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

DualEC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Nonce =
                                             20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput = <empty>

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

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

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F


    nonce is
                                             20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"
```

```
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                    01 00000100
        00010203 04050607 08090A0B 0C0D0E0F 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                            F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


    temp =
                                            F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


s is
                                            F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                            F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A
```

```
s is
                                        5FFEFE90 005C75B2
      CBEF01A9 A3887F7A 80430A4F 6FF0A196 28CE1610 96350C75


r is
                                        C0CCFF51 63C388F7
      91E96F10 52D5C8F0 BD6FBF71 44839C48 90FF8548 7C5C1270


------------
tmp is
                                            FF51 63C388F7
      91E96F10 52D5C8F0 BD6FBF71 44839C48 90FF8548 7C5C1270


------------
i=1
t is
                                        5FFEFE90 005C75B2
      CBEF01A9 A3887F7A 80430A4F 6FF0A196 28CE1610 96350C75


s is
                                        11C42D2D 4A98B054
      AE25746E DA4E147A 9308E68B B91B7788 BA140B8B E18CEA1A


r is
                                        DDE82E4C 9849AF51
      8AE68DEB 14D3A627 02BBDE4B 98AB2117 65FD87AC A12FC2A6


------------
tmp is
                                FF5163C3 88F791E9 6F1052D5
      C8F0BD6F BF714483 9C4890FF 85487C5C 12702E4C 9849AF51
      8AE68DEB 14D3A627 02BBDE4B 98AB2117 65FD87AC A12FC2A6


------------
s is
                                        DDBD9639 34E3E942
      8CCC5C84 175C70D6 4D31CF0B E3CE141D 61F3D297 D87CF0B4
```

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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                            DDBD9639 34E3E942
        8CCC5C84 175C70D6 4D31CF0B E3CE141D 61F3D297 D87CF0B4


  s is
                                            2B79FE2B F483248C
        E845B587 11469A0B 01A4B263 F1565570 34D2B409 B6CEDA66


  r is
                                            6F0B9A0A 11F2DFB8
        8F726055 9DD8DA61 34EB2B34 CC0415FA 8FD0474D B6B85E1A


  ------------
  tmp is
                                                9A0A 11F2DFB8
        8F726055 9DD8DA61 34EB2B34 CC0415FA 8FD0474D B6B85E1A


  ------------
  i=1
  t is
                                            2B79FE2B F483248C
        E845B587 11469A0B 01A4B263 F1565570 34D2B409 B6CEDA66


  s is
                                            38BB1AF3 9E3826B2
        EE6BAA80 93ADD16E 4035E2B1 A843CCF8 9DA4D5B4 29B2E571
```

```
  r is
                                          307E0838 5F41B435
        DF81296B 1B4EDF66 E0107C08 44E3D28A 89B05046 B89177F2


  ------------
  tmp is
                                  9A0A11F2 DFB88F72 60559DD8
        DA6134EB 2B34CC04 15FA8FD0 474DB6B8 5E1A0838 5F41B435
        DF81296B 1B4EDF66 E0107C08 44E3D28A 89B05046 B89177F2


  ------------
  s is
                                          73722037 B3B07CE9
        0A55ADB8 612AB20E 0525F499 7D0207C7 813A2B31 9E7A2DA6


rnd_val is
                                  9A0A11F2 DFB88F72 60559DD8
        DA6134EB 2B34CC04 15FA8FD0 474DB6B8 5E1A0838 5F41B435
        DF81296B 1B4EDF66 E0107C08 44E3D28A 89B05046 B89177F2


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

DualEC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F


    EntropyInput1 (for Reseed1) =
                          80818283 84858687 88898A8B 8C8D8E8F


    EntropyInput2 (for Reseed2) =
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
```

```
    Nonce =
                                            20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput1  =
                         60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput2  =
                         A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


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

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

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                         00010203 04050607 08090A0B 0C0D0E0F


    nonce is
                                            20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                     01 00000100
        00010203 04050607 08090A0B 0C0D0E0F 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                                          F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


    temp =
                                          F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


s is
                                          F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
                        60616263 64656667 68696A6B 6C6D6E6F


    requested_number_of_bits is 480
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 60616263 64656667 68696A6B 6C6D6E6F


    Hash(counter||no_of_bits_to_return||input_string) is
                                          1971EF06 D6518B33
        336E7701 1D9E34D9 ECE74E43 EC2BE92C 053526A8 B8807FCA


    temp =
                                          1971EF06 D6518B33
```

```
      336E7701 1D9E34D9 ECE74E43 EC2BE92C 053526A8 B8807FCA


------------
i=0
t is
                                          EC8C589E 6484D9BB
      D1B2C4DC 11289A89 9759475A A1931D5E 35B026DB AA30E380


s is
                                          5F064198 5EA2043C
      DEBD8380 852676B3 8BAA49B2 C85B6821 7C746DE2 4F03E627


r is
                                          2B1FC08E 954FCD48
      6D0B0934 A0236692 AC705A83 5D1A3C94 D2ACD468 4AB26E97


------------
tmp is
                                              C08E 954FCD48
      6D0B0934 A0236692 AC705A83 5D1A3C94 D2ACD468 4AB26E97


------------
i=1
t is
                                          5F064198 5EA2043C
      DEBD8380 852676B3 8BAA49B2 C85B6821 7C746DE2 4F03E627


s is
                                          5BE1CB12 82E9CDC9
      3DD30A8A F23ECD4F 36591ADA 96DF76A8 1314226D BFA18A92


r is
                                          90108D7D 42E73CC0
      6D6EC147 2C63E51B ED7F7151 8395836E 2052BBD7 3A20CABB


------------
tmp is
                                C08E954F CD486D0B 0934A023
```

```
        6692AC70 5A835D1A 3C94D2AC D4684AB2 6E978D7D 42E73CC0
        6D6EC147 2C63E51B ED7F7151 8395836E 2052BBD7 3A20CABB


  ------------
  s is
                                            31406B18 A2764288
        6EC67852 835838D9 FC9FD279 1F9960B9 809DF42B B52BAC5C


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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    requested_number_of_bits is 480
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    Hash(counter||no_of_bits_to_return||input_string) is
                                            27881CBD D6B3C655
        5FE3EF70 59B5FEFC E86DF84C 255D832A A1E1091C 79D9FFF9


    temp =
                                            27881CBD D6B3C655
        5FE3EF70 59B5FEFC E86DF84C 255D832A A1E1091C 79D9FFF9


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

```
i=0
t is
                                        16C877A5 74C584DD
      31259722 DAEDC625 14F22A35 3AC4E393 217CFD37 CCF253A5


s is
                                        36C76642 BD5B0F60
      73FD4784 18C48BD4 ABB6AC5D 252C9649 6DAEEA58 48060F9D


r is
                                        31081D76 DEE36FCC
      5F9478C1 12EAFA1C 4CCD0635 435A6F3A 247A3BA3 849790B5


------------
tmp is
                                            1D76 DEE36FCC
      5F9478C1 12EAFA1C 4CCD0635 435A6F3A 247A3BA3 849790B5


------------
i=1
t is
                                        36C76642 BD5B0F60
      73FD4784 18C48BD4 ABB6AC5D 252C9649 6DAEEA58 48060F9D


s is
                                        D76BD5B5 4F2B26EB
      2EE4A79C 53AF57C4 E73B3F2B CD9E2430 C82DD251 8125B46B


r is
                                        15CA2450 70E95C1A
      67BE7A39 BFB213F2 C0EFCC17 1A3253DA 6D54DA43 62EA2099


------------
tmp is
                                1D76DEE3 6FCC5F94 78C112EA
      FA1C4CCD 0635435A 6F3A247A 3BA38497 90B52450 70E95C1A
      67BE7A39 BFB213F2 C0EFCC17 1A3253DA 6D54DA43 62EA2099
```

```
  ------------
  s is
                                          6CB3B3D3 09120EEB
        251C808B A104D660 99C8B794 B9ED537F B79BEC24 F935BCB3


rnd_val is
                                 1D76DEE3 6FCC5F94 78C112EA
        FA1C4CCD 0635435A 6F3A247A 3BA38497 90B52450 70E95C1A
        67BE7A39 BFB213F2 C0EFCC17 1A3253DA 6D54DA43 62EA2099


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

DualEC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                        00010203 04050607 08090A0B 0C0D0E0F


    EntropyInput1 (for Reseed1) =
                        80818283 84858687 88898A8B 8C8D8E8F


    EntropyInput2 (for Reseed2) =
                        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Nonce =
                                          20212223 24252627


    PersonalizationString =
                        40414243 44454647 48494A4B 4C4D4E4F


    AdditionalInput = <empty>

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

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

```
DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                            00010203 04050607 08090A0B 0C0D0E0F


    nonce is
                                              20212223 24252627


    personal_str is
                            40414243 44454647 48494A4B 4C4D4E4F


    prediction_resistance_flag = "No PredictionResistance"

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 00010203 04050607 08090A0B 0C0D0E0F
        20212223 24252627 40414243 44454647 48494A4B 4C4D4E4F


    Hash(counter||no_of_bits_to_return||input_string) is
                                              48306692 AF00A3F6
        1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


    temp =
                                              48306692 AF00A3F6
        1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


s is
                                              48306692 AF00A3F6
        1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


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

```
First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                            48306692 AF00A3F6
        1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


  s is
                                            07220A43 46B8BDCB
        FF430F10 82A022FA 98C76EF1 4CB72ABB AED09239 8979075C


  r is
                                            E3413AB0 95CC493A
        8730D70D E923108B 2E471079 9044FFC2 7D0A1156 250DDF97


  ------------
  tmp is
                                                3AB0 95CC493A
        8730D70D E923108B 2E471079 9044FFC2 7D0A1156 250DDF97


  ------------
  i=1
  t is
                                            07220A43 46B8BDCB
        FF430F10 82A022FA 98C76EF1 4CB72ABB AED09239 8979075C


  s is
                                            DBFB35E7 65853122
        DBC73725 0E8CA258 2EE963BF 558623F3 FE296EB2 58D2B212


  r is
```

```
                                          8821E8B0 5ACE055E
      49F3E3F5 B928CCD1 8317A3E6 8FCB0B6F 0459ADF9 ECF79C87


  ------------
  tmp is
                                 3AB095CC 493A8730 D70DE923
      108B2E47 10799044 FFC27D0A 1156250D DF97E8B0 5ACE055E
      49F3E3F5 B928CCD1 8317A3E6 8FCB0B6F 0459ADF9 ECF79C87


  ------------
  s is
                                          51338CAF 4ACC90DB
      2AB01EFA 386BCD9A A3D218AF 38A5F953 87606B24 75E70E3A


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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                          51338CAF 4ACC90DB
      2AB01EFA 386BCD9A A3D218AF 38A5F953 87606B24 75E70E3A


  s is
                                          9519EAFE 8981CE23
      1073C826 1BCCD88B 69E75951 F2AF69D6 629B4541 01D8BFAD


  r is
                                          A83D7B90 2FC35B0A
      F50F57F8 822936D0 8A96E41B 16967C6B 1AA0BC05 032F0D53


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

```
  tmp is
                                                  7B90 2FC35B0A
        F50F57F8 822936D0 8A96E41B 16967C6B 1AA0BC05 032F0D53


  ------------
  i=1
  t is
                                            9519EAFE 8981CE23
        1073C826 1BCCD88B 69E75951 F2AF69D6 629B4541 01D8BFAD


  s is
                                            FD5E645A 56976F29
        75742607 B18FA7E1 30192BCD E1DE9430 CB0BA656 1B41A231


  r is
                                            2789919D C587B664
        C883E2FE 8F394800 2FCD8BCB FC4706BC AA2075EF 6BF41167


  ------------
  tmp is
                                  7B902FC3 5B0AF50F 57F88229
        36D08A96 E41B1696 7C6B1AA0 BC05032F 0D53919D C587B664
        C883E2FE 8F394800 2FCD8BCB FC4706BC AA2075EF 6BF41167


  ------------
  s is
                                            5C4B76D2 04F17E37
        C01EA94A D09DE5A4 6BE71997 328E1C7E 85FC290B CF435505


rnd_val is
                                  7B902FC3 5B0AF50F 57F88229
        36D08A96 E41B1696 7C6B1AA0 BC05032F 0D53919D C587B664
        C883E2FE 8F394800 2FCD8BCB FC4706BC AA2075EF 6BF41167


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

DualEC_DRBG

    Requested Security Strength = 128
```

```
    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
                         00010203 04050607 08090A0B 0C0D0E0F


    EntropyInput1 (for Reseed1) =
                         80818283 84858687 88898A8B 8C8D8E8F


    EntropyInput2 (for Reseed2) =
                         C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Nonce =
                                             20212223 24252627


    PersonalizationString =
                         40414243 44454647 48494A4B 4C4D4E4F


    AdditionalInput1  =
                         60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput2  =
                         A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


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

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

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                         00010203 04050607 08090A0B 0C0D0E0F


    nonce is
                                             20212223 24252627
```

```
    personal_str is
                          40414243 44454647 48494A4B 4C4D4E4F


    prediction_resistance_flag = "No PredictionResistance"

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 00010203 04050607 08090A0B 0C0D0E0F
        20212223 24252627 40414243 44454647 48494A4B 4C4D4E4F


    Hash(counter||no_of_bits_to_return||input_string) is
                                             48306692 AF00A3F6
        1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


    temp =
                                             48306692 AF00A3F6
        1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


s is
                                             48306692 AF00A3F6
        1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F
```

```
  requested_number_of_bits is 480
Hash_df()
----------------------------
  no_of_bits_to_return = 256

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

  i = 1

  counter||no_of_bits_to_return||input_string is
            01 00000100 60616263 64656667 68696A6B 6C6D6E6F


  Hash(counter||no_of_bits_to_return||input_string) is
                                          1971EF06 D6518B33
      336E7701 1D9E34D9 ECE74E43 EC2BE92C 053526A8 B8807FCA


  temp =
                                          1971EF06 D6518B33
      336E7701 1D9E34D9 ECE74E43 EC2BE92C 053526A8 B8807FCA


------------
i=0
t is
                                          51418994 795128C5
      22EAF14C FC1DCE68 0A8B490A 70E67165 BA4DDEDB C0DEA379


s is
                                          28C1806A FCF56F49
      08362DB4 0FA1245B 9E998CE3 0AE2A5DA F57E4D3C 2C44ECEE


r is
                                          27423B68 A1D95ED0
      312150AC 19911897 80F37EC5 0E75249F 915CD806 BBA0C44F


------------
tmp is
                                              3B68 A1D95ED0
      312150AC 19911897 80F37EC5 0E75249F 915CD806 BBA0C44F
```

```
  ------------
  i=1
  t is
                                          28C1806A FCF56F49
        08362DB4 0FA1245B 9E998CE3 0AE2A5DA F57E4D3C 2C44ECEE


  s is
                                          7B37CB05 75C300B3
        4928C5F9 FD1237E6 FCEE99FC 0D4FD7D6 071DB5DD 93D20B31


  r is
                                          E9259E3A 919B2390
        805E1E90 C1D2D1C8 23B17B96 DB44535B 72E0CFB6 2723529D


  ------------
  tmp is
                                  3B68A1D9 5ED03121 50AC1991
        189780F3 7EC50E75 249F915C D806BBA0 C44F9E3A 919B2390
        805E1E90 C1D2D1C8 23B17B96 DB44535B 72E0CFB6 2723529D


  ------------
  s is
                                          8E0D63D9 788C13A4
        5615F270 2D9DA602 D8BA211E 6E5E8586 CB3822BB ABBCC7DD


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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    requested_number_of_bits is 480
  Hash_df()
  ----------------------------
    no_of_bits_to_return = 256
```

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

  i = 1

  counter||no_of_bits_to_return||input_string is
            01 00000100 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


  Hash(counter||no_of_bits_to_return||input_string) is
                                          27881CBD D6B3C655
      5FE3EF70 59B5FEFC E86DF84C 255D832A A1E1091C 79D9FFF9


  temp =
                                          27881CBD D6B3C655
      5FE3EF70 59B5FEFC E86DF84C 255D832A A1E1091C 79D9FFF9


------------
i=0
t is
                                          A9857F64 AE3FD5F1
      09F61D00 742858FE 30D7D952 4B0306AC 6AD92BA7 D2653824


s is
                                          C5EF4CF0 C33DD22F
      204FD138 282533DD 3B9D7812 167899C8 8E71B22C 78602C57


r is
                                          A676250B 933475E3
      BD4FC85D 97FD7978 34B599DE DEDF8B6F 15474E1F 31B4AF21


------------
tmp is
                                              250B 933475E3
      BD4FC85D 97FD7978 34B599DE DEDF8B6F 15474E1F 31B4AF21


------------
i=1
t is
                                          C5EF4CF0 C33DD22F
```

```
        204FD138 282533DD 3B9D7812 167899C8 8E71B22C 78602C57


  s is
                                            DA9644BD 977A1508
        7F58F877 1A886253 A32E8B5D 9855DC48 460AF031 BAC3896C


  r is
                                            8D0F5CFA 7A8C0A02
        96A2E374 B3886BB0 CC7E49DB B1932456 4B451E64 F12864F9


  ------------
  tmp is
                                  250B9334 75E3BD4F C85D97FD
        797834B5 99DEDEDF 8B6F1547 4E1F31B4 AF215CFA 7A8C0A02
        96A2E374 B3886BB0 CC7E49DB B1932456 4B451E64 F12864F9


  ------------
  s is
                                            A2F2449A CA6D389C
        D8DAD909 D8AF9818 0F9D97B1 9EC14FF8 03076E87 3D1C9115


rnd_val is
                                  250B9334 75E3BD4F C85D97FD
        797834B5 99DEDEDF 8B6F1547 4E1F31B4 AF215CFA 7A8C0A02
        96A2E374 B3886BB0 CC7E49DB B1932456 4B451E64 F12864F9


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

DualEC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                          00010203 04050607 08090A0B 0C0D0E0F


    EntropyInput1 (for Reseed1) =
```

```
                        80818283 84858687 88898A8B 8C8D8E8F


    EntropyInput2 (for Reseed2) =
                        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Nonce =
                                             20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput = <empty>

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

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

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                        00010203 04050607 08090A0B 0C0D0E0F


    nonce is
                                             20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                   01 00000100
        00010203 04050607 08090A0B 0C0D0E0F 20212223 24252627
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                                            F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


    temp =
                                            F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


s is
                                            F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                          80818283 84858687 88898A8B 8C8D8E8F


    additional_input is  <empty>

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
```

```
                                                 01 00000100
        F5FDB798 B2D55288 E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472
        30850073 12B09C4A 80818283 84858687 88898A8B 8C8D8E8F


    Hash(counter||no_of_bits_to_return||input_string) is
                                            5B1DEA76 192287BB
        9C8157EA 5260A02D F4EFD5AB 0DF0948D 63780564 5554479E


    temp =
                                            5B1DEA76 192287BB
        9C8157EA 5260A02D F4EFD5AB 0DF0948D 63780564 5554479E


s is
                                            5B1DEA76 192287BB
        9C8157EA 5260A02D F4EFD5AB 0DF0948D 63780564 5554479E


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                            5B1DEA76 192287BB
        9C8157EA 5260A02D F4EFD5AB 0DF0948D 63780564 5554479E


  s is
                                            47F46DB7 B18F1D4C
        041140C3 BC8767AD B9103687 3FB275D2 77FE728B BAE1F584


  r is
                                            A5438C77 288EDBEA
        9A742464 F78D55E3 3593C1BF 5F9D8CD8 609D6D53 BAC4E4B4


  ------------
  tmp is
```

```
                                                  8C77 288EDBEA
      9A742464 F78D55E3 3593C1BF 5F9D8CD8 609D6D53 BAC4E4B4


  ------------
  i=1
  t is
                                            47F46DB7 B18F1D4C
      041140C3 BC8767AD B9103687 3FB275D2 77FE728B BAE1F584


  s is
                                            DF51738B BB438BF6
      B1FAA44D 1E561ACD A0B7EF6B 36C402CD 03CE82C0 77CE330F


  r is
                                            25F22252 A227A99B
      AD0F2358 B05955CD 35723B54 9401C71C 9C1F32F8 A2018E24


  ------------
  tmp is
                                  8C77288E DBEA9A74 2464F78D
      55E33593 C1BF5F9D 8CD8609D 6D53BAC4 E4B42252 A227A99B
      AD0F2358 B05955CD 35723B54 9401C71C 9C1F32F8 A2018E24


  ------------
  s is
                                            B2142494 19F0F84A
      F4D54B42 9509CBA8 F5835661 70A3710B 1FF7EAE5 64504A63


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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
Generate FAILED: Reseed is required
```

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

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                           C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    additional_input is  <empty>

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                      01 00000100
        B2142494 19F0F84A F4D54B42 9509CBA8 F5835661 70A3710B
        1FF7EAE5 64504A63 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Hash(counter||no_of_bits_to_return||input_string) is
                                             6BA22FDD 08909D88
        5A6A3B1D 6D1632C0 7AF24024 2935D4D9 55103EB1 5BB92E04


    temp =
                                             6BA22FDD 08909D88
        5A6A3B1D 6D1632C0 7AF24024 2935D4D9 55103EB1 5BB92E04


s is
                                             6BA22FDD 08909D88
        5A6A3B1D 6D1632C0 7AF24024 2935D4D9 55103EB1 5BB92E04


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
```

```
------------
i=0
t is
                                        6BA22FDD 08909D88
      5A6A3B1D 6D1632C0 7AF24024 2935D4D9 55103EB1 5BB92E04


s is
                                        B22FAD78 8AF6890F
      D4322A2B BC14A063 91F983AD DD3C56CA 7C04799D D99A18F0


r is
                                        3BA856EC A61C64F6
      9C1C232E 992623C7 1418BD0B 96D78311 8FAAD94A 09E3A9DB


------------
tmp is
                                            56EC A61C64F6
      9C1C232E 992623C7 1418BD0B 96D78311 8FAAD94A 09E3A9DB


------------
i=1
t is
                                        B22FAD78 8AF6890F
      D4322A2B BC14A063 91F983AD DD3C56CA 7C04799D D99A18F0


s is
                                        5DCD988F 0DC87671
      E4907A4A 52E0A024 B2F88A3F ADEC28B4 28DD2B57 ACD478E1


r is
                                        16E974D1 5E805BA7
      F1462599 5CA77612 B2EF7A05 863699EC BABF70D3 D422C014


------------
tmp is
                                56ECA61C 64F69C1C 232E9926
      23C71418 BD0B96D7 83118FAA D94A09E3 A9DB74D1 5E805BA7
      F1462599 5CA77612 B2EF7A05 863699EC BABF70D3 D422C014
```

```
  ------------
  s is
                                          A4E6B504 E112C915
        DEF15EB4 EB78EB3E 722E248E 82B9F810 C666C984 E43F0FCF


rnd_val is
                                 56ECA61C 64F69C1C 232E9926
        23C71418 BD0B96D7 83118FAA D94A09E3 A9DB74D1 5E805BA7
        F1462599 5CA77612 B2EF7A05 863699EC BABF70D3 D422C014


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

DualEC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                        00010203 04050607 08090A0B 0C0D0E0F


    EntropyInput1 (for Reseed1) =
                        80818283 84858687 88898A8B 8C8D8E8F


    EntropyInput2 (for Reseed2) =
                        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Nonce =
                                          20212223 24252627


    PersonalizationString = <empty>

    AdditionalInput1  =
                        60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput2  =
                        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
```

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

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

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                          00010203 04050607 08090A0B 0C0D0E0F


    nonce is
                                             20212223 24252627


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                       01 00000100
        00010203 04050607 08090A0B 0C0D0E0F 20212223 24252627


    Hash(counter||no_of_bits_to_return||input_string) is
                                             F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


    temp =
                                             F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A


s is
                                             F5FDB798 B2D55288
        E2DCB3DD 0CB6AE50 7BBE0919 4DB8F472 30850073 12B09C4A
```

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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F


    requested_number_of_bits is 480
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                          80818283 84858687 88898A8B 8C8D8E8F


    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F


  Hash_df()
  ----------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 F5FDB798 B2D55288 E2DCB3DD 0CB6AE50
        7BBE0919 4DB8F472 30850073 12B09C4A 80818283 84858687
        88898A8B 8C8D8E8F 60616263 64656667 68696A6B 6C6D6E6F


    Hash(counter||no_of_bits_to_return||input_string) is
                                             8100942E F294225C
        24D0CCF5 5840770F 814EC45C F6A0BB36 28263FE8 099B1D1F
```

```
    temp =
                                                8100942E F294225C
        24D0CCF5 5840770F 814EC45C F6A0BB36 28263FE8 099B1D1F


s is
                                                8100942E F294225C
        24D0CCF5 5840770F 814EC45C F6A0BB36 28263FE8 099B1D1F


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                                8100942E F294225C
        24D0CCF5 5840770F 814EC45C F6A0BB36 28263FE8 099B1D1F


  s is
                                                60D7E8F7 CB33C5A5
        2D090E43 BD26A3EA 5764CFB2 E6CF4743 0AF74DF5 A28AAC59


  r is
                                                5B1FA5C3 97DFEB54
        0E86F047 0E9625D5 C5AC2D50 016FB201 E8DF574F 2201DFBB


  ------------
  tmp is
                                                    A5C3 97DFEB54
        0E86F047 0E9625D5 C5AC2D50 016FB201 E8DF574F 2201DFBB


  ------------
  i=1
  t is
                                                60D7E8F7 CB33C5A5
        2D090E43 BD26A3EA 5764CFB2 E6CF4743 0AF74DF5 A28AAC59
```

```
  s is
                                          06288C70 188402B0
        14887772 4B477EBD 40E62110 6270CBA6 5792C2D2 847C86AD


  r is
                                          B38242A7 99FEB9E2
        38AAD301 A4933822 50EEE60D 2E2927E5 00E848E5 7535ABD1


  ------------
  tmp is
                                  A5C397DF EB540E86 F0470E96
        25D5C5AC 2D50016F B201E8DF 574F2201 DFBB42A7 99FEB9E2
        38AAD301 A4933822 50EEE60D 2E2927E5 00E848E5 7535ABD1


  ------------
  s is
                                          93EF7B5F 358590E4
        E6DF5A98 94678FEE 009123B7 88483A68 7EE6D629 2928B3DD


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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
                        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    requested_number_of_bits is 480
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
```

```
    additional_input is
                          A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 93EF7B5F 358590E4 E6DF5A98 94678FEE
        009123B7 88483A68 7EE6D629 2928B3DD C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    Hash(counter||no_of_bits_to_return||input_string) is
                                             186A98AB 693C65C1
        D5196A10 703A89C9 5D1E25C8 B21849D2 8D09D987 C2C6BA44


    temp =
                                             186A98AB 693C65C1
        D5196A10 703A89C9 5D1E25C8 B21849D2 8D09D987 C2C6BA44


s is
                                             186A98AB 693C65C1
        D5196A10 703A89C9 5D1E25C8 B21849D2 8D09D987 C2C6BA44


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                             186A98AB 693C65C1
        D5196A10 703A89C9 5D1E25C8 B21849D2 8D09D987 C2C6BA44
```

```
s is
                                        3980714F B4C5ED77
      5AF5E80E 5B1D3EB2 D8018EDE 95222FAD 2C203151 D7E2CC8F


r is
                                        222ABF98 94630BEB
      AF0A0EDF E726285E B055FD2E D678B766 73803DD3 27F49DBE


------------
tmp is
                                            BF98 94630BEB
      AF0A0EDF E726285E B055FD2E D678B766 73803DD3 27F49DBE


------------
i=1
t is
                                        3980714F B4C5ED77
      5AF5E80E 5B1D3EB2 D8018EDE 95222FAD 2C203151 D7E2CC8F


s is
                                        A99DFD75 FEA1F1EA
      03A4937F A040781B 06568FA5 46B0C859 F246C3BE 02910AE0


r is
                                        AE6BDE87 D3E447A6
      EB73B5D5 C52A4007 8132677F 412E9E7D E32B9B1C B32421B9


------------
tmp is
                                BF989463 0BEBAF0A 0EDFE726
      285EB055 FD2ED678 B7667380 3DD327F4 9DBEDE87 D3E447A6
      EB73B5D5 C52A4007 8132677F 412E9E7D E32B9B1C B32421B9


------------
s is
                                        CE70C30B ECC61502
      548EE461 F9A4F714 433B4A07 541F6823 44FBEF3A 9E1A9827
```

```
rnd_val is
                                BF989463 0BEBAF0A 0EDFE726
        285EB055 FD2ED678 B7667380 3DD327F4 9DBEDE87 D3E447A6
        EB73B5D5 C52A4007 8132677F 412E9E7D E32B9B1C B32421B9


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

DualEC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                        00010203 04050607 08090A0B 0C0D0E0F


    EntropyInput1 (for Reseed1) =
                        80818283 84858687 88898A8B 8C8D8E8F


    EntropyInput2 (for Reseed2) =
                        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Nonce =
                                            20212223 24252627


    PersonalizationString =
                        40414243 44454647 48494A4B 4C4D4E4F


    AdditionalInput = <empty>

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

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

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
```

```
                        00010203 04050607 08090A0B 0C0D0E0F


    nonce is
                                             20212223 24252627


    personal_str is
                        40414243 44454647 48494A4B 4C4D4E4F


    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 00010203 04050607 08090A0B 0C0D0E0F
        20212223 24252627 40414243 44454647 48494A4B 4C4D4E4F


    Hash(counter||no_of_bits_to_return||input_string) is
                                             48306692 AF00A3F6
        1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


    temp =
                                             48306692 AF00A3F6
        1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


s is
                                             48306692 AF00A3F6
        1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


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

First call to Generate

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

```
DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                          80818283 84858687 88898A8B 8C8D8E8F


    additional_input is  <empty>

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                   01 00000100
        48306692 AF00A3F6 1184864D E183FAB1 E66C0749 9CCD9849
        BF78F873 785EDCB3 80818283 84858687 88898A8B 8C8D8E8F


    Hash(counter||no_of_bits_to_return||input_string) is
                                            B8F6A9DD 0AB21123
        FCC40457 1E90FECF AD3F2412 41C15577 DBA50C9F A888E37B


    temp =
                                            B8F6A9DD 0AB21123
        FCC40457 1E90FECF AD3F2412 41C15577 DBA50C9F A888E37B


s is
                                            B8F6A9DD 0AB21123
        FCC40457 1E90FECF AD3F2412 41C15577 DBA50C9F A888E37B
```

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                            B8F6A9DD 0AB21123
        FCC40457 1E90FECF AD3F2412 41C15577 DBA50C9F A888E37B


  s is
                                            1C8D0AC6 6A850666
        4E70CC42 23F109BC D3B1DA1F 531D9E50 92D9C5A0 40781E73


  r is
                                            FCF84A5C 82ADD86A
        FFB9F9FD 7597BC59 532F767E ED26547E EB072586 BBF9D540


  ------------
  tmp is
                                                4A5C 82ADD86A
        FFB9F9FD 7597BC59 532F767E ED26547E EB072586 BBF9D540


  ------------
  i=1
  t is
                                            1C8D0AC6 6A850666
        4E70CC42 23F109BC D3B1DA1F 531D9E50 92D9C5A0 40781E73


  s is
                                            32F03EEE 59A6862A
        88FC0490 49F2695B F6DD969D 10758C41 79DC8269 5EE19749


  r is
                                            6D18F5AC 80C2F1D9
        167CA3AD A2ABFF91 96501175 9F68581C B49F3DD9 01D9B16F
```

```
  ------------
  tmp is
                                  4A5C82AD D86AFFB9 F9FD7597
        BC59532F 767EED26 547EEB07 2586BBF9 D540F5AC 80C2F1D9
        167CA3AD A2ABFF91 96501175 9F68581C B49F3DD9 01D9B16F


  ------------
  s is
                                            B9B256D0 F088A9D2
        CDE0CD8D C50D3F2E D5BDC632 14352901 2FF690C6 36797F58


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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                          C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    additional_input is  <empty>

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                  01 00000100
```

```
        B9B256D0 F088A9D2 CDE0CD8D C50D3F2E D5BDC632 14352901
        2FF690C6 36797F58 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Hash(counter||no_of_bits_to_return||input_string) is
                                            03D8AA3A 8D6D46E7
        2E5AE8CB E0BB2835 76DD4669 FABEA280 31F69B38 2699E320


    temp =
                                            03D8AA3A 8D6D46E7
        2E5AE8CB E0BB2835 76DD4669 FABEA280 31F69B38 2699E320


s is
                                            03D8AA3A 8D6D46E7
        2E5AE8CB E0BB2835 76DD4669 FABEA280 31F69B38 2699E320


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                            03D8AA3A 8D6D46E7
        2E5AE8CB E0BB2835 76DD4669 FABEA280 31F69B38 2699E320


  s is
                                            32207F17 5B02FA3E
        BCC9F293 B3FE074D DEDA6D7E AC481615 B8A1C460 CE1B41A8


  r is
                                            D01B37AA 3C613D8A
        E18A3F78 09F8C702 03E93952 7C70A559 434FE57C 4D62C3FC


  ------------
  tmp is
                                                37AA 3C613D8A
```

```
      E18A3F78 09F8C702 03E93952 7C70A559 434FE57C 4D62C3FC


  ------------
  i=1
  t is
                                           32207F17 5B02FA3E
      BCC9F293 B3FE074D DEDA6D7E AC481615 B8A1C460 CE1B41A8


  s is
                                           C4944CAF F5F32BF2
      D004209A 66482C57 D3345F67 C01F647F 5C249681 F66FA94F


  r is
                                           E28442FD 4F6F3479
      97B563EE E9AE1163 AC05022F 5A12CF16 E22680BF E53CAD8C


  ------------
  tmp is
                                  37AA3C61 3D8AE18A 3F7809F8
      C70203E9 39527C70 A559434F E57C4D62 C3FC42FD 4F6F3479
      97B563EE E9AE1163 AC05022F 5A12CF16 E22680BF E53CAD8C


  ------------
  s is
                                           FD9CECE2 7535A492
      0232C4AA F84D4474 D36A93C5 186F71C4 E2997909 3F8471E9


rnd_val is
                                  37AA3C61 3D8AE18A 3F7809F8
      C70203E9 39527C70 A559434F E57C4D62 C3FC42FD 4F6F3479
      97B563EE E9AE1163 AC05022F 5A12CF16 E22680BF E53CAD8C


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

DualEC_DRBG

    Requested Security Strength = 128

    Requested Hash Algorithm = SHA-256
```

```
    prediction_resistance_flag = "ENABLED"
    EntropyInput =
                         00010203 04050607 08090A0B 0C0D0E0F


    EntropyInput1 (for Reseed1) =
                         80818283 84858687 88898A8B 8C8D8E8F


    EntropyInput2 (for Reseed2) =
                         C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    Nonce =
                                             20212223 24252627


    PersonalizationString =
                         40414243 44454647 48494A4B 4C4D4E4F


    AdditionalInput1  =
                         60616263 64656667 68696A6B 6C6D6E6F


    AdditionalInput2  =
                         A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


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

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

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
                         00010203 04050607 08090A0B 0C0D0E0F


    nonce is
                                             20212223 24252627


    personal_str is
                         40414243 44454647 48494A4B 4C4D4E4F
```

```
    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 00010203 04050607 08090A0B 0C0D0E0F
        20212223 24252627 40414243 44454647 48494A4B 4C4D4E4F


    Hash(counter||no_of_bits_to_return||input_string) is
                                            48306692 AF00A3F6
        1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


    temp =
                                            48306692 AF00A3F6
        1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


s is
                                            48306692 AF00A3F6
        1184864D E183FAB1 E66C0749 9CCD9849 BF78F873 785EDCB3


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F


    requested_number_of_bits is 480
Generate FAILED: Reseed is required
```

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

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                          80818283 84858687 88898A8B 8C8D8E8F


    additional_input is
                          60616263 64656667 68696A6B 6C6D6E6F


  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 48306692 AF00A3F6 1184864D E183FAB1
        E66C0749 9CCD9849 BF78F873 785EDCB3 80818283 84858687
        88898A8B 8C8D8E8F 60616263 64656667 68696A6B 6C6D6E6F


    Hash(counter||no_of_bits_to_return||input_string) is
                                              5D43947D 5BD466C7
        53E20C75 14AA8A14 3CE6D37F 5ED751D2 0797BAB3 56BB2B51


    temp =
                                              5D43947D 5BD466C7
        53E20C75 14AA8A14 3CE6D37F 5ED751D2 0797BAB3 56BB2B51


s is
                                              5D43947D 5BD466C7
        53E20C75 14AA8A14 3CE6D37F 5ED751D2 0797BAB3 56BB2B51


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>
```

```
  requested_number_of_bits is 480
------------
i=0
t is
                                          5D43947D 5BD466C7
      53E20C75 14AA8A14 3CE6D37F 5ED751D2 0797BAB3 56BB2B51


s is
                                          EC1BBA64 B4505E98
      D12175B6 A4083728 35373206 BB3BFD35 CAEC666F 4666CDDF


r is
                                          0B9FBA81 AD8C5F06
      ED4A785D E6CD736D 65E554EB E620033F 6F0E5488 140D064D


------------
tmp is
                                              BA81 AD8C5F06
      ED4A785D E6CD736D 65E554EB E620033F 6F0E5488 140D064D


------------
i=1
t is
                                          EC1BBA64 B4505E98
      D12175B6 A4083728 35373206 BB3BFD35 CAEC666F 4666CDDF


s is
                                          1AE0ECE9 63EF66BC
      84E9DB9E 71DB018A E898F1AD 3E23D1AD B1EC7F25 F2D29115


r is
                                          8805351C AA3EAB50
      306CA8CF D682472D D3EEEFD5 DD7E7742 C9EAB9AE 0BEDF69D


------------
tmp is
                                 BA81AD8C 5F06ED4A 785DE6CD
      736D65E5 54EBE620 033F6F0E 5488140D 064D351C AA3EAB50
```

```
        306CA8CF D682472D D3EEEFD5 DD7E7742 C9EAB9AE 0BEDF69D


  ------------
  s is
                                            42751559 C0AB1C14
        6C572FCD C3759E34 82EF69EB E632DFA8 6256E0B9 915ED67F


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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
                         A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    requested_number_of_bits is 480
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                         C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF


    additional_input is
                         A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


  Hash_df()
  ---------------------------
    no_of_bits_to_return = 256

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

    i = 1

    counter||no_of_bits_to_return||input_string is
              01 00000100 42751559 C0AB1C14 6C572FCD C3759E34
        82EF69EB E632DFA8 6256E0B9 915ED67F C0C1C2C3 C4C5C6C7
```

```
        C8C9CACB CCCDCECF A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF


    Hash(counter||no_of_bits_to_return||input_string) is
                                            A1BDA7BF 75E06332
        6F58AFFD 08370308 B74A7FEB 41236318 A7F7525D FA858B4F


    temp =
                                            A1BDA7BF 75E06332
        6F58AFFD 08370308 B74A7FEB 41236318 A7F7525D FA858B4F


s is
                                            A1BDA7BF 75E06332
        6F58AFFD 08370308 B74A7FEB 41236318 A7F7525D FA858B4F


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 480
  ------------
  i=0
  t is
                                            A1BDA7BF 75E06332
        6F58AFFD 08370308 B74A7FEB 41236318 A7F7525D FA858B4F


  s is
                                            49D25672 4DCFA4D8
        4FD10072 AEC159C9 B8EFAC1D 9068784F 1ED562D4 84BA81FF


  r is
                                            4AA4BB9C 38A24410
        25BEBD6C 20EC630B D26F8AF5 E92D5B10 1F9F3609 F2AD30D7


  ------------
  tmp is
                                                BB9C 38A24410
        25BEBD6C 20EC630B D26F8AF5 E92D5B10 1F9F3609 F2AD30D7
```

```
  ------------
  i=1
  t is
                                          49D25672 4DCFA4D8
        4FD10072 AEC159C9 B8EFAC1D 9068784F 1ED562D4 84BA81FF


  s is
                                          361AEC57 BD228951
        E38E5D67 F9A43BFB 1D79389E 88C1394E A33DF322 8C27D415


  r is
                                          1751F982 A78DFA43
        DAAB53ED B2C14F41 2BB5DD2D B7FB2123 B313A40D 934F775C


  ------------
  tmp is
                                 BB9C38A2 441025BE BD6C20EC
        630BD26F 8AF5E92D 5B101F9F 3609F2AD 30D7F982 A78DFA43
        DAAB53ED B2C14F41 2BB5DD2D B7FB2123 B313A40D 934F775C


  ------------
  s is
                                          70E9DD58 60AB91BF
        92E743C3 FAFC74A3 8D39FD77 04091EE9 B0F6C5F1 F4B26B71


rnd_val is
                                 BB9C38A2 441025BE BD6C20EC
        630BD26F 8AF5E92D 5B101F9F 3609F2AD 30D7F982 A78DFA43
        DAAB53ED B2C14F41 2BB5DD2D B7FB2123 B313A40D 934F775C
```

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

DualEC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


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


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput = <empty>

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

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

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"
```

```
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                        01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B


    Hash(counter||no_of_bits_to_return||input_string) is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


    temp =
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


s is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916
```

```
s is
      F2FC3FD8 D0AA88D4 72FB707A 21BE6746 3E2DE7DF 74064A88
      C8164CAE FE7C8610 843DFCC6 FE485BF4 6B9E4EDF A27F5DCC


r is
      8A671F85 8858B653 57D6360E 1ED8F847 5767B08D AB30718C
      CA01C6FA E77A4BDC E2702C76 D0FB4758 EA1ED6AA 587CFD26


------------
tmp is
          1F85 8858B653 57D6360E 1ED8F847 5767B08D AB30718C
      CA01C6FA E77A4BDC E2702C76 D0FB4758 EA1ED6AA 587CFD26


------------
i=1
t is
      F2FC3FD8 D0AA88D4 72FB707A 21BE6746 3E2DE7DF 74064A88
      C8164CAE FE7C8610 843DFCC6 FE485BF4 6B9E4EDF A27F5DCC


s is
      8207B70B 4C1E9251 0BB3A9B0 1B6AA417 B13C9209 9DF08249
      72E8E211 53A3C3A4 C5A9F26C A1534212 5325C40F BE945C2C


r is
      7D59B901 1DC8A75D 0B415419 3BB2C179 8FFA52BC AB208310
      3CD2AAD4 4BEED56D 042FC2B8 915D7D9B ED6437EF EB1582EE


------------
tmp is
               1F858858 B65357D6 360E1ED8 F8475767 B08DAB30
      718CCA01 C6FAE77A 4BDCE270 2C76D0FB 4758EA1E D6AA587C
      FD26B901 1DC8A75D 0B415419 3BB2C179 8FFA52BC AB208310
      3CD2AAD4 4BEED56D 042FC2B8 915D7D9B ED6437EF EB1582EE


------------
s is
      44BF1783 A6B7894D C897B34B 3BC6EDD7 413A1F6C 7E88D519
      D9ED2E36 A425BF36 E198FBC6 9B648DA9 D963E3B9 FAE2C447
```

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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        44BF1783 A6B7894D C897B34B 3BC6EDD7 413A1F6C 7E88D519
        D9ED2E36 A425BF36 E198FBC6 9B648DA9 D963E3B9 FAE2C447


  s is
        70053ED7 AA7B499D AE7C42C1 165EF827 CDA13E2B C0D168C2
        A7DB64B1 681135C9 0A5CFB5A 8323AF2B 7B3FE552 7ABE627D


  r is
        A3486E4A AB639382 12C870F2 4BB067A3 2CA9E7FC 23435D41
        1729268C 8BA6F90E 87074D04 888CE2CC 5A916B7A C93FEDE8


  ------------
  tmp is
            6E4A AB639382 12C870F2 4BB067A3 2CA9E7FC 23435D41
        1729268C 8BA6F90E 87074D04 888CE2CC 5A916B7A C93FEDE8


  ------------
  i=1
  t is
        70053ED7 AA7B499D AE7C42C1 165EF827 CDA13E2B C0D168C2
        A7DB64B1 681135C9 0A5CFB5A 8323AF2B 7B3FE552 7ABE627D


  s is
        806E73C1 4153EEA2 4956B2DD CB071E7A 3EC380AF 7B0B58D3
        E628559E 93A0CB03 7D7AFF79 14E4FE5F BAB17979 F2B1EADA
```

```
  r is
        0FE65E29 95645DFC C4CE44B9 FB41F1BF CC5E9F59 EE3A8E1B
        8F85247F 741B7C48 0521EE6B F8BA319B 59048E65 F08FAA76


  ------------
  tmp is
                 6E4AAB63 938212C8 70F24BB0 67A32CA9 E7FC2343
        5D411729 268C8BA6 F90E8707 4D04888C E2CC5A91 6B7AC93F
        EDE85E29 95645DFC C4CE44B9 FB41F1BF CC5E9F59 EE3A8E1B
        8F85247F 741B7C48 0521EE6B F8BA319B 59048E65 F08FAA76


  ------------
  s is
        40199D10 CB37B6DA 8430A41D 0453374C 1E961A2C 5BB7941A
        007CAE18 B0E9B553 603D85BC 18FBEA1C CD108F85 F7B94BDC


rnd_val is
                 6E4AAB63 938212C8 70F24BB0 67A32CA9 E7FC2343
        5D411729 268C8BA6 F90E8707 4D04888C E2CC5A91 6B7AC93F
        EDE85E29 95645DFC C4CE44B9 FB41F1BF CC5E9F59 EE3A8E1B
        8F85247F 741B7C48 0521EE6B F8BA319B 59048E65 F08FAA76


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

DualEC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


    EntropyInput2 (for Reseed2) =
```

```
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput1  =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    AdditionalInput2  =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


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

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

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                        01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


    temp =
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


s is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    requested_number_of_bits is 736
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                  01 00000180
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    Hash(counter||no_of_bits_to_return||input_string) is
        1DF233C6 2DC2E629 D1255A25 0E87BED1 B26E6ADA D1DE4DE7
        0D84A331 AE09EA46 4A626E6A 3EE7E31F B2E9D581 60C62506
```

```
  temp =
      1DF233C6 2DC2E629 D1255A25 0E87BED1 B26E6ADA D1DE4DE7
      0D84A331 AE09EA46 4A626E6A 3EE7E31F B2E9D581 60C62506


------------
i=0
t is
      EE101B0B 1F2D06C8 DE9E66A1 687EB4B1 932C985A 23FB87A2
      75086936 30431DB3 067DC37A 866FFCA0 57E552C9 66256C10


s is
      87B2F560 6E29B0FB BE43F68C CB66808C 55BFFE7C 67E8D6DF
      D011E9A3 9172614F 25F2DDCD 18F3BB4B 0EFB359C FDC05D18


r is
      E513F534 620C9FAC A8B7A7D5 0285FAF4 C29128EC 622A4B49
      EA3AB8C9 056F5019 42534953 4B00B72E 1D870CF7 8B4ACF53


------------
tmp is
          F534 620C9FAC A8B7A7D5 0285FAF4 C29128EC 622A4B49
      EA3AB8C9 056F5019 42534953 4B00B72E 1D870CF7 8B4ACF53


------------
i=1
t is
      87B2F560 6E29B0FB BE43F68C CB66808C 55BFFE7C 67E8D6DF
      D011E9A3 9172614F 25F2DDCD 18F3BB4B 0EFB359C FDC05D18


s is
      00769F7D 31700CBE D808128B 02C74C06 B5F92312 289EAF03
      E96AAFDF CDF9D248 0CAE4ED5 682E8C5E D2BCFB9B A49C096A


r is
      806D75C2 FEF7E440 92697D96 9AE3C3DB 909AF09D 1D87587B
      30AADF5D F9B9F14F 549A0871 00A0137C 16DFB4A6 12C2AA0E
```

```
  ------------
  tmp is
                 F534620C 9FACA8B7 A7D50285 FAF4C291 28EC622A
        4B49EA3A B8C9056F 50194253 49534B00 B72E1D87 0CF78B4A
        CF5375C2 FEF7E440 92697D96 9AE3C3DB 909AF09D 1D87587B
        30AADF5D F9B9F14F 549A0871 00A0137C 16DFB4A6 12C2AA0E


  ------------
  s is
        258B2AC7 FC3CDBC9 74089A54 2B1FF289 13B97D01 8253BDF3
        BE28A9A8 85801E9A 66387D12 4F0ADCA5 B3631A44 B48AAC5F


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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


    requested_number_of_bits is 736
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                  01 00000180
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


    Hash(counter||no_of_bits_to_return||input_string) is
        46EE6038 F6F0DC33 FBF6BA3D 19141D5A 2DBF240D 7D9D85F6
        0DB6BC42 6ABCFC8F D5171DFD A919A2FA 3100054B 9B0B4CC1
```

```
  temp =
      46EE6038 F6F0DC33 FBF6BA3D 19141D5A 2DBF240D 7D9D85F6
      0DB6BC42 6ABCFC8F D5171DFD A919A2FA 3100054B 9B0B4CC1


------------
i=0
t is
      63654AFF 0ACC07FA 8FFE2069 320BEFD3 3E06590C FFCE3805
      B39E15EA EF3CE215 B32F60EF E6137E5F 82631F0F 2F81E09E


s is
      0FDAB8E7 D5D67674 E92EF0DA B3EA6E7F 9CA8AE18 8922A917
      18BE1476 B0097C2D 5A546D47 F7888B32 383F1219 68811459


r is
      386F8018 59605617 F9B9CC4D 484E85F5 FD7DEF0A 6E0AECA4
      1D6E523C E4985928 C60D5E1C 41DF06BA 64987967 1A98AB43


------------
tmp is
          8018 59605617 F9B9CC4D 484E85F5 FD7DEF0A 6E0AECA4
      1D6E523C E4985928 C60D5E1C 41DF06BA 64987967 1A98AB43


------------
i=1
t is
      0FDAB8E7 D5D67674 E92EF0DA B3EA6E7F 9CA8AE18 8922A917
      18BE1476 B0097C2D 5A546D47 F7888B32 383F1219 68811459


s is
      CE5F019A F577B9A1 B9FC7444 BE896F31 DCA8C513 48376D40
      6CA03A30 6F3C6507 F4B2F020 B2E10A20 957D352F 8F158416


r is
      3D36843F 80BFDFC6 8F614439 5D1698D6 8FCDA6C0 800345DB
      DBA6689C 33BA050A 1F1EA52F EB649A62 9328CC53 6F711B7C


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

```
  tmp is
                80185960 5617F9B9 CC4D484E 85F5FD7D EF0A6E0A
        ECA41D6E 523CE498 5928C60D 5E1C41DF 06BA6498 79671A98
        AB43843F 80BFDFC6 8F614439 5D1698D6 8FCDA6C0 800345DB
        DBA6689C 33BA050A 1F1EA52F EB649A62 9328CC53 6F711B7C


  ------------
  s is
        64508503 BCF8F875 F5D5E5D4 B66E9377 D631405D 5AAD357E
        062EE7D3 384E5FE5 E4BCB1A6 630A0353 003A3320 E1ABBAA6


rnd_val is
                80185960 5617F9B9 CC4D484E 85F5FD7D EF0A6E0A
        ECA41D6E 523CE498 5928C60D 5E1C41DF 06BA6498 79671A98
        AB43843F 80BFDFC6 8F614439 5D1698D6 8FCDA6C0 800345DB
        DBA6689C 33BA050A 1F1EA52F EB649A62 9328CC53 6F711B7C


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

DualEC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


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


    Nonce =
                                20212223 24252627 28292A2B


    PersonalizationString =
```

```
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    AdditionalInput = <empty>

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

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

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    prediction_resistance_flag = "No PredictionResistance"

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                        01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    Hash(counter||no_of_bits_to_return||input_string) is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


    temp =
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
```

```
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


s is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


  s is
        A2E1B617 1D631A2E A0363469 64A650F1 A7748CEE 97D5F3DD
        767CACD2 03A40682 FE5DF995 611FFEBF E1A48917 14850D3A


  r is
        5A30E6A3 0AB0C9AF CBA673E4 F1C94B3D B1F0C7D7 8B3D87B9
        67281BE1 E7B3CAF5 200AED50 2C26B84F C169FE83 36BD2327


  ------------
  tmp is
            E6A3 0AB0C9AF CBA673E4 F1C94B3D B1F0C7D7 8B3D87B9
        67281BE1 E7B3CAF5 200AED50 2C26B84F C169FE83 36BD2327


  ------------
  i=1
  t is
        A2E1B617 1D631A2E A0363469 64A650F1 A7748CEE 97D5F3DD
```

```
        767CACD2 03A40682 FE5DF995 611FFEBF E1A48917 14850D3A


  s is
        029B765D EFF6471C FCB50530 1F748D1F 11EBE53C B56900A4
        9D3C6F8C 3F196E53 1C7B9640 7005D201 956DCC57 0EFC0195


  r is
        21F81CB2 99812F2C F1955AA6 3FC36204 4ABA246E F1610F9E
        DC613924 A84A00F8 DB3FC65C 13373F31 71EB2084 8FA9A70E


  ------------
  tmp is
                 E6A30AB0 C9AFCBA6 73E4F1C9 4B3DB1F0 C7D78B3D
        87B96728 1BE1E7B3 CAF5200A ED502C26 B84FC169 FE8336BD
        23271CB2 99812F2C F1955AA6 3FC36204 4ABA246E F1610F9E
        DC613924 A84A00F8 DB3FC65C 13373F31 71EB2084 8FA9A70E


  ------------
  s is
        6D96C3E9 B559B30B 765BF521 DB141F82 AF8092EE DD2A8052
        6069A452 D623ABAE 3696A224 8F509BB0 738885F2 6F0DC48A


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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        6D96C3E9 B559B30B 765BF521 DB141F82 AF8092EE DD2A8052
        6069A452 D623ABAE 3696A224 8F509BB0 738885F2 6F0DC48A


  s is
```

```
      3B5154FD FE0EEB95 401DF1A4 81528DE5 1E3B02D7 2C9EBB24
      EB0037FA 149F11BD F7AB93FE 21D32977 3EA8B3A4 BD9CADE4


r is
      64458585 764DF1C8 6EA12ACC B882525B F6217B44 74865EBF
      DA367B86 57FA8047 1139BAC6 26172B9F 219DF2CE 9099F658


------------
tmp is
          8585 764DF1C8 6EA12ACC B882525B F6217B44 74865EBF
      DA367B86 57FA8047 1139BAC6 26172B9F 219DF2CE 9099F658


------------
i=1
t is
      3B5154FD FE0EEB95 401DF1A4 81528DE5 1E3B02D7 2C9EBB24
      EB0037FA 149F11BD F7AB93FE 21D32977 3EA8B3A4 BD9CADE4


s is
      724C35C6 80ED0254 7B8F134F 7083B917 E1D5F9C1 A0AC5D3A
      692E7AC3 E1BC3300 4C521576 095E230F 04ABE2D4 CDD55CAE


r is
      5CE433E0 7CD1A8DD 80468779 EA3C2662 0A2C9C9F 5C7EFCDD
      C036E6F6 C8BF7031 6D3C37FC 246A4CC7 9B3F1DB9 71D72ED0


------------
tmp is
               8585764D F1C86EA1 2ACCB882 525BF621 7B447486
      5EBFDA36 7B8657FA 80471139 BAC62617 2B9F219D F2CE9099
      F65833E0 7CD1A8DD 80468779 EA3C2662 0A2C9C9F 5C7EFCDD
      C036E6F6 C8BF7031 6D3C37FC 246A4CC7 9B3F1DB9 71D72ED0


------------
s is
      56A02C8F E41C3B1A 9F2D6B6F 418F2F8C 83216C5B 52712185
      38B66E54 D2479749 D22CFE83 5EEF4FC8 3E680A45 4249A567
```

```
rnd_val is
                 8585764D F1C86EA1 2ACCB882 525BF621 7B447486
        5EBFDA36 7B8657FA 80471139 BAC62617 2B9F219D F2CE9099
        F65833E0 7CD1A8DD 80468779 EA3C2662 0A2C9C9F 5C7EFCDD
        C036E6F6 C8BF7031 6D3C37FC 246A4CC7 9B3F1DB9 71D72ED0


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

DualEC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


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


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    AdditionalInput1  =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    AdditionalInput2  =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


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

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

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    nonce is
                                20212223 24252627 28292A2B


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    prediction_resistance_flag = "No PredictionResistance"

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                       01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    Hash(counter||no_of_bits_to_return||input_string) is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


    temp =
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


s is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F
```

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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    requested_number_of_bits is 736
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                  01 00000180
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    Hash(counter||no_of_bits_to_return||input_string) is
        1DF233C6 2DC2E629 D1255A25 0E87BED1 B26E6ADA D1DE4DE7
        0D84A331 AE09EA46 4A626E6A 3EE7E31F B2E9D581 60C62506


    temp =
        1DF233C6 2DC2E629 D1255A25 0E87BED1 B26E6ADA D1DE4DE7
        0D84A331 AE09EA46 4A626E6A 3EE7E31F B2E9D581 60C62506


  ------------
  i=0
  t is
        2747E904 F2CAA5D1 37E5382C 5138CC92 ECD8C298 DEF2700F
        BE87BB43 7AC58E4A 425CE7BD CC79864B FB3C3A48 54D39C59


  s is
        70636843 2A0D70BF 00244A45 E4FEA8C4 28E7D778 344EF939
```

```
      FEE7C4BC D0E50906 BBE5437A AA537741 A5EF3C6E C623E5D0


r is
      D22413F6 EA9BBA7B ABDC2A52 A3B9FD73 D65ECAA6 38A04C74
      BCCA2ACD E6FD29FE A4B5D884 E095E87D 1B7C0DEB 9D377AD8


------------
tmp is
          13F6 EA9BBA7B ABDC2A52 A3B9FD73 D65ECAA6 38A04C74
      BCCA2ACD E6FD29FE A4B5D884 E095E87D 1B7C0DEB 9D377AD8


------------
i=1
t is
      70636843 2A0D70BF 00244A45 E4FEA8C4 28E7D778 344EF939
      FEE7C4BC D0E50906 BBE5437A AA537741 A5EF3C6E C623E5D0


s is
      B2BD4448 6B311865 14EB9217 A0B8C120 9C84F045 2FB4537D
      7C15CD34 875B5FE3 0AB3F82F 2D4FB274 3159BDEC 4FA73C20


r is
      12551FBF EEA2D5EF 82C0F6F5 2B9FCC35 9E769AC9 DF2A876C
      58BAF216 57814F3E 66D1680B 1D4EBD65 581E4253 4F85197D


------------
tmp is
               13F6EA9B BA7BABDC 2A52A3B9 FD73D65E CAA638A0
      4C74BCCA 2ACDE6FD 29FEA4B5 D884E095 E87D1B7C 0DEB9D37
      7AD81FBF EEA2D5EF 82C0F6F5 2B9FCC35 9E769AC9 DF2A876C
      58BAF216 57814F3E 66D1680B 1D4EBD65 581E4253 4F85197D


------------
s is
      17EACDB6 7EC46403 6741189C BFA507A9 57279F54 B089160D
      29D42AB5 19759164 07506EDF EA8BA231 461E73A7 EBAFB1DE


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

```
Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


    requested_number_of_bits is 736
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                  01 00000180
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


    Hash(counter||no_of_bits_to_return||input_string) is
        46EE6038 F6F0DC33 FBF6BA3D 19141D5A 2DBF240D 7D9D85F6
        0DB6BC42 6ABCFC8F D5171DFD A919A2FA 3100054B 9B0B4CC1


    temp =
        46EE6038 F6F0DC33 FBF6BA3D 19141D5A 2DBF240D 7D9D85F6
        0DB6BC42 6ABCFC8F D5171DFD A919A2FA 3100054B 9B0B4CC1


  ------------
  i=0
  t is
        5104AD8E 8834B830 9CB7A2A1 A6B11AF3 7A98BB59 CD1493FB
        246296F7 73C96DEB D2477322 439200CB 771E76EC 70A4FD1F


  s is
        3FD8CA8C BE1597E1 2DC5A32E 35F22DE1 2791DA06 DEC6BB92
        EB6476FE EEDEF970 2601C0E6 FF663F99 8311CFB0 A4C15BE6
```

```
  r is
        2402FC0A 36F4D20F 8F83BE34 30AA3C36 A4919182 1A82072B
        BC3D5AFF 8D7EC394 84D64627 7CE87599 B6FE8CCA 98625597


  ------------
  tmp is
            FC0A 36F4D20F 8F83BE34 30AA3C36 A4919182 1A82072B
        BC3D5AFF 8D7EC394 84D64627 7CE87599 B6FE8CCA 98625597


  ------------
  i=1
  t is
        3FD8CA8C BE1597E1 2DC5A32E 35F22DE1 2791DA06 DEC6BB92
        EB6476FE EEDEF970 2601C0E6 FF663F99 8311CFB0 A4C15BE6


  s is
        80FA1CF8 26484C63 453011FE A35D2396 EA90C79B 59102132
        C03E1CD5 C69AF0CF 19A7F583 9D3DD13A 3D5B7EF2 83E2C69A


  r is
        2E8D03A1 0F4DE106 6BFD30B8 0C325E77 4B512525 BC6D3734
        4C939063 68243D31 F89E99C4 D2A6E9BE B24D5F72 67360DCA


  ------------
  tmp is
                 FC0A36F4 D20F8F83 BE3430AA 3C36A491 91821A82
        072BBC3D 5AFF8D7E C39484D6 46277CE8 7599B6FE 8CCA9862
        559703A1 0F4DE106 6BFD30B8 0C325E77 4B512525 BC6D3734
        4C939063 68243D31 F89E99C4 D2A6E9BE B24D5F72 67360DCA


  ------------
  s is
        39EB1BA2 6F6F487F E07FD5B8 A8A40287 5DB93D9F 6BB0797D
        BC38A71D 68B0CA41 6199DF43 134B881E 6048885B 3C44B5A9


rnd_val is
                 FC0A36F4 D20F8F83 BE3430AA 3C36A491 91821A82
        072BBC3D 5AFF8D7E C39484D6 46277CE8 7599B6FE 8CCA9862
```

```
        559703A1 0F4DE106 6BFD30B8 0C325E77 4B512525 BC6D3734
        4C939063 68243D31 F89E99C4 D2A6E9BE B24D5F72 67360DCA


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

DualEC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


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


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput = <empty>

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

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

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    nonce is
                                    20212223 24252627 28292A2B
```

```
    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                        01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B


    Hash(counter||no_of_bits_to_return||input_string) is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


    temp =
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


s is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
Generate FAILED: Reseed is required
*************************************************************
```

```
DualEC_DRBG_Reseed_algorithm

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


    additional_input is  <empty>

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                  01 00000180
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


    Hash(counter||no_of_bits_to_return||input_string) is
        32FC492B 99BAB8A8 BC3EFEEF F7955E4D 81788F69 1D18801D
        3EA1AD48 17133B8C C0AC41D5 A13C60F2 5D0A8061 6A9D3D81


    temp =
        32FC492B 99BAB8A8 BC3EFEEF F7955E4D 81788F69 1D18801D
        3EA1AD48 17133B8C C0AC41D5 A13C60F2 5D0A8061 6A9D3D81


s is
        32FC492B 99BAB8A8 BC3EFEEF F7955E4D 81788F69 1D18801D
        3EA1AD48 17133B8C C0AC41D5 A13C60F2 5D0A8061 6A9D3D81


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
```

```
------------
i=0
t is
      32FC492B 99BAB8A8 BC3EFEEF F7955E4D 81788F69 1D18801D
      3EA1AD48 17133B8C C0AC41D5 A13C60F2 5D0A8061 6A9D3D81


s is
      CE1E095D 226B5C74 BF3E2ED2 E271DF6C 98214823 D12C9D11
      6DC1E21A 839D7000 3646B810 058ADBAF E3992B68 A713265F


r is
      F6C5CC78 8F70FB08 F256D960 4333630D 85936D40 0F45718D
      C3F939A8 B9F6F75D 3E4EC17D 68FBB924 AEACB702 129548FA


------------
tmp is
          CC78 8F70FB08 F256D960 4333630D 85936D40 0F45718D
      C3F939A8 B9F6F75D 3E4EC17D 68FBB924 AEACB702 129548FA


------------
i=1
t is
      CE1E095D 226B5C74 BF3E2ED2 E271DF6C 98214823 D12C9D11
      6DC1E21A 839D7000 3646B810 058ADBAF E3992B68 A713265F


s is
      4D15B54C F35F02E1 6FFD87A2 7CFA8CDD F663CFD6 EF61087F
      14904E07 E4427164 99937058 5B1388DA 282EF95F 9094A42C


r is
      BFD263CE 9BCB8217 6639B64D E890A470 25B55823 12FE934E
      F0D0A126 97C0F05D 2DA108CC ADB511BA 0EB62F40 51BB2354


------------
tmp is
               CC788F70 FB08F256 D9604333 630D8593 6D400F45
      718DC3F9 39A8B9F6 F75D3E4E C17D68FB B924AEAC B7021295
      48FA63CE 9BCB8217 6639B64D E890A470 25B55823 12FE934E
      F0D0A126 97C0F05D 2DA108CC ADB511BA 0EB62F40 51BB2354
```

```
  ------------
  s is
        51B364B8 88A04C1C 0F03B49E E2936F07 33646485 1330CB1E
        4B3F40EE 4F3C04AC 017D393F 1C571FD0 1028AB62 30ECDA6C


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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    additional_input is  <empty>

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                  01 00000180
        51B364B8 88A04C1C 0F03B49E E2936F07 33646485 1330CB1E
        4B3F40EE 4F3C04AC 017D393F 1C571FD0 1028AB62 30ECDA6C
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
        A981E9D6 AC1C712A 69ED13B6 14E252CC BB65CD75 0C3C66F7
        40613F19 96F2C244 FC301679 449D440C 7D605111 1FE9AC42


    temp =
        A981E9D6 AC1C712A 69ED13B6 14E252CC BB65CD75 0C3C66F7
        40613F19 96F2C244 FC301679 449D440C 7D605111 1FE9AC42


s is
        A981E9D6 AC1C712A 69ED13B6 14E252CC BB65CD75 0C3C66F7
        40613F19 96F2C244 FC301679 449D440C 7D605111 1FE9AC42


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        A981E9D6 AC1C712A 69ED13B6 14E252CC BB65CD75 0C3C66F7
        40613F19 96F2C244 FC301679 449D440C 7D605111 1FE9AC42


  s is
        63AD9407 333FDE6F 1BC287E3 C481A78E 34AD4BE9 EC2F0ACC
        7CDB1D01 87BC6C72 5470BF03 41F2BF72 145B01C2 3ECB7232


  r is
        21C22C92 2EA620D7 6E4137B3 15EBC29E 518F8095 1B3F0E61
        73FA2BFD 94A230EE 513EE2E4 EB330D80 2F620DD2 4911534E


  ------------
  tmp is
            2C92 2EA620D7 6E4137B3 15EBC29E 518F8095 1B3F0E61
        73FA2BFD 94A230EE 513EE2E4 EB330D80 2F620DD2 4911534E


  ------------
  i=1
```

```
  t is
        63AD9407 333FDE6F 1BC287E3 C481A78E 34AD4BE9 EC2F0ACC
        7CDB1D01 87BC6C72 5470BF03 41F2BF72 145B01C2 3ECB7232


  s is
        F0664F09 A819C032 7174D687 859509EF C82AFE96 AD132D70
        7F528B39 AB54103C CC8414E6 E9EE91D9 DD2D5135 08EC7B18


  r is
        9930C0F9 5A1F1D44 A2125F5D 57476A66 6FC37209 2B55D0D6
        8B49738F 5BC466EC 206AB3CF 6A972B38 BCFAE5FC D53C7E21


  ------------
  tmp is
                 2C922EA6 20D76E41 37B315EB C29E518F 80951B3F
        0E6173FA 2BFD94A2 30EE513E E2E4EB33 0D802F62 0DD24911
        534EC0F9 5A1F1D44 A2125F5D 57476A66 6FC37209 2B55D0D6
        8B49738F 5BC466EC 206AB3CF 6A972B38 BCFAE5FC D53C7E21


  ------------
  s is
        62154AE1 587BB30F 09ACF488 9ED4B44C 42C1EEB7 49631CBC
        79BC4F15 6E3A0778 83A6AB20 BEE81B90 787E7696 F1A59CF7


rnd_val is
                 2C922EA6 20D76E41 37B315EB C29E518F 80951B3F
        0E6173FA 2BFD94A2 30EE513E E2E4EB33 0D802F62 0DD24911
        534EC0F9 5A1F1D44 A2125F5D 57476A66 6FC37209 2B55D0D6
        8B49738F 5BC466EC 206AB3CF 6A972B38 BCFAE5FC D53C7E21


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

DualEC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
```

```
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


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


    Nonce =
                                    20212223 24252627 28292A2B


    PersonalizationString = <empty>

    AdditionalInput1  =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    AdditionalInput2  =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


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

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

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    nonce is
                                    20212223 24252627 28292A2B


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 384
```

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                       01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B


    Hash(counter||no_of_bits_to_return||input_string) is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


    temp =
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


s is
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    requested_number_of_bits is 736
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
```

```
    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                  01 00000180
        F3E228CD 32EFE0E1 0FBB3C84 66F90A60 2142F280 F225CA45
        788CCA07 9E4AF7F5 4C1FAD10 B8881FBF E50C8748 06E34916
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    Hash(counter||no_of_bits_to_return||input_string) is
        6F0CF28C 7B226E42 698B1ACF 1FE859B1 9E585D8A CCE91C27
        101AFF9F E6E860EA ED22DEFD 26D9F43D 70EC620B DAA870E3


    temp =
        6F0CF28C 7B226E42 698B1ACF 1FE859B1 9E585D8A CCE91C27
        101AFF9F E6E860EA ED22DEFD 26D9F43D 70EC620B DAA870E3


s is
        6F0CF28C 7B226E42 698B1ACF 1FE859B1 9E585D8A CCE91C27
        101AFF9F E6E860EA ED22DEFD 26D9F43D 70EC620B DAA870E3


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
```

```
      6F0CF28C 7B226E42 698B1ACF 1FE859B1 9E585D8A CCE91C27
      101AFF9F E6E860EA ED22DEFD 26D9F43D 70EC620B DAA870E3


s is
      04184A7A DE35DE09 06BC174C 1DA79FBA FE6AB1E8 5631910D
      38665DD4 08F751E3 3C6A75BB 6AC7E52F 31BA716D B3FBDD67


r is
      7A88FE55 601BF734 49301370 5CCEB76E 44AAD483 73F742E7
      2B83D470 1FA65492 55F1CDE6 21795352 2FF973BA 4F6EC96D


------------
tmp is
          FE55 601BF734 49301370 5CCEB76E 44AAD483 73F742E7
      2B83D470 1FA65492 55F1CDE6 21795352 2FF973BA 4F6EC96D


------------
i=1
t is
      04184A7A DE35DE09 06BC174C 1DA79FBA FE6AB1E8 5631910D
      38665DD4 08F751E3 3C6A75BB 6AC7E52F 31BA716D B3FBDD67


s is
      AC57A08B EDD6099E 1D473001 AD5FE71E 8FB91D2C D851DAF0
      07C078FB B66C5498 20B51779 424742B2 AF3A2F33 B903D91E


r is
      8F6B2BDC F14A76BE 7DEB6178 1E34B993 35BD714F 17C91739
      B4E2AB57 E36E9C31 16E215D3 D94FCFAD 53263687 4875CAC7


------------
tmp is
               FE55601B F7344930 13705CCE B76E44AA D48373F7
      42E72B83 D4701FA6 549255F1 CDE62179 53522FF9 73BA4F6E
      C96D2BDC F14A76BE 7DEB6178 1E34B993 35BD714F 17C91739
      B4E2AB57 E36E9C31 16E215D3 D94FCFAD 53263687 4875CAC7


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

```
  s is
        94110169 CEA534FB B7FE6B2A 5ED5A998 D5E2A707 3D1BD763
        7676242A 8E8B64C5 E49E049B B070B2A4 4CDEDE76 D9E6DA60


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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


    requested_number_of_bits is 736
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                  01 00000180
        94110169 CEA534FB B7FE6B2A 5ED5A998 D5E2A707 3D1BD763
        7676242A 8E8B64C5 E49E049B B070B2A4 4CDEDE76 D9E6DA60
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
        48D959C7 AB3F44CA BB50A056 C5947261 B34EC266 DACE1029
        18A6AFB1 0978C407 9B3C9866 A431182D 0F7415DA D510D1F0


    temp =
        48D959C7 AB3F44CA BB50A056 C5947261 B34EC266 DACE1029
        18A6AFB1 0978C407 9B3C9866 A431182D 0F7415DA D510D1F0


s is
        48D959C7 AB3F44CA BB50A056 C5947261 B34EC266 DACE1029
        18A6AFB1 0978C407 9B3C9866 A431182D 0F7415DA D510D1F0


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        48D959C7 AB3F44CA BB50A056 C5947261 B34EC266 DACE1029
        18A6AFB1 0978C407 9B3C9866 A431182D 0F7415DA D510D1F0


  s is
        F086349E 5D200ACD 3821E708 164EE368 81175E1A 4EA66CF7
        E8C96B8D 8B7E67A0 96533ECD A1D0892E B5FB019D 2091E7A8


  r is
        4B05F5E5 9D0ABADE 81F62FFA B9D4A6A2 6FF20001 6608A721
        5E389858 FFED83FB C75CFD33 DBA6688C 89AA32AD 22E480EA


  ------------
  tmp is
            F5E5 9D0ABADE 81F62FFA B9D4A6A2 6FF20001 6608A721
        5E389858 FFED83FB C75CFD33 DBA6688C 89AA32AD 22E480EA
```

```
  ------------
  i=1
  t is
        F086349E 5D200ACD 3821E708 164EE368 81175E1A 4EA66CF7
        E8C96B8D 8B7E67A0 96533ECD A1D0892E B5FB019D 2091E7A8


  s is
        F0E8044F DB6805D8 6D95CCF3 E00A14D6 EB583EA4 9168F666
        8BE21578 9D7FD0DD F866B894 AFDC9A36 EF8BE64D 3F62996A


  r is
        27563D04 EADFB355 67B67564 207E64B7 7844E8E4 A87502D5
        02DBBB6D 8277F1CA CDB7CF8D 293D09DB 7DD59A95 0821507A


  ------------
  tmp is
                 F5E59D0A BADE81F6 2FFAB9D4 A6A26FF2 00016608
        A7215E38 9858FFED 83FBC75C FD33DBA6 688C89AA 32AD22E4
        80EA3D04 EADFB355 67B67564 207E64B7 7844E8E4 A87502D5
        02DBBB6D 8277F1CA CDB7CF8D 293D09DB 7DD59A95 0821507A


  ------------
  s is
        63B09B71 7CEE9988 D4C20A67 2EF7A070 43114545 49BD6BDA
        008BD303 A227F3E7 4AC2EF83 14B2A36E 5AB44DB7 ED5765FD


rnd_val is
                 F5E59D0A BADE81F6 2FFAB9D4 A6A26FF2 00016608
        A7215E38 9858FFED 83FBC75C FD33DBA6 688C89AA 32AD22E4
        80EA3D04 EADFB355 67B67564 207E64B7 7844E8E4 A87502D5
        02DBBB6D 8277F1CA CDB7CF8D 293D09DB 7DD59A95 0821507A


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

DualEC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384
```

```
    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


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


    Nonce =
                                 20212223 24252627 28292A2B


    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    AdditionalInput = <empty>

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

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

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    nonce is
                                 20212223 24252627 28292A2B


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 384
```

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                       01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    Hash(counter||no_of_bits_to_return||input_string) is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


    temp =
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


s is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
```

```
    additional_input is  <empty>

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                 01 00000180
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


    Hash(counter||no_of_bits_to_return||input_string) is
        DC6F1374 8FEEECE2 3E20DFB3 3F6FD202 6526BF56 506D21AE
        5EBCE30F C3676D44 4DB0324B F6F1326F DA6D1095 C08BE9F5


    temp =
        DC6F1374 8FEEECE2 3E20DFB3 3F6FD202 6526BF56 506D21AE
        5EBCE30F C3676D44 4DB0324B F6F1326F DA6D1095 C08BE9F5


s is
        DC6F1374 8FEEECE2 3E20DFB3 3F6FD202 6526BF56 506D21AE
        5EBCE30F C3676D44 4DB0324B F6F1326F DA6D1095 C08BE9F5


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        DC6F1374 8FEEECE2 3E20DFB3 3F6FD202 6526BF56 506D21AE
        5EBCE30F C3676D44 4DB0324B F6F1326F DA6D1095 C08BE9F5
```

```
s is
      7A5716FE 96AD1AE2 7579A5DC E9446D90 9F04FF26 0E4F719F
      3D7F0EDF C164AEC3 F5074788 DA07A9B6 3BF3149B 239A486C


r is
      97DE7103 B98CEB33 C6199267 23A49B0F E8E80A9E DE9D433A
      519080E6 2344386C 3DCAD93F 72BBAA25 DE7857C1 63AA3669


------------
tmp is
          7103 B98CEB33 C6199267 23A49B0F E8E80A9E DE9D433A
      519080E6 2344386C 3DCAD93F 72BBAA25 DE7857C1 63AA3669


------------
i=1
t is
      7A5716FE 96AD1AE2 7579A5DC E9446D90 9F04FF26 0E4F719F
      3D7F0EDF C164AEC3 F5074788 DA07A9B6 3BF3149B 239A486C


s is
      314CF789 29E60365 7D212745 C19F1BD2 E058506A CF8FDE7D
      E72EFE12 04FE0BA6 9040E57B 5E1E0723 B82272D3 D1B55C02


r is
      095C8643 FEE94B62 610D34B0 6D753350 9D072FB3 3F83F0AD
      CD91CE33 FE65D273 A4515684 DA401FE0 005F44E4 4EB090B0


------------
tmp is
               7103B98C EB33C619 926723A4 9B0FE8E8 0A9EDE9D
      433A5190 80E62344 386C3DCA D93F72BB AA25DE78 57C163AA
      36698643 FEE94B62 610D34B0 6D753350 9D072FB3 3F83F0AD
      CD91CE33 FE65D273 A4515684 DA401FE0 005F44E4 4EB090B0


------------
s is
      1E501974 59C49108 A6542E1F F84A34A1 4918CAB4 F3E623C0
      609C174A 4CDF8E99 E19A3DBD 4735AC17 A5ECF846 E2D620A0
```

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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    additional_input is  <empty>

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                    01 00000180
        1E501974 59C49108 A6542E1F F84A34A1 4918CAB4 F3E623C0
        609C174A 4CDF8E99 E19A3DBD 4735AC17 A5ECF846 E2D620A0
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    Hash(counter||no_of_bits_to_return||input_string) is
        0A20975D E8D09863 134DDC5C 005C8F9C 4011D107 BAF39BBB
        B297BBC3 74484713 8E714B3E D2AF559D 294C6C53 EF714313


    temp =
        0A20975D E8D09863 134DDC5C 005C8F9C 4011D107 BAF39BBB
        B297BBC3 74484713 8E714B3E D2AF559D 294C6C53 EF714313
```

```
s is
        0A20975D E8D09863 134DDC5C 005C8F9C 4011D107 BAF39BBB
        B297BBC3 74484713 8E714B3E D2AF559D 294C6C53 EF714313


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        0A20975D E8D09863 134DDC5C 005C8F9C 4011D107 BAF39BBB
        B297BBC3 74484713 8E714B3E D2AF559D 294C6C53 EF714313


  s is
        A83687F0 1C8C2CD0 B10ED7DF 7E13F0EF C400CB4C 53526AB5
        2F752202 C7371876 DA247179 9759F3E4 82A5863A 49ECA73A


  r is
        C779FA07 A143E761 F3EB103B D499CB9D FDAFA38D 3EF0BB5E
        976BEC85 B5C99230 809FCEB8 F1CAC958 284E603A F32549B2


  ------------
  tmp is
            FA07 A143E761 F3EB103B D499CB9D FDAFA38D 3EF0BB5E
        976BEC85 B5C99230 809FCEB8 F1CAC958 284E603A F32549B2


  ------------
  i=1
  t is
        A83687F0 1C8C2CD0 B10ED7DF 7E13F0EF C400CB4C 53526AB5
        2F752202 C7371876 DA247179 9759F3E4 82A5863A 49ECA73A


  s is
        608EFF3D E73BB7E5 7082495C 6A8DF173 1B73EA1E 606D95E8
```

```
        4DEA5BFD 033255C0 82E615B6 021F5B8B 4D2A2402 D767F601


  r is
        64214F65 38534E26 3F1AB60C FB2D7C68 E573C69C C89B413D
        E5C82713 AE09431C BFE9F234 6F46A72F E5B95685 0A3C9AB1


  ------------
  tmp is
                 FA07A143 E761F3EB 103BD499 CB9DFDAF A38D3EF0
        BB5E976B EC85B5C9 9230809F CEB8F1CA C958284E 603AF325
        49B24F65 38534E26 3F1AB60C FB2D7C68 E573C69C C89B413D
        E5C82713 AE09431C BFE9F234 6F46A72F E5B95685 0A3C9AB1


  ------------
  s is
        E1AC17AF 5A333A4B 7AB0FF6C 1C8A3062 165778AF 8809B3FC
        3F382E08 5BFF098C 8C85546C 2E7056F3 7517BB95 13FC87C0


rnd_val is
                 FA07A143 E761F3EB 103BD499 CB9DFDAF A38D3EF0
        BB5E976B EC85B5C9 9230809F CEB8F1CA C958284E 603AF325
        49B24F65 38534E26 3F1AB60C FB2D7C68 E573C69C C89B413D
        E5C82713 AE09431C BFE9F234 6F46A72F E5B95685 0A3C9AB1


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

DualEC_DRBG

    Requested Security Strength = 192

    Requested Hash Algorithm = SHA-384

    prediction_resistance_flag = "ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
```

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


    Nonce =
                                20212223 24252627 28292A2B


    PersonalizationString =
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    AdditionalInput1  =
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    AdditionalInput2  =
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


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

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

DualEC_DRBG_Instantiate_algorithm

    entropy_input is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617


    nonce is
                                20212223 24252627 28292A2B


    personal_str is
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 384

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

```
    i = 1

    counter||no_of_bits_to_return||input_string is
                       01 00000180 00010203 04050607 08090A0B
        0C0D0E0F 10111213 14151617 20212223 24252627 28292A2B
        40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657


    Hash(counter||no_of_bits_to_return||input_string) is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


    temp =
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


s is
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    requested_number_of_bits is 736
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697


    additional_input is
```

```
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                 01 00000180
        3AB5DAC2 DF0843F8 E6C06209 5FBF7243 5EB6A842 0F2C3DE8
        B3031872 D4CC640C 083E89D7 F29E6554 49D5EFC9 3415B95F
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
        60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677


    Hash(counter||no_of_bits_to_return||input_string) is
        028A28E0 392066C1 C704C425 8A9BB572 6EADB894 6E744A00
        FC69EFEC D4B4C43B 86EE0B0F 661D6820 E9E9BE06 1AFCF90B


    temp =
        028A28E0 392066C1 C704C425 8A9BB572 6EADB894 6E744A00
        FC69EFEC D4B4C43B 86EE0B0F 661D6820 E9E9BE06 1AFCF90B


s is
        028A28E0 392066C1 C704C425 8A9BB572 6EADB894 6E744A00
        FC69EFEC D4B4C43B 86EE0B0F 661D6820 E9E9BE06 1AFCF90B


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        028A28E0 392066C1 C704C425 8A9BB572 6EADB894 6E744A00
        FC69EFEC D4B4C43B 86EE0B0F 661D6820 E9E9BE06 1AFCF90B
```

```
s is
      0D315A80 5EA251EB 10DB2488 2F72A7C5 9586987B 26F4DF57
      25382F25 55689022 A4DBB37D 09573EAF 62FDA1AD 1B522A61


r is
      30289F27 C6E67022 B9B11D86 420CB8A3 DDF58CB2 48CBF202
      1CEC9E02 23B117D7 DB380E7B 79EF871D 0EB6EC7D A1D7DBB7


------------
tmp is
          9F27 C6E67022 B9B11D86 420CB8A3 DDF58CB2 48CBF202
      1CEC9E02 23B117D7 DB380E7B 79EF871D 0EB6EC7D A1D7DBB7


------------
i=1
t is
      0D315A80 5EA251EB 10DB2488 2F72A7C5 9586987B 26F4DF57
      25382F25 55689022 A4DBB37D 09573EAF 62FDA1AD 1B522A61


s is
      147E494E 2408CA55 32EFA7BE 16DA7999 370835A7 D69C8A7A
      DC30EA97 AA03FA57 302EC436 0C697569 8BAA7CA6 03272BD8


r is
      0033CECE 60301506 E0CE12EC 7295620D 3641BE27 BFE2AACA
      E5C02F51 8AAB6B69 AAB3B4FA 95AF8D22 8F81E66E 226FD5C8


------------
tmp is
               9F27C6E6 7022B9B1 1D86420C B8A3DDF5 8CB248CB
      F2021CEC 9E0223B1 17D7DB38 0E7B79EF 871D0EB6 EC7DA1D7
      DBB7CECE 60301506 E0CE12EC 7295620D 3641BE27 BFE2AACA
      E5C02F51 8AAB6B69 AAB3B4FA 95AF8D22 8F81E66E 226FD5C8


------------
s is
      1C3B30AE 6F28022D 658AA75C AE4B533A 6863A914 C136122C
```

```
        C34CA3B3 0ACBE79E E10A2A1C 9D140B49 5C104E9B 4B65F15D


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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


    requested_number_of_bits is 736
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7


    additional_input is
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


  Hash_df()
  ---------------------------
    no_of_bits_to_return = 384

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                                 01 00000180
        1C3B30AE 6F28022D 658AA75C AE4B533A 6863A914 C136122C
        C34CA3B3 0ACBE79E E10A2A1C 9D140B49 5C104E9B 4B65F15D
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
        DBFB441D 9C174B30 30B002C6 8E04D6C0 46BE866E 7FA2D980
        6DB64B62 344878F4 7C264158 565011A3 792B4DDE 119474FD


    temp =
        DBFB441D 9C174B30 30B002C6 8E04D6C0 46BE866E 7FA2D980
        6DB64B62 344878F4 7C264158 565011A3 792B4DDE 119474FD


s is
        DBFB441D 9C174B30 30B002C6 8E04D6C0 46BE866E 7FA2D980
        6DB64B62 344878F4 7C264158 565011A3 792B4DDE 119474FD


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 736
  ------------
  i=0
  t is
        DBFB441D 9C174B30 30B002C6 8E04D6C0 46BE866E 7FA2D980
        6DB64B62 344878F4 7C264158 565011A3 792B4DDE 119474FD


  s is
        1A94EC0E 06333F8C 73285506 0716E5C3 A7B87C64 18D52462
        4E8920D7 7C49B122 7D9F7514 59384FCE 30BF19AC EDABBE0F


  r is
        BBFF821B 7F5B7334 4B4CA9BA EE05AE2B 68280DE4 F6BE2764
        C4337423 0B7C1CAA 22AF5C37 F0350871 B23B1DE3 F36BA487


  ------------
  tmp is
            821B 7F5B7334 4B4CA9BA EE05AE2B 68280DE4 F6BE2764
        C4337423 0B7C1CAA 22AF5C37 F0350871 B23B1DE3 F36BA487


  ------------
  i=1
```

```
  t is
        1A94EC0E 06333F8C 73285506 0716E5C3 A7B87C64 18D52462
        4E8920D7 7C49B122 7D9F7514 59384FCE 30BF19AC EDABBE0F


  s is
        D9D28A06 CCF032B7 615DCBDA CDC61464 F63A9902 AC414A8C
        BA1DE90F 2DC8CE3B 00A65425 24350049 EF92E299 101F5E59


  r is
        B44733D6 039F7482 3B5B1570 23303B6D 5D008392 58345DC8
        9EC3B223 B2992557 823DDA40 DF90436E A1FB45F9 64260014


  ------------
  tmp is
                 821B7F5B 73344B4C A9BAEE05 AE2B6828 0DE4F6BE
        2764C433 74230B7C 1CAA22AF 5C37F035 0871B23B 1DE3F36B
        A48733D6 039F7482 3B5B1570 23303B6D 5D008392 58345DC8
        9EC3B223 B2992557 823DDA40 DF90436E A1FB45F9 64260014


  ------------
  s is
        D102E664 BD76234F D34D8E9D AA3101C5 F69DE66E D97CF85A
        2B27FDB3 28232303 E043E118 46C737CD 9F67C68D D1F693B7


rnd_val is
                 821B7F5B 73344B4C A9BAEE05 AE2B6828 0DE4F6BE
        2764C433 74230B7C 1CAA22AF 5C37F035 0871B23B 1DE3F36B
        A48733D6 039F7482 3B5B1570 23303B6D 5D008392 58345DC8
        9EC3B223 B2992557 823DDA40 DF90436E A1FB45F9 64260014
```

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

DualEC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

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


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


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


    Nonce =
                        20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput = <empty>

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

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

DualEC_DRBG_Instantiate_algorithm

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


    nonce is
                        20212223 24252627 28292A2B 2C2D2E2F
```

```
  personal_str is  <empty>

  prediction_resistance_flag = "No PredictionResistance"

Hash_df()
---------------------------
  no_of_bits_to_return = 521

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

  i = 1

  counter||no_of_bits_to_return||input_string is
                                                  01 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                       E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


  temp =
                       E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


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

  i = 2

  counter||no_of_bits_to_return||input_string is
                                                  02 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                       0BF4E84E 26C435F1 A8C9DDAF B866D3E9
      C7556662 F08A12DA AE1B2239 3FDBEE40 5525C9EB 5A450CF2
      909A7569 FC96F424 56BD7D86 65B70B4D EB24620D FD48A7BF
```

```
    temp =
                    E4CD 803E82C6 D10E8D8F 3E5A2A80 F4A49F5C
        3DE4E594 6995FBE2 131F6A3D AC66DB4D EE1AAC0C 37DABBB3
        1BB5F688 5BF6E94B FB19BD1C D4FCE1D9 68407E2A D9FA0BF4


s is
                      01 C99B007D 058DA21D 1B1E7CB4 5501E949
        3EB87BC9 CB28D32B F7C4263E D47B58CD B69BDC35 58186FB5
        7766376B ED10B7ED D297F633 7A39A9F9 C3B2D080 FC55B3F4


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                    01C9 9B007D05 8DA21D1B 1E7CB455 01E9493E
        B87BC9CB 28D32BF7 C4263ED4 7B58CDB6 9BDC3558 186FB577
        66376BED 10B7EDD2 97F6337A 39A9F9C3 B2D080FC 55B3F417


  s is
                    0184 DFADEDF9 52E25461 BB4AA1BE 30E71E61
        78684D7F E6B3780F FF07BA03 F6DF20C3 AED0F51B C87AF6EC
        BBE2B5B5 5C655A45 9E025132 56DBE4A6 C49D6030 7C083F80


  r is
                    006A 697A8313 798EE1D1 89871268 3F2D0B0D
        EE580414 6ABA64FD A8DB4E53 9CC8D1E5 9C74EE5A A48E73E9
        58C8EC85 DD529D42 E68B4F7E 02FFAF3E 3EF8312A EA68BC08


  ------------
  tmp is
```

```
                        7A8313 798EE1D1 89871268 3F2D0B0D
      EE580414 6ABA64FD A8DB4E53 9CC8D1E5 9C74EE5A A48E73E9
      58C8EC85 DD529D42 E68B4F7E 02FFAF3E 3EF8312A EA68BC08


  ------------
  i=1
  t is
                    0184 DFADEDF9 52E25461 BB4AA1BE 30E71E61
      78684D7F E6B3780F FF07BA03 F6DF20C3 AED0F51B C87AF6EC
      BBE2B5B5 5C655A45 9E025132 56DBE4A6 C49D6030 7C083F80


  s is
                    018C 12DF4800 2EACB926 2FF30ED4 602163F6
      DDAB9311 2D7B4DCE EAD88297 D3CFE0CF D90945EE F01945BE
      D9BDC506 907B28E8 7B999F72 1F739A6E F745BD2A A5BAD725


  r is
                    019C F8A41488 5E60A7DF 0B55F9D9 0210B319
      E9B8FD23 E078A415 3636F29A A3CAC819 8CB1D5D8 46151653
      ECE275A5 91089261 238014E5 05841006 5AB8229E B9115E8E


  ------------
  tmp is
                                              7A83 13798EE1
      D1898712 683F2D0B 0DEE5804 146ABA64 FDA8DB4E 539CC8D1
      E59C74EE 5AA48E73 E958C8EC 85DD529D 42E68B4F 7E02FFAF
      3E3EF831 2AEA68BC 08A41488 5E60A7DF 0B55F9D9 0210B319
      E9B8FD23 E078A415 3636F29A A3CAC819 8CB1D5D8 46151653
      ECE275A5 91089261 238014E5 05841006 5AB8229E B9115E8E


  ------------
  s is
                    00D7 29C6A475 1C7D84A8 D3E87130 520B9A2B
      BAF45403 4BDD399F CFB17E68 4CA699E1 23F5DB62 662800F4
      75A9968C 5B6ADD38 BB881123 82F60261 1129C3A0 337EF399


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

Second call to Generate
```

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                     00D7 29C6A475 1C7D84A8 D3E87130 520B9A2B
        BAF45403 4BDD399F CFB17E68 4CA699E1 23F5DB62 662800F4
        75A9968C 5B6ADD38 BB881123 82F60261 1129C3A0 337EF399


  s is
                     01AB 2E84F361 48B8F19E 32CDC76A DA4B89CF
        4CB51665 03EA392A 694C42D4 EBC5EC40 4002F74F 147310C0
        F19C202B 0B8C723A A80EBE3D 856B9BFC 575CF0CE 4636FE40


  r is
                     0187 19918B5D 79E64664 966D954B C5E2946B
        F48F061B F0C2701C 3C2D1F75 EA821E1D A05D5B3C 2C4EEA24
        6E806B53 BF6BDB3F 3D53A3AE 756C2A45 C7260397 3A3DE1BC


  ------------
  tmp is
                         918B5D 79E64664 966D954B C5E2946B
        F48F061B F0C2701C 3C2D1F75 EA821E1D A05D5B3C 2C4EEA24
        6E806B53 BF6BDB3F 3D53A3AE 756C2A45 C7260397 3A3DE1BC


  ------------
  i=1
  t is
                     01AB 2E84F361 48B8F19E 32CDC76A DA4B89CF
        4CB51665 03EA392A 694C42D4 EBC5EC40 4002F74F 147310C0
        F19C202B 0B8C723A A80EBE3D 856B9BFC 575CF0CE 4636FE40


  s is
                     00F0 1FEAFD93 DE04000C 2A462427 46D650CD
        17630E80 E0C328FB A8B83509 345BBC18 2B3398F5 AC3E08AD
        F104E177 9C7B14D6 9FCC879E DD521C42 0223C48C 0D1D04E1
```

```
  r is
                    01A2 BB367C28 3CA124A5 589CEAB3 0E5D2D74
        8A40DD87 4FF15B03 2CF4F4B2 AAD590B0 DB91A0D3 8FCE93C5
        AAD4E55A C482F86F F06FAE66 B7C7CCA7 E45557E1 A5A3B85D


  ------------
  tmp is
                                                 918B 5D79E646
        64966D95 4BC5E294 6BF48F06 1BF0C270 1C3C2D1F 75EA821E
        1DA05D5B 3C2C4EEA 246E806B 53BF6BDB 3F3D53A3 AE756C2A
        45C72603 973A3DE1 BC367C28 3CA124A5 589CEAB3 0E5D2D74
        8A40DD87 4FF15B03 2CF4F4B2 AAD590B0 DB91A0D3 8FCE93C5
        AAD4E55A C482F86F F06FAE66 B7C7CCA7 E45557E1 A5A3B85D


  ------------
  s is
                    0178 3BF15984 3C3128B6 5859F3FE 386C7626
        17D41636 10290433 2108DC6C 316FAA03 6A07AA57 EE0E1B9B
        F764E118 0F3A2BA1 A6AC29E1 D6A302A0 85508337 38555EE8


rnd_val is
                                                 918B 5D79E646
        64966D95 4BC5E294 6BF48F06 1BF0C270 1C3C2D1F 75EA821E
        1DA05D5B 3C2C4EEA 246E806B 53BF6BDB 3F3D53A3 AE756C2A
        45C72603 973A3DE1 BC367C28 3CA124A5 589CEAB3 0E5D2D74
        8A40DD87 4FF15B03 2CF4F4B2 AAD590B0 DB91A0D3 8FCE93C5
        AAD4E55A C482F86F F06FAE66 B7C7CCA7 E45557E1 A5A3B85D


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

DualEC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

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

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


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


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

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


    AdditionalInput2  =
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

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

DualEC_DRBG_Instantiate_algorithm

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


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "No PredictionResistance"
```

```
Hash_df()
----------------------------
  no_of_bits_to_return = 521

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

  i = 1

  counter||no_of_bits_to_return||input_string is
                                                  01 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                       E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


  temp =
                       E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


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

  i = 2

  counter||no_of_bits_to_return||input_string is
                                                  02 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                       0BF4E84E 26C435F1 A8C9DDAF B866D3E9
      C7556662 F08A12DA AE1B2239 3FDBEE40 5525C9EB 5A450CF2
      909A7569 FC96F424 56BD7D86 65B70B4D EB24620D FD48A7BF


  temp =
                  E4CD 803E82C6 D10E8D8F 3E5A2A80 F4A49F5C
      3DE4E594 6995FBE2 131F6A3D AC66DB4D EE1AAC0C 37DABBB3
```

```
        1BB5F688 5BF6E94B FB19BD1C D4FCE1D9 68407E2A D9FA0BF4


s is
                      01 C99B007D 058DA21D 1B1E7CB4 5501E949
        3EB87BC9 CB28D32B F7C4263E D47B58CD B69BDC35 58186FB5
        7766376B ED10B7ED D297F633 7A39A9F9 C3B2D080 FC55B3F4


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

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


    requested_number_of_bits is 1008
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 521

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 00000209 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    Hash(counter||no_of_bits_to_return||input_string) is
                          DD40BFFA 030E77F8 FA7D9879 56C20710
        375466E8 3CB744D8 C0446A19 281AC290 6B67BD14 F2D61258
        FABDD1B3 26CE70C3 A1598A72 68CCBAA0 8C8A2627 3214342D


    temp =
                          DD40BFFA 030E77F8 FA7D9879 56C20710
        375466E8 3CB744D8 C0446A19 281AC290 6B67BD14 F2D61258
        FABDD1B3 26CE70C3 A1598A72 68CCBAA0 8C8A2627 3214342D
```

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

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 00000209 60616263 64656667
      68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


  Hash(counter||no_of_bits_to_return||input_string) is
                        65976B23 DEBAE6F7 53B1ACC6 F0D9ADCF
      CB60A084 FA65AC58 81966BB9 8CD2EBCD 65575220 B97738B9
      5E3E883D B4078A79 F792E81E D23C19A1 8625F9B2 D681A407


  temp =
                  DD40 BFFA030E 77F8FA7D 987956C2 07103754
      66E83CB7 44D8C044 6A19281A C2906B67 BD14F2D6 1258FABD
      D1B326CE 70C3A159 8A7268CC BAA08C8A 26273214 342D6597


------------
i=0
t is
                  0073 1A7F8903 914DECEF E54C46F8 85E76950
      10B619B2 465A9A77 4CF20C84 4EDDED60 54A61CBD B44B0482
      1D940DA0 8C566A90 24E2D7AB A0DCB8DA A69CCE98 7DDBAEDC


s is
                  0123 1265E5A0 1AC55186 49AF0A53 7B9F1E7F
      CB0068CD 6B8BE36C D18FC8CE 194C5EEC FCEBA029 B45DC1F0
      3438D2F1 5B75E1EF 2C03BB3E EE7B25EF 875D25B5 47D71582


r is
                  012F A2C12142 4391C2D8 C9C494BA 80BB4C14
      CC7BAA11 DA7CBEA8 32635EC5 957C1913 E45A694C 9F33FADD
      FAFAD854 8B6AE7F3 827B9DD5 1A2E89D8 A452E6B1 13A8D437


------------
tmp is
                         C12142 4391C2D8 C9C494BA 80BB4C14
```

```
      CC7BAA11 DA7CBEA8 32635EC5 957C1913 E45A694C 9F33FADD
      FAFAD854 8B6AE7F3 827B9DD5 1A2E89D8 A452E6B1 13A8D437


  ------------
  i=1
  t is
                  0123 1265E5A0 1AC55186 49AF0A53 7B9F1E7F
      CB0068CD 6B8BE36C D18FC8CE 194C5EEC FCEBA029 B45DC1F0
      3438D2F1 5B75E1EF 2C03BB3E EE7B25EF 875D25B5 47D71582


  s is
                  0121 DA398754 ED51D31B BC0E3D9C 25DA44B8
      8C58588D 3EA1BD70 84278D83 3CB75BDB 65938DE9 4C0C917B
      D26F31FE 60CB8611 B7BE8DC4 B9A73D4A BC34A80C D8769F8B


  r is
                  01CE 4D103CEC C778E5F1 5F87C168 B0D3E95D
      E2556C17 141637D9 04F05A3B 6F3B22B5 0B95B06C E82808B0
      6661EFC7 E8B793C5 F05BE585 897BB8EE 32BA550F F8743764


  ------------
  tmp is
                                                C121 424391C2
      D8C9C494 BA80BB4C 14CC7BAA 11DA7CBE A832635E C5957C19
      13E45A69 4C9F33FA DDFAFAD8 548B6AE7 F3827B9D D51A2E89
      D8A452E6 B113A8D4 37103CEC C778E5F1 5F87C168 B0D3E95D
      E2556C17 141637D9 04F05A3B 6F3B22B5 0B95B06C E82808B0
      6661EFC7 E8B793C5 F05BE585 897BB8EE 32BA550F F8743764


  ------------
  s is
                  01E7 96661838 BBFB2277 3A52BF87 9BE0C63B
      AE1A66FA CB0C761A 9361B15E 08E97565 089391BF 274EBDEF
      7A281444 D4D6B492 35A0FA55 D36442EF 4688C9BA D60DB8BB


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

Second call to Generate

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

```
DualEC_DRBG_Generate_algorithm

    additional_input is
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    requested_number_of_bits is 1008
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 521

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 00000209 A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    Hash(counter||no_of_bits_to_return||input_string) is
                           DB75DB8E 03FA70C0 3ECD5F40 1DCE9119
        2CE3529B 213AB30F ED9781FD FB7576AB C820CD47 E953366B
        08CC3413 31C6D719 696B36E6 95E7A768 31AA2A3C 5299A50E


    temp =
                           DB75DB8E 03FA70C0 3ECD5F40 1DCE9119
        2CE3529B 213AB30F ED9781FD FB7576AB C820CD47 E953366B
        08CC3413 31C6D719 696B36E6 95E7A768 31AA2A3C 5299A50E


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

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 00000209 A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    Hash(counter||no_of_bits_to_return||input_string) is
                           941A4B0B 5B8431CD 2CEAC831 7B434043
        A2D385D1 7D912713 448773CA 4D3FC3C4 4397BD98 5AA68BDB
```

```
      01E39E52 6601E95C DD0002AC 0DD1B479 4476B12C 4DF0EF7A


  temp =
                  DB75 DB8E03FA 70C03ECD 5F401DCE 91192CE3
      529B213A B30FED97 81FDFB75 76ABC820 CD47E953 366B08CC
      341331C6 D719696B 36E695E7 A76831AA 2A3C5299 A50E941A


------------
i=0
t is
                  0051 7DD1043F 4F1AA20A A0EC3FBC 06C2F462
      68BF50B8 BE6A69C1 BC624AA8 E20422F5 49091E6D 81226BFE
      E2403227 59788640 E3CD377E 1C2A928C 12DCB11F E547A593


s is
                  0183 5B2634CD 556890DD 9B1872C6 7701AA3F
      EE112A27 3521BFDD 3DC0C047 AF3EBC43 44C615B6 85877378
      0B61DFE9 D59409CF BB30CB68 9B433D98 A917070E 535F0112


r is
                  0091 3990182A E9EBE7AC B67F5198 56E5A591
      F2AECAB9 3E0D3BFE CDFAC9BA 3263A346 61F682DC 8A9919F8
      184CAE4E 0E7CBD0E 97484985 728C2129 6E3FD78B 544586F0


------------
tmp is
                        90182A E9EBE7AC B67F5198 56E5A591
      F2AECAB9 3E0D3BFE CDFAC9BA 3263A346 61F682DC 8A9919F8
      184CAE4E 0E7CBD0E 97484985 728C2129 6E3FD78B 544586F0


------------
i=1
t is
                  0183 5B2634CD 556890DD 9B1872C6 7701AA3F
      EE112A27 3521BFDD 3DC0C047 AF3EBC43 44C615B6 85877378
      0B61DFE9 D59409CF BB30CB68 9B433D98 A917070E 535F0112


s is
                  0073 D92FFD61 4142EC08 313ECC5B 7836DF5F
```

```
        49538058 22742606 99212E29 7F2906CA F7AF9478 A8F036B2
        A3D6090F FD111C0C E8E68345 7870131A E883D6B8 B90E15B0


  r is
                    01B0 A8B84ECE C65888F2 7C435787 9ABC41C9
        874CB9DD FE50D295 A09C5CB0 503C6605 64185B13 F715C39B
        321F921D 3F110679 C3A0793A B713A933 509CE35D 94A0534B


  ------------
  tmp is
                                                9018 2AE9EBE7
        ACB67F51 9856E5A5 91F2AECA B93E0D3B FECDFAC9 BA3263A3
        4661F682 DC8A9919 F8184CAE 4E0E7CBD 0E974849 85728C21
        296E3FD7 8B544586 F0B84ECE C65888F2 7C435787 9ABC41C9
        874CB9DD FE50D295 A09C5CB0 503C6605 64185B13 F715C39B
        321F921D 3F110679 C3A0793A B713A933 509CE35D 94A0534B


  ------------
  s is
                    0165 2BE6B646 E49827CE 61BF98AF 4028194D
        AF0C8B23 506CA931 9EAC5953 1BA39AB8 BF3F0109 2A9EACAA
        AB8C8AE8 EC90AA94 69867DDD DC0FFE71 12A82ADB 15A308BD


rnd_val is
                                                9018 2AE9EBE7
        ACB67F51 9856E5A5 91F2AECA B93E0D3B FECDFAC9 BA3263A3
        4661F682 DC8A9919 F8184CAE 4E0E7CBD 0E974849 85728C21
        296E3FD7 8B544586 F0B84ECE C65888F2 7C435787 9ABC41C9
        874CB9DD FE50D295 A09C5CB0 503C6605 64185B13 F715C39B
        321F921D 3F110679 C3A0793A B713A933 509CE35D 94A0534B


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

DualEC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
```

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


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


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


Nonce =
                        20212223 24252627 28292A2B 2C2D2E2F


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


AdditionalInput = <empty>

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

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

DualEC_DRBG_Instantiate_algorithm

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


nonce is
                        20212223 24252627 28292A2B 2C2D2E2F


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


prediction_resistance_flag = "No PredictionResistance"
```

```
Hash_df()
----------------------------
  no_of_bits_to_return = 521

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

  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 00000209 00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
      20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
      48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


  Hash(counter||no_of_bits_to_return||input_string) is
                       FFAE2834 4D1E7E85 C08DCD7A 4643D401
      2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
      9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


  temp =
                       FFAE2834 4D1E7E85 C08DCD7A 4643D401
      2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
      9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


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

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 00000209 00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
      20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
      48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


  Hash(counter||no_of_bits_to_return||input_string) is
                       13B24000 56345ED8 7121E329 23656AF5
      63CB0C9F 6FA3F671 1A31A9EE 306A0962 01A9509E 8EEDA764
      EA71EFC6 9FE343AB 0CFD0CEF 5B7547C0 A1D66875 2BE96C9E


  temp =
```

```
                    FFAE 28344D1E 7E85C08D CD7A4643 D4012FDC
       1557F001 231750ED 5169571D F59C2783 5ECB69B3 53149744
       C13B022F D21F1797 B2065676 6C32943D A50D3ED3 74BD13B2


s is
                      01 FF5C5068 9A3CFD0B 811B9AF4 8C87A802
       5FB82AAF E002462E A1DAA2D2 AE3BEB38 4F06BD96 D366A629
       2E898276 045FA43E 2F2F640C ACECD865 287B4A1A 7DA6E97A


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                    01FF 5C50689A 3CFD0B81 1B9AF48C 87A8025F
       B82AAFE0 02462EA1 DAA2D2AE 3BEB384F 06BD96D3 66A6292E
       89827604 5FA43E2F 2F640CAC ECD86528 7B4A1A7D A6E97A27


  s is
                    007E 47C9EB86 4BBD8EE2 318C49C8 E830C129
       0F3187A3 E426A3F9 D1B956AC DFF74E9F 527E523C 52B576C1
       FD400C98 089B76D7 840212D5 222EC870 0C6002D3 EA4B842F


  r is
                    01B9 4CB233F4 1CF7DA2F 6F3FD39C 2F9301C3
       9352A16D 0035143E 27F970F6 3C205E7B 5C5D59A4 48DB4D96
       2D9A8C57 C6ADD612 D024D5B5 2D3B800E 163838EB 173AE77F


  ------------
  tmp is
                        B233F4 1CF7DA2F 6F3FD39C 2F9301C3
       9352A16D 0035143E 27F970F6 3C205E7B 5C5D59A4 48DB4D96
```

```
      2D9A8C57 C6ADD612 D024D5B5 2D3B800E 163838EB 173AE77F


  ------------
  i=1
  t is
                   007E 47C9EB86 4BBD8EE2 318C49C8 E830C129
      0F3187A3 E426A3F9 D1B956AC DFF74E9F 527E523C 52B576C1
      FD400C98 089B76D7 840212D5 222EC870 0C6002D3 EA4B842F


  s is
                   01E5 761AE4AE 582DA988 08B0E444 9EBF11EB
      8F42685E 204A128C F38AC41B ECF17CCF C139C3E3 52CC5E68
      603A9B1E CD179648 F70F6C66 4BE2F6B7 7BC78FF1 F3A52A11


  r is
                   0168 95B56219 F41A9238 49628632 6F011DCB
      2E09037E ED6680E0 3324474A 2410E0FB 0541A168 107DEF5B
      ED3B468F 8EF30276 3D7FE745 C85720F8 A33C52C4 42370E60


  ------------
  tmp is
                                                B233 F41CF7DA
      2F6F3FD3 9C2F9301 C39352A1 6D003514 3E27F970 F63C205E
      7B5C5D59 A448DB4D 962D9A8C 57C6ADD6 12D024D5 B52D3B80
      0E163838 EB173AE7 7FB56219 F41A9238 49628632 6F011DCB
      2E09037E ED6680E0 3324474A 2410E0FB 0541A168 107DEF5B
      ED3B468F 8EF30276 3D7FE745 C85720F8 A33C52C4 42370E60


  ------------
  s is
                   0109 37EBC4D9 37641E0C 57D80A32 AD16FFF5
      40A54D29 2E71491C 857D5DC1 B8DB4AE2 D374A356 921C4F67
      5A6421BE EB6D43DD 3B9E3DF3 19B2958D 8A86153E A3312B7C


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

Second call to Generate

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

```
DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                     0109 37EBC4D9 37641E0C 57D80A32 AD16FFF5
        40A54D29 2E71491C 857D5DC1 B8DB4AE2 D374A356 921C4F67
        5A6421BE EB6D43DD 3B9E3DF3 19B2958D 8A86153E A3312B7C


  s is
                     01DC DA5DDB2F 61019B11 9B3B6818 64B9042C
        A9829995 84A9C3DD F726A398 AAE586FC BC517A19 BD51D421
        40785C4E 6D498E3D B4FF90D2 8D8B7A80 C61432AA BF4AE9B3


  r is
                     01B7 12EEAF0F AEDE0D3E 25B25A79 48F1B3DE
        57972757 1FDA50E7 921E2D43 F59F2815 12AF3DDA 8A3E8AF6
        BE0F6202 C97DEA78 2B9A13C7 5D042306 7527F266 1D49A5BF


  ------------
  tmp is
                         EEAF0F AEDE0D3E 25B25A79 48F1B3DE
        57972757 1FDA50E7 921E2D43 F59F2815 12AF3DDA 8A3E8AF6
        BE0F6202 C97DEA78 2B9A13C7 5D042306 7527F266 1D49A5BF


  ------------
  i=1
  t is
                     01DC DA5DDB2F 61019B11 9B3B6818 64B9042C
        A9829995 84A9C3DD F726A398 AAE586FC BC517A19 BD51D421
        40785C4E 6D498E3D B4FF90D2 8D8B7A80 C61432AA BF4AE9B3


  s is
                     01BC 1B45D8D0 779FC5C8 68F53A20 98745744
        C5BDA16E 9D907A74 86E8A772 BE037D8E D2B199B7 F84719B3
        974649C2 0BD29410 9BA708F5 46F94A51 21C5CBA1 E2014A5B
```

```
  r is
                    010F 1B251DA4 A5750971 48B17EEF 8164CB47
        CC42B4B7 BF926827 A7E2E8E4 EB681C03 B6279C50 8F98F064
        594CD5C6 E0157A8B 3AFB6B12 B597F0B1 955D58A9 F5A2AA5B


  ------------
  tmp is
                                                EEAF 0FAEDE0D
        3E25B25A 7948F1B3 DE579727 571FDA50 E7921E2D 43F59F28
        1512AF3D DA8A3E8A F6BE0F62 02C97DEA 782B9A13 C75D0423
        067527F2 661D49A5 BF251DA4 A5750971 48B17EEF 8164CB47
        CC42B4B7 BF926827 A7E2E8E4 EB681C03 B6279C50 8F98F064
        594CD5C6 E0157A8B 3AFB6B12 B597F0B1 955D58A9 F5A2AA5B


  ------------
  s is
                    01A7 1FE27958 AAB33D33 764E22C1 C8237BA3
        A3AE7C4A 179A9F7D AC1A2809 D71185A8 182FF9C8 1185E779
        5FAA1BC8 DEBA36BD CE88BC27 E7845C5C 049001E7 7DE4E845


rnd_val is
                                                EEAF 0FAEDE0D
        3E25B25A 7948F1B3 DE579727 571FDA50 E7921E2D 43F59F28
        1512AF3D DA8A3E8A F6BE0F62 02C97DEA 782B9A13 C75D0423
        067527F2 661D49A5 BF251DA4 A5750971 48B17EEF 8164CB47
        CC42B4B7 BF926827 A7E2E8E4 EB681C03 B6279C50 8F98F064
        594CD5C6 E0157A8B 3AFB6B12 B597F0B1 955D58A9 F5A2AA5B


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

DualEC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

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

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


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


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


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


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


    AdditionalInput2  =
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

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

DualEC_DRBG_Instantiate_algorithm

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


    nonce is
                          20212223 24252627 28292A2B 2C2D2E2F


    personal_str is
                                            40414243 44454647
```

```
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


  prediction_resistance_flag = "No PredictionResistance"

Hash_df()
---------------------------
  no_of_bits_to_return = 521

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

  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 00000209 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


  Hash(counter||no_of_bits_to_return||input_string) is
                        FFAE2834 4D1E7E85 C08DCD7A 4643D401
    2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
    9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


  temp =
                        FFAE2834 4D1E7E85 C08DCD7A 4643D401
    2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
    9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


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

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 00000209 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


  Hash(counter||no_of_bits_to_return||input_string) is
                        13B24000 56345ED8 7121E329 23656AF5
    63CB0C9F 6FA3F671 1A31A9EE 306A0962 01A9509E 8EEDA764
```

```
        EA71EFC6 9FE343AB 0CFD0CEF 5B7547C0 A1D66875 2BE96C9E


    temp =
                        FFAE 28344D1E 7E85C08D CD7A4643 D4012FDC
        1557F001 231750ED 5169571D F59C2783 5ECB69B3 53149744
        C13B022F D21F1797 B2065676 6C32943D A50D3ED3 74BD13B2


s is
                          01 FF5C5068 9A3CFD0B 811B9AF4 8C87A802
        5FB82AAF E002462E A1DAA2D2 AE3BEB38 4F06BD96 D366A629
        2E898276 045FA43E 2F2F640C ACECD865 287B4A1A 7DA6E97A


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

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


    requested_number_of_bits is 1008
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 521

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                  01 00000209 60616263 64656667
        68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


    Hash(counter||no_of_bits_to_return||input_string) is
                            DD40BFFA 030E77F8 FA7D9879 56C20710
        375466E8 3CB744D8 C0446A19 281AC290 6B67BD14 F2D61258
        FABDD1B3 26CE70C3 A1598A72 68CCBAA0 8C8A2627 3214342D
```

```
temp =
                     DD40BFFA 030E77F8 FA7D9879 56C20710
    375466E8 3CB744D8 C0446A19 281AC290 6B67BD14 F2D61258
    FABDD1B3 26CE70C3 A1598A72 68CCBAA0 8C8A2627 3214342D


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

i = 2

counter||no_of_bits_to_return||input_string is
                            02 00000209 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


Hash(counter||no_of_bits_to_return||input_string) is
                     65976B23 DEBAE6F7 53B1ACC6 F0D9ADCF
    CB60A084 FA65AC58 81966BB9 8CD2EBCD 65575220 B97738B9
    5E3E883D B4078A79 F792E81E D23C19A1 8625F9B2 D681A407


temp =
                 DD40 BFFA030E 77F8FA7D 987956C2 07103754
    66E83CB7 44D8C044 6A19281A C2906B67 BD14F2D6 1258FABD
    D1B326CE 70C3A159 8A7268CC BAA08C8A 26273214 342D6597


------------
i=0
t is
                 0045 DD2F9C9C 2012FA75 E0AA0621 03A62231
    10E77F99 6CCF9F21 5276E0FE 0E6E1899 C9C7BF36 CA8298DB
    F2211049 C345B96D 9C70E87D 75AD2431 6F065419 8E8120EC


s is
                 007E EA32A86F BC93635F 30E0A1C8 56BBDE35
    00E5111D DD21B932 6994FD0E E7714F27 2A29D975 45A39FEA
    8C3EE3C7 87DA3C5F 1C0EFC08 10C77B60 DF9EC715 CBAA14B4


r is
                 008D B19462C0 6F93A486 99E4783A B1543A0D
    F9174859 BBBC60D7 36163FE7 45BFF4FA 73F2577B BCC4FB1F
```

```
      6C0A7A53 8F57FB61 A386B236 C183A714 A5B0ACE3 D4D43302


------------
tmp is
                          9462C0 6F93A486 99E4783A B1543A0D
      F9174859 BBBC60D7 36163FE7 45BFF4FA 73F2577B BCC4FB1F
      6C0A7A53 8F57FB61 A386B236 C183A714 A5B0ACE3 D4D43302


------------
i=1
t is
                   007E EA32A86F BC93635F 30E0A1C8 56BBDE35
      00E5111D DD21B932 6994FD0E E7714F27 2A29D975 45A39FEA
      8C3EE3C7 87DA3C5F 1C0EFC08 10C77B60 DF9EC715 CBAA14B4


s is
                   01CC 4EE0CC06 83713A92 F7306BB2 208983D2
      06275779 4EC9018F 78BD5967 FCE18C90 374CDFBA 2D7142BF
      B55E24BB 5D72BB6D 2C6940AB 7C229C53 C8CF8DEB 699A8B63


r is
                   0077 2943A243 0193DF55 5FE116DE 25A7BC5A
      EA1A3E35 15D0026C A1F77B1E 84158DE7 F4E7A400 74368611
      4FD580B5 EE792444 6749B8D0 984D4B4F 3AF9D75A BC055F8B


------------
tmp is
                                                  9462 C06F93A4
      8699E478 3AB1543A 0DF91748 59BBBC60 D736163F E745BFF4
      FA73F257 7BBCC4FB 1F6C0A7A 538F57FB 61A386B2 36C183A7
      14A5B0AC E3D4D433 0243A243 0193DF55 5FE116DE 25A7BC5A
      EA1A3E35 15D0026C A1F77B1E 84158DE7 F4E7A400 74368611
      4FD580B5 EE792444 6749B8D0 984D4B4F 3AF9D75A BC055F8B


------------
s is
                   00C9 B2309A19 05D548A4 A50607F2 E48FB4F5
      1634A566 09BE01C3 1B0EAE8E 4490A582 0AE5EFA5 9E2BA363
      98E7DA97 4DD3DCF8 9DEF6432 F8B22640 930B2C72 9C54E4CA
```

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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    requested_number_of_bits is 1008
  Hash_df()
  ---------------------------
    no_of_bits_to_return = 521

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                01 00000209 A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    Hash(counter||no_of_bits_to_return||input_string) is
                          DB75DB8E 03FA70C0 3ECD5F40 1DCE9119
        2CE3529B 213AB30F ED9781FD FB7576AB C820CD47 E953366B
        08CC3413 31C6D719 696B36E6 95E7A768 31AA2A3C 5299A50E


    temp =
                          DB75DB8E 03FA70C0 3ECD5F40 1DCE9119
        2CE3529B 213AB30F ED9781FD FB7576AB C820CD47 E953366B
        08CC3413 31C6D719 696B36E6 95E7A768 31AA2A3C 5299A50E


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

    i = 2

    counter||no_of_bits_to_return||input_string is
                                02 00000209 A0A1A2A3 A4A5A6A7
```

```
      A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


  Hash(counter||no_of_bits_to_return||input_string) is
                           941A4B0B 5B8431CD 2CEAC831 7B434043
      A2D385D1 7D912713 448773CA 4D3FC3C4 4397BD98 5AA68BDB
      01E39E52 6601E95C DD0002AC 0DD1B479 4476B12C 4DF0EF7A


  temp =
                      DB75 DB8E03FA 70C03ECD 5F401DCE 91192CE3
      529B213A B30FED97 81FDFB75 76ABC820 CD47E953 366B08CC
      341331C6 D719696B 36E695E7 A76831AA 2A3C5299 A50E941A


------------
i=0
t is
                      017F 5987861E F134C8D9 3FB887C9 79AD86AC
      D0919324 7CD81E18 340D5578 AE7DF212 4B7F6077 38477572
      008FFCF4 C07DEE2A 4B82A919 37FCF623 C75F54D7 AF1EF9E2


s is
                      002E 0F52033E 2A853582 B286F4DE 50D509B5
      8D68D0D8 68A7403B B0C9B806 A3CC092B 7C5BC376 47FD7D8A
      4BECC9DA C1B1E701 4EF154C8 8A3BC58F 6E932255 144AD0A6


r is
                      01CA 8B789408 89105781 A9DCAAA2 0D1B8A0F
      2FDC1572 373F5175 51E015F5 04F260C2 5C4B7AE7 C4C012F1
      07670EDE 138FCD6E 690240F4 A184801A E84664E3 5299B4B3


------------
tmp is
                        789408 89105781 A9DCAAA2 0D1B8A0F
      2FDC1572 373F5175 51E015F5 04F260C2 5C4B7AE7 C4C012F1
      07670EDE 138FCD6E 690240F4 A184801A E84664E3 5299B4B3


------------
i=1
t is
                      002E 0F52033E 2A853582 B286F4DE 50D509B5
```

```
        8D68D0D8 68A7403B B0C9B806 A3CC092B 7C5BC376 47FD7D8A
        4BECC9DA C1B1E701 4EF154C8 8A3BC58F 6E932255 144AD0A6


  s is
                    00A3 40652AF2 F5C3A4A6 F2A9CDC0 775CD7D3
        86E930B3 D80B271F 1FF86BF7 79D7B042 B85234F4 5814AAF5
        00F509ED 890980A4 C4603074 5F190C73 BF4B4E84 6AAB9111


  r is
                    00BE 3CCEA434 4724560B 0E8BC01E 6F4DE330
        A94E31B0 4E88A93F 7C8DAFAE F749E23B F92961A5 B81F2DDD
        7C465E21 15DB831A BBFEFDBD F399E8E8 4C822AD6 A674F210


  ------------
  tmp is
                                                7894 08891057
        81A9DCAA A20D1B8A 0F2FDC15 72373F51 7551E015 F504F260
        C25C4B7A E7C4C012 F107670E DE138FCD 6E690240 F4A18480
        1AE84664 E35299B4 B3CEA434 4724560B 0E8BC01E 6F4DE330
        A94E31B0 4E88A93F 7C8DAFAE F749E23B F92961A5 B81F2DDD
        7C465E21 15DB831A BBFEFDBD F399E8E8 4C822AD6 A674F210


  ------------
  s is
                    014E CB76781E 6CA03B01 CE5664C7 11A26260
        EBEA9536 92176FA6 987A8070 F4C5418C 617D949B DA529DE0
        43EB2619 54F8A4A5 4F2AEE0D 693D12C0 AF365029 34B1AF5E


rnd_val is
                                                7894 08891057
        81A9DCAA A20D1B8A 0F2FDC15 72373F51 7551E015 F504F260
        C25C4B7A E7C4C012 F107670E DE138FCD 6E690240 F4A18480
        1AE84664 E35299B4 B3CEA434 4724560B 0E8BC01E 6F4DE330
        A94E31B0 4E88A93F 7C8DAFAE F749E23B F92961A5 B81F2DDD
        7C465E21 15DB831A BBFEFDBD F399E8E8 4C822AD6 A674F210


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

DualEC_DRBG
```

```
    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

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


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


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


    Nonce =
                        20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

    AdditionalInput = <empty>

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

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

DualEC_DRBG_Instantiate_algorithm

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


    nonce is
                        20212223 24252627 28292A2B 2C2D2E2F


    personal_str is  <empty>

    prediction_resistance_flag = "PredictionResistance"
```

```
Hash_df()
----------------------------
  no_of_bits_to_return = 521

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

  i = 1

  counter||no_of_bits_to_return||input_string is
                                                  01 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                       E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


  temp =
                       E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


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

  i = 2

  counter||no_of_bits_to_return||input_string is
                                                  02 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                       0BF4E84E 26C435F1 A8C9DDAF B866D3E9
      C7556662 F08A12DA AE1B2239 3FDBEE40 5525C9EB 5A450CF2
      909A7569 FC96F424 56BD7D86 65B70B4D EB24620D FD48A7BF


  temp =
                  E4CD 803E82C6 D10E8D8F 3E5A2A80 F4A49F5C
      3DE4E594 6995FBE2 131F6A3D AC66DB4D EE1AAC0C 37DABBB3
```

```
        1BB5F688 5BF6E94B FB19BD1C D4FCE1D9 68407E2A D9FA0BF4


s is
                      01 C99B007D 058DA21D 1B1E7CB4 5501E949
        3EB87BC9 CB28D32B F7C4263E D47B58CD B69BDC35 58186FB5
        7766376B ED10B7ED D297F633 7A39A9F9 C3B2D080 FC55B3F4


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

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


    additional_input is  <empty>

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 521

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                              010000 0209E4CD
        803E82C6 D10E8D8F 3E5A2A80 F4A49F5C 3DE4E594 6995FBE2
        131F6A3D AC66DB4D EE1AAC0C 37DABBB3 1BB5F688 5BF6E94B
        FB19BD1C D4FCE1D9 68407E2A D9FA0B80 80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                         6FF8D7B4 7F5CB216 28E52304 2C2EE652
        44989379 160501FB 3385FA1E 969DCE4F 7E767642 7280F8B0
        CE10DAE5 232CEB20 17981B0D 63B21295 E8169BDA 9B3ACC02


    temp =
                         6FF8D7B4 7F5CB216 28E52304 2C2EE652
        44989379 160501FB 3385FA1E 969DCE4F 7E767642 7280F8B0
        CE10DAE5 232CEB20 17981B0D 63B21295 E8169BDA 9B3ACC02


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

    i = 2

    counter||no_of_bits_to_return||input_string is
                                              020000 0209E4CD
        803E82C6 D10E8D8F 3E5A2A80 F4A49F5C 3DE4E594 6995FBE2
        131F6A3D AC66DB4D EE1AAC0C 37DABBB3 1BB5F688 5BF6E94B
        FB19BD1C D4FCE1D9 68407E2A D9FA0B80 80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    Hash(counter||no_of_bits_to_return||input_string) is
                         CD251E66 D6CDD324 FAE2776E E4A929DB
        B40B7FBF 3F507A25 26F9F641 99823BED 2546D568 0E294FA1
        FE22D539 98721A5E 9AC16DB2 03BAA2D6 D490B4BE 780E63AB


    temp =
                     6FF8 D7B47F5C B21628E5 23042C2E E6524498
        93791605 01FB3385 FA1E969D CE4F7E76 76427280 F8B0CE10
        DAE5232C EB201798 1B0D63B2 1295E816 9BDA9B3A CC02CD25


s is
                       00 DFF1AF68 FEB9642C 51CA4608 585DCCA4
        893126F2 2C0A03F6 670BF43D 2D3B9C9E FCECEC84 E501F161
        9C21B5CA 4659D640 2F30361A C764252B D02D37B5 36759805


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

```
DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                     00DF F1AF68FE B9642C51 CA460858 5DCCA489
        3126F22C 0A03F667 0BF43D2D 3B9C9EFC ECEC84E5 01F1619C
        21B5CA46 59D6402F 30361AC7 64252BD0 2D37B536 7598059A


  s is
                     0083 30653E13 A4748FFB A78E01AB 49190611
        22F66327 2C458D53 9AF06964 6B599B77 C2CA8C26 4FE9C88A
        6775E827 CC6212D5 6EE4C16E 18FEC8B0 1E6ECB33 DAD5725C


  r is
                     01F0 94CC7035 C730405C F5DF7137 ED9E1074
        4B75B540 AFFC68EB 564B71C0 F737E8F6 56B61719 40497FA9
        0D8F383E FB6FC671 7BA14AAA 164EF566 41C0F513 312551DC


  ------------
  tmp is
                         CC7035 C730405C F5DF7137 ED9E1074
        4B75B540 AFFC68EB 564B71C0 F737E8F6 56B61719 40497FA9
        0D8F383E FB6FC671 7BA14AAA 164EF566 41C0F513 312551DC


  ------------
  i=1
  t is
                     0083 30653E13 A4748FFB A78E01AB 49190611
        22F66327 2C458D53 9AF06964 6B599B77 C2CA8C26 4FE9C88A
        6775E827 CC6212D5 6EE4C16E 18FEC8B0 1E6ECB33 DAD5725C


  s is
                     01B9 93CFCFFE 46AC4CBF A396EC57 8D9A53DB
        547F7A3A 2374D4FD FE358857 1A8176D0 4D3F8247 8C172202
        98192057 62A89E00 8FD25175 C54F8DC5 C9F29323 3006F035
```

```
  r is
                    0173 83D21D0A 5B0DBDCD 97F627E9 68DFD752
        56C11CF2 BCCA5822 EAACE796 A34CB7D2 F8CD8CC6 DBE76274
        498289BB C4C2F1CA DA6185D8 2605CF99 2EC285BC 4945EE9E


  ------------
  tmp is
                                                CC70 35C73040
        5CF5DF71 37ED9E10 744B75B5 40AFFC68 EB564B71 C0F737E8
        F656B617 1940497F A90D8F38 3EFB6FC6 717BA14A AA164EF5
        6641C0F5 13312551 DCD21D0A 5B0DBDCD 97F627E9 68DFD752
        56C11CF2 BCCA5822 EAACE796 A34CB7D2 F8CD8CC6 DBE76274
        498289BB C4C2F1CA DA6185D8 2605CF99 2EC285BC 4945EE9E


  ------------
  s is
                    0070 45526E05 494A03D2 35B291BC 79A8E138
        3DE73F74 AEF11435 527FBDA7 FF116508 148193D4 68609096
        87BE6855 099206DE 1E1D8F8D DD87FD8C EC321F19 B9E67338


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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is  <empty>
```

```
Hash_df()
----------------------------
  no_of_bits_to_return = 521

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

  i = 1

  counter||no_of_bits_to_return||input_string is
                                              010000 02093822
      A93702A4 A501E91A D948DE3C D4709C1E F39FBA57 788A1AA9
      3FDED3FF 88B2840A 40C9EA34 30484B43 DF342A84 C9036F0F
      0EC7C6EE C3FEC676 190F8CDC F3399C00 C0C1C2C3 C4C5C6C7
      C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


  Hash(counter||no_of_bits_to_return||input_string) is
                          9F748EAB 34B6E861 36A34F9B 50E0E695
      F78C9E12 4C90F392 6B8A174F F7CFF986 99097F61 675E346B
      FE834A45 7A8347D4 1825D774 E4E45B98 74AE6810 D9D5F758


  temp =
                          9F748EAB 34B6E861 36A34F9B 50E0E695
      F78C9E12 4C90F392 6B8A174F F7CFF986 99097F61 675E346B
      FE834A45 7A8347D4 1825D774 E4E45B98 74AE6810 D9D5F758


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

  i = 2

  counter||no_of_bits_to_return||input_string is
                                              020000 02093822
      A93702A4 A501E91A D948DE3C D4709C1E F39FBA57 788A1AA9
      3FDED3FF 88B2840A 40C9EA34 30484B43 DF342A84 C9036F0F
      0EC7C6EE C3FEC676 190F8CDC F3399C00 C0C1C2C3 C4C5C6C7
      C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


  Hash(counter||no_of_bits_to_return||input_string) is
                          33740A7D 1EF1977F 507E9177 C152BEA5
      C70DB477 0267C11D 1C1019A7 DEC43331 9E15FFC8 B4298E36
      3DCCE478 1C824BAF E19422B7 214C0492 E8900E5A 492E103B
```

```
    temp =
                     9F74 8EAB34B6 E86136A3 4F9B50E0 E695F78C
        9E124C90 F3926B8A 174FF7CF F9869909 7F61675E 346BFE83
        4A457A83 47D41825 D774E4E4 5B9874AE 6810D9D5 F7583374


s is
                       01 3EE91D56 696DD0C2 6D469F36 A1C1CD2B
        EF193C24 9921E724 D7142E9F EF9FF30D 3212FEC2 CEBC68D7
        FD06948A F5068FA8 304BAEE9 C9C8B730 E95CD021 B3ABEEB0


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                     013E E91D5669 6DD0C26D 469F36A1 C1CD2BEF
        193C2499 21E724D7 142E9FEF 9FF30D32 12FEC2CE BC68D7FD
        06948AF5 068FA830 4BAEE9C9 C8B730E9 5CD021B3 ABEEB066


  s is
                     0152 3C6A9E3F 8676F0CF 659B9AA0 12524176
        45178E38 1AB13BAA 171F9317 66AE6B7D 295CE3C6 21A29228
        50BA7236 5F5709CD 2DC0EB4E DADFE148 3CDD4A11 FFE03182


  r is
                     012B 5B0E6C32 9AD1BE68 1EB1E6F5 E03A89E3
        D80153D6 CCDD5A3E CF865003 EE4A2DE5 A23B7F43 681361CF
        AFC3A3FE F17777E7 5CF9D668 5573C887 A3962CB9 55076D45


  ------------
  tmp is
                         0E6C32 9AD1BE68 1EB1E6F5 E03A89E3
        D80153D6 CCDD5A3E CF865003 EE4A2DE5 A23B7F43 681361CF
        AFC3A3FE F17777E7 5CF9D668 5573C887 A3962CB9 55076D45
```

```
------------
i=1
t is
                    0152 3C6A9E3F 8676F0CF 659B9AA0 12524176
      45178E38 1AB13BAA 171F9317 66AE6B7D 295CE3C6 21A29228
      50BA7236 5F5709CD 2DC0EB4E DADFE148 3CDD4A11 FFE03182


s is
                    014D 744125FF 85FA1354 EE5A5F07 1D594335
      0603543C 17149140 B87907C7 85B984F0 4C3DE2AF 2B8F186B
      F30442D3 250BA25B E0ADADE3 0D25F8ED 3578E4AB E7A9FCAF


r is
                    0137 31D6F1E4 5EE4B8CB 31A4731C DA031FA2
      815B6D34 E29F2603 526CE186 576F4CCA 3FEDF7F8 ACDB37C9
      9D762706 ABE4967D 44739C8C FCFCC76C 58B1ED24 3AC394C0


------------
tmp is
                                                 0E6C 329AD1BE
      681EB1E6 F5E03A89 E3D80153 D6CCDD5A 3ECF8650 03EE4A2D
      E5A23B7F 43681361 CFAFC3A3 FEF17777 E75CF9D6 685573C8
      87A3962C B955076D 45D6F1E4 5EE4B8CB 31A4731C DA031FA2
      815B6D34 E29F2603 526CE186 576F4CCA 3FEDF7F8 ACDB37C9
      9D762706 ABE4967D 44739C8C FCFCC76C 58B1ED24 3AC394C0


------------
s is
                    00DD 55587B02 0FD02426 2799D5E8 9A1A839F
      4B04EC08 BCE4836F 19464A7F D0002EF0 40BC621A 48782B1B
      1D403002 AEE59428 0F0675A9 C691A764 2ED6DBC6 C26B1771


rnd_val is
                                                 0E6C 329AD1BE
      681EB1E6 F5E03A89 E3D80153 D6CCDD5A 3ECF8650 03EE4A2D
      E5A23B7F 43681361 CFAFC3A3 FEF17777 E75CF9D6 685573C8
      87A3962C B955076D 45D6F1E4 5EE4B8CB 31A4731C DA031FA2
      815B6D34 E29F2603 526CE186 576F4CCA 3FEDF7F8 ACDB37C9
      9D762706 ABE4967D 44739C8C FCFCC76C 58B1ED24 3AC394C0
```

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

DualEC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

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


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


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


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


    PersonalizationString = <empty>

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


    AdditionalInput2  =
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

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

DualEC_DRBG_Instantiate_algorithm
```

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


  nonce is
                       20212223 24252627 28292A2B 2C2D2E2F


  personal_str is  <empty>

  prediction_resistance_flag = "PredictionResistance"

Hash_df()
----------------------------
  no_of_bits_to_return = 521

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

  i = 1

  counter||no_of_bits_to_return||input_string is
                                                 01 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
      18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


  Hash(counter||no_of_bits_to_return||input_string) is
                       E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


  temp =
                       E4CD803E 82C6D10E 8D8F3E5A 2A80F4A4
      9F5C3DE4 E5946995 FBE2131F 6A3DAC66 DB4DEE1A AC0C37DA
      BBB31BB5 F6885BF6 E94BFB19 BD1CD4FC E1D96840 7E2AD9FA


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

  i = 2

  counter||no_of_bits_to_return||input_string is
                                                 02 00000209
      00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
```

```
        18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F


    Hash(counter||no_of_bits_to_return||input_string) is
                             0BF4E84E 26C435F1 A8C9DDAF B866D3E9
        C7556662 F08A12DA AE1B2239 3FDBEE40 5525C9EB 5A450CF2
        909A7569 FC96F424 56BD7D86 65B70B4D EB24620D FD48A7BF


    temp =
                         E4CD 803E82C6 D10E8D8F 3E5A2A80 F4A49F5C
        3DE4E594 6995FBE2 131F6A3D AC66DB4D EE1AAC0C 37DABBB3
        1BB5F688 5BF6E94B FB19BD1C D4FCE1D9 68407E2A D9FA0BF4


s is
                           01 C99B007D 058DA21D 1B1E7CB4 5501E949
        3EB87BC9 CB28D32B F7C4263E D47B58CD B69BDC35 58186FB5
        7766376B ED10B7ED D297F633 7A39A9F9 C3B2D080 FC55B3F4


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

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


    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

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


    additional_input is
```

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


Hash_df()
---------------------------
  no_of_bits_to_return = 521

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

  i = 1

  counter||no_of_bits_to_return||input_string is
                          010000 0209E4CD 803E82C6 D10E8D8F
    3E5A2A80 F4A49F5C 3DE4E594 6995FBE2 131F6A3D AC66DB4D
    EE1AAC0C 37DABBB3 1BB5F688 5BF6E94B FB19BD1C D4FCE1D9
    68407E2A D9FA0B80 80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C9D9E9F 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


  Hash(counter||no_of_bits_to_return||input_string) is
                        B55DB916 3FE7CD2C 33683701 6001C24E
    94DF2D24 90EE2EB4 7AF051FB E7F186A3 B46217B2 D998E376
    EE66AE04 61CA6155 8E5906EE 12D9D633 A4F37C7B 79B47667


  temp =
                        B55DB916 3FE7CD2C 33683701 6001C24E
    94DF2D24 90EE2EB4 7AF051FB E7F186A3 B46217B2 D998E376
    EE66AE04 61CA6155 8E5906EE 12D9D633 A4F37C7B 79B47667


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

  i = 2

  counter||no_of_bits_to_return||input_string is
                          020000 0209E4CD 803E82C6 D10E8D8F
    3E5A2A80 F4A49F5C 3DE4E594 6995FBE2 131F6A3D AC66DB4D
    EE1AAC0C 37DABBB3 1BB5F688 5BF6E94B FB19BD1C D4FCE1D9
    68407E2A D9FA0B80 80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C9D9E9F 60616263 64656667
    68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                         C8EFD0FA 5CA2202E F0F719FE EBB712AB
        1A47E1D0 82F5391B 82D05FFB C90AF393 736F7AF1 22798AA1
        1E7394FB 57297FE1 CD8E0C13 274DA456 F2FADB85 7643AF08


    temp =
                     B55D B9163FE7 CD2C3368 37016001 C24E94DF
        2D2490EE 2EB47AF0 51FBE7F1 86A3B462 17B2D998 E376EE66
        AE0461CA 61558E59 06EE12D9 D633A4F3 7C7B79B4 7667C8EF


s is
                       01 6ABB722C 7FCF9A58 66D06E02 C003849D
        29BE5A49 21DC5D68 F5E0A3F7 CFE30D47 68C42F65 B331C6ED
        DCCD5C08 C394C2AB 1CB20DDC 25B3AC67 49E6F8F6 F368ECCF


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                     016A BB722C7F CF9A5866 D06E02C0 03849D29
        BE5A4921 DC5D68F5 E0A3F7CF E30D4768 C42F65B3 31C6EDDC
        CD5C08C3 94C2AB1C B20DDC25 B3AC6749 E6F8F6F3 68ECCF91


  s is
                     01FE 071FA43E E7329DCC A1E0D757 A4B0C5BA
        ACE64803 CA78DAE6 E0A9869A D1E2F691 9F890FA4 C4FFC098
        34AF37FB BDB33678 17E5290B 1F4E5933 0BA1D05A 341A40BC


  r is
                     01DF 6F00DB66 B6372D8D 6DC38BBE 048063D9
        AB0F7CDD 49A06DEC 668DE109 039D22DA D7A0B4A7 A68855DA
        752C8EDC 1CD36111 28C5C664 C6349543 9437C423 8482333B


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

```
tmp is
                        00DB66 B6372D8D 6DC38BBE 048063D9
      AB0F7CDD 49A06DEC 668DE109 039D22DA D7A0B4A7 A68855DA
      752C8EDC 1CD36111 28C5C664 C6349543 9437C423 8482333B


------------
i=1
t is
                   01FE 071FA43E E7329DCC A1E0D757 A4B0C5BA
      ACE64803 CA78DAE6 E0A9869A D1E2F691 9F890FA4 C4FFC098
      34AF37FB BDB33678 17E5290B 1F4E5933 0BA1D05A 341A40BC


s is
                   00EB 5EFF4CA1 532110A5 D7B9E7BF 4799B003
      19D323E7 57192AF5 6905F82E C361355E 8845A00E 8D7EA8A3
      E01FEFDE E8BD6E4B 32E12386 714CC431 9C2782DD F3739149


r is
                   0084 34E66A41 05A0F2E9 EF462C42 49A5468A
      0E7E6736 063A19E9 ACA84639 66B76B5D 6C5B17D5 8648D1A4
      A22FF4FA 1FF847BA 8E814E8F 323F9D71 75FF4EBD 592C72F9


------------
tmp is
                                                 00DB 66B6372D
      8D6DC38B BE048063 D9AB0F7C DD49A06D EC668DE1 09039D22
      DAD7A0B4 A7A68855 DA752C8E DC1CD361 1128C5C6 64C63495
      439437C4 23848233 3BE66A41 05A0F2E9 EF462C42 49A5468A
      0E7E6736 063A19E9 ACA84639 66B76B5D 6C5B17D5 8648D1A4
      A22FF4FA 1FF847BA 8E814E8F 323F9D71 75FF4EBD 592C72F9


------------
s is
                   011E 23D41ACD 554D5DAC 41B0D98E 18738D4C
      C3E2187C 0380965A CF4DB981 81C37208 5A021E70 3FEC3EFF
      9845A783 1CB515C4 C90EC470 675AC92E AB389748 F4455656


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

Second call to Generate
```

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

DualEC_DRBG_Generate_algorithm

    additional_input is
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


  Hash_df()
  ---------------------------
    no_of_bits_to_return = 521

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                            010000 02098F11 EA0D66AA A6AED620
        D86CC70C 39C6A661 F10C3E01 C04B2D67 A6DCC0C0 E1B9042D
        010F381F F61F7FCC 22D3C18E 5A8AE264 87623833 AD649755
        9C4BA47A 22AB2B00 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    Hash(counter||no_of_bits_to_return||input_string) is
                          9B3A66CC 3A3753CE 6176E75C 6EA2FF41
        FEB59307 B1A0D8A1 619E6893 5252752B 0D50B904 D6475151
```

```
        D3020756 6898B346 1FD25534 2F8796E4 BED89701 2F41B635


    temp =
                         9B3A66CC 3A3753CE 6176E75C 6EA2FF41
        FEB59307 B1A0D8A1 619E6893 5252752B 0D50B904 D6475151
        D3020756 6898B346 1FD25534 2F8796E4 BED89701 2F41B635


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

    i = 2

    counter||no_of_bits_to_return||input_string is
                            020000 02098F11 EA0D66AA A6AED620
        D86CC70C 39C6A661 F10C3E01 C04B2D67 A6DCC0C0 E1B9042D
        010F381F F61F7FCC 22D3C18E 5A8AE264 87623833 AD649755
        9C4BA47A 22AB2B00 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    Hash(counter||no_of_bits_to_return||input_string) is
                         A6ED31D8 A3A99462 1EC4E4CB AE6F54D5
        0533FCC4 7228EF3B 39020F11 F0A090BE 9011002E C0174CC2
        0DC17A4B EC691BFD B1C6D86B 5D2BEC24 3A5D1E7C 4FE55AB2


    temp =
                     9B3A 66CC3A37 53CE6176 E75C6EA2 FF41FEB5
        9307B1A0 D8A1619E 68935252 752B0D50 B904D647 5151D302
        07566898 B3461FD2 55342F87 96E4BED8 97012F41 B635A6ED


s is
                       01 3674CD98 746EA79C C2EDCEB8 DD45FE83
        FD6B260F 6341B142 C33CD126 A4A4EA56 1AA17209 AC8EA2A3
        A6040EAC D131668C 3FA4AA68 5F0F2DC9 7DB12E02 5E836C6B


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>
```

```
  requested_number_of_bits is 1008
------------
i=0
t is
                   0136 74CD9874 6EA79CC2 EDCEB8DD 45FE83FD
      6B260F63 41B142C3 3CD126A4 A4EA561A A17209AC 8EA2A3A6
      040EACD1 31668C3F A4AA685F 0F2DC97D B12E025E 836C6B4D


s is
                   004F F1C9791A 4FA39027 3229B6AF 7502DA85
      0D16DC48 A8410530 6D79167D CABA439C 98EB0218 793A7780
      EC7DE88B 9C696570 3A4737BC 81818934 402AAEBA A7C49B37


r is
                   0025 290CB8DC 021E0057 CD78A001 77C81DAF
      3D06E48A 0B0D15BB 407D4527 25FA2A1C 8D95292A 6D8A977F
      DD9B3457 1E8E6E37 560251F5 75AEFC8B A99F5871 1AEEC222


------------
tmp is
                         0CB8DC 021E0057 CD78A001 77C81DAF
      3D06E48A 0B0D15BB 407D4527 25FA2A1C 8D95292A 6D8A977F
      DD9B3457 1E8E6E37 560251F5 75AEFC8B A99F5871 1AEEC222


------------
i=1
t is
                   004F F1C9791A 4FA39027 3229B6AF 7502DA85
      0D16DC48 A8410530 6D79167D CABA439C 98EB0218 793A7780
      EC7DE88B 9C696570 3A4737BC 81818934 402AAEBA A7C49B37


s is
                   01C2 036F2107 7A6360FC 31A1FEE3 28910608
      C96A154C 0B0DB6CF 83BB542B D40767B2 0F727CF2 94BB6437
      904C6163 56A3C07C 89E546BC F5400BDA F4B22ECA 62AA0A9A


r is
                   0036 CF8180B8 A636D434 E8800BCA A47F7540
      6CA0E2FD 888C1F66 C0601E50 C8999B90 3579ED1A 8FB2B0E7
      379EBC72 DEDA031A D02DFDEE 2714125E 2556F5FE AE6ECED4
```

```
  ------------
  tmp is
                                                  0CB8 DC021E00
        57CD78A0 0177C81D AF3D06E4 8A0B0D15 BB407D45 2725FA2A
        1C8D9529 2A6D8A97 7FDD9B34 571E8E6E 37560251 F575AEFC
        8BA99F58 711AEEC2 228180B8 A636D434 E8800BCA A47F7540
        6CA0E2FD 888C1F66 C0601E50 C8999B90 3579ED1A 8FB2B0E7
        379EBC72 DEDA031A D02DFDEE 2714125E 2556F5FE AE6ECED4


  ------------
  s is
                     0057 DBAB7BCE DC39393F 9B284879 57CB8685
        E0A83F7E D76919DE 812A969F 8E188096 7F90013B 682934D2
        67FDC778 AB0C7501 861BD33D A241E632 B17AE8FF 463713CC


rnd_val is
                                                  0CB8 DC021E00
        57CD78A0 0177C81D AF3D06E4 8A0B0D15 BB407D45 2725FA2A
        1C8D9529 2A6D8A97 7FDD9B34 571E8E6E 37560251 F575AEFC
        8BA99F58 711AEEC2 228180B8 A636D434 E8800BCA A47F7540
        6CA0E2FD 888C1F66 C0601E50 C8999B90 3579ED1A 8FB2B0E7
        379EBC72 DEDA031A D02DFDEE 2714125E 2556F5FE AE6ECED4


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

DualEC_DRBG

    Requested Security Strength = 256

    Requested Hash Algorithm = SHA-512

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


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

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


    Nonce =
                         20212223 24252627 28292A2B 2C2D2E2F


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


    AdditionalInput = <empty>

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

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

DualEC_DRBG_Instantiate_algorithm

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


    nonce is
                         20212223 24252627 28292A2B 2C2D2E2F


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


    prediction_resistance_flag = "PredictionResistance"

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 521

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

    i = 1
```

```
counter||no_of_bits_to_return||input_string is
                            01 00000209 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


Hash(counter||no_of_bits_to_return||input_string) is
                        FFAE2834 4D1E7E85 C08DCD7A 4643D401
    2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
    9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


temp =
                        FFAE2834 4D1E7E85 C08DCD7A 4643D401
    2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
    9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


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

i = 2

counter||no_of_bits_to_return||input_string is
                            02 00000209 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


Hash(counter||no_of_bits_to_return||input_string) is
                        13B24000 56345ED8 7121E329 23656AF5
    63CB0C9F 6FA3F671 1A31A9EE 306A0962 01A9509E 8EEDA764
    EA71EFC6 9FE343AB 0CFD0CEF 5B7547C0 A1D66875 2BE96C9E


temp =
                  FFAE 28344D1E 7E85C08D CD7A4643 D4012FDC
    1557F001 231750ED 5169571D F59C2783 5ECB69B3 53149744
    C13B022F D21F1797 B2065676 6C32943D A50D3ED3 74BD13B2


s is
                      01 FF5C5068 9A3CFD0B 811B9AF4 8C87A802
    5FB82AAF E002462E A1DAA2D2 AE3BEB38 4F06BD96 D366A629
```

```
        2E898276 045FA43E 2F2F640C ACECD865 287B4A1A 7DA6E97A


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

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


    additional_input is  <empty>

  Hash_df()
  ---------------------------
    no_of_bits_to_return = 521

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                                              010000 0209FFAE
        28344D1E 7E85C08D CD7A4643 D4012FDC 1557F001 231750ED
        5169571D F59C2783 5ECB69B3 53149744 C13B022F D21F1797
        B2065676 6C32943D A50D3ED3 74BD1380 80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    Hash(counter||no_of_bits_to_return||input_string) is
                            A07EDE04 6D52F125 7BDD31EF 41A32A49
        D2D3CF41 D02C865E 20640917 0DC9F36A E2E3BFFF 58A8788A
        471D90C6 7C48BD28 8DF9296A E544BC8F 1CD6ED9F 87003A2B
```

```
    temp =
                         A07EDE04 6D52F125 7BDD31EF 41A32A49
        D2D3CF41 D02C865E 20640917 0DC9F36A E2E3BFFF 58A8788A
        471D90C6 7C48BD28 8DF9296A E544BC8F 1CD6ED9F 87003A2B


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

    i = 2

    counter||no_of_bits_to_return||input_string is
                                              020000 0209FFAE
        28344D1E 7E85C08D CD7A4643 D4012FDC 1557F001 231750ED
        5169571D F59C2783 5ECB69B3 53149744 C13B022F D21F1797
        B2065676 6C32943D A50D3ED3 74BD1380 80818283 84858687
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F


    Hash(counter||no_of_bits_to_return||input_string) is
                         88AFEFF9 553A9792 50A85B63 6278976C
        EFD5FC41 7FCCD2C3 AEA6450B 3C69BAF1 DE0A92C5 FE79D405
        831E047A A14674EF 66760CC7 561CEBF3 5BB15AF6 69254A76


    temp =
                     A07E DE046D52 F1257BDD 31EF41A3 2A49D2D3
        CF41D02C 865E2064 09170DC9 F36AE2E3 BFFF58A8 788A471D
        90C67C48 BD288DF9 296AE544 BC8F1CD6 ED9F8700 3A2B88AF


s is
                       01 40FDBC08 DAA5E24A F7BA63DE 83465493
        A5A79E83 A0590CBC 40C8122E 1B93E6D5 C5C77FFE B150F114
        8E3B218C F8917A51 1BF252D5 CA89791E 39ADDB3F 0E007457


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
```

```
i=0
t is
                  0140 FDBC08DA A5E24AF7 BA63DE83 465493A5
      A79E83A0 590CBC40 C8122E1B 93E6D5C5 C77FFEB1 50F1148E
      3B218CF8 917A511B F252D5CA 89791E39 ADDB3F0E 00745711


s is
                  00D8 F65E802E 31FDC676 86170D85 F56F2103
      687D9306 4F80CCD7 DB6317C5 E587D493 2F2910F2 AC40965D
      7B33F1DF 08AFFE47 B2306033 5506E429 8B6A8631 A484BB6B


r is
                  0012 0E4B447A E985BCC4 861F3A8A BACB4F80
      F0B04D38 4207959B 2743FF28 DFBD3712 6C29C526 5358AD7B
      0B127286 CE944EDB FAA116A9 DC2D0274 A975BF25 7C340311


------------
tmp is
                        4B447A E985BCC4 861F3A8A BACB4F80
      F0B04D38 4207959B 2743FF28 DFBD3712 6C29C526 5358AD7B
      0B127286 CE944EDB FAA116A9 DC2D0274 A975BF25 7C340311


------------
i=1
t is
                  00D8 F65E802E 31FDC676 86170D85 F56F2103
      687D9306 4F80CCD7 DB6317C5 E587D493 2F2910F2 AC40965D
      7B33F1DF 08AFFE47 B2306033 5506E429 8B6A8631 A484BB6B


s is
                  00AB 4412E019 B6C40EA4 CA845A6B D9D09C94
      D4A4FA91 7EFDBC4E 3E27BC78 A85881F9 7763DCD0 56CAC5E7
      5207F8EF 329AF0C1 8B9DB00B 4D0A22EF EAE79794 2065C2AB


r is
                  0171 03820FA8 2B10C121 D8981D2C C6EFB51F
      329EBA69 9FFBD410 3D1DBDDB 561962D3 43EA46C3 6D1FF67B
      A6AFEE12 F0EE580A 6050D746 44ACF69D D9A390B6 8BC2543B
```

```
  ------------
  tmp is
                                                 4B44 7AE985BC
        C4861F3A 8ABACB4F 80F0B04D 38420795 9B2743FF 28DFBD37
        126C29C5 265358AD 7B0B1272 86CE944E DBFAA116 A9DC2D02
        74A975BF 257C3403 11820FA8 2B10C121 D8981D2C C6EFB51F
        329EBA69 9FFBD410 3D1DBDDB 561962D3 43EA46C3 6D1FF67B
        A6AFEE12 F0EE580A 6050D746 44ACF69D D9A390B6 8BC2543B


  ------------
  s is
                     0119 402C8A29 037AFEE3 3FB82018 90FAE7AE
        C1D2E13D 885248E9 B747A434 A0496733 5E7D0CAE D7FC08B3
        89B58456 C8756ED8 8E151427 640438A0 8F06A0DD 6BF5F187


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

Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
****************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                                             C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is  <empty>

  Hash_df()
  ----------------------------
    no_of_bits_to_return = 521

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

```
i = 1

counter||no_of_bits_to_return||input_string is
                                          010000 02098CA0
    16451481 BD7F719F DC100C48 7D73D760 E9709EC4 292474DB
    A3D21A50 24B399AF 3E86576B FE0459C4 DAC22B64 3AB76C47
    0A8A13B2 021C5047 83506EB5 FAF8C380 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


Hash(counter||no_of_bits_to_return||input_string) is
                      B6577447 85583872 B8633A71 26638396
    F7350FC6 CC052AA8 06E4A3C3 483DBDDA D0D29DF3 29141612
    35372020 0498EAF3 D6C7C134 6A09B2D6 BE60B293 E15309EC


temp =
                      B6577447 85583872 B8633A71 26638396
    F7350FC6 CC052AA8 06E4A3C3 483DBDDA D0D29DF3 29141612
    35372020 0498EAF3 D6C7C134 6A09B2D6 BE60B293 E15309EC


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

i = 2

counter||no_of_bits_to_return||input_string is
                                          020000 02098CA0
    16451481 BD7F719F DC100C48 7D73D760 E9709EC4 292474DB
    A3D21A50 24B399AF 3E86576B FE0459C4 DAC22B64 3AB76C47
    0A8A13B2 021C5047 83506EB5 FAF8C380 C0C1C2C3 C4C5C6C7
    C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


Hash(counter||no_of_bits_to_return||input_string) is
                      44C6D1E4 6E0A7743 509B225C 91D076B9
    326F147D 74EEA7EE 264B8BB0 D12574FC C12CEE44 3FD86689
    DA878137 C4210E53 D779E53A FCFD1FFF 8BC7B62C 4C43B770


temp =
                  B657 74478558 3872B863 3A712663 8396F735
    0FC6CC05 2AA806E4 A3C3483D BDDAD0D2 9DF32914 16123537
    20200498 EAF3D6C7 C1346A09 B2D6BE60 B293E153 09EC44C6
```

```
s is
                      01 6CAEE88F 0AB070E5 70C674E2 4CC7072D
        EE6A1F8D 980A5550 0DC94786 907B7BB5 A1A53BE6 52282C24
        6A6E4040 0931D5E7 AD8F8268 D41365AD 7CC16527 C2A613D8


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                    016C AEE88F0A B070E570 C674E24C C7072DEE
        6A1F8D98 0A55500D C9478690 7B7BB5A1 A53BE652 282C246A
        6E404009 31D5E7AD 8F8268D4 1365AD7C C16527C2 A613D889


  s is
                    019D 73484D48 3CE45ADA 93CBA87E 0B6FBCB0
        30E324E6 02181283 0F4ECE02 932B2C73 459BA189 2AD98D84
        31BE1970 86A37ABB E86F19A8 ABA2BCB0 6C489969 08D68491


  r is
                    007A 84D594BB AB5DFB63 471DC655 2B009B88
        6AD1DB71 19516668 F1E88675 F5E42501 E0BAC65C 03EC2042
        5388895F B7D0B994 7213DB93 4E5F859A 6C785DE0 C78F872F


  ------------
  tmp is
                          D594BB AB5DFB63 471DC655 2B009B88
        6AD1DB71 19516668 F1E88675 F5E42501 E0BAC65C 03EC2042
        5388895F B7D0B994 7213DB93 4E5F859A 6C785DE0 C78F872F


  ------------
  i=1
  t is
                    019D 73484D48 3CE45ADA 93CBA87E 0B6FBCB0
        30E324E6 02181283 0F4ECE02 932B2C73 459BA189 2AD98D84
        31BE1970 86A37ABB E86F19A8 ABA2BCB0 6C489969 08D68491
```

```
  s is
                    0199 67CF5600 3F48081D A94DBF1B DA67B985
        4CC9D3A2 57A912E4 61695F89 C0ED6F7C E2991072 0A6E6E8E
        273BE496 0D5FE2D5 C40BE028 1E0CC219 A8C41C10 4F5D7643


  r is
                    0121 ABF43EAE EC7F9044 19D2264E C9DD1130
        FB62F847 10460B4C BF8C4964 1B56D428 D1085F42 91FDE162
        01F18E10 4DAE3A6D 9A4AC46B B908E56E 22EDB4B8 843B6038


  ------------
  tmp is
                                                D594 BBAB5DFB
        63471DC6 552B009B 886AD1DB 71195166 68F1E886 75F5E425
        01E0BAC6 5C03EC20 42538889 5FB7D0B9 947213DB 934E5F85
        9A6C785D E0C78F87 2FF43EAE EC7F9044 19D2264E C9DD1130
        FB62F847 10460B4C BF8C4964 1B56D428 D1085F42 91FDE162
        01F18E10 4DAE3A6D 9A4AC46B B908E56E 22EDB4B8 843B6038


  ------------
  s is
                    0122 77038985 6741F22A 744C4050 7B5F7010
        F2CAD7D8 CA1FFEE9 B3155675 A0711010 435992D2 067F766F
        FBB5F25E 4E216B95 A120CCD8 F60CD374 0949B974 B12BB35A


rnd_val is
                                                D594 BBAB5DFB
        63471DC6 552B009B 886AD1DB 71195166 68F1E886 75F5E425
        01E0BAC6 5C03EC20 42538889 5FB7D0B9 947213DB 934E5F85
        9A6C785D E0C78F87 2FF43EAE EC7F9044 19D2264E C9DD1130
        FB62F847 10460B4C BF8C4964 1B56D428 D1085F42 91FDE162
        01F18E10 4DAE3A6D 9A4AC46B B908E56E 22EDB4B8 843B6038


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

DualEC_DRBG

    Requested Security Strength = 256
```

```
    Requested Hash Algorithm = SHA-512

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


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


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


    Nonce =
                          20212223 24252627 28292A2B 2C2D2E2F


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


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


    AdditionalInput2  =
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


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

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

DualEC_DRBG_Instantiate_algorithm

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

```
  nonce is
                        20212223 24252627 28292A2B 2C2D2E2F


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


  prediction_resistance_flag = "PredictionResistance"

Hash_df()
----------------------------
  no_of_bits_to_return = 521

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

  i = 1

  counter||no_of_bits_to_return||input_string is
                              01 00000209 00010203 04050607
      08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
      20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
      48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


  Hash(counter||no_of_bits_to_return||input_string) is
                        FFAE2834 4D1E7E85 C08DCD7A 4643D401
      2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
      9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


  temp =
                        FFAE2834 4D1E7E85 C08DCD7A 4643D401
      2FDC1557 F0012317 50ED5169 571DF59C 27835ECB 69B35314
      9744C13B 022FD21F 1797B206 56766C32 943DA50D 3ED374BD


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

  i = 2

  counter||no_of_bits_to_return||input_string is
                              02 00000209 00010203 04050607
```

```
        08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
        20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F


    Hash(counter||no_of_bits_to_return||input_string) is
                            13B24000 56345ED8 7121E329 23656AF5
        63CB0C9F 6FA3F671 1A31A9EE 306A0962 01A9509E 8EEDA764
        EA71EFC6 9FE343AB 0CFD0CEF 5B7547C0 A1D66875 2BE96C9E


    temp =
                        FFAE 28344D1E 7E85C08D CD7A4643 D4012FDC
        1557F001 231750ED 5169571D F59C2783 5ECB69B3 53149744
        C13B022F D21F1797 B2065676 6C32943D A50D3ED3 74BD13B2


s is
                          01 FF5C5068 9A3CFD0B 811B9AF4 8C87A802
        5FB82AAF E002462E A1DAA2D2 AE3BEB38 4F06BD96 D366A629
        2E898276 045FA43E 2F2F640C ACECD865 287B4A1A 7DA6E97A


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

First call to Generate

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

DualEC_DRBG_Generate_algorithm

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


    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

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

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


Hash_df()
----------------------------
  no_of_bits_to_return = 521

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

  i = 1

  counter||no_of_bits_to_return||input_string is
                         010000 0209FFAE 28344D1E 7E85C08D
      CD7A4643 D4012FDC 1557F001 231750ED 5169571D F59C2783
      5ECB69B3 53149744 C13B022F D21F1797 B2065676 6C32943D
      A50D3ED3 74BD1380 80818283 84858687 88898A8B 8C8D8E8F
      90919293 94959697 98999A9B 9C9D9E9F 60616263 64656667
      68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F


  Hash(counter||no_of_bits_to_return||input_string) is
                       46015029 C46238FF 075EAF04 77141082
      B71E8CE1 1EF7D77B E990C0E2 70475F5B 945CB46A F8E5FB44
      60C7ADB6 A0468132 DBB830D5 80823A12 5EA250B3 65149682


  temp =
                       46015029 C46238FF 075EAF04 77141082
      B71E8CE1 1EF7D77B E990C0E2 70475F5B 945CB46A F8E5FB44
      60C7ADB6 A0468132 DBB830D5 80823A12 5EA250B3 65149682


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

  i = 2

  counter||no_of_bits_to_return||input_string is
                         020000 0209FFAE 28344D1E 7E85C08D
      CD7A4643 D4012FDC 1557F001 231750ED 5169571D F59C2783
      5ECB69B3 53149744 C13B022F D21F1797 B2065676 6C32943D
      A50D3ED3 74BD1380 80818283 84858687 88898A8B 8C8D8E8F
      90919293 94959697 98999A9B 9C9D9E9F 60616263 64656667
      68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
```

```
    Hash(counter||no_of_bits_to_return||input_string) is
                         481B45CC 7118C054 581CE5C8 327BC255
        576BE388 FEFA4E7A FD60C16B F9DD0759 4D5A834A 782528E2
        5678F76A 8952798C 7507C78D 1DC43E75 DB0D9240 E50688B9


    temp =
                     4601 5029C462 38FF075E AF047714 1082B71E
        8CE11EF7 D77BE990 C0E27047 5F5B945C B46AF8E5 FB4460C7
        ADB6A046 8132DBB8 30D58082 3A125EA2 50B36514 9682481B


s is
                       00 8C02A053 88C471FE 0EBD5E08 EE282105
        6E3D19C2 3DEFAEF7 D32181C4 E08EBEB7 28B968D5 F1CBF688
        C18F5B6D 408D0265 B77061AB 01047424 BD44A166 CA292D04


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

DualEC_DRBG_Generate_algorithm

    additional_input is  <empty>

    requested_number_of_bits is 1008
  ------------
  i=0
  t is
                     008C 02A05388 C471FE0E BD5E08EE 2821056E
        3D19C23D EFAEF7D3 2181C4E0 8EBEB728 B968D5F1 CBF688C1
        8F5B6D40 8D0265B7 7061AB01 047424BD 44A166CA 292D0490


  s is
                     009F AC93AA48 4BC03AA2 72F00C74 FFAB2FD8
        32466448 88005AAB 4881F8D8 721163FD D97DAC86 B9D3F61D
        6C0D7AE9 7C114C5C 72482217 8634F2A9 55F1BAD5 3FACAA4C


  r is
                     0127 16C7ED88 A2C6901C 04802BA2 BB042629
        21B19664 835A4A3C 002CB9F1 3E35E3DE B3698A43 6BF1C85B
        070E9E69 77CA78A5 130905AA 0C01A941 30F5133D F904A4AC
```

```
------------
tmp is
                          C7ED88 A2C6901C 04802BA2 BB042629
      21B19664 835A4A3C 002CB9F1 3E35E3DE B3698A43 6BF1C85B
      070E9E69 77CA78A5 130905AA 0C01A941 30F5133D F904A4AC


------------
i=1
t is
                   009F AC93AA48 4BC03AA2 72F00C74 FFAB2FD8
      32466448 88005AAB 4881F8D8 721163FD D97DAC86 B9D3F61D
      6C0D7AE9 7C114C5C 72482217 8634F2A9 55F1BAD5 3FACAA4C


s is
                   0195 41808856 E77C1E0E 5921347B 658CBF72
      2286FF22 542119F6 484E8365 35F5A448 11FFEB2F CCDCF87A
      A0E6F8A9 32E404AA 28793F91 123B4B72 6B7FD74B 7170819A


r is
                   00FB E2F59A7D D01227E8 FCA1C8D5 1F093839
      46ECD950 11310476 0D7E216C AF581FE9 D3AACE6F C4CDDC4C
      CD736D26 A60BE8BE 2A6A78CD 752D1EC7 CCC80263 8B177307


------------
tmp is
                                                C7ED 88A2C690
      1C04802B A2BB0426 2921B196 64835A4A 3C002CB9 F13E35E3
      DEB3698A 436BF1C8 5B070E9E 6977CA78 A5130905 AA0C01A9
      4130F513 3DF904A4 ACF59A7D D01227E8 FCA1C8D5 1F093839
      46ECD950 11310476 0D7E216C AF581FE9 D3AACE6F C4CDDC4C
      CD736D26 A60BE8BE 2A6A78CD 752D1EC7 CCC80263 8B177307


------------
s is
                   0001 E2928DB7 FEB26C5A 4078C4B9 D12014E4
      D15FC2AA ECCCBE4F 1CF0D35B 7AF6DD60 B960D18D 547C0C0F
      310B832D F33961B7 1553D019 8D83DC74 1165FCA5 759478C7


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

```
Second call to Generate

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

DualEC_DRBG_Generate_algorithm

    additional_input is
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    requested_number_of_bits is 1008
Generate FAILED: Reseed is required
*************************************************************

DualEC_DRBG_Reseed_algorithm

    entropy_input is
                                            C0C1C2C3 C4C5C6C7
        C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF


    additional_input is
                                            A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


  Hash_df()
  ---------------------------
    no_of_bits_to_return = 521

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

    i = 1

    counter||no_of_bits_to_return||input_string is
                            010000 020900F1 4946DBFF 59362D20
        3C625CE8 900A7268 AFE15576 665F278E 7869ADBD 7B6EB05C
        B068C6AA 3E060798 85C196F9 9CB0DB8A A9E80CC6 C1EE3A08
        B2FE52BA CA3C6380 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    Hash(counter||no_of_bits_to_return||input_string) is
```

```
                        F8A5ADF3 B0C52B4A 48ECAF75 E4610EFD
        7AF72B36 8C2567D1 941DB67F A608ED5C BB3363F8 4BA8E080
        EE86BEA5 EEADC93D 8B130FB6 D35A7A48 1F6FDAB0 7C1090C2


    temp =
                        F8A5ADF3 B0C52B4A 48ECAF75 E4610EFD
        7AF72B36 8C2567D1 941DB67F A608ED5C BB3363F8 4BA8E080
        EE86BEA5 EEADC93D 8B130FB6 D35A7A48 1F6FDAB0 7C1090C2


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

    i = 2

    counter||no_of_bits_to_return||input_string is
                          020000 020900F1 4946DBFF 59362D20
        3C625CE8 900A7268 AFE15576 665F278E 7869ADBD 7B6EB05C
        B068C6AA 3E060798 85C196F9 9CB0DB8A A9E80CC6 C1EE3A08
        B2FE52BA CA3C6380 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF A0A1A2A3 A4A5A6A7
        A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF


    Hash(counter||no_of_bits_to_return||input_string) is
                        474C0D33 75C318A8 FED8EF73 696B9E5E
        3AA7244A 5F7B92C9 504DDED4 29F0B2E0 F93DD3B7 6D79E142
        F7BDE638 635A1B5A CF6EDACB 74A60ACA 6DF0BB20 316CC953


    temp =
                      F8A5 ADF3B0C5 2B4A48EC AF75E461 0EFD7AF7
        2B368C25 67D1941D B67FA608 ED5CBB33 63F84BA8 E080EE86
        BEA5EEAD C93D8B13 0FB6D35A 7A481F6F DAB07C10 90C2474C


s is
                         01 F14B5BE7 618A5694 91D95EEB C8C21DFA
        F5EE566D 184ACFA3 283B6CFF 4C11DAB9 7666C7F0 9751C101
        DD0D7D4B DD5B927B 16261F6D A6B4F490 3EDFB560 F8212184


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

DualEC_DRBG_Generate_algorithm
```

```
  additional_input is  <empty>

  requested_number_of_bits is 1008
------------
i=0
t is
                   01F1 4B5BE761 8A569491 D95EEBC8 C21DFAF5
      EE566D18 4ACFA328 3B6CFF4C 11DAB976 66C7F097 51C101DD
      0D7D4BDD 5B927B16 261F6DA6 B4F4903E DFB560F8 2121848E


s is
                   0050 F49247E7 838E0870 E127C9DA 71FC315C
      72AE5B72 EDA017C4 385853A5 6F576F1D 21711BFA 4E14A261
      4A0C6381 5FD4C255 1024FACD DDD48FFA A95FD223 5583E7FE


r is
                   0105 CF83B78B 20678544 12EEB24A EA86064D
      510C68FD 96DBF94E AC1BC202 2752D755 8AEB9F97 B9CBC1B9
      648FE4D8 8E2C82A6 F530675E 1DB92D39 6D6D85BD AD2A23CB


------------
tmp is
                         83B78B 20678544 12EEB24A EA86064D
      510C68FD 96DBF94E AC1BC202 2752D755 8AEB9F97 B9CBC1B9
      648FE4D8 8E2C82A6 F530675E 1DB92D39 6D6D85BD AD2A23CB


------------
i=1
t is
                   0050 F49247E7 838E0870 E127C9DA 71FC315C
      72AE5B72 EDA017C4 385853A5 6F576F1D 21711BFA 4E14A261
      4A0C6381 5FD4C255 1024FACD DDD48FFA A95FD223 5583E7FE


s is
                   0144 5F925D29 26DA7FEF C2321DE0 4291E6A2
      1D1CE2E0 996C30C4 22B3B7B6 E9A082F4 29D7C99D 7705C43A
      350FF0D9 94D00279 DF9AD924 BBF89BEA 6815CC57 9456C3D3


r is
                   0144 7DD10AD8 08ECCCFB FC811EB6 8AE835E4
```

```
      912E011D D10A4399 C8DE2D9D 88F81B61 68B05D28 2B9DAC1E
      65E0A45F 61043E1F A047870D D582295E 6C50DD11 85B13594


  ------------
  tmp is
                                                 83B7 8B206785
      4412EEB2 4AEA8606 4D510C68 FD96DBF9 4EAC1BC2 022752D7
      558AEB9F 97B9CBC1 B9648FE4 D88E2C82 A6F53067 5E1DB92D
      396D6D85 BDAD2A23 CBD10AD8 08ECCCFB FC811EB6 8AE835E4
      912E011D D10A4399 C8DE2D9D 88F81B61 68B05D28 2B9DAC1E
      65E0A45F 61043E1F A047870D D582295E 6C50DD11 85B13594


  ------------
  s is
                     016D 61DC3D5D 4D16A71F CAFAC01A 0386F31B
      15C55FF0 761A21D9 406B317B BB567F9C E892DEB7 02FD5895
      882B71DF 19D757F4 76BCC728 373F63F0 1FB5B85D ABDD1E27


rnd_val is
                                                 83B7 8B206785
      4412EEB2 4AEA8606 4D510C68 FD96DBF9 4EAC1BC2 022752D7
      558AEB9F 97B9CBC1 B9648FE4 D88E2C82 A6F53067 5E1DB92D
      396D6D85 BDAD2A23 CBD10AD8 08ECCCFB FC811EB6 8AE835E4
      912E011D D10A4399 C8DE2D9D 88F81B61 68B05D28 2B9DAC1E
      65E0A45F 61043E1F A047870D D582295E 6C50DD11 85B13594
```