAB8 D7329E35 184FD28D 770AC51D
        336DA5D7 EBA3FA18 838EBE10 8E21C9E4 94A36DBE 4472A4F2
        ED843084 0DB297BC E1937722 613A9C4A A40E4DAF D2B0CF3E
        DA9CBA9E 0845E054 58A4B5A1 4762B94D A524D1F6 8C8285C2
        FC5D084D 78C2461A 26422E9D C3923E0D 76C61B94 C750F5C2
        4EACD0B7 ED5333F1 A37A1FE2 8B408830 3078792B AB2E778A
        278D961F E19AB3C8 6B11F052 7251EA85 E6170D8C 3A52C4FD
        315A1B44 2BA1B894 33EFBA77 7E3E8F5C 708AC0E7 D272FDA4
        AD3FA896 5FAB84AA 115D08A6 C46C358E 5555DCA4 18BAFEFB


counter is <18>
P-poss is
        B48DB99E 290ED791 29B6B89D EAB9D8AA C3B770D9 46E94E78
        100F9054 183D1159 1B053AE5 57C5A539 33FC8B0B 342EAF38
        BDA1324B 42BC7ED8 0E3F8545 D7510925 8D69B28B 2F564CDE
        4FB44328 32B2DC68 306D87F0 B3D448AD 4F4E7C65 B761CB10
        6B683D58 8261A56E E9ECE592 8B71BD4A 955EE11C CBEF2343
        EE2A0432 133FAED1 E7AFFC87 5FCC3DC1 1FC7F50D 57FA511A
        9D43C670 C7DC6140 9DB03D32 D1516404 73AE5026 1D39C747
        2D12D498 876BEC92 C82C1587 0C6FD482 7562936F A28B1FA6
        9D53ABC4 9F2A11B6 E7C71B7F 77A92E8C 17531354 54AF6936
        8C7B99D4 8D45B9B3 F55C90F0 6CD38ECC 33B6521A A2DB124A
        C04269C2 AF59180F AD67CACD 5362A2A9 BDA21208 56A83460
        161375E4 8C6A2F28 5BB89A09 2F01575D 578AAAF0 F38BE534
        4696085A 2944FE90 AD0100CE 2357796C 6A7834E5 26906566
        AA48A22A 29AB9551 6CF549D0 1E0C9961 A0BD4F92 59A8144B
        2E1343F3 8061F357 31129C44 18A01093 287621B3 CAC2B087
        38CAB217 6F278884 497CF060 62B65F54 F2F5222F CAAB1C25


counter is <19>
```

```
P-poss is
        84BCDAC2 B91A48BA FD4F1386 85E50E8B 58F01314 A1F0BFD5
        D3CA4A51 844A996C F8AA80B6 C047DE7C D44472E9 8C1AD995
        0BB1BC05 3A28908B EB929361 5F4809BB 3100C794 3D859FFF
        CF15B0FE 270D6024 97BD288B 83846C93 91ED6C22 226AE8EA
        D83C060B B67A5B1A 3020C065 37C7BA82 167E5653 877D1023
        D1A28207 9B287738 4E4DE268 5AEDE86A DFDA3CCF 4C92907A
        41D1D5B8 88EC184C 99008501 C3DC8FFF D380B50E 64C2E945
        3ED83F16 32CAAE3C B9E0039F 63AC9260 0545684C 559AAB1F
        5C6863FA 91C01640 F33FD137 15227D4B 2CCDAC17 DCC50242
        F9DDBA39 297FD7ED 053D6976 109A18C5 182991E2 01889C5E
        E25205F2 3535D163 3C75065E AA0D3719 7D6FAE05 07DF91D0
        D8D5C9E7 50A08F3C 82A39695 B7E080CF 241DC332 CFB0334B
        49B3AE64 E8656B47 8FB60296 C5D57D0B 59B94CB2 B05EE82D
        170910CA 8DD37586 F4D0078A 92FB8279 77241B8C 6FC3B7BB
        3DD79F9D 2DA2B341 D92C41A6 6EA2D242 F009488C 079DCE84
        DFAAE0D9 FDF6710D 768F4AA7 1F30FAC0 F8C70C89 1355B8A3


counter is <20>
P-poss is
        90066455 B5CFC38F 9CAA4A48 B4281F29 2C260FEE F01FD610
        37E56258 A7795A1C 7AD46076 982CE6BB 956936C6 AB4DCFE0
        5E678458 6940CA54 4B9B2140 E1EB523F 009D20A7 E7880E4E
        5BFA690F 1B9004A2 7811CD99 04AF7042 0EEFD6EA 11EF7DA1
        29F58835 FF56B89F AA637BC9 AC2EFAAB 90340222 9F491D8D
        3485261C D068699B 6BA58A1D DBBEF6DB 51E8FE34 E8A78E54
        2D7BA351 C21EA8D8 F1D29F5D 5D159394 87E27F44 16B0CA63
        2C59EFD1 B1EB6651 1A5A0FBF 615B766C 5862D0BD 8A3FE7A0
        E0DA0FB2 FE1FCB19 E8F9996A 8EA0FCCD E5381752 38FC8B0E
        E6F29AF7 F642773E BE8CD540 2415A014 51A84047 6B2FCEB0
        E388D30D 4B376C37 FE401C2A 2C2F941D AD179C54 0C1C8CE0
        30D460C4 D983BE9A B0B20F69 144C1AE1 3F9383EA 1C08504F
        B0BF3215 03EFE434 88310DD8 DC77EC5B 8349B8BF E97C2C56
        0EA878DE 87C11E3D 597F1FEA 742D73EE C7F37BE4 3949EF1A
        0D15C3F3 E3FC0A83 35617055 AC91328E C22B50FC 15B941D3
        D1624CD8 8BC25F3E 941FDDC6 20068958 1BFEC416 B4B2CB73


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

P is
        90066455 B5CFC38F 9CAA4A48 B4281F29 2C260FEE F01FD610
        37E56258 A7795A1C 7AD46076 982CE6BB 956936C6 AB4DCFE0
        5E678458 6940CA54 4B9B2140 E1EB523F 009D20A7 E7880E4E
        5BFA690F 1B9004A2 7811CD99 04AF7042 0EEFD6EA 11EF7DA1
```

29F58835 FF56B89F AA637BC9 AC2EFAAB 90340222 9F491D8D
3485261C D068699B 6BA58A1D DBBEF6DB 51E8FE34 E8A78E54
2D7BA351 C21EA8D8 F1D29F5D 5D159394 87E27F44 16B0CA63
2C59EFD1 B1EB6651 1A5A0FBF 615B766C 5862D0BD 8A3FE7A0
E0DA0FB2 FE1FCB19 E8F9996A 8EA0FCCD E5381752 38FC8B0E
E6F29AF7 F642773E BE8CD540 2415A014 51A84047 6B2FCEB0
E388D30D 4B376C37 FE401C2A 2C2F941D AD179C54 0C1C8CE0
30D460C4 D983BE9A B0B20F69 144C1AE1 3F9383EA 1C08504F
B0BF3215 03EFE434 88310DD8 DC77EC5B 8349B8BF E97C2C56
0EA878DE 87C11E3D 597F1FEA 742D73EE C7F37BE4 3949EF1A
0D15C3F3 E3FC0A83 35617055 AC91328E C22B50FC 15B941D3
D1624CD8 8BC25F3E 941FDDC6 20068958 1BFEC416 B4B2CB73

Q is

CFA0478A 54717B08
CE64805B 76E5B142 49A77A48 38469DF7 F7DC987E FCCFB11D

Seed is

193AFCA7 C1E77B3C
1ECC618C 81322E47 B8B8B997 C9C83515 C59CC446 C2D9BD47

counter is <20>

G is

5E5CBA99 2E0A680D 885EB903 AEA78E4A 45A46910 3D448EDE
3B7ACCC5 4D521E37 F84A4BDD 5B06B097 0CC2D2BB B715F7B8
2846F9A0 C393914C 792E6A92 3E2117AB 805276A9 75AADB52
61D91673 EA9AAFFE ECBFA618 3DFCB5D3 B7332AA1 9275AFA1
F8EC0B60 FB6F66CC 23AE4870 791D5982 AAD1AA94 85FD8F4A
60126FEB 2CF05DB8 A7F0F09B 3397F393 7F2E90B9 E5B9C9B6
EFEF642B C48351C4 6FB171B9 BFA9EF17 A961CE96 C7E7A7CC
3D3D03DF AD1078BA 21DA4251 98F07D24 81622BCE 45969D9C
4D6063D7 2AB7A0F0 8B2F49A7 CC6AF335 E08C4720 E31476B6
7299E231 F8BD90B3 9AC3AE3B E0C6B6CA CEF8289A 2E2873D5
8E51E029 CAFBD55E 6841489A B66B5B4B 9BA6E2F7 84660896
AFF387D9 2844CCB8 B6947549 6DE19DA2 E58259B0 90489AC8
E62363CD F82CFD8E F2A427AB CD65750B 506F56DD E3B98856
7A88126B 914D7828 E2B63A6D 7ED0747E C59E0E0A 23CE7D8A
74C1D2C2 A7AFB6A2 9799620F 00E11C33 787F7DED 3B30E1A2
2D09F1FB DA1ABBBF BF25CAE0 5A13F812 E34563F9 9410E73B

H is

```
============================================================

Domain Parameter Validation
    P is
        90066455 B5CFC38F 9CAA4A48 B4281F29 2C260FEE F01FD610
        37E56258 A7795A1C 7AD46076 982CE6BB 956936C6 AB4DCFE0
        5E678458 6940CA54 4B9B2140 E1EB523F 009D20A7 E7880E4E
        5BFA690F 1B9004A2 7811CD99 04AF7042 0EEFD6EA 11EF7DA1
        29F58835 FF56B89F AA637BC9 AC2EFAAB 90340222 9F491D8D
        3485261C D068699B 6BA58A1D DBBEF6DB 51E8FE34 E8A78E54
        2D7BA351 C21EA8D8 F1D29F5D 5D159394 87E27F44 16B0CA63
        2C59EFD1 B1EB6651 1A5A0FBF 615B766C 5862D0BD 8A3FE7A0
        E0DA0FB2 FE1FCB19 E8F9996A 8EA0FCCD E5381752 38FC8B0E
        E6F29AF7 F642773E BE8CD540 2415A014 51A84047 6B2FCEB0
        E388D30D 4B376C37 FE401C2A 2C2F941D AD179C54 0C1C8CE0
        30D460C4 D983BE9A B0B20F69 144C1AE1 3F9383EA 1C08504F
        B0BF3215 03EFE434 88310DD8 DC77EC5B 8349B8BF E97C2C56
        0EA878DE 87C11E3D 597F1FEA 742D73EE C7F37BE4 3949EF1A
        0D15C3F3 E3FC0A83 35617055 AC91328E C22B50FC 15B941D3
        D1624CD8 8BC25F3E 941FDDC6 20068958 1BFEC416 B4B2CB73


    Q is
                                              CFA0478A 54717B08
        CE64805B 76E5B142 49A77A48 38469DF7 F7DC987E FCCFB11D


    domain_parameter_seed is
                                              193AFCA7 C1E77B3C
        1ECC618C 81322E47 B8B8B997 C9C83515 C59CC446 C2D9BD47


    counter = 20
    hashlen = 256

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

Qtest is
                                              CFA0478A 54717B08
        CE64805B 76E5B142 49A77A48 38469DF7 F7DC987E FCCFB11D


Q-prime:
```

```
                                                CFA0478A 54717B08
        CE64805B 76E5B142 49A77A48 38469DF7 F7DC987E FCCFB11D


i is <0>
Ptest is
        FAE86624 F049677F 74A3A82A 47172382 C4DDD6A0 30235767
        9C01D515 5237D1F8 D5C44771 32AF0CD1 07EAA68D F3533CAE
        7AC63141 00891ADB D38C0DC2 E98F4845 B9B55A56 E6E6CB60
        B0746082 546FA2D5 E0A7B1FF 343E9064 A2CED218 48E3F867
        D36C6EC9 114E8979 53D55E97 DEC4F275 B561BF48 874E86B8
        BC3D6239 FD578E1C F70D4AD7 57167EC5 6E2DD1ED A625C275
        2703D15A DF792D7D DE945C74 F959287B 90A93D06 839E2746
        6BC99EC8 17F04701 7314EAB4 D29EEEE7 BBA3FFDD F81D2F41
        BCE7AEC8 59D41B90 83680B8B 391BD5BB 8B7A1FB6 7ECC9966
        A809C6E2 BF7FE740 64C4B2A1 F6FD2DF4 12108196 919A8466
        BBFA160F FD587D86 0A57F501 73F4573C D52601FD AAFDCCDA
        4A46360E 17815B7E F99D5638 F3CA77FE 7FC29D00 DA7658A1
        B6328992 7EB57130 F5A930B7 6EC7BAAB 763BFAE1 D2EF3117
        BA3BFFA0 4CE5032F 903F0F73 79D7585B 61B18A08 1AE530CE
        215430AD B405E898 FB56DE0E BCDEC916 78550CE8 FE8A50CB
        61865E32 07D0E850 211E6FFC 7BFAC761 0B4AC5A8 03ED16E3


i is <1>
Ptest is
        9B61EDFD 3799EBE0 51174E5E 2046D800 C7A707F1 09B06DD6
        EB36CC12 928B654E 1DCE4F9C E1F6C470 5053A481 C8E1319C
        662A5CD7 3F95CF14 602573FF 8854AF34 8E59C1D8 AEC3A810
        E850642F 5C86AC78 6AB2FA56 3E8AF968 2A80CF51 AF301B81
        C8F78D7E DCE68E35 BF515864 F1D9D1CA 369F9955 BC0B7E1A
        7C15A02E EA39A618 B6B8052B 101F2205 ACB1AF6F 7A027BC2
        C6C32C6E 0487C903 167ED829 804E91D0 23CEF7E2 F588B0D5
        CF56706D 25363DF8 7183B64A 601E7E2E E70942F7 53DB7095
        E8E46E98 6B0B51AC E0FFEFBD B68E8257 048DAAD3 1551DD59
        B0C40D8F 16794607 857EE499 5C2EEC4A 7F6D03E9 3B603766
        F17D34C2 DE37CD0F 1D1A46EE AB7CE002 D2306FC1 3EEE644F
        C2ACC33F 339D5D84 C3E6E3A8 648AB9F2 4EF802B5 5FD5026D
        568C863B 7A686E08 DF6AEB8C CFEC7035 6A7B5DCF D5A0DE11
        BD19F353 A7544B2D C17D8E2C 04EA6820 54B83323 72B35690
        033BFC85 E0F0FB4C 941395B9 DC957688 7AA890B8 89B188A1
        AF97A904 71C49163 68A548FB DEFD1BD2 3431850B 4E79739F


i is <2>
Ptest is
```

```
        8AA72CF0 AC9F4E00 78BFA1B6 6DBB247F 5FDA1E1B 8E4BD619
        21A0EB04 6F618C27 3B2AA65A 23DFBEDB 0E4F5A69 CEFB5B52
        8FA0D7FA A5A105A2 1999313A 0B931A56 51952197 2EF1BDDC
        B8BAB1BB E9B43404 F2CD4787 13ED971E 2CFF6D4D DD4183E5
        3039639A 1C204E61 1E3E74DC 9C63B901 30DF2D75 9AB4DBD6
        1D8C2680 1BD13DB2 4212C62C 1F47EB9B A92116AB E1F4A60C
        D1FFC047 7859EBEC F201023D 9109D48F F8A108BA D627B647
        9E8B8E82 3FD20B5B 5F7E248D A1A71675 D0D33A4E 68C2320B
        687BE02F 1163FAF2 034CBAF9 D1B8FBD7 E1EC221A C90A3000
        14C6F448 801DF31F 6883166C 02C3CD53 73E1E6E2 10339A55
        3CDED645 1A1CFD21 4BC09CA4 2C45EB99 01A8A447 AFC7B193
        B3FBC14D 7E880B54 DAADB4B2 E3E9B624 68CAC5CE C29B4485
        43B79FE9 8AADAE9C 29D02E92 77248018 A9F645A5 00F71376
        A1EEBE4E 5F185BE1 DE441789 BAC8B598 399B9E47 DBCC551D
        0905337B D9F4790F 95FC23CE C0174D5F B72883FB EA2D7FF3
        9FFBD161 387F417C 6F907A37 7D6BAB01 5A9FE93F 2A391F0F


i is <3>
Ptest is
        B493FCBF 54DC2074 AADFC9E5 5FD009C5 7FBEA7E1 83F6AFA3
        E663B24E 14866BF0 E4B17955 3868DAFC DB39FCA3 98B7BD45
        128AA32E E1BAC2E9 8D6CCFD4 23CD8BEF 1430758E FD841F80
        A7981854 967344A5 8E750788 A84B9B8F 337B2237 46B16618
        10440FB0 CC9BE03E 017FB4F3 69D4EF13 3E1BFA49 D75C7EC2
        C2E9BA64 8794E412 FA303A31 E37C8F11 EA9F5E7B 147DE0BE
        CA6B415C F3F1DCF1 0C3434AC 6A317BD5 248C930D 25E55798
        17E2DDCD E1F80FCC 18DD5A7A CEB11A76 8133BE33 66F48047
        C0FA44D4 C4D09286 948813E6 C85DF209 0C9039E8 D411676C
        0B69E1AD 3AF68E01 164F070B 296C8CCD 1FE2932E A9F93248
        2644283A A5D6D13A B60F9C38 A3DED7D3 2A8420C0 799E877E
        E99FAD0B E6806B6C 5FFAE61B 76FA5A24 53053FE1 E837ADFC
        018AD3D6 E7132E1B B4054E95 3117F727 9D6B8FAF 4A2D21AB
        D53C213C BB87DC74 E565FA33 D99889F9 21634A9B 8C13B51F
        2123289B E361AD53 8E465A1A 7D5AEDB6 A48BCED0 A68BC075
        20D74472 D197E558 9001C983 CB64EB1C A2C6B455 5A35B691


i is <4>
Ptest is
        ACD260BC 6960F75B 83F0FEA9 81E12830 47443A74 E8C9CA44
        6232EB2F C00647BF 7CEB5BF8 E4C87B25 1E8975D6 961ED1F9
        50832BFD 6A961067 D8F54399 CD16B8B7 AF2A5CA3 E55D04F7
        178F9463 B6535185 E56A062F 1B8E33E4 D66FD49F 0E957BC6
        DAB4ACEA 855A4F50 AD3ECD2A 36BBC949 ABB7ED63 037AC8D4
        04DE7B59 75A629C9 125222BE F3BAD80C D243CD4C 7982ADA5
```

4BE34897 B76E88A9 68FA1A3F 745EEE54 A534CF6B B5D2491E
9477E402 C9231A2D C3ABC49B 6CEDF902 F2F1AD08 E3BBFB60
7199F805 899EC861 71C0D2E1 6CC8BDEE EA9C1ADA B9A5A8B5
DB9D48AC F574302B 15EFA9EC 5D9EB399 1076C7FC FB00F3C2
CFDBC5E1 C478ADD5 39D3A726 A21F9ED3 D6BC9F62 86FAC55B
D6CBA195 E4C6B466 A0CBB0B4 FF1432C6 0C2EB1F1 748C05F8
87AC2952 48E71077 06C1405A 8E4E625D E2CFCADE F11B3A8D
681EEFD4 1D566C66 7810A939 E8AF0112 CDCC18F7 23F7F4C5
895181FE CFC0F128 9F207F3B D401D185 7314F470 ED1F7653
73364B2F 1FE65193 8CD504CE D41BA99F 4427A06E 1C8D60D9

i is <5>
Ptest is
93572BFA ACBA114D 782E3C6F 807BD096 F13BB98F 9E5D4220
92302F74 F646AE60 2B443B72 DC7360FD 502B88CD BDA92F30
6363E8EA 9AEDAC7D 9E3785F3 82D486BD 3B58C930 92FCC483
47A7845F FF312653 C2F8A88A A464A45A 0160E859 3F224009
5A172C7D B1119F51 135AF365 7D89E1CC FA6CCFAF 28020E6F
393D4A3B 535609D9 73E9C9FD B8B814D6 9CB871F3 12AB7A0C
802A0D30 FAF10C4D 0D7A79F5 3C49D832 C0B5C053 A8C4A70B
64B99EEE 126909AC 6F775F8D 5520115E BDEEEB9C C1CDACEF
4CB7312E 2A08F4CC 5F9055E6 454A360F 34CBDE30 DBDF172D
C80262AC 8C70586E 6020F49D 5E1EFFAB 2CF8926C A579338A
E19D0E28 F44CD3E9 F47ED9DE 427E9E02 8CAF1EFB 6801DEF2
942342BE 354275AA E4B2980C 9C1C1102 F2734341 64EDCA15
7318C78A A85F384A 15ED227A AB1857A1 76B493A2 FA604CAC
16E197FC 36F66A7D 7019A2F9 FCE5990E 3D696660 35DE9F6B
F550D7FA 9F2AA1FB 7E88C1CF EF6AA0E4 105E1409 3A8E44E0
E97EE3D8 0BC2F082 93C4BB11 DE2EB3EA 16BD2FCA 81DAEC9B

i is <6>
Ptest is
E3C27D66 3B0222CC F7675856 5377F848 C05629B8 5D61B74A
CC579F2B AB058935 232A2152 02554CAB A23BF0F5 DFFAE105
C571662A 833D17C3 7E2FB38C A935E579 49C77B49 BE70C6BC
7092F5CB E252AC1A 236841C0 71F93C97 126EB19D 6F7D25EE
ACDCDDF6 C5927138 9D158725 C999DD7A 5962889E DC520BE7
A1ACBF01 FDF897EA E92A300E 91971994 9B6247AE 6DE46751
B86B7D6C 29F13E93 9E425FB5 ED3D149D 298AE3F3 644CE56D
EC9D2E40 37B74100 78C35B84 58065B2E 0DF30EF2 3E0E33AF
7DFA1488 E1FE53EF A3BA0457 055909D3 7DB30784 EC0103C6
B3D5EB80 7E92091B 6A8A7610 530F9CC4 B0C85119 3D63B39F
D93B7B7D B8AFE4FD 98C3B662 B8D9237A 278451B8 0A44FE6C
C4CDE302 4CFD1FA1 A0CF4E2D 4C13C54B 7E9CE188 E7BA6A5C

8B6E202F E4DB7561 F713A806 53E9070A 23634319 CBB5834D
147C282D F4B786B6 9431EFBE CDAA6141 E02F6785 4E2A80AA
DA3B3BC4 59AC10BF 42785E24 B12BDF9F EC84A490 86548C75
ED82B01A AD353915 100B26A6 0B15749E BDFCB37B C7AB36EF

i is <7>
Ptest is
946930B2 A57FF80E 21CA4DF9 A8BAA2B5 665CDF1C D921640F
41EAA714 649287BD 517A8101 658C5B1A 0DB1B63A C243F212
A10A4F40 2F01ED0C C85C0AAE E0A6875D CCCAFED8 5CE902F2
CD2F947E 296DD24F 55EF1421 71390D0D 93450D83 0806D365
CEFA5865 4F544E34 0DEEA2D5 9E71C4D6 F468B9BE 4878FCEC
F4A67BEF 63DFFC26 F64137AF B1CDAF68 C08481D3 03FA2D5C
DD2D5E5B B9EE9AD9 8BB19932 B1709A41 EEC0AC86 E7335393
42ACF5E3 C1AEEB8D 865DA91D 774A6D1B C70C57EE EFAFF0F3
3ED3127B 0BC32309 206E8470 AE8FEC19 DFEB3164 D5CC34F9
06094751 137226E3 FA3C59BC 6258D0FB 2BC59A4D 8DC834BA
5C54C39F 3B4624EA 0D1115DE 4BBAC3FC AA2FEE15 ED63B829
9752B211 354D26CC 5291CC58 E02F058F E0206DBE 4EC3B740
263CA745 1F4A3327 8E992EA3 C38C5EB9 AB46D04B A38BA6A6
FCA35519 9E817A93 46F572DB 8A344C1A 68074229 7343AFC9
3831C7C0 356769EC 53B45852 C1A25F84 32D70E2E 8DB94AAA
D7B068C3 B637DB70 7E540D03 D9CB8A45 CA71C5D2 6D8D52B3

i is <8>
Ptest is
AE7B5322 41894E21 D741E54B 32AFFEF8 1E89178D CAAEC33E
630E74B3 211B92A8 E4CF9082 F7ADACB1 BAB41DE4 A41B5D87
EECFDF8D CEFE53F2 FE279D1D 287CE9A1 0B7C8BB9 E04EACE6
F4A03DB1 B5D123F8 69E72D97 6225B2DB 4BE4DF75 FE707135
0EE35373 C70449DC 79D02448 6BDB35D0 21552FA9 26A33DBB
39BD90FB 8E490C9C C1A621C5 EBE37C47 CB3F5951 1C42F657
A25CEC1C 17808A8A 373BAA88 5D068310 1E4E69AF 6CA2A813
2B3000E8 B338BAD8 DA59C9B9 6892CC57 45A54C39 4A6CE562
63059EC9 7BEF13F3 D7E2B6BA 009AFC8B A26B5ABB BEDAD818
3F9292D8 A7F81DC3 A57BB82D 7F148A89 F7B6B29E A6BA0A59
AEF0313B 3226354B E5DA60FD A5A68094 95BB070F 4048B928
B03858C8 A7A53ED1 0B5E7D35 721EA20E E85D79B6 4DE59F8B
E6F53D98 F246AD14 77960717 6B365E01 5AD43CB3 5427257B
07A5C767 76633EBA E76F6775 35AAA282 3795A7DE 875029F5
61370D41 720D8624 3834E70E BD87D9C0 6FCEE6B4 CAEB8346
2507ADCD 1079AE37 2993604F 2BC22CA9 BBBE0348 2EB22B07

i is <9>
Ptest is
EDD290F6 29FE3F62 4A804F66 03A67AAD 093E36BA B38B8E2B
5EA4F424 1E4790D1 C93F99FA DE79723F 8D4A1048 9252B87A
5D3A3591 672D8C70 FEB4A482 3669D839 D934051B 13EBA0C0
00BBE9ED 7B558ECB 0BDE4248 1C1CB415 84C04180 EBF113DD
D070CA58 82816BD9 E9462A7B EA33BC30 AB5DB257 FA13DB12
BC7DF4CB 9C277A17 12E59B8B E80187DC D0A4E599 9F3A534B
A033B0D1 EDDF520E 27C98024 34434EFC 35C00A44 9F7BA936
2C240261 CA2100A9 48F4B632 F79A01A2 703FE0EE 99F673E3
352D5694 ABA85A45 4DFEE1F1 13F01D3C E3ACA647 EFCA9ECB
C8F47786 2E4A1A24 E6D62B25 4516F48E 634F2B26 DA68B62C
B024824C 84912BB8 E9673B71 A34955C9 B0EDD9DF 263694DC
E3A2E535 27669F46 CBB694A3 B42D790C BFE3C026 6216513D
ABA878E1 6DA72D53 16C8CF98 4135D736 06F1D087 E227BD42
43C0F0F9 F0E17D0F A18DC5CA 3D8ACEC7 1B0135D1 CCE3875A
D6FC3F06 45ABAB03 FE864720 1962F58A 01F177CE 4764B952
76B8FE34 80375DDA F8D0A01C CE38E2F1 6C5A1D15 96E94DBD

i is <10>
Ptest is
E5017E69 2365A37D 59DB01E2 DA3D2A75 4E66BA53 DA3F51A6
24980991 19E2FD74 E8E085E3 390ABE2A B119B90A 6640EE96
C7F5B47B A54D8E68 4467CDFE D9A43430 5559B0CC ED8530FD
B4AA581E BE179E98 B25EDAD2 C5670BFD 41FA4AFC 686E7613
8985F3D8 E2EEB17C AB5DFF5E 970F9262 054D493B FBD5E379
A6D9847E 4F59F77E 8467A3BE 44D0B242 1555EE54 7D8F7F6A
B147BAFB D59FCA60 3C4ABB67 D59E30C6 2F9673E6 61EF60FD
F96FB3A0 5AE8CD8A 8EDB64EF 7A8C0323 EB0531FA 171CA82C
42C5AF10 D151EC62 4A1B2864 86E9C36E AC93EA01 3A30BDAC
EF9305A6 76C877B1 1D8067A0 A1D7F7F2 14E69083 334DD3EF
F0B2B8FA F31235DC 0AEBFAA9 41EF8771 5DC4849A FC23BD83
C5915740 A0E980BF 9F98BF7C 62E541BD 7B562CBD C4740196
E8D4BC32 B3A6F427 EABABA21 F212E13B 3C6A5D36 B26B98CB
56AF706C 12BCCE97 737F2F8B 44292F1A 9F03F836 C59E7A52
DB0020D1 5F2C1035 C32976EB 88269535 569E2780 0CD01DA3
F189FE93 305B3558 BB6E7F0F 9ECA2941 CCF1F422 617D62E9

i is <11>
Ptest is
80A6DFDE EAFC13F4 9235C4AB 5A8421BA C5E0DC85 D4E213DD
256BD092 EF59A901 C7E1C7C4 C9BD4E9F D3096B18 733C6F42
2D913852 30567257 3B28C76A 8945DE17 2880EB41 A64AF29D
F2F85B9D CFBBA13C 8EEC5EA4 5D163502 537139F3 505F9D54

6E341DB0 917D0523 F94FF2F9 39D5E2D3 65A3112E B14DBF04
1B8A0D03 E2739A9D 709AFAF5 8CD94597 B4998ADC 8B451226
B001BCF0 A85FF570 92C5BE8A DD2ACD67 6CD9EA11 65BC8AAC
9D90A630 DFFD0BF5 6ECC1865 C9995D0C 7D6947A6 A1B6593F
15B20238 0B328975 FB17A626 A40AF916 C30DB156 57E8233F
4A5E6EF7 51921CA3 74D991A9 61CE2836 7A19EC14 0B1986BA
045692E8 866026AB 10565D13 B92A0781 3A3B32EC D0FC7973
10FC6FA0 72C90A32 DAFCDAD4 2289930D 568ACF58 FC6B1E26
D3B8ECF4 56FCAE24 9EFF52E6 5C41111B 86A27FBC 8A5C1044
F7C0EA60 0EA26DE2 1D3E6B9D E98D55C6 87047822 CF33F63E
B550847A 3E21414F 6E6970DC 98E1D1FC 034FC04D AF4D8596
87747EC0 9F00A1C2 57AC03C5 4A0A5B3C 7D3E5714 B0CDA453

i is <12>
Ptest is
D7D0622D 3E8CD92C 338AB6EC 4A7F4BDF 5492EDB7 D27A7ADB
B4A1094B 57D07E15 30B3F231 84BB5975 7DCE9AE8 0ABFE36E
9CE72CF9 6A9C0B70 931F6CBA F0EB0C7A 798222C2 0259FF54
8E6698F8 B18BACB9 A46DC963 93DA6C31 5BC6EC0A A3117766
DA2FD54F EAA09194 0A272948 F796F4BA 79138019 3C85CD89
AE9542B6 63A29C8D 785F38DC 4B191201 67ADF60E 45D58790
818B819E FA754CFE 449FD6EF F3202BEF 5BB086FE 23E59C06
E7B2242B B6609E0E D233D2F9 97B9DAB5 1ECF8EE3 938D9201
9A30B6A7 DC5AF615 C4425DDF CE6453AE FCDF4532 EEA1AF2C
B3D1D18E 952FB9FE 97184B49 658395E5 10A3B6F3 BD455940
88EA1390 2DA98F55 1EB2A8E9 21429CDE 03F6079F 4152C21A
EC98C041 E1E95EBD 7E30D7AD B5A2F274 A097B318 410F7D82
6D068B13 3A242149 9CCF24B0 C1E4655E 35F987D4 D62E4055
9B9F69D0 D726228A 50885D71 6F452114 AA3EFC7F E8BFB375
8954C38E FB7B0655 833ABFDE CBA1ECA7 3DC0E23E A32C8C5D
45ECA296 362E09CB 1AF51730 70DF6B97 27303417 06F9BAFB

i is <13>
Ptest is
E5821965 6BA316E9 2EBE5F38 3C01742D 139399DF 199D5542
7A53897C 1ABE0847 370E02E7 AA63B64C D34030E5 F2D3A92E
09B872AD 8D4CB288 68C49B23 44F5927C AE608459 95022207
EF454E3B 915AD405 2E49B356 7E562A4E 72DE9CE4 4B938A2F
1ACFBB43 350062C1 A56626B7 FB346A6B C9DA4362 C7BDC1C0
CC7AFC35 185899BE 9E379059 33F911B6 29699F30 A25465D4
2198F9BF 88CC1F12 64A0252E 2A24CD9F BD7AA5A0 D41C357C
120A3062 553CF62D B773BEF9 DD1233B4 51906D6F 19EF82B7
8D5B2DD3 A2FC908F E52CEAD8 F957FE68 32611C33 665AE111
7C59253F 40140E77 B420D0B1 71EF8757 BDA1E835 79129E82

8DD4750D A3EE3547 D9D97C14 AADE4831 D8E8FDC4 9E1F4B57
B03EF191 588E875A 1FDC9A20 5088A739 CBA03432 00D76B6F
77748D8F BC4835BA 1FF4F593 AF4D4E38 40507710 728F6AF6
02208B8C 64BB29C5 D0B83B01 36A19847 C703C679 F6105CED
04ECC034 23E09852 9A8EEBBF F5806C98 D8B739AD 6C586267
36AB3C6A ABEF6438 F35FB4A4 BFD7080A 698A4556 A4D4B007

i is <14>
Ptest is
F42A2499 E759967E 8567BAA3 6E129CAF 1BB645AF D2F6F783
4D70D329 E3C11EFB 99CFD23B 4A2074BB 15D418BE 8D3D5455
A707EA58 13C7A6B2 9E976DB8 10749C13 6058639E 4C5CDD70
7A2DA522 1C279DA3 24B1330E 8EB7FF7A F86599D3 5C935153
3DEEC55F 1966C0DA D18C8900 FDE7ADE9 C2198165 EE4AE016
5A7A1652 BE161570 13698E14 2F0C5B82 3A63E642 09D4B699
0B67D147 FFF12F45 FC63A729 4052B95D 589BB768 692D34C4
6BC3F53F 654FAB44 F94FD719 C4E126A2 4CD937B3 5199A118
D934090A 34332AE7 50CBB30C 72302C31 5F3EB334 606E01AE
7F1BAC85 484B6A32 F11FC1F8 ED16C307 D7810A32 0CA9159D
3F5551DB CF518EF4 527F4CF0 43EC949E 55C377F2 3F6B21EA
F569EF96 DD1B8D33 978856DC BE8D9759 7D3FCD81 B8DB5F35
24F498D7 1E2FE609 77886CE7 CACF6D51 5A3ABBD2 318220FE
72281232 4057E9AE 17ECA34B 0D54F5CD 738112F4 17A0D078
B359757C C8B8D1D5 281DC515 C4B7197B 36C0A14C 682C0C54
D387DFB2 946F5539 5EDA2AF3 69A9C01B FF1A7EE5 06EF37F1

i is <15>
Ptest is
B33C3A30 A945012D 1EC49256 6CB862BE A2FC0A0C E92551C8
AD87058C 0C48F8DA 9083223B 08AEDF18 0AB46E7B 20ADEF02
C2037DAF 85483F51 4AA5FE35 14F45783 DBBD29F7 8E949C6A
14E4DD3A C21F006D 7FA2A698 3DBC5D8F 4FD4B2CF ECBCF3AD
51B9ADBE 88A0089D B5ECA1C4 43AC2CF8 91322ABA 0038DFB4
E8B8B96F 21CC0669 F90AA76C 524BB61C E5409009 707F02DF
A4C8D1FF F095F5D3 8B61060E 318CEA65 3A4EE63D 9B42C81C
A74E6F80 9CB44C06 BA9DD7E4 25FBFC24 B062CD7A 5E11593F
77147A1E 27A484BF 28A5A943 F10406F2 0D6B4128 235E1A52
51D41982 2641DC9F DEAFD2B8 D5602E6E 71E58191 E6C39E7D
E8C50476 1E5F99D2 6E32A9AC 8E623822 EF2DA15C D812502C
F036215F 316FDC7F 1F9F562A 44A2D344 3FA012B8 A6DC3649
A0EE6708 A11595C4 3943B535 4C52681C B99F5B62 FBD4E3F8
4540DFBC 6B4B658B EF7EF985 FCDF0607 12548E31 DCAC6B7C
A0872375 8CABFEF2 93D78374 79CE5D75 1FA76711 62834BF8
4A616E66 67F713DF 68ED6B50 BE442B3A 4DF24C45 1172DBC7

i is <16>
Ptest is
	CD43E22A 8CB85350 4668F95E EF9ACA30 2BEB6835 8A8544D8
	881593AC EA0B28AE 117D4DD9 0A261D46 43888126 E15BD244
	BD85FD00 6014B53D 415E8AF9 3388231A 161AEC4E 23CB4F9E
	09D9A72E C84A90CF F59CB45E 17154523 B44423C0 AAEE9AA3
	F3C2F0CE 963AB483 99E588B0 677BA217 DC350B60 49BB325A
	E9BE0559 56C89B6A DC287641 EF3A9621 E17F3D6A 555BE901
	029387F6 62C4B3E7 300098AF 9012C627 DC6324FA DBE64062
	07D286CC C306257A A1F69304 4CFADE50 E47A2648 EEBD0962
	5C68A7B2 9B0AEA7F 8B7965A0 15C34F0E 65293018 43C97CF2
	EC7765EC 7A5E98F0 AA24689D BC4E45CF 3D88E316 4DB6118D
	DCA1B9E8 8D7EB607 CA44A35B 2468EFCC 9674CF3B 7FD1ADD3
	097FC243 7B23F611 920C52AF EB1586E8 AF0225DC 1256F6E7
	5167DC35 C397A699 B47313F4 B766E10F CEE76061 7EB4AE45
	100D5A33 71584907 D4302636 D32B9CCC 5DC4DFC7 4E7B01B0
	4808BBBC C2712F89 DF86B40B 13D2F7D2 E910C611 F0EC2D32
	52098AF9 394E4DB5 C61528F9 6FB1F7E1 F74716F2 5B32EF81

i is <17>
Ptest is
	CB971CF0 2E727719 593E9B86 4C5A196E 5B0438B3 F3D97824
	E67B6437 67561C84 DFAE8F36 4DF3E47E F7B26D10 00B28940
	7BB95ADB 6F5ADECD 7AB3607F CBE547D0 98F271FE 5066D82F
	01CC2B1F 8DF7EEB4 3B6A3A15 456D5055 AAF20F6F 8814615C
	3A694450 13B6A14A A8E324DE 8FA4754C 08E3D6F0 EC962967
	AFCC3CCE 509E7E82 C0F49061 A42485EE D65AA639 DA1841E8
	5816D9AA 9B305FFF 02FB6C2B AF741471 AB7F49B6 B9C04FB7
	D8D9D7CB 0C59BF68 4B78CAB8 D7329E35 184FD28D 770AC51D
	336DA5D7 EBA3FA18 838EBE10 8E21C9E4 94A36DBE 4472A4F2
	ED843084 0DB297BC E1937722 613A9C4A A40E4DAF D2B0CF3E
	DA9CBA9E 0845E054 58A4B5A1 4762B94D A524D1F6 8C8285C2
	FC5D084D 78C2461A 26422E9D C3923E0D 76C61B94 C750F5C2
	4EACD0B7 ED5333F1 A37A1FE2 8B408830 3078792B AB2E778A
	278D961F E19AB3C8 6B11F052 7251EA85 E6170D8C 3A52C4FD
	315A1B44 2BA1B894 33EFBA77 7E3E8F5C 708AC0E7 D272FDA4
	AD3FA896 5FAB84AA 115D08A6 C46C358E 5555DCA4 18BAFEFB

i is <18>
Ptest is
	B48DB99E 290ED791 29B6B89D EAB9D8AA C3B770D9 46E94E78
	100F9054 183D1159 1B053AE5 57C5A539 33FC8B0B 342EAF38

BDA1324B 42BC7ED8 0E3F8545 D7510925 8D69B28B 2F564CDE
4FB44328 32B2DC68 306D87F0 B3D448AD 4F4E7C65 B761CB10
6B683D58 8261A56E E9ECE592 8B71BD4A 955EE11C CBEF2343
EE2A0432 133FAED1 E7AFFC87 5FCC3DC1 1FC7F50D 57FA511A
9D43C670 C7DC6140 9DB03D32 D1516404 73AE5026 1D39C747
2D12D498 876BEC92 C82C1587 0C6FD482 7562936F A28B1FA6
9D53ABC4 9F2A11B6 E7C71B7F 77A92E8C 17531354 54AF6936
8C7B99D4 8D45B9B3 F55C90F0 6CD38ECC 33B6521A A2DB124A
C04269C2 AF59180F AD67CACD 5362A2A9 BDA21208 56A83460
161375E4 8C6A2F28 5BB89A09 2F01575D 578AAAF0 F38BE534
4696085A 2944FE90 AD0100CE 2357796C 6A7834E5 26906566
AA48A22A 29AB9551 6CF549D0 1E0C9961 A0BD4F92 59A8144B
2E1343F3 8061F357 31129C44 18A01093 287621B3 CAC2B087
38CAB217 6F278884 497CF060 62B65F54 F2F5222F CAAB1C25

i is <19>
Ptest is
84BCDAC2 B91A48BA FD4F1386 85E50E8B 58F01314 A1F0BFD5
D3CA4A51 844A996C F8AA80B6 C047DE7C D44472E9 8C1AD995
0BB1BC05 3A28908B EB929361 5F4809BB 3100C794 3D859FFF
CF15B0FE 270D6024 97BD288B 83846C93 91ED6C22 226AE8EA
D83C060B B67A5B1A 3020C065 37C7BA82 167E5653 877D1023
D1A28207 9B287738 4E4DE268 5AEDE86A DFDA3CCF 4C92907A
41D1D5B8 88EC184C 99008501 C3DC8FFF D380B50E 64C2E945
3ED83F16 32CAAE3C B9E0039F 63AC9260 0545684C 559AAB1F
5C6863FA 91C01640 F33FD137 15227D4B 2CCDAC17 DCC50242
F9DDBA39 297FD7ED 053D6976 109A18C5 182991E2 01889C5E
E25205F2 3535D163 3C75065E AA0D3719 7D6FAE05 07DF91D0
D8D5C9E7 50A08F3C 82A39695 B7E080CF 241DC332 CFB0334B
49B3AE64 E8656B47 8FB60296 C5D57D0B 59B94CB2 B05EE82D
170910CA 8DD37586 F4D0078A 92FB8279 77241B8C 6FC3B7BB
3DD79F9D 2DA2B341 D92C41A6 6EA2D242 F009488C 079DCE84
DFAAE0D9 FDF6710D 768F4AA7 1F30FAC0 F8C70C89 1355B8A3

i is <20>
Ptest is
90066455 B5CFC38F 9CAA4A48 B4281F29 2C260FEE F01FD610
37E56258 A7795A1C 7AD46076 982CE6BB 956936C6 AB4DCFE0
5E678458 6940CA54 4B9B2140 E1EB523F 009D20A7 E7880E4E
5BFA690F 1B9004A2 7811CD99 04AF7042 0EEFD6EA 11EF7DA1
29F58835 FF56B89F AA637BC9 AC2EFAAB 90340222 9F491D8D
3485261C D068699B 6BA58A1D DBBEF6DB 51E8FE34 E8A78E54
2D7BA351 C21EA8D8 F1D29F5D 5D159394 87E27F44 16B0CA63
2C59EFD1 B1EB6651 1A5A0FBF 615B766C 5862D0BD 8A3FE7A0

```
        E0DA0FB2 FE1FCB19 E8F9996A 8EA0FCCD E5381752 38FC8B0E
        E6F29AF7 F642773E BE8CD540 2415A014 51A84047 6B2FCEB0
        E388D30D 4B376C37 FE401C2A 2C2F941D AD179C54 0C1C8CE0
        30D460C4 D983BE9A B0B20F69 144C1AE1 3F9383EA 1C08504F
        B0BF3215 03EFE434 88310DD8 DC77EC5B 8349B8BF E97C2C56
        0EA878DE 87C11E3D 597F1FEA 742D73EE C7F37BE4 3949EF1A
        0D15C3F3 E3FC0A83 35617055 AC91328E C22B50FC 15B941D3
        D1624CD8 8BC25F3E 941FDDC6 20068958 1BFEC416 B4B2CB73


Ptest is probably prime
----------------------------------------------------------------

Parameters are VALID


================================================================

Key Pair Generation

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

C is
                         D298FF1F 1F8FBF81 E5387EC3 A4AB42A7
        8DF3586A 0FA22B38 EDD20194 AAD9E9E8 EE50B6CC C3B42EAF


X is
                                           3ABC1587 297CE7B9
        EA1AD665 1CF2BC4D 7F92ED25 CABC8553 F567D1B4 0EBB8764


Y is
        8B891C86 92D3DE87 5879390F 2698B26F BECCA6B0 75535DCE
        6B0C8625 77F9FA0D EF6074E7 A7624121 224A5958 96ABD4CD
        A56B2CEF B942E025 D2A4282F FAA98A48 CDB47E1A 6FCB5CFB
        393EF35A F9DF9131 02BB303C 2B5C36C3 F8FC04ED 7B8B69FE
        FE0CF3E1 FC05CFA7 13B3435B 2656E913 BA8874AE A9F93600
        6AEB448B CD005D18 EC3562A3 3D04CF25 C8D3D698 44343442
        FA3DB7DE 618C5E2D A064573E 61E6D558 1BFB694A 23AC87FD
        5B52D62E 954E1376 DB8DDB52 4FFC0D46 9DF97879 2EE44173
        8E5DB05A 7DC43E94 C11A2E7A 4FBE3830 71FA36D2 A7EC8A93
        88FE1C4F 79888A99 D3B61056 97C2556B 79BB4D7E 781CEBB3
        D4866AD8 25A5E830 84607228 9FDBC941 FA679CA8 2F5F78B7
        461B2404 DB883D21 5F4E0676 CF549395 0AC55916 97BFEA8D
        1EE6EC01 6B89BA51 CAFB5F9C 84C989FA 117375E9 4578F28B
```

```
        E0B34CE0 545DA462 66FD77F6 2D8F2CEE 92AB7701 2AFEBC11
        008985A8 21CD2D97 8C7E6FE7 499D1AAF 8DE632C2 1BB48CA5
        CBF9F310 98FD3FD3 854C49A6 5D920174 4AACE540 354974F9


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

===============================================================

Per-Message Secret Number Generation

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

C is
                           BECFFA86 C79F5610 CFB30ACC 86464439
        7F09937A 7BFEE0F2 68EF2134 DE28ADBE 4737FBBD E9C6D225


K is
                                            A6902C1E 6E3943C5
        62806158 8A8B007B CCEA91DB F1291548 3F04B24A B0678BEE


Kinv is
                                            BF78FB41 492AD962
        4CB85084 22592D07 BF68F5B1 8061A54B 095BE138 A514644C


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

===============================================================

Signature Generation

    hashlen = 256
    Msg is 616263

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

K is
                                            A6902C1E 6E3943C5
        62806158 8A8B007B CCEA91DB F1291548 3F04B24A B0678BEE


Kinv is
                                            BF78FB41 492AD962
```

```
        4CB85084 22592D07 BF68F5B1 8061A54B 095BE138 A514644C


R is
                                            5F184E64 5A38BE8F
        B4A6871B 6503A9D1 2924C7AB E04B7141 0066C2EC A6E3BE3E


Z = Hash(msg) is
                                            BA7816BF 8F01CFEA
        414140DE 5DAE2223 B00361A3 96177A9C B410FF61 F20015AD


S is
                                            91EB0C7B A3D4B9B6
        0B825C3D 9F2CADA8 A2C9D772 3267B033 CBCDCF88 03DB9C18


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

Signature:
  R is
                                            5F184E64 5A38BE8F
        B4A6871B 6503A9D1 2924C7AB E04B7141 0066C2EC A6E3BE3E


  S is
                                            91EB0C7B A3D4B9B6
        0B825C3D 9F2CADA8 A2C9D772 3267B033 CBCDCF88 03DB9C18


===========================================================

Signature Verification

    hashlen = 256
    Msg is 616263

    R is
                                            5F184E64 5A38BE8F
        B4A6871B 6503A9D1 2924C7AB E04B7141 0066C2EC A6E3BE3E


    S is
                                            91EB0C7B A3D4B9B6
        0B825C3D 9F2CADA8 A2C9D772 3267B033 CBCDCF88 03DB9C18
```

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

W is
                                                193AE905 9CE5413F
        DC5885FA 40E34F84 FEE416E1 948F02B7 2554FA98 DE5ACCB9


Z = Hash(msg) is
                                                BA7816BF 8F01CFEA
        414140DE 5DAE2223 B00361A3 96177A9C B410FF61 F20015AD


U1 is
                                                1DCD033E 23A7B6C5
        B8B46163 DF9D5664 7C3F6C13 73A3F85E BFE7BF78 A5F0F092


U2 is
                                                00CF91C2 77E51AF7
        1BF773D0 D098975F 9622BA56 A55F3525 8EA86546 451B7913


V1 is
        752E2E4B 19477201 AD650E2B 48EB0237 70585753 0E916736
        0F213840 ADE77EB0 C44602EB 8759D2E6 452EEDA2 EAD4A81F
        6330C5E7 AC571F08 0BDD8180 7EC1DB25 EA0AF572 C2170F30
        FA5B80A6 FA7FB95B 5CF2CB85 8D773AE7 5E3589BA C978709A
        B76917FB 1128A1AC AA66E4D0 CE6FBA16 778CA5CA 9E3F7BA5
        552B78B5 A4FFD15D B406BF6D EB0D58D4 569DA528 CA464DB8
        CB12AB2F 2CDD557C 6D3B32E6 2034F2B9 96B6CF0C 91D952D4
        027A4D4C 2A03F738 8DCD2984 50AD29B4 6709E8B9 0D292043
        8BA60304 E84FEF07 577C2C32 60612E6F F921B423 305A579E
        6CDDB414 8AED712C 5E6C7A9B 466D34F9 C3A65B25 694EBDD6
        5C78E47F 59FA1AE6 20C3BE98 10BD12B3 BCDB5200 02E68BA7
        6EAAC22E 85A36046 126AB333 5469746E C3204150 0C480A32
        EB10B002 B91494E1 93FF7C70 49E2B55A C718998E 018A4E4D
        D32C1353 CFDC624C 2593F593 2AA9695C 87044ED8 4D01BFE9
        AFF24C5E 958B681B 96267E21 24C3A033 7C860D3F DE36FFE0
        AE93C972 EB170240 457CB6C5 634EA559 A8683E23 CFE4B1A4


V2 is
        5A924B92 6ABD532D 96F1998A B4F9D42E ED4A1004 006222EF
        69010CF4 BE5AEF76 52497B8E 2B5E477F 8D66E319 6693E6B8
```

```
        32AE6563 9737E2C0 80867FED 28F2AC3F 7D724F47 16EBFDB1
        F54095E7 B5F88EE1 54FC7031 84C4FB5A 157F893A 567B1354
        34B9A6EB CB389582 6E5D980E 6ADB8BF1 3CE39BB0 9EFF338B
        3DB546C0 081F1DCB 30D5BBCB 5EC7DE9E 1855828A A1B372F9
        107BDDCD 4D848A08 A2AA2C3B 1CA8E53C E3573A4E 05103FF0
        5741005B F83165E9 CC833499 8E0FEA0F 783712BC FB9FB452
        A8406096 CF44B4E5 3201D63C CD543687 78BD94CE 8DA19983
        90F6FF8E 218A0265 B5F48884 79886C5E 5248B03B 7E4FBDFD
        427B7710 CAF90ADC 17F191A2 A504C07F A41D0A04 C8CC1A60
        FC723CD3 C68EB0FA B7B10814 2ADB93BA B8E804CC 7164347F
        09237270 54442D0A E7C10B78 902EECD0 26857C27 D65EEDD7
        125B1491 9E89D8D8 6BAF0716 BE7D91F4 B5AA5342 2EAB35C2
        73E9427C AD5BA080 BB8DCA41 E6DC4EC9 CDE3686A E6D997F3
        5EF36F15 B99DCF72 2C13D810 6700CB42 07151FC1 17B2F923


V is
                                                5F184E64 5A38BE8F
        B4A6871B 6503A9D1 2924C7AB E04B7141 0066C2EC A6E3BE3E


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

Signature is verified
```