

```
#####
```

CTR_DRBG

Requested Security Strength = 112

prediction_resistance_flag = "NOT ENABLED"

EntropyInput =

00 01020304

05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C

EntropyInput1 (for Reseed1) =

80 81828384

85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C

EntropyInput2 (for Reseed2) =

C0 C1C2C3C4

C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBD

Nonce =

202122 23242526

PersonalizationString = <empty>

AdditionalInput = <empty>

```
#####
```

```
*****
```

CTR_DRBG_Instantiate_algorithm - with derivation function

entropy_input is

00 01020304

05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C

nonce is

202122 23242526

personal_str is <empty>

```
prediction_resistance_flag = "No PredictionResistance"
```

```
-----  
Block_Cipher_df
```

```
input_str is
```

```
00010203 04050607 08090A0B  
0C0D0E0F 10111213 14151617 18191A1B 1C202122 23242526
```

```
number_of_bits_to_return = 232
```

```
S is
```

```
00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F  
10111213 14151617 18191A1B 1C202122 23242526 80000000
```

```
-----
```

```
BCC
```

```
IV is
```

```
00000000 00000000
```

```
IV || S is
```

```
00000000 00000000  
00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F  
10111213 14151617 18191A1B 1C202122 23242526 80000000
```

```
temp is
```

```
4A2145C3 52BD4642
```

```
-----
```

```
BCC
```

```
IV is
```

```
00000001 00000000
```

```
IV || S is
```

00000001 00000000
00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

temp is

4A2145C3 52BD4642 EEB5E70D CAE11D42

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000
00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

temp is

4A2145C3 52BD4642 EEB5E70D CAE11D42 82FD02F7 B62641C4

BCC

IV is

00000003 00000000

IV || S is

00000003 00000000
00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

temp is

4A2145C3 52BD4642
EEB5E70D CAE11D42 82FD02F7 B62641C4 BAE575D6 E7411566

Key is

4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

2641C4BA E575D6E7

Block #1

Blockin 2641C4BA E575D6E7

Blockout B4300B8B 7D547B40

BlockEncrypt

Key is

4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

2641C4BA E575D6E7

X = BlockEncrypt(Key, X) is

B4300B8B 7D547B40

temp is

B4300B8B 7D547B40

Block #1

Blockin B4300B8B 7D547B40

Blockout 599CFD0E B13B1607

BlockEncrypt

Key is

4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

B4300B8B 7D547B40

X = BlockEncrypt(Key, X) is

599CFD0E B13B1607

temp is

B4300B8B 7D547B40 599CFD0E B13B1607

Block #1

Blockin 599CFD0E B13B1607

Blockout 2398EF59 1553A5A3

BlockEncrypt

Key is

4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

599CFD0E B13B1607

X = BlockEncrypt(Key, X) is

2398EF59 1553A5A3

temp is

B4300B8B 7D547B40 599CFD0E B13B1607 2398EF59 1553A5A3

Block #1

Blockin 2398EF59 1553A5A3

Blockout A10292FE FE535642

BlockEncrypt

Key is

4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

2398EF59 1553A5A3

X = BlockEncrypt(Key, X) is

A10292FE FE535642

temp is

B4300B8B 7D547B40
599CFD0E B13B1607 2398EF59 1553A5A3 A10292FE FE535642

requested_bits is

B4 300B8B7D
547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE

seed_material is

B4 300B8B7D
547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE

Update

provided_data is

B4 300B8B7D
547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE

While loop

Key is

00 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000001

Block #1
Blockin 00000000 00000001
Blockout 166B40B4 4ABA4BD6

output_block is
166B40B4 4ABA4BD6

temp is
166B40B4 4ABA4BD6

While loop

Key is
00 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000002

Block #1
Blockin 00000000 00000002
Blockout 06E7EA22 CE92708F

output_block is
06E7EA22 CE92708F

temp is
166B40B4 4ABA4BD6 06E7EA22 CE92708F

While loop

Key is
00 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000003

Block #1
Blockin 00000000 00000003
Blockout 4EB190C9 A2FA169C

output_block is
4EB190C9 A2FA169C

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

While loop

Key is
00 0000000 0000000 0000000 0000000 0000000

V is
00000000 00000004

Block #1
Blockin 00000000 00000004
Blockout D2FD8867 D50D2DFE

output_block is
D2FD8867 D50D2DFE

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

temp XOR provided_data is
A2 5B4B3F37
EE30965F 7B172C7F A966886D 297F90B7 A9B33F73 FF1A992B

Key is
A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is

A9B33F73 FF1A992B

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is <empty>

Block #1

Blockin A9B33F73 FF1A992C

Blockout ABC88224 514D0316

Block #1

Blockin A9B33F73 FF1A992D

Blockout EA3D48AE E3C9A2B4

Update

provided_data is

00 00000000

00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is

A9B33F73 FF1A992E

Block #1
Blockin A9B33F73 FF1A992E
Blockout 27CE2546 E5F9CE73

output_block is
27CE2546 E5F9CE73

temp is
27CE2546 E5F9CE73

While loop

Key is
A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is
A9B33F73 FF1A992F

Block #1
Blockin A9B33F73 FF1A992F
Blockout AC843CE9 A9F8B369

output_block is
AC843CE9 A9F8B369

temp is
27CE2546 E5F9CE73 AC843CE9 A9F8B369

While loop

Key is
A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is

A9B33F73 FF1A9930

Block #1

Blockin A9B33F73 FF1A9930
Blockout D6053CD6 D4543E9B

output_block is

D6053CD6 D4543E9B

temp is

27CE2546 E5F9CE73 AC843CE9 A9F8B369 D6053CD6 D4543E9B

While loop

Key is

A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is

A9B33F73 FF1A9931

Block #1

Blockin A9B33F73 FF1A9931
Blockout CF882969 5162BE82

output_block is

CF882969 5162BE82

temp is

27CE2546 E5F9CE73

AC843CE9 A9F8B369 D6053CD6 D4543E9B CF882969 5162BE82

temp XOR provided_data is

27 CE2546E5

F9CE73AC 843CE9A9 F8B369D6 053CD6D4 543E9BCF 88296951

Key is

27 CE2546E5 F9CE73AC 843CE9A9 F8B369D6 053CD6D4

V is

543E9BCF 88296951

rnd_val is

ABC88224 514D0316 EA3D48AE E3C9A2B4

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is <empty>

Block #1

Blockin 543E9BCF 88296952

Blockout D3D3F372 E43E7ABD

Block #1

Blockin 543E9BCF 88296953

Blockout C4FA2937 43EED076

Update

provided_data is

00 00000000

00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

27 CE2546E5 F9CE73AC 843CE9A9 F8B369D6 053CD6D4

V is

543E9BCF 88296954

Block #1

Blockin 543E9BCF 88296954
Blockout 4966D8DE 011D2169

output_block is

4966D8DE 011D2169

temp is

4966D8DE 011D2169

While loop

Key is

27 CE2546E5 F9CE73AC 843CE9A9 F8B369D6 053CD6D4

V is

543E9BCF 88296955

Block #1

Blockin 543E9BCF 88296955
Blockout D0EA8DCA 25F59A82

output_block is

D0EA8DCA 25F59A82

temp is

4966D8DE 011D2169 D0EA8DCA 25F59A82

While loop

Key is

27 CE2546E5 F9CE73AC 843CE9A9 F8B369D6 053CD6D4

V is

543E9BCF 88296956

Block #1

Blockin 543E9BCF 88296956

Blockout 9C246045 E5453E30

output_block is

9C246045 E5453E30

temp is

4966D8DE 011D2169 D0EA8DCA 25F59A82 9C246045 E5453E30

While loop

Key is

27 CE2546E5 F9CE73AC 843CE9A9 F8B369D6 053CD6D4

V is

543E9BCF 88296957

Block #1

Blockin 543E9BCF 88296957

Blockout 6D98529D 4CF1B0A6

output_block is

6D98529D 4CF1B0A6

temp is

4966D8DE 011D2169

D0EA8DCA 25F59A82 9C246045 E5453E30 6D98529D 4CF1B0A6

temp XOR provided_data is

49 66D8DE01
1D2169D0 EA8DCA25 F59A829C 246045E5 453E306D 98529D4C

Key is

49 66D8DE01 1D2169D0 EA8DCA25 F59A829C 246045E5

V is

453E306D 98529D4C

rnd_val is

D3D3F372 E43E7ABD C4FA2937 43EED076

#####

CTR_DRBG

Requested Security Strength = 112

prediction_resistance_flag = "NOT ENABLED"

EntropyInput =

00 01020304

05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C

EntropyInput1 (for Reseed1) =

80 81828384

85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C

EntropyInput2 (for Reseed2) =

C0 C1C2C3C4

C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBD

Nonce =

202122 23242526

PersonalizationString = <empty>

AdditionalInput1 =

60 61626364

65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C

AdditionalInput2 =
A0 A1A2A3A4
A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC

#####
#####

CTR_DRBG_Instantiate_algorithm - with derivation function

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

nonce is

202122 23242526

personal_str is <empty>

prediction_resistance_flag = "No PredictionResistance"

Block_Cipher_df

input_str is
00010203 04050607 08090A0B
0C0D0E0F 10111213 14151617 18191A1B 1C202122 23242526

number_of_bits_to_return = 232

S is
00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000

00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

temp is

4A2145C3 52BD4642

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000

00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

temp is

4A2145C3 52BD4642 EEB5E70D CAE11D42

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000

00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

temp is
4A2145C3 52BD4642 EEB5E70D CAE11D42 82FD02F7 B62641C4

BCC

IV is
00000003 00000000

IV || S is
00000003 00000000
00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

temp is
4A2145C3 52BD4642
EEB5E70D CAE11D42 82FD02F7 B62641C4 BAE575D6 E7411566

Key is
4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is
2641C4BA E575D6E7

Block #1
Blockin 2641C4BA E575D6E7
Blockout B4300B8B 7D547B40

BlockEncrypt

Key is
4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

2641C4BA E575D6E7

X = BlockEncrypt(Key, X) is

B4300B8B 7D547B40

temp is

B4300B8B 7D547B40

Block #1

Blockin B4300B8B 7D547B40

Blockout 599CFD0E B13B1607

BlockEncrypt

Key is

4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

B4300B8B 7D547B40

X = BlockEncrypt(Key, X) is

599CFD0E B13B1607

temp is

B4300B8B 7D547B40 599CFD0E B13B1607

Block #1

Blockin 599CFD0E B13B1607

Blockout 2398EF59 1553A5A3

BlockEncrypt

Key is

4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

599CFD0E B13B1607

X = BlockEncrypt(Key, X) is

2398EF59 1553A5A3

temp is

B4300B8B 7D547B40 599CFD0E B13B1607 2398EF59 1553A5A3

Block #1

Blockin 2398EF59 1553A5A3

Blockout A10292FE FE535642

BlockEncrypt

Key is

4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

2398EF59 1553A5A3

X = BlockEncrypt(Key, X) is

A10292FE FE535642

temp is

B4300B8B 7D547B40

599CFD0E B13B1607 2398EF59 1553A5A3 A10292FE FE535642

requested_bits is

B4 300B8B7D

547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE

seed_material is

B4 300B8B7D

547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE

Update

provided_data is

B4 300B8B7D

547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE

While loop

Key is

00 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000001

Block #1

Blockin 00000000 00000001

Blockout 166B40B4 4ABA4BD6

output_block is

166B40B4 4ABA4BD6

temp is

166B40B4 4ABA4BD6

While loop

Key is

00 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000002

Block #1
Blockin 00000000 00000002
Blockout 06E7EA22 CE92708F

output_block is
06E7EA22 CE92708F

temp is
166B40B4 4ABA4BD6 06E7EA22 CE92708F

While loop

Key is
00 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000003

Block #1
Blockin 00000000 00000003
Blockout 4EB190C9 A2FA169C

output_block is
4EB190C9 A2FA169C

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

While loop

Key is
00 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000004

Block #1

Blockin 00000000 00000004

Blockout D2FD8867 D50D2DFE

output_block is

D2FD8867 D50D2DFE

temp is

166B40B4 4ABA4BD6

06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE

temp XOR provided_data is

A2 5B4B3F37

EE30965F 7B172C7F A966886D 297F90B7 A9B33F73 FF1A992B

Key is

A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is

A9B33F73 FF1A992B

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is

60 61626364

65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C

additional_input <> NULL, process appropriately

Block_Cipher_df

input_str is

60 61626364
65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C

number_of_bits_to_return = 232

S is

0000001D 0000001D 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000 0000001D 0000001D 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000

temp is

A9DAAC27 BD128BB4

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000 0000001D 0000001D 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000

temp is
A9DAAC27 BD128BB4 08EB0C8C 15DB001C

BCC

IV is
00000002 00000000

IV || S is
00000002 00000000 0000001D 0000001D 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000

temp is
A9DAAC27 BD128BB4 08EB0C8C 15DB001C 68175B62 9929DBB3

BCC

IV is
00000003 00000000

IV || S is
00000003 00000000 0000001D 0000001D 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000

temp is
A9DAAC27 BD128BB4
08EB0C8C 15DB001C 68175B62 9929DBB3 EBF330CD 6977A3C0

Key is
A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299

X is

29DBB3EB F330CD69

Block #1
Blockin 29DBB3EB F330CD69
Blockout 68099422 99837788

BlockEncrypt

Key is
A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299

X is

29DBB3EB F330CD69

X = BlockEncrypt(Key, X) is
68099422 99837788

temp is

68099422 99837788

Block #1
Blockin 68099422 99837788
Blockout 1665F614 303AD2C0

BlockEncrypt

Key is
A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299

X is

68099422 99837788

X = BlockEncrypt(Key, X) is
1665F614 303AD2C0

temp is

68099422 99837788 1665F614 303AD2C0

Block #1

Blockin 1665F614 303AD2C0

Blockout 3EEA906C 48996C3C

BlockEncrypt

Key is

A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299

X is

1665F614 303AD2C0

X = BlockEncrypt(Key, X) is

3EEA906C 48996C3C

temp is

68099422 99837788 1665F614 303AD2C0 3EEA906C 48996C3C

Block #1

Blockin 3EEA906C 48996C3C

Blockout 22131B5A 94AF9E8C

BlockEncrypt

Key is

A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299

X is

3EEA906C 48996C3C

X = BlockEncrypt(Key, X) is

22131B5A 94AF9E8C

temp is

68099422 99837788

1665F614 303AD2C0 3EEA906C 48996C3C 22131B5A 94AF9E8C

requested_bits is

68 09942299

83778816 65F61430 3AD2C03E EA906C48 996C3C22 131B5A94

Update

provided_data is

68 09942299

83778816 65F61430 3AD2C03E EA906C48 996C3C22 131B5A94

While loop

Key is

A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is

A9B33F73 FF1A992C

Block #1

Blockin A9B33F73 FF1A992C

Blockout ABC88224 514D0316

output_block is

ABC88224 514D0316

temp is

ABC88224 514D0316

While loop

Key is

A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is

A9B33F73 FF1A992D

Block #1

Blockin A9B33F73 FF1A992D

Blockout EA3D48AE E3C9A2B4

output_block is

EA3D48AE E3C9A2B4

temp is

ABC88224 514D0316 EA3D48AE E3C9A2B4

While loop

Key is

A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is

A9B33F73 FF1A992E

Block #1

Blockin A9B33F73 FF1A992E

Blockout 27CE2546 E5F9CE73

output_block is

27CE2546 E5F9CE73

temp is

ABC88224 514D0316 EA3D48AE E3C9A2B4 27CE2546 E5F9CE73

While loop

Key is

A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is

A9B33F73 FF1A992F

Block #1

Blockin A9B33F73 FF1A992F

Blockout AC843CE9 A9F8B369

output_block is

AC843CE9 A9F8B369

temp is

ABC88224 514D0316

EA3D48AE E3C9A2B4 27CE2546 E5F9CE73 AC843CE9 A9F8B369

temp XOR provided_data is

C3 C11606C8

CE749EFC 58BEBAD3 F3707419 24B52AAD 60A24F8E 9727B33D

Key is

C3 C11606C8 CE749EFC 58BEBAD3 F3707419 24B52AAD

V is

60A24F8E 9727B33D

Block #1

Blockin 60A24F8E 9727B33E

Blockout D4564EE0 72ACA5BD

Block #1

Blockin 60A24F8E 9727B33F

Blockout 279536E1 4F94CB12

Update

provided_data is

68 09942299

83778816 65F61430 3AD2C03E EA906C48 996C3C22 131B5A94

While loop

Key is

C3 C11606C8 CE749EFC 58BEBAD3 F3707419 24B52AAD

V is

60A24F8E 9727B340

Block #1

Blockin 60A24F8E 9727B340

Blockout 22066DF2 B2647580

output_block is

22066DF2 B2647580

temp is

22066DF2 B2647580

While loop

Key is

C3 C11606C8 CE749EFC 58BEBAD3 F3707419 24B52AAD

V is

60A24F8E 9727B341

Block #1
Blockin 60A24F8E 9727B341
Blockout 8F2219FC 67C1EF3F

output_block is
8F2219FC 67C1EF3F

temp is
22066DF2 B2647580 8F2219FC 67C1EF3F

While loop

Key is
C3 C11606C8 CE749EFC 58BEBAD3 F3707419 24B52AAD

V is
60A24F8E 9727B342

Block #1
Blockin 60A24F8E 9727B342
Blockout A78B1FEF 0CC07F38

output_block is
A78B1FEF 0CC07F38

temp is
22066DF2 B2647580 8F2219FC 67C1EF3F A78B1FEF 0CC07F38

While loop

Key is
C3 C11606C8 CE749EFC 58BEBAD3 F3707419 24B52AAD

V is

60A24F8E 9727B343

Block #1
Blockin 60A24F8E 9727B343
Blockout EBF91126 56BE9085

output_block is
EBF91126 56BE9085

temp is
22066DF2 B2647580
8F2219FC 67C1EF3F A78B1FEF 0CC07F38 EBF91126 56BE9085

temp XOR provided_data is
4A 0FF9D02B
E7020899 47EFE857 FB3DFF99 618F8344 591304C9 EA0A7CC2

Key is
4A 0FF9D02B E7020899 47EFE857 FB3DFF99 618F8344

V is
591304C9 EA0A7CC2

rnd_val is
D4564EE0 72ACA5BD 279536E1 4F94CB12

Second call to Generate

CTR_DRBG_Generate
requested_number_of_bits = 128
additional_input is
A0 A1A2A3A4
A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC

additional_input <> NULL, process appropriately

Block_Cipher_df

input_str is

A0 A1A2A3A4
A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBB

number_of_bits_to_return = 232

S is

0000001D 0000001D A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000

temp is

89213498 76E519BE

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7

A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000

temp is

89213498 76E519BE FC10164B 5A8722CE

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000

temp is

89213498 76E519BE FC10164B 5A8722CE 5C92E9C1 6F213C22

BCC

IV is

00000003 00000000

IV || S is

00000003 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000

temp is

89213498 76E519BE

FC10164B 5A8722CE 5C92E9C1 6F213C22 9B946180 1B6BAA48

Key is

89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F

X is

213C229B 9461801B

Block #1

Blockin 213C229B 9461801B
Blockout 07669398 0A486518

BlockEncrypt

Key is

89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F

X is

213C229B 9461801B

X = BlockEncrypt(Key, X) is

07669398 0A486518

temp is

07669398 0A486518

Block #1

Blockin 07669398 0A486518
Blockout DC19FECA F56EF259

BlockEncrypt

Key is

89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F

X is

07669398 0A486518

X = BlockEncrypt(Key, X) is
DC19FECA F56EF259

temp is
07669398 0A486518 DC19FECA F56EF259

Block #1
Blockin DC19FECA F56EF259
Blockout 0FF65EF1 FE9A7410

BlockEncrypt

Key is
89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F

X is
DC19FECA F56EF259

X = BlockEncrypt(Key, X) is
0FF65EF1 FE9A7410

temp is
07669398 0A486518 DC19FECA F56EF259 0FF65EF1 FE9A7410

Block #1
Blockin 0FF65EF1 FE9A7410
Blockout 8C1FC048 1C36F198

BlockEncrypt

Key is
89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F

X is
0FF65EF1 FE9A7410

X = BlockEncrypt(Key, X) is
8C1FC048 1C36F198

temp is
07669398 0A486518
DC19FECA F56EF259 0FF65EF1 FE9A7410 8C1FC048 1C36F198

requested_bits is
07 6693980A
486518DC 19FECAF5 6EF2590F F65EF1FE 9A74108C 1FC0481C

Update

provided_data is
07 6693980A
486518DC 19FECAF5 6EF2590F F65EF1FE 9A74108C 1FC0481C

While loop

Key is
4A 0FF9D02B E7020899 47EFE857 FB3DFF99 618F8344

V is
591304C9 EA0A7CC3

Block #1
Blockin 591304C9 EA0A7CC3
Blockout 9635E4B7 B32E5C48

output_block is
9635E4B7 B32E5C48

temp is

9635E4B7 B32E5C48

While loop

Key is

4A 0FF9D02B E7020899 47EFE857 FB3DFF99 618F8344

V is

591304C9 EA0A7CC4

Block #1

Blockin 591304C9 EA0A7CC4

Blockout 282A17EC C27079E4

output_block is

282A17EC C27079E4

temp is

9635E4B7 B32E5C48 282A17EC C27079E4

While loop

Key is

4A 0FF9D02B E7020899 47EFE857 FB3DFF99 618F8344

V is

591304C9 EA0A7CC5

Block #1

Blockin 591304C9 EA0A7CC5

Blockout 88315A82 0680A9C8

output_block is

88315A82 0680A9C8

temp is
9635E4B7 B32E5C48 282A17EC C27079E4 88315A82 0680A9C8

While loop

Key is
4A 0FF9D02B E7020899 47EFE857 FB3DFF99 618F8344

V is

591304C9 EA0A7CC6

Block #1
Blockin 591304C9 EA0A7CC6
Blockout A12A7C65 AE8DFB7F

output_block is
A12A7C65 AE8DFB7F

temp is
9635E4B7 B32E5C48
282A17EC C27079E4 88315A82 0680A9C8 A12A7C65 AE8DFB7F

temp XOR provided_data is
91 53772FB9
663950F4 33E92637 1E8BBD87 C70473F8 1ADDD82D 35BC2DB2

Key is
91 53772FB9 663950F4 33E92637 1E8BBD87 C70473F8

V is
1ADDD82D 35BC2DB2

Block #1
Blockin 1ADDD82D 35BC2DB3
Blockout 1CCD9AFE F15A9679

Block #1
Blockin 1ADDD82D 35BC2DB4
Blockout BA75E352 25585DEA

Update

provided_data is
07 6693980A
486518DC 19FECAF5 6EF2590F F65EF1FE 9A74108C 1FC0481C

While loop

Key is
91 53772FB9 663950F4 33E92637 1E8BBD87 C70473F8

V is

1ADDD82D 35BC2DB5

Block #1
Blockin 1ADDD82D 35BC2DB5
Blockout 36CF2571 806190D4

output_block is
36CF2571 806190D4

temp is

36CF2571 806190D4

While loop

Key is
91 53772FB9 663950F4 33E92637 1E8BBD87 C70473F8

V is

1ADDD82D 35BC2DB6

Block #1

Blockin 1ADDD82D 35BC2DB6

Blockout BD6179FA AB46D4B0

output_block is

BD6179FA AB46D4B0

temp is

36CF2571 806190D4 BD6179FA AB46D4B0

While loop

Key is

91 53772FB9 663950F4 33E92637 1E8BBB87 C70473F8

V is

1ADDD82D 35BC2DB7

Block #1

Blockin 1ADDD82D 35BC2DB7

Blockout A5452BC5 EFC172BE

output_block is

A5452BC5 EFC172BE

temp is

36CF2571 806190D4 BD6179FA AB46D4B0 A5452BC5 EFC172BE

While loop

Key is

91 53772FB9 663950F4 33E92637 1E8BBB87 C70473F8

V is

1ADDD82D 35BC2DB8

Block #1

Blockin 1ADDD82D 35BC2DB8
Blockout BAF89D04 7DEF27ED

output_block is

BAF89D04 7DEF27ED

temp is

36CF2571 806190D4

BD6179FA AB46D4B0 A5452BC5 EFC172BE BAF89D04 7DEF27ED

temp XOR provided_data is

31 A9B6E98A

29F5CC61 7887305E 2826E9AA B3753411 5B06AE36 E75D4C61

Key is

31 A9B6E98A 29F5CC61 7887305E 2826E9AA B3753411

V is

5B06AE36 E75D4C61

rnd_val is

1CCD9AFE F15A9679 BA75E352 25585DEA

#####

CTR_DRBG

Requested Security Strength = 112

prediction_resistance_flag = "NOT ENABLED"

EntropyInput =

00 01020304

05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C

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

```
EntropyInput2 (for Reseed2) =
                                C0 C1C2C3C4
    C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBD
```

```
Nonce =
        202122 23242526
```

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

```
AdditionalInput = <empty>
```

```
#####
*****
```

```
CTR_DRBG_Instantiate_algorithm - with derivation function
```

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

```
nonce is
        202122 23242526
```

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

```
prediction_resistance_flag = "No PredictionResistance"
```

```
-----
```

Block_Cipher_df

input_str is

```
00 01020304 05060708 090A0B0C 0D0E0F10  
11121314 15161718 191A1B1C 20212223 24252640 41424344  
45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C
```

number_of_bits_to_return = 232

S is

```
00000041 0000001D  
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617  
18191A1B 1C202122 23242526 40414243 44454647 48494A4B  
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000
```

BCC

IV is

```
00000000 00000000
```

IV || S is

```
00000000 00000000 00000041 0000001D  
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617  
18191A1B 1C202122 23242526 40414243 44454647 48494A4B  
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000
```

temp is

```
BF5C8905 7D02B0A6
```

BCC

IV is

```
00000001 00000000
```

IV || S is

00000001 00000000 00000041 0000001D
00010203 04050607 08090A0B 0C0D0EOF 10111213 14151617
18191A1B 1C202122 23242526 40414243 44454647 48494A4B
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000

temp is

BF5C8905 7D02B0A6 77FE7647 E9554668

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000 00000041 0000001D
00010203 04050607 08090A0B 0C0D0EOF 10111213 14151617
18191A1B 1C202122 23242526 40414243 44454647 48494A4B
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000

temp is

BF5C8905 7D02B0A6 77FE7647 E9554668 AE4D8DE0 DB992E46

BCC

IV is

00000003 00000000

IV || S is

00000003 00000000 00000041 0000001D
00010203 04050607 08090A0B 0C0D0EOF 10111213 14151617
18191A1B 1C202122 23242526 40414243 44454647 48494A4B
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000

temp is

BF5C8905 7D02B0A6

77FE7647 E9554668 AE4D8DE0 DB992E46 83E1389F 33A1E91F

Key is

BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is

992E4683 E1389F33

Block #1

Blockin 992E4683 E1389F33

Blockout 70F9F85E 350177E5

BlockEncrypt

Key is

BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is

992E4683 E1389F33

X = BlockEncrypt(Key, X) is

70F9F85E 350177E5

temp is

70F9F85E 350177E5

Block #1

Blockin 70F9F85E 350177E5

Blockout B228D49C 6374BBB6

BlockEncrypt

Key is

BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is

70F9F85E 350177E5

X = BlockEncrypt(Key, X) is

B228D49C 6374BBB6

temp is

70F9F85E 350177E5 B228D49C 6374BBB6

Block #1

Blockin B228D49C 6374BBB6

Blockout EA3DCFFA 463099CA

BlockEncrypt

Key is

BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is

B228D49C 6374BBB6

X = BlockEncrypt(Key, X) is

EA3DCFFA 463099CA

temp is

70F9F85E 350177E5 B228D49C 6374BBB6 EA3DCFFA 463099CA

Block #1

Blockin EA3DCFFA 463099CA

Blockout F0781291 15A9A8E8

BlockEncrypt

Key is

BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is

EA3DCFFA 463099CA

X = BlockEncrypt(Key, X) is

F0781291 15A9A8E8

temp is

70F9F85E 350177E5

B228D49C 6374BBB6 EA3DCFFA 463099CA F0781291 15A9A8E8

requested_bits is

70 F9F85E35

0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115

seed_material is

70 F9F85E35

0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115

Update

provided_data is

70 F9F85E35

0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115

While loop

Key is

00 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000001

Block #1
Blockin 00000000 00000001
Blockout 166B40B4 4ABA4BD6

output_block is
166B40B4 4ABA4BD6

temp is
166B40B4 4ABA4BD6

While loop

Key is
00 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000002

Block #1
Blockin 00000000 00000002
Blockout 06E7EA22 CE92708F

output_block is
06E7EA22 CE92708F

temp is
166B40B4 4ABA4BD6 06E7EA22 CE92708F

While loop

Key is
00 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000003

Block #1

Blockin 00000000 00000003

Blockout 4EB190C9 A2FA169C

output_block is

4EB190C9 A2FA169C

temp is

166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C

While loop

Key is

00 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000004

Block #1

Blockin 00000000 00000004

Blockout D2FD8867 D50D2DFE

output_block is

D2FD8867 D50D2DFE

temp is

166B40B4 4ABA4BD6

06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE

temp XOR provided_data is

66 92B8EA7F

BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4 CA8F5622 859AF6C0

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C0

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is <empty>

Block #1

Blockin CA8F5622 859AF6C1

Blockout 760BED7D 92B083B1

Block #1

Blockin CA8F5622 859AF6C2

Blockout 0AF31CF0 656081EB

Update

provided_data is

00 00000000

00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C3

Block #1

Blockin CA8F5622 859AF6C3

Blockout 51D241F0 2DA51012

output_block is

51D241F0 2DA51012

temp is

51D241F0 2DA51012

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C4

Block #1

Blockin CA8F5622 859AF6C4

Blockout AAF72BA5 971324B4

output_block is

AAF72BA5 971324B4

temp is

51D241F0 2DA51012 AAF72BA5 971324B4

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C5

Block #1

Blockin CA8F5622 859AF6C5
Blockout DE98EFE1 F7E66820

output_block is

DE98EFE1 F7E66820

temp is

51D241F0 2DA51012 AAF72BA5 971324B4 DE98EFE1 F7E66820

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C6

Block #1

Blockin CA8F5622 859AF6C6
Blockout 77D41DF0 D0B555E0

output_block is

77D41DF0 D0B555E0

temp is

51D241F0 2DA51012

AAF72BA5 971324B4 DE98EFE1 F7E66820 77D41DF0 D0B555E0

temp XOR provided_data is

51 D241F02D

A51012AA F72BA597 1324B4DE 98EFE1F7 E6682077 D41DF0D0

Key is

51 D241F02D A51012AA F72BA597 1324B4DE 98EFE1F7

V is

E6682077 D41DF0D0

rnd_val is

760BED7D 92B083B1 0AF31CF0 656081EB

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is <empty>

Block #1

Blockin E6682077 D41DF0D1

Blockout FD1AC414 82384D82

Block #1

Blockin E6682077 D41DF0D2

Blockout 3CF3FD6F 0E6C88B3

Update

provided_data is

00 00000000

00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

51 D241F02D A51012AA F72BA597 1324B4DE 98EFE1F7

V is

E6682077 D41DF0D3

Block #1

Blockin E6682077 D41DF0D3

Blockout B928604D 47360185

output_block is

B928604D 47360185

temp is

B928604D 47360185

While loop

Key is

51 D241F02D A51012AA F72BA597 1324B4DE 98EFE1F7

V is

E6682077 D41DF0D4

Block #1

Blockin E6682077 D41DF0D4

Blockout 4667FB5F 7ECEF1E0

output_block is

4667FB5F 7ECEF1E0

temp is

B928604D 47360185 4667FB5F 7ECEF1E0

While loop

Key is

51 D241F02D A51012AA F72BA597 1324B4DE 98EFE1F7

V is

E6682077 D41DF0D5

Block #1

Blockin E6682077 D41DF0D5
Blockout 090D3F82 5ADB078F

output_block is

090D3F82 5ADB078F

temp is

B928604D 47360185 4667FB5F 7ECEF1E0 090D3F82 5ADB078F

While loop

Key is

51 D241F02D A51012AA F72BA597 1324B4DE 98EFE1F7

V is

E6682077 D41DF0D6

Block #1

Blockin E6682077 D41DF0D6
Blockout 6CB64FC1 4C6821E0

output_block is

6CB64FC1 4C6821E0

temp is

B928604D 47360185
4667FB5F 7ECEF1E0 090D3F82 5ADB078F 6CB64FC1 4C6821E0

temp XOR provided_data is
B9 28604D47
36018546 67FB5F7E CEF1E009 0D3F825A DB078F6C B64FC14C

Key is
B9 28604D47 36018546 67FB5F7E CEF1E009 0D3F825A

V is
DB078F6C B64FC14C

rnd_val is
FD1AC414 82384D82 3CF3FD6F 0E6C88B3

#####

CTR_DRBG

Requested Security Strength = 112

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

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

EntropyInput2 (for Reseed2) =
C0 C1C2C3C4
C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBD**C**

Nonce =
202122 23242526

PersonalizationString =

40 41424344
45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C

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

AdditionalInput2 =
A0 A1A2A3A4
A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC

#####

CTR_DRBG_Instantiate_algorithm - with derivation function

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

nonce is
202122 23242526

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

prediction_resistance_flag = "No PredictionResistance"

Block_Cipher_df

input_str is
00 01020304 05060708 090A0B0C 0D0E0F10
11121314 15161718 191A1B1C 20212223 24252640 41424344
45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C

number_of_bits_to_return = 232

S is

00010203	04050607	08090A0B	0C0D0E0F	10111213	14151617	00000041	0000001D
18191A1B	1C202122	23242526	40414243	44454647	48494A4B		
4C4D4E4F	50515253	54555657	58595A5B	5C800000	00000000		

BCC

IV is

00000000	00000000	00000041	0000001D
----------	----------	----------	----------

IV || S is

00010203	04050607	08090A0B	0C0D0E0F	10111213	14151617	00000000	00000000
18191A1B	1C202122	23242526	40414243	44454647	48494A4B		
4C4D4E4F	50515253	54555657	58595A5B	5C800000	00000000		

temp is

BF5C8905	7D02B0A6
----------	----------

BCC

IV is

00000001	00000000	00000041	0000001D
----------	----------	----------	----------

IV || S is

00010203	04050607	08090A0B	0C0D0E0F	10111213	14151617	00000001	0000001D
18191A1B	1C202122	23242526	40414243	44454647	48494A4B		
4C4D4E4F	50515253	54555657	58595A5B	5C800000	00000000		

temp is

BF5C8905	7D02B0A6	77FE7647	E9554668
----------	----------	----------	----------

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000 00000041 0000001D
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C202122 23242526 40414243 44454647 48494A4B
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000

temp is

BF5C8905 7D02B0A6 77FE7647 E9554668 AE4D8DE0 DB992E46

BCC

IV is

00000003 00000000

IV || S is

00000003 00000000 00000041 0000001D
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C202122 23242526 40414243 44454647 48494A4B
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000

temp is

BF5C8905 7D02B0A6
77FE7647 E9554668 AE4D8DE0 DB992E46 83E1389F 33A1E91F

Key is

BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is
992E4683 E1389F33

Block #1
Blockin 992E4683 E1389F33
Blockout 70F9F85E 350177E5

BlockEncrypt

Key is
BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is
992E4683 E1389F33

X = BlockEncrypt(Key, X) is
70F9F85E 350177E5

temp is
70F9F85E 350177E5

Block #1
Blockin 70F9F85E 350177E5
Blockout B228D49C 6374BBB6

BlockEncrypt

Key is
BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is
70F9F85E 350177E5

X = BlockEncrypt(Key, X) is
B228D49C 6374BBB6

temp is

70F9F85E 350177E5 B228D49C 6374BBB6

Block #1

Blockin B228D49C 6374BBB6

Blockout EA3DCFFA 463099CA

BlockEncrypt

Key is

BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is

B228D49C 6374BBB6

X = BlockEncrypt(Key, X) is

EA3DCFFA 463099CA

temp is

70F9F85E 350177E5 B228D49C 6374BBB6 EA3DCFFA 463099CA

Block #1

Blockin EA3DCFFA 463099CA

Blockout F0781291 15A9A8E8

BlockEncrypt

Key is

BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is

EA3DCFFA 463099CA

X = BlockEncrypt(Key, X) is
F0781291 15A9A8E8

temp is
70F9F85E 350177E5
B228D49C 6374BBB6 EA3DCFFA 463099CA F0781291 15A9A8E8

requested_bits is
70 F9F85E35
0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115

seed_material is
70 F9F85E35
0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115

Update

provided_data is
70 F9F85E35
0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115

While loop

Key is
00 0000000 0000000 0000000 0000000 0000000

V is
00000000 00000001

Block #1
Blockin 00000000 00000001
Blockout 166B40B4 4ABA4BD6

output_block is
166B40B4 4ABA4BD6

temp is

166B40B4 4ABA4BD6

While loop

Key is

00 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000002

Block #1

Blockin 00000000 00000002

Blockout 06E7EA22 CE92708F

output_block is

06E7EA22 CE92708F

temp is

166B40B4 4ABA4BD6 06E7EA22 CE92708F

While loop

Key is

00 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000003

Block #1

Blockin 00000000 00000003

Blockout 4EB190C9 A2FA169C

output_block is

4EB190C9 A2FA169C

temp is

166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C

While loop

Key is

00 0000000 0000000 0000000 0000000 0000000

V is

00000000 00000004

Block #1

Blockin 00000000 00000004

Blockout D2FD8867 D50D2DFE

output_block is

D2FD8867 D50D2DFE

temp is

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

temp XOR provided_data is

66 92B8EA7F
BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4 CA8F5622 859AF6C0

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C0

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is

60 61626364
65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C

additional_input <> NULL, process appropriately

Block_Cipher_df

input_str is

60 61626364
65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C

number_of_bits_to_return = 232

S is

0000001D 0000001D 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000 0000001D 0000001D 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000

temp is

A9DAAC27 BD128BB4

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000 0000001D 0000001D 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000

temp is

A9DAAC27 BD128BB4 08EB0C8C 15DB001C

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000 0000001D 0000001D 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000

temp is

A9DAAC27 BD128BB4 08EB0C8C 15DB001C 68175B62 9929DBB3

BCC

IV is

00000003 00000000

IV || S is

00000003 00000000 0000001D 0000001D 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C800000

temp is

A9AAC27 BD128BB4
08EB0C8C 15DB001C 68175B62 9929DBB3 EBF330CD 6977A3C0

Key is

A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299

X is

29DBB3EB F330CD69

Block #1

Blockin 29DBB3EB F330CD69
Blockout 68099422 99837788

BlockEncrypt

Key is

A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299

X is

29DBB3EB F330CD69

X = BlockEncrypt(Key, X) is

68099422 99837788

temp is

68099422 99837788

Block #1

Blockin 68099422 99837788
Blockout 1665F614 303AD2C0

BlockEncrypt

Key is

A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299

X is

68099422 99837788

X = BlockEncrypt(Key, X) is

1665F614 303AD2C0

temp is

68099422 99837788 1665F614 303AD2C0

Block #1

Blockin 1665F614 303AD2C0

Blockout 3EEA906C 48996C3C

BlockEncrypt

Key is

A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299

X is

1665F614 303AD2C0

X = BlockEncrypt(Key, X) is

3EEA906C 48996C3C

temp is

68099422 99837788 1665F614 303AD2C0 3EEA906C 48996C3C

Block #1

Blockin 3EEA906C 48996C3C
Blockout 22131B5A 94AF9E8C

BlockEncrypt

Key is

A9 DAAC27BD 128BB408 EB0C8C15 DB001C68 175B6299

X is

3EEA906C 48996C3C

X = BlockEncrypt(Key, X) is

22131B5A 94AF9E8C

temp is

68099422 99837788

1665F614 303AD2C0 3EEA906C 48996C3C 22131B5A 94AF9E8C

requested_bits is

68 09942299

83778816 65F61430 3AD2C03E EA906C48 996C3C22 131B5A94

Update

provided_data is

68 09942299

83778816 65F61430 3AD2C03E EA906C48 996C3C22 131B5A94

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C1

Block #1

Blockin CA8F5622 859AF6C1

Blockout 760BED7D 92B083B1

output_block is

760BED7D 92B083B1

temp is

760BED7D 92B083B1

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C2

Block #1

Blockin CA8F5622 859AF6C2

Blockout 0AF31CF0 656081EB

output_block is

0AF31CF0 656081EB

temp is

760BED7D 92B083B1 0AF31CF0 656081EB

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C3

Block #1

Blockin CA8F5622 859AF6C3

Blockout 51D241F0 2DA51012

output_block is

51D241F0 2DA51012

temp is

760BED7D 92B083B1 0AF31CF0 656081EB 51D241F0 2DA51012

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C4

Block #1

Blockin CA8F5622 859AF6C4

Blockout AAF72BA5 971324B4

output_block is

AAF72BA5 971324B4

temp is

760BED7D 92B083B1

0AF31CF0 656081EB 51D241F0 2DA51012 AAF72BA5 971324B4

temp XOR provided_data is

1E 02795F0B

33F4391C 96EAE455 5A532B6F 38D19C65 3C7C2E88 E430FF03

Key is
1E 02795F0B 33F4391C 96EAE455 5A532B6F 38D19C65

V is
3C7C2E88 E430FF03

Block #1
Blockin 3C7C2E88 E430FF04
Blockout 7A4C1D7A DC8A67FD

Block #1
Blockin 3C7C2E88 E430FF05
Blockout B50100ED 23583A2C

Update

provided_data is
68 09942299
83778816 65F61430 3AD2C03E EA906C48 996C3C22 131B5A94

While loop

Key is
1E 02795F0B 33F4391C 96EAE455 5A532B6F 38D19C65

V is
3C7C2E88 E430FF06

Block #1
Blockin 3C7C2E88 E430FF06
Blockout E389E6D3 774C1B77

output_block is
E389E6D3 774C1B77

temp is

E389E6D3 774C1B77

While loop

Key is

1E 02795F0B 33F4391C 96EAE455 5A532B6F 38D19C65

V is

3C7C2E88 E430FF07

Block #1

Blockin 3C7C2E88 E430FF07

Blockout 95098FD6 517B8586

output_block is

95098FD6 517B8586

temp is

E389E6D3 774C1B77 95098FD6 517B8586

While loop

Key is

1E 02795F0B 33F4391C 96EAE455 5A532B6F 38D19C65

V is

3C7C2E88 E430FF08

Block #1

Blockin 3C7C2E88 E430FF08

Blockout 39FA9717 298A170E

output_block is

39FA9717 298A170E

temp is
E389E6D3 774C1B77 95098FD6 517B8586 39FA9717 298A170E

While loop

Key is
1E 02795F0B 33F4391C 96EAE455 5A532B6F 38D19C65

V is

3C7C2E88 E430FF09

Block #1

Blockin 3C7C2E88 E430FF09
Blockout C4D08986 886423EA

output_block is

C4D08986 886423EA

temp is

E389E6D3 774C1B77
95098FD6 517B8586 39FA9717 298A170E C4D08986 886423EA

temp XOR provided_data is

8B 8072F1EE
CF6CFF83 6C79C261 41574607 10077B61 137B32E6 C392DC1C

Key is

8B 8072F1EE CF6CFF83 6C79C261 41574607 10077B61

V is

137B32E6 C392DC1C

rnd_val is

7A4C1D7A DC8A67FD B50100ED 23583A2C

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is

A0 A1A2A3A4

A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC

additional_input <> NULL, process appropriately

Block_Cipher_df

input_str is

A0 A1A2A3A4

A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC

number_of_bits_to_return = 232

S is

0000001D 0000001D A0A1A2A3 A4A5A6A7

A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7

A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000

temp is
89213498 76E519BE

BCC

IV is
00000001 00000000

IV || S is
00000001 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000

temp is
89213498 76E519BE FC10164B 5A8722CE

BCC

IV is
00000002 00000000

IV || S is
00000002 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000

temp is
89213498 76E519BE FC10164B 5A8722CE 5C92E9C1 6F213C22

BCC

IV is
00000003 00000000

IV || S is
00000003 00000000 0000001D 0000001D A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BC800000

temp is
89213498 76E519BE
FC10164B 5A8722CE 5C92E9C1 6F213C22 9B946180 1B6BAA48

Key is
89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F

X is
213C229B 9461801B

Block #1
Blockin 213C229B 9461801B
Blockout 07669398 0A486518

BlockEncrypt

Key is
89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F

X is
213C229B 9461801B

X = BlockEncrypt(Key, X) is
07669398 0A486518

temp is
07669398 0A486518

Block #1
Blockin 07669398 0A486518
Blockout DC19FECA F56EF259

BlockEncrypt

Key is
89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F

X is

07669398 0A486518

X = BlockEncrypt(Key, X) is
DC19FECA F56EF259

temp is

07669398 0A486518 DC19FECA F56EF259

Block #1
Blockin DC19FECA F56EF259
Blockout 0FF65EF1 FE9A7410

BlockEncrypt

Key is
89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F

X is

DC19FECA F56EF259

X = BlockEncrypt(Key, X) is
0FF65EF1 FE9A7410

temp is

07669398 0A486518 DC19FECA F56EF259 0FF65EF1 FE9A7410

Block #1
Blockin 0FF65EF1 FE9A7410
Blockout 8C1FC048 1C36F198

BlockEncrypt

Key is
89 21349876 E519BEFC 10164B5A 8722CE5C 92E9C16F

X is
0FF65EF1 FE9A7410

X = BlockEncrypt(Key, X) is
8C1FC048 1C36F198

temp is
07669398 0A486518
DC19FECA F56EF259 0FF65EF1 FE9A7410 8C1FC048 1C36F198

requested_bits is
07 6693980A
486518DC 19FECAF5 6EF2590F F65EF1FE 9A74108C 1FC0481C

Update

provided_data is
07 6693980A
486518DC 19FECAF5 6EF2590F F65EF1FE 9A74108C 1FC0481C

While loop

Key is

8B 8072F1EE CF6CFF83 6C79C261 41574607 10077B61

V is

137B32E6 C392DC1D

Block #1

Blockin 137B32E6 C392DC1D

Blockout 71ACF298 A91A853C

output_block is

71ACF298 A91A853C

temp is

71ACF298 A91A853C

While loop

Key is

8B 8072F1EE CF6CFF83 6C79C261 41574607 10077B61

V is

137B32E6 C392DC1E

Block #1

Blockin 137B32E6 C392DC1E

Blockout 0B536A49 52A621E3

output_block is

0B536A49 52A621E3

temp is

71ACF298 A91A853C 0B536A49 52A621E3

While loop

Key is

8B 8072F1EE CF6CFF83 6C79C261 41574607 10077B61

V is

137B32E6 C392DC1F

Block #1

Blockin 137B32E6 C392DC1F

Blockout B73EC34D 076FA884

output_block is

B73EC34D 076FA884

temp is

71ACF298 A91A853C 0B536A49 52A621E3 B73EC34D 076FA884

While loop

Key is

8B 8072F1EE CF6CFF83 6C79C261 41574607 10077B61

V is

137B32E6 C392DC20

Block #1

Blockin 137B32E6 C392DC20

Blockout 8D840694 E86E372F

output_block is

8D840694 E86E372F

temp is

71ACF298 A91A853C

0B536A49 52A621E3 B73EC34D 076FA884 8D840694 E86E372F

temp XOR provided_data is
76 CA6100A3
52E024D7 4A9483A7 C8D3BAB8 C89DBCF9 F5DC9401 9BC6DCF4

Key is
76 CA6100A3 52E024D7 4A9483A7 C8D3BAB8 C89DBCF9

V is
F5DC9401 9BC6DCF4

Block #1
Blockin F5DC9401 9BC6DCF5
Blockout 43044D31 1C0E0754

Block #1
Blockin F5DC9401 9BC6DCF6
Blockout 1CA5C8B0 916976B2

Update

provided_data is
07 6693980A
486518DC 19FECAF5 6EF2590F F65EF1FE 9A74108C 1FC0481C

While loop

Key is
76 CA6100A3 52E024D7 4A9483A7 C8D3BAB8 C89DBCF9

V is
F5DC9401 9BC6DCF7

Block #1
Blockin F5DC9401 9BC6DCF7
Blockout CEF879E1 B6EF8D6F

output_block is
CEF879E1 B6EF8D6F

temp is
CEF879E1 B6EF8D6F

While loop

Key is
76 CA6100A3 52E024D7 4A9483A7 C8D3BAB8 C89DBCF9

V is
F5DC9401 9BC6DCF8

Block #1
Blockin F5DC9401 9BC6DCF8
Blockout 59D0D09C E0588BF2

output_block is
59D0D09C E0588BF2

temp is
CEF879E1 B6EF8D6F 59D0D09C E0588BF2

While loop

Key is
76 CA6100A3 52E024D7 4A9483A7 C8D3BAB8 C89DBCF9

V is
F5DC9401 9BC6DCF9

Block #1
Blockin F5DC9401 9BC6DCF9

Blockout 913215D6 1DA82FF7

output_block is

913215D6 1DA82FF7

temp is

CEF879E1 B6EF8D6F 59D0D09C E0588BF2 913215D6 1DA82FF7

While loop

Key is

76 CA6100A3 52E024D7 4A9483A7 C8D3BAB8 C89DBCF9

V is

F5DC9401 9BC6DCFA

Block #1

Blockin F5DC9401 9BC6DCFA

Blockout 4B2886B9 052DEFEB

output_block is

4B2886B9 052DEFEB

temp is

CEF879E1 B6EF8D6F

59D0D09C E0588BF2 913215D6 1DA82FF7 4B2886B9 052DEFEB

temp XOR provided_data is

C9 9EEA79BC

A7E87785 C92E5615 3679AB9E C44B27E3 325BE7C7 3746F119

Key is

C9 9EEA79BC A7E87785 C92E5615 3679AB9E C44B27E3

V is

325BE7C7 3746F119

```
rnd_val is  
43044D31 1C0E0754 1CA5C8B0 916976B2
```

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

```
CTR_DRBG
```

```
Requested Security Strength = 112
```

```
prediction_resistance_flag = "ENABLED"  
EntropyInput =
```

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

```
EntropyInput1 (for Reseed1) =
```

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

```
EntropyInput2 (for Reseed2) =
```

```
C0 C1C2C3C4  
C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBD
```

```
Nonce =
```

```
202122 23242526
```

```
PersonalizationString = <empty>
```

```
AdditionalInput = <empty>
```

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

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

```
CTR_DRBG_Instantiate_algorithm - with derivation function
```

```
entropy_input is
```

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

nonce is

202122 23242526

personal_str is <empty>

prediction_resistance_flag = "PredictionResistance"

Block_Cipher_df

input_str is

00010203 04050607 08090A0B
0C0D0E0F 10111213 14151617 18191A1B 1C202122 23242526

number_of_bits_to_return = 232

S is

00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000
00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

temp is

4A2145C3 52BD4642

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000

00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

temp is

4A2145C3 52BD4642 EEB5E70D CAE11D42

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000

00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

temp is

4A2145C3 52BD4642 EEB5E70D CAE11D42 82FD02F7 B62641C4

BCC

IV is

00000003 00000000

IV || S is

00000003 00000000

00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

temp is

4A2145C3 52BD4642
EEB5E70D CAE11D42 82FD02F7 B62641C4 BAE575D6 E7411566

Key is

4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

2641C4BA E575D6E7

Block #1

Blockin 2641C4BA E575D6E7
Blockout B4300B8B 7D547B40

BlockEncrypt

Key is

4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

2641C4BA E575D6E7

X = BlockEncrypt(Key, X) is

B4300B8B 7D547B40

temp is

B4300B8B 7D547B40

Block #1

Blockin B4300B8B 7D547B40
Blockout 599CFD0E B13B1607

BlockEncrypt

Key is

4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

B4300B8B 7D547B40

X = BlockEncrypt(Key, X) is

599CFD0E B13B1607

temp is

B4300B8B 7D547B40 599CFD0E B13B1607

Block #1

Blockin 599CFD0E B13B1607

Blockout 2398EF59 1553A5A3

BlockEncrypt

Key is

4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

599CFD0E B13B1607

X = BlockEncrypt(Key, X) is

2398EF59 1553A5A3

temp is

B4300B8B 7D547B40 599CFD0E B13B1607 2398EF59 1553A5A3

Block #1

Blockin 2398EF59 1553A5A3

Blockout A10292FE FE535642

BlockEncrypt

Key is

4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

2398EF59 1553A5A3

X = BlockEncrypt(Key, X) is

A10292FE FE535642

temp is

B4300B8B 7D547B40

599CFD0E B13B1607 2398EF59 1553A5A3 A10292FE FE535642

requested_bits is

B4 300B8B7D

547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE

seed_material is

B4 300B8B7D

547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE

Update

provided_data is

B4 300B8B7D

547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE

While loop

Key is

00 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000001

Block #1

Blockin 00000000 00000001
Blockout 166B40B4 4ABA4BD6

output_block is

166B40B4 4ABA4BD6

temp is

166B40B4 4ABA4BD6

While loop

Key is

00 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000002

Block #1

Blockin 00000000 00000002
Blockout 06E7EA22 CE92708F

output_block is

06E7EA22 CE92708F

temp is

166B40B4 4ABA4BD6 06E7EA22 CE92708F

While loop

Key is

00 0000000 0000000 0000000 0000000 0000000

V is

00000000 00000003

Block #1

Blockin 00000000 00000003

Blockout 4EB190C9 A2FA169C

output_block is

4EB190C9 A2FA169C

temp is

166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C

While loop

Key is

00 0000000 0000000 0000000 0000000 0000000

V is

00000000 00000004

Block #1

Blockin 00000000 00000004

Blockout D2FD8867 D50D2DFE

output_block is

D2FD8867 D50D2DFE

temp is

166B40B4 4ABA4BD6

06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE

temp XOR provided_data is

```
A2 5B4B3F37  
EE30965F 7B172C7F A966886D 297F90B7 A9B33F73 FF1A992B
```

Key is

```
A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7
```

V is

```
A9B33F73 FF1A992B
```

First call to Generate

```
*****
```

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is <empty>

Generate FAILED: Reseed is required

```
*****
```

CTR_DRBG_Reseed

entropy_input is

```
80 81828384
```

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

additional_input is <empty>

Block_Cipher_df

input_str is

```
80 81828384
```

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

number_of_bits_to_return = 232

S is

0000001D 0000001D 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000 0000001D 0000001D 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000

temp is

B435EC36 31249E3D

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000 0000001D 0000001D 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000

temp is

B435EC36 31249E3D A735CE05 7E609075

BCC

IV is

00000002 00000000

IV || S is
00000002 00000000 0000001D 0000001D 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000

temp is
B435EC36 31249E3D A735CE05 7E609075 CA6920F2 1DF7CB3D

BCC

IV is
00000003 00000000

IV || S is
00000003 00000000 0000001D 0000001D 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000

temp is
B435EC36 31249E3D
A735CE05 7E609075 CA6920F2 1DF7CB3D 6547CE54 BA8A17A5

Key is
B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D

X is
F7CB3D65 47CE54BA

Block #1
Blockin F7CB3D65 47CE54BA
Blockout 7D3F6CAF 387E4C9A

BlockEncrypt

Key is

B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D

X is

F7CB3D65 47CE54BA

X = BlockEncrypt(Key, X) is

7D3F6CAF 387E4C9A

temp is

7D3F6CAF 387E4C9A

Block #1

Blockin 7D3F6CAF 387E4C9A

Blockout 1A5787D4 81378C06

BlockEncrypt

Key is

B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D

X is

7D3F6CAF 387E4C9A

X = BlockEncrypt(Key, X) is

1A5787D4 81378C06

temp is

7D3F6CAF 387E4C9A 1A5787D4 81378C06

Block #1

Blockin 1A5787D4 81378C06

Blockout C409511D DB736F2D

BlockEncrypt

Key is

B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D

X is

1A5787D4 81378C06

X = BlockEncrypt(Key, X) is

C409511D DB736F2D

temp is

7D3F6CAF 387E4C9A 1A5787D4 81378C06 C409511D DB736F2D

Block #1

Blockin C409511D DB736F2D

Blockout D4CB361F 4C1392A0

BlockEncrypt

Key is

B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D

X is

C409511D DB736F2D

X = BlockEncrypt(Key, X) is

D4CB361F 4C1392A0

temp is

7D3F6CAF 387E4C9A

1A5787D4 81378C06 C409511D DB736F2D D4CB361F 4C1392A0

requested_bits is

7D 3F6CAF38

7E4C9A1A 5787D481 378C06C4 09511DDB 736F2DD4 CB361F4C

Update

provided_data is

7D 3F6CAF38

7E4C9A1A 5787D481 378C06C4 09511DDB 736F2DD4 CB361F4C

While loop

Key is

A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is

A9B33F73 FF1A992C

Block #1

Blockin A9B33F73 FF1A992C

Blockout ABC88224 514D0316

output_block is

ABC88224 514D0316

temp is

ABC88224 514D0316

While loop

Key is

A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is

A9B33F73 FF1A992D

Block #1
Blockin A9B33F73 FF1A992D
Blockout EA3D48AE E3C9A2B4

output_block is
EA3D48AE E3C9A2B4

temp is
ABC88224 514D0316 EA3D48AE E3C9A2B4

While loop

Key is
A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is
A9B33F73 FF1A992E

Block #1
Blockin A9B33F73 FF1A992E
Blockout 27CE2546 E5F9CE73

output_block is
27CE2546 E5F9CE73

temp is
ABC88224 514D0316 EA3D48AE E3C9A2B4 27CE2546 E5F9CE73

While loop

Key is
A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is

A9B33F73 FF1A992F

Block #1

Blockin A9B33F73 FF1A992F

Blockout AC843CE9 A9F8B369

output_block is

AC843CE9 A9F8B369

temp is

ABC88224 514D0316

EA3D48AE E3C9A2B4 27CE2546 E5F9CE73 AC843CE9 A9F8B369

temp XOR provided_data is

D6 F7EE8B69

334F8CF0 6ACF7A62 FE2EB2E3 C7745B3E 8AA15E78 4F0AF6E5

Key is

D6 F7EE8B69 334F8CF0 6ACF7A62 FE2EB2E3 C7745B3E

V is

8AA15E78 4F0AF6E5

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is <empty>

Block #1

Blockin 8AA15E78 4F0AF6E6

Blockout 8FB78ABC A75C9F28

Block #1

Blockin 8AA15E78 4F0AF6E7

Blockout 4E974E36 141866BC

Update

provided_data is

00 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

D6 F7EE8B69 334F8CF0 6ACF7A62 FE2EB2E3 C7745B3E

V is

8AA15E78 4F0AF6E8

Block #1

Blockin 8AA15E78 4F0AF6E8

Blockout 8E30D7EE C6D9C99D

output_block is

8E30D7EE C6D9C99D

temp is

8E30D7EE C6D9C99D

While loop

Key is

D6 F7EE8B69 334F8CF0 6ACF7A62 FE2EB2E3 C7745B3E

V is

8AA15E78 4F0AF6E9

Block #1

Blockin 8AA15E78 4F0AF6E9
Blockout 83C99986 9BB24B13

output_block is
83C99986 9BB24B13

temp is
8E30D7EE C6D9C99D 83C99986 9BB24B13

While loop

Key is
D6 F7EE8B69 334F8CF0 6ACF7A62 FE2EB2E3 C7745B3E

V is
8AA15E78 4F0AF6EA

Block #1
Blockin 8AA15E78 4F0AF6EA
Blockout C2EC88E6 D3496FDA

output_block is
C2EC88E6 D3496FDA

temp is
8E30D7EE C6D9C99D 83C99986 9BB24B13 C2EC88E6 D3496FDA

While loop

Key is
D6 F7EE8B69 334F8CF0 6ACF7A62 FE2EB2E3 C7745B3E

V is
8AA15E78 4F0AF6EB

Block #1
Blockin 8AA15E78 4F0AF6EB
Blockout 6CFFF2EA DAFF7F6D

output_block is
6CFFF2EA DAFF7F6D

temp is
8E30D7EE C6D9C99D
83C99986 9BB24B13 C2EC88E6 D3496FDA 6CFFF2EA DAFF7F6D

temp XOR provided_data is
8E 30D7EEC6
D9C99D83 C999869B B24B13C2 EC88E6D3 496FDA6C FFF2EADA

Key is
8E 30D7EEC6 D9C99D83 C999869B B24B13C2 EC88E6D3

V is
496FDA6C FFF2EADA

rnd_val is
8FB78ABC A75C9F28 4E974E36 141866BC

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is <empty>

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

entropy_input is

C0 C1C2C3C4
C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBD**C**

additional_input is <empty>

Block_Cipher_df

input_str is

C0 C1C2C3C4
C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBD**C**

number_of_bits_to_return = 232

S is

0000001D 0000001D C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000

temp is

75D864A6 B6D27B8E

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000

temp is

75D864A6 B6D27B8E F1B88BC4 D95D7412

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000

temp is

75D864A6 B6D27B8E F1B88BC4 D95D7412 DA1D4B49 3894DD64

BCC

IV is

00000003 00000000

IV || S is

00000003 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000

temp is

75D864A6 B6D27B8E
F1B88BC4 D95D7412 DA1D4B49 3894DD64 1F27605F F6EAC071

Key is
75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938

X is

94DD641F 27605FF6

Block #1

Blockin 94DD641F 27605FF6
Blockout 1A1AD191 C4A0E7D1

BlockEncrypt

Key is

75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938

X is

94DD641F 27605FF6

X = BlockEncrypt(Key, X) is

1A1AD191 C4A0E7D1

temp is

1A1AD191 C4A0E7D1

Block #1

Blockin 1A1AD191 C4A0E7D1
Blockout EA461812 450132A6

BlockEncrypt

Key is

75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938

X is

1A1AD191 C4A0E7D1

X = BlockEncrypt(Key, X) is

EA461812 450132A6

temp is

1A1AD191 C4A0E7D1 EA461812 450132A6

Block #1

Blockin EA461812 450132A6

Blockout A84F5E05 D0A53DBD

BlockEncrypt

Key is

75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938

X is

EA461812 450132A6

X = BlockEncrypt(Key, X) is

A84F5E05 D0A53DBD

temp is

1A1AD191 C4A0E7D1 EA461812 450132A6 A84F5E05 D0A53DBD

Block #1

Blockin A84F5E05 D0A53DBD

Blockout BCDC595B A4B22114

BlockEncrypt

Key is

75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938

X is

A84F5E05 D0A53DBD

X = BlockEncrypt(Key, X) is

BCDC595B A4B22114

temp is

1A1AD191 C4A0E7D1

EA461812 450132A6 A84F5E05 D0A53DBD BCDC595B A4B22114

requested_bits is

1A 1AD191C4

A0E7D1EA 46181245 0132A6A8 4F5E05D0 A53DBDBC DC595BA4

Update

provided_data is

1A 1AD191C4

A0E7D1EA 46181245 0132A6A8 4F5E05D0 A53DBDBC DC595BA4

While loop

Key is

8E 30D7EEC6 D9C99D83 C999869B B24B13C2 EC88E6D3

V is

496FDA6C FFF2EADB

Block #1

Blockin 496FDA6C FFF2EADB

Blockout 8C96A647 4EEBF343

output_block is
8C96A647 4EEBF343

temp is
8C96A647 4EEBF343

While loop

Key is
8E 30D7EEC6 D9C99D83 C999869B B24B13C2 EC88E6D3

V is
496FDA6C FFF2EADC

Block #1
Blockin 496FDA6C FFF2EADC
Blockout CB5C81A8 1AFEC815

output_block is
CB5C81A8 1AFEC815

temp is
8C96A647 4EEBF343 CB5C81A8 1AFEC815

While loop

Key is
8E 30D7EEC6 D9C99D83 C999869B B24B13C2 EC88E6D3

V is
496FDA6C FFF2EADD

Block #1

Blockin 496FDA6C FFF2EADD
Blockout B2ECD7A2 B186E741

output_block is
22ECD7A2 B186E741

temp is
8C96A647 4EEBF343 CB5C81A8 1AFEC815 22ECD7A2 B186E741

While loop

Key is
8E 30D7EEC6 D9C99D83 C999869B B24B13C2 EC88E6D3

V is
496FDA6C FFF2EADE

Block #1
Blockin 496FDA6C FFF2EADE
Blockout B92231DC 44D71E5B

output_block is
B92231DC 44D71E5B

temp is
8C96A647 4EEBF343
CB5C81A8 1AFEC815 22ECD7A2 B186E741 B92231DC 44D71E5B

temp XOR provided_data is
96 8C77D68A
4B149221 1A99BA5F FFFAB38A A389A761 23DAFC05 FE6887E0

Key is
96 8C77D68A 4B149221 1A99BA5F FFFAB38A A389A761

V is

23DAFC05 FE6887E0

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is <empty>

Block #1

Blockin 23DAFC05 FE6887E1

Blockout 9D9745FF 31C42A44

Block #1

Blockin 23DAFC05 FE6887E2

Blockout 88CBB771 B13B5D86

Update

provided_data is

00 0000000

00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

96 8C77D68A 4B149221 1A99BA5F FFFAB38A A389A761

V is

23DAFC05 FE6887E3

Block #1

Blockin 23DAFC05 FE6887E3

Blockout 7F7365D7 ED0AB324

output_block is

7F7365D7 ED0AB324

temp is

7F7365D7 ED0AB324

While loop

Key is

96 8C77D68A 4B149221 1A99BA5F FFFAB38A A389A761

V is

23DAFC05 FE6887E4

Block #1

Blockin 23DAFC05 FE6887E4

Blockout DD1F46F2 8132DC76

output_block is

DD1F46F2 8132DC76

temp is

7F7365D7 ED0AB324 DD1F46F2 8132DC76

While loop

Key is

96 8C77D68A 4B149221 1A99BA5F FFFAB38A A389A761

V is

23DAFC05 FE6887E5

Block #1

Blockin 23DAFC05 FE6887E5

Blockout 7A768AD8 F0F37B4D

output_block is

7A768AD8 F0F37B4D

temp is

7F7365D7 ED0AB324 DD1F46F2 8132DC76 7A768AD8 F0F37B4D

While loop

Key is

96 8C77D68A 4B149221 1A99BA5F FFFAB38A A389A761

V is

23DAFC05 FE6887E6

Block #1

Blockin 23DAFC05 FE6887E6

Blockout DE770AB1 EF6B435C

output_block is

DE770AB1 EF6B435C

temp is

7F7365D7 ED0AB324
DD1F46F2 8132DC76 7A768AD8 F0F37B4D DE770AB1 EF6B435C

temp XOR provided_data is

7F 7365D7ED
0AB324DD 1F46F281 32DC767A 768AD8F0 F37B4DDE 770AB1EF

Key is

7F 7365D7ED 0AB324DD 1F46F281 32DC767A 768AD8F0

V is

F37B4DDE 770AB1EF

```
rnd_val is  
9D9745FF 31C42A44 88CBB771 B13B5D86
```

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

```
CTR_DRBG
```

```
Requested Security Strength = 112
```

```
prediction_resistance_flag = "ENABLED"
```

```
EntropyInput =
```

```
00 01020304
```

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

```
EntropyInput1 (for Reseed1) =
```

```
80 81828384
```

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

```
EntropyInput2 (for Reseed2) =
```

```
C0 C1C2C3C4
```

```
C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBD
```

```
Nonce =
```

```
202122 23242526
```

```
PersonalizationString = <empty>
```

```
AdditionalInput1 =
```

```
60 61626364
```

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

```
AdditionalInput2 =
```

```
A0 A1A2A3A4
```

```
A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC
```

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

```
*****
```

CTR_DRBG_Instantiate_algorithm - with derivation function

entropy_input is

00 01020304
05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C

nonce is

202122 23242526

personal_str is <empty>

prediction_resistance_flag = "PredictionResistance"

Block_Cipher_df

input_str is

00010203 04050607 08090A0B
0C0D0E0F 10111213 14151617 18191A1B 1C202122 23242526

number_of_bits_to_return = 232

S is

00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000

00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

temp is

4A2145C3 52BD4642

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000

00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

temp is

4A2145C3 52BD4642 EEB5E70D CAE11D42

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000

00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

temp is

4A2145C3 52BD4642 EEB5E70D CAE11D42 82FD02F7 B62641C4

BCC

IV is

00000003 00000000

IV || S is

00000003 00000000
00000024 0000001D 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C202122 23242526 80000000

temp is

4A2145C3 52BD4642
EEB5E70D CAE11D42 82FD02F7 B62641C4 BAE575D6 E7411566

Key is

4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

2641C4BA E575D6E7

Block #1

Blockin 2641C4BA E575D6E7
Blockout B4300B8B 7D547B40

BlockEncrypt

Key is

4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

2641C4BA E575D6E7

X = BlockEncrypt(Key, X) is

B4300B8B 7D547B40

temp is

B4300B8B 7D547B40

Block #1
Blockin B4300B8B 7D547B40
Blockout 599CFD0E B13B1607

BlockEncrypt

Key is
4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

B4300B8B 7D547B40

X = BlockEncrypt(Key, X) is
599CFD0E B13B1607

temp is

B4300B8B 7D547B40 599CFD0E B13B1607

Block #1
Blockin 599CFD0E B13B1607
Blockout 2398EF59 1553A5A3

BlockEncrypt

Key is
4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is

599CFD0E B13B1607

X = BlockEncrypt(Key, X) is
2398EF59 1553A5A3

temp is

B4300B8B 7D547B40 599CFD0E B13B1607 2398EF59 1553A5A3

Block #1
Blockin 2398EF59 1553A5A3
Blockout A10292FE FE535642

BlockEncrypt

Key is
4A 2145C352 BD4642EE B5E70DCA E11D4282 FD02F7B6

X is
2398EF59 1553A5A3

X = BlockEncrypt(Key, X) is
A10292FE FE535642

temp is
B4300B8B 7D547B40
599CFD0E B13B1607 2398EF59 1553A5A3 A10292FE FE535642

requested_bits is
B4 300B8B7D
547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE

seed_material is
B4 300B8B7D
547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE

Update

provided_data is
B4 300B8B7D
547B4059 9CFD0EB1 3B160723 98EF5915 53A5A3A1 0292FEFE

While loop

Key is

00 0000000 0000000 0000000 0000000 0000000

V is

00000000 00000001

Block #1

Blockin 0000000 00000001

Blockout 166B40B4 4ABA4BD6

output_block is

166B40B4 4ABA4BD6

temp is

166B40B4 4ABA4BD6

While loop

Key is

00 0000000 0000000 0000000 0000000 0000000

V is

00000000 00000002

Block #1

Blockin 0000000 00000002

Blockout 06E7EA22 CE92708F

output_block is

06E7EA22 CE92708F

temp is

166B40B4 4ABA4BD6 06E7EA22 CE92708F

While loop

Key is

00 0000000 0000000 0000000 0000000 0000000

V is

00000000 00000003

Block #1

Blockin 0000000 0000003

Blockout 4EB190C9 A2FA169C

output_block is

4EB190C9 A2FA169C

temp is

166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C

While loop

Key is

00 0000000 0000000 0000000 0000000 0000000

V is

00000000 00000004

Block #1

Blockin 0000000 0000004

Blockout D2FD8867 D50D2DFE

output_block is

D2FD8867 D50D2DFE

temp is

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

temp XOR provided_data is

A2 5B4B3F37
EE30965F 7B172C7F A966886D 297F90B7 A9B33F73 FF1A992B

Key is

A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is

A9B33F73 FF1A992B

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is

60 61626364
65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

entropy_input is

80 81828384
85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C

additional_input is

60 61626364
65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C

Block_Cipher_df

input_str is

8081 82838485 86878889
8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C60 61626364
65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C

number_of_bits_to_return = 232

S is

0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C606162 63646566 6768696A
6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000
0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C606162 63646566 6768696A
6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000

temp is

58B3B0F6 8DD4432B

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000

0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C606162 63646566 6768696A
6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000

temp is

58B3B0F6 8DD4432B FE91AF80 FC822A3B

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000

0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C606162 63646566 6768696A
6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000

temp is

58B3B0F6 8DD4432B FE91AF80 FC822A3B 16D6D0E6 185F1A8D

BCC

IV is

00000003 00000000

IV || S is

00000003 00000000

0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C606162 63646566 6768696A
6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000

temp is
58B3B0F6 8DD4432B
FE91AF80 FC822A3B 16D6D0E6 185F1A8D 6A2FC76E 4B22E671

Key is
58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618

X is
5F1A8D6A 2FC76E4B

Block #1
Blockin 5F1A8D6A 2FC76E4B
Blockout 8C09C342 0E2573AD

BlockEncrypt

Key is
58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618

X is
5F1A8D6A 2FC76E4B

X = BlockEncrypt(Key, X) is
8C09C342 0E2573AD

temp is
8C09C342 0E2573AD

Block #1
Blockin 8C09C342 0E2573AD
Blockout 6112E91C 0CAD6C1C

BlockEncrypt

Key is

58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618

X is

8C09C342 0E2573AD

X = BlockEncrypt(Key, X) is

6112E91C 0CAD6C1C

temp is

8C09C342 0E2573AD 6112E91C 0CAD6C1C

Block #1

Blockin 6112E91C 0CAD6C1C

Blockout 164907D9 2BF94019

BlockEncrypt

Key is

58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618

X is

6112E91C 0CAD6C1C

X = BlockEncrypt(Key, X) is

164907D9 2BF94019

temp is

8C09C342 0E2573AD 6112E91C 0CAD6C1C 164907D9 2BF94019

Block #1

Blockin 164907D9 2BF94019

Blockout 1E666F08 6A5CDA45

BlockEncrypt

Key is

58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618

X is

164907D9 2BF94019

X = BlockEncrypt(Key, X) is

1E666F08 6A5CDA45

temp is

8C09C342 0E2573AD

6112E91C 0CAD6C1C 164907D9 2BF94019 1E666F08 6A5CDA45

requested_bits is

8C 09C3420E

2573AD61 12E91C0C AD6C1C16 4907D92B F940191E 666F086A

Update

provided_data is

8C 09C3420E

2573AD61 12E91C0C AD6C1C16 4907D92B F940191E 666F086A

While loop

Key is

A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is

A9B33F73 FF1A992C

Block #1
Blockin A9B33F73 FF1A992C
Blockout ABC88224 514D0316

output_block is
ABC88224 514D0316

temp is
ABC88224 514D0316

While loop

Key is
A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is
A9B33F73 FF1A992D

Block #1
Blockin A9B33F73 FF1A992D
Blockout EA3D48AE E3C9A2B4

output_block is
EA3D48AE E3C9A2B4

temp is
ABC88224 514D0316 EA3D48AE E3C9A2B4

While loop

Key is
A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is
A9B33F73 FF1A992E

Block #1
Blockin A9B33F73 FF1A992E
Blockout 27CE2546 E5F9CE73

output_block is
27CE2546 E5F9CE73

temp is
ABC88224 514D0316 EA3D48AE E3C9A2B4 27CE2546 E5F9CE73

While loop

Key is
A2 5B4B3F37 EE30965F 7B172C7F A966886D 297F90B7

V is
A9B33F73 FF1A992F

Block #1
Blockin A9B33F73 FF1A992F
Blockout AC843CE9 A9F8B369

output_block is
AC843CE9 A9F8B369

temp is
ABC88224 514D0316
EA3D48AE E3C9A2B4 27CE2546 E5F9CE73 AC843CE9 A9F8B369

temp XOR provided_data is
27 C141665F
6870BB8B 2FA1B2EF 64CEA831 87229FCE 008E6AB2 E253E1C3

Key is
27 C141665F 6870BB8B 2FA1B2EF 64CEA831 87229FCE

V is

008E6AB2 E253E1C3

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is <empty>

Block #1

Blockin 008E6AB2 E253E1C4

Blockout 0E389920 A09B485A

Block #1

Blockin 008E6AB2 E253E1C5

Blockout A4ABD0CA 7E60D89C

Update

provided_data is

00 00000000

00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

27 C141665F 6870BB8B 2FA1B2EF 64CEA831 87229FCE

V is

008E6AB2 E253E1C6

Block #1

Blockin 008E6AB2 E253E1C6

Blockout E86795D8 9BEA95E8

output_block is

E86795D8 9BEA95E8

temp is

E86795D8 9BEA95E8

While loop

Key is

27 C141665F 6870BB8B 2FA1B2EF 64CEA831 87229FCE

V is

008E6AB2 E253E1C7

Block #1

Blockin 008E6AB2 E253E1C7

Blockout D96797E7 9FBF96CF

output_block is

D96797E7 9FBF96CF

temp is

E86795D8 9BEA95E8 D96797E7 9FBF96CF

While loop

Key is

27 C141665F 6870BB8B 2FA1B2EF 64CEA831 87229FCE

V is

008E6AB2 E253E1C8

Block #1

Blockin 008E6AB2 E253E1C8
Blockout EF2F0302 1D6B4659

output_block is
EF2F0302 1D6B4659

temp is
E86795D8 9BEA95E8 D96797E7 9FBF96CF EF2F0302 1D6B4659

While loop

Key is
27 C141665F 6870BB8B 2FA1B2EF 64CEA831 87229FCE

V is

008E6AB2 E253E1C9

Block #1
Blockin 008E6AB2 E253E1C9
Blockout CBE50DE0 C2F290F8

output_block is
CBE50DE0 C2F290F8

temp is
E86795D8 9BEA95E8
D96797E7 9FBF96CF EF2F0302 1D6B4659 CBE50DE0 C2F290F8

temp XOR provided_data is
E8 6795D89B
EA95E8D9 6797E79F BF96CFEF 2F03021D 6B4659CB E50DE0C2

Key is
E8 6795D89B EA95E8D9 6797E79F BF96CFEF 2F03021D

V is

6B4659CB E50DE0C2

rnd_val is
0E389920 A09B485A A4ABD0CA 7E60D89C

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is
A0 A1A2A3A4
A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

entropy_input is
C0 C1C2C3C4
C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBD

additional_input is
A0 A1A2A3A4
A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC

Block_Cipher_df

input_str is
C0C1 C2C3C4C5 C6C7C8C9
CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCA0 A1A2A3A4
A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC

number_of_bits_to_return = 232

S is

0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBBC8000 00000000

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000

0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBBC8000 00000000

temp is

D9863A5A 51A096BD

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000

0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBBC8000 00000000

temp is

D9863A5A 51A096BD F2424B3F 81E02A6A

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000

0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBBC8000 00000000

temp is

D9863A5A 51A096BD F2424B3F 81E02A6A 451263CA 7D8B9E2A

BCC

IV is

00000003 00000000

IV || S is

00000003 00000000

0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBBC8000 00000000

temp is

D9863A5A 51A096BD
F2424B3F 81E02A6A 451263CA 7D8B9E2A 7BDA3AEE 6EF73C33

Key is

D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D

X is
8B9E2A7B DA3AEE6E

Block #1
Blockin 8B9E2A7B DA3AEE6E
Blockout B1161FE3 3849916E

BlockEncrypt

Key is
D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D

X is
8B9E2A7B DA3AEE6E

X = BlockEncrypt(Key, X) is
B1161FE3 3849916E

temp is
B1161FE3 3849916E

Block #1
Blockin B1161FE3 3849916E
Blockout F1F20C6E 141630BE

BlockEncrypt

Key is
D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D

X is
B1161FE3 3849916E

X = BlockEncrypt(Key, X) is
F1F20C6E 141630BE

temp is

B1161FE3 3849916E F1F20C6E 141630BE

Block #1

Blockin F1F20C6E 141630BE

Blockout 20E312AC 5E3EDC6E

BlockEncrypt

Key is

D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D

X is

F1F20C6E 141630BE

X = BlockEncrypt(Key, X) is

20E312AC 5E3EDC6E

temp is

B1161FE3 3849916E F1F20C6E 141630BE 20E312AC 5E3EDC6E

Block #1

Blockin 20E312AC 5E3EDC6E

Blockout 7E5A819E D1AC80D7

BlockEncrypt

Key is

D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D

X is

20E312AC 5E3EDC6E

X = BlockEncrypt(Key, X) is
7E5A819E D1AC80D7

temp is
B1161FE3 3849916E
F1F20C6E 141630BE 20E312AC 5E3EDC6E 7E5A819E D1AC80D7

requested_bits is
B1 161FE338
49916EF1 F20C6E14 1630BE20 E312AC5E 3EDC6E7E 5A819ED1

Update

provided_data is
B1 161FE338
49916EF1 F20C6E14 1630BE20 E312AC5E 3EDC6E7E 5A819ED1

While loop

Key is
E8 6795D89B EA95E8D9 6797E79F BF96CFEF 2F03021D

V is
6B4659CB E50DE0C3

Block #1
Blockin 6B4659CB E50DE0C3
Blockout 70DDFA87 A0397904

output_block is
70DDFA87 A0397904

temp is
70DDFA87 A0397904

While loop

Key is

E8 6795D89B EA95E8D9 6797E79F BF96CFEF 2F03021D

V is

6B4659CB E50DE0C4

Block #1

Blockin 6B4659CB E50DE0C4

Blockout FE4FBE4C 6A424E69

output_block is

FE4FBE4C 6A424E69

temp is

70DDFA87 A0397904 FE4FBE4C 6A424E69

While loop

Key is

E8 6795D89B EA95E8D9 6797E79F BF96CFEF 2F03021D

V is

6B4659CB E50DE0C5

Block #1

Blockin 6B4659CB E50DE0C5

Blockout 13554524 8F4F80F9

output_block is

13554524 8F4F80F9

temp is

70DDFA87 A0397904 FE4FBE4C 6A424E69 13554524 8F4F80F9

While loop

Key is

E8 6795D89B EA95E8D9 6797E79F BF96CFEF 2F03021D

V is

6B4659CB E50DE0C6

Block #1

Blockin 6B4659CB E50DE0C6

Blockout B9E4F088 CD467B59

output_block is

B9E4F088 CD467B59

temp is

70DDFA87 A0397904

FE4FBE4C 6A424E69 13554524 8F4F80F9 B9E4F088 CD467B59

temp XOR provided_data is

C1 CBE56498

70E86A0F BDB2227E 547ED733 B65788D1 715C97C7 BE71161C

Key is

C1 CBE56498 70E86A0F BDB2227E 547ED733 B65788D1

V is

715C97C7 BE71161C

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is <empty>

Block #1

Blockin 715C97C7 BE71161D
Blockout F4478EC6 659A0D35

Block #1

Blockin 715C97C7 BE71161E
Blockout 77625B0C 73A211DD

Update

provided_data is

00 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

C1 CBE56498 70E86A0F BDB2227E 547ED733 B65788D1

V is

715C97C7 BE71161F

Block #1

Blockin 715C97C7 BE71161F
Blockout 37A7C1A9 50C0FB8B

output_block is

37A7C1A9 50C0FB8B

temp is

37A7C1A9 50C0FB8B

While loop

Key is

C1 CBE56498 70E86A0F BDB2227E 547ED733 B65788D1

V is

715C97C7 BE711620

Block #1

Blockin 715C97C7 BE711620

Blockout C21DABCB FDDA18B1

output_block is

C21DABCB FDDA18B1

temp is

37A7C1A9 50C0FB8B C21DABCB FDDA18B1

While loop

Key is

C1 CBE56498 70E86A0F BDB2227E 547ED733 B65788D1

V is

715C97C7 BE711621

Block #1

Blockin 715C97C7 BE711621

Blockout 9BB6CC23 85CD194A

output_block is

9BB6CC23 85CD194A

temp is

37A7C1A9 50C0FB8B C21DABCB FDDA18B1 9BB6CC23 85CD194A

While loop

Key is

C1 CBE56498 70E86A0F BDB2227E 547ED733 B65788D1

V is

715C97C7 BE711622

Block #1

Blockin 715C97C7 BE711622

Blockout C7CE7521 4803115B

output_block is

C7CE7521 4803115B

temp is

37A7C1A9 50C0FB8B

C21DABCB FDDA18B1 9BB6CC23 85CD194A C7CE7521 4803115B

temp XOR provided_data is

37 A7C1A950

C0FB8BC2 1DABCBFD DA18B19B B6CC2385 CD194AC7 CE752148

Key is

37 A7C1A950 C0FB8BC2 1DABCBFD DA18B19B B6CC2385

V is

CD194AC7 CE752148

rnd_val is

F4478EC6 659A0D35 77625B0C 73A211DD

#####

CTR_DRBG

Requested Security Strength = 112

prediction_resistance_flag = "ENABLED"

EntropyInput =

00 01020304

05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C

EntropyInput1 (for Reseed1) =

80 81828384

85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C

EntropyInput2 (for Reseed2) =

C0 C1C2C3C4

C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBD

Nonce =

202122 23242526

PersonalizationString =

40 41424344

45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C

AdditionalInput = <empty>

#####

CTR_DRBG_Instantiate_algorithm - with derivation function

entropy_input is

00 01020304

05060708 090A0B0C 0D0E0F10 11121314 15161718 191A1B1C

nonce is

202122 23242526

personal_str is

40 41424344

45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C

prediction_resistance_flag = "PredictionResistance"

Block_Cipher_df

input_str is

00 01020304 05060708 090A0B0C 0D0E0F10
11121314 15161718 191A1B1C 20212223 24252640 41424344
45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C

number_of_bits_to_return = 232

S is

00000041 0000001D
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C202122 23242526 40414243 44454647 48494A4B
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000 00000041 0000001D
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C202122 23242526 40414243 44454647 48494A4B
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000

temp is

BF5C8905 7D02B0A6

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000 00000041 0000001D
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C202122 23242526 40414243 44454647 48494A4B
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000

temp is

BF5C8905 7D02B0A6 77FE7647 E9554668

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000 00000041 0000001D
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C202122 23242526 40414243 44454647 48494A4B
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000

temp is

BF5C8905 7D02B0A6 77FE7647 E9554668 AE4D8DE0 DB992E46

BCC

IV is

00000003 00000000

IV || S is

00000003 00000000 00000041 0000001D
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617

18191A1B 1C202122 23242526 40414243 44454647 48494A4B
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000

temp is

BF5C8905 7D02B0A6
77FE7647 E9554668 AE4D8DE0 DB992E46 83E1389F 33A1E91F

Key is

BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is

992E4683 E1389F33

Block #1

Blockin 992E4683 E1389F33
Blockout 70F9F85E 350177E5

BlockEncrypt

Key is

BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is

992E4683 E1389F33

X = BlockEncrypt(Key, X) is

70F9F85E 350177E5

temp is

70F9F85E 350177E5

Block #1

Blockin 70F9F85E 350177E5
Blockout B228D49C 6374BBB6

BlockEncrypt

Key is

BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is

70F9F85E 350177E5

X = BlockEncrypt(Key, X) is

B228D49C 6374BBB6

temp is

70F9F85E 350177E5 B228D49C 6374BBB6

Block #1

Blockin B228D49C 6374BBB6

Blockout EA3DCFFA 463099CA

BlockEncrypt

Key is

BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is

B228D49C 6374BBB6

X = BlockEncrypt(Key, X) is

EA3DCFFA 463099CA

temp is

70F9F85E 350177E5 B228D49C 6374BBB6 EA3DCFFA 463099CA

Block #1

Blockin EA3DCFFA 463099CA
Blockout F0781291 15A9A8E8

BlockEncrypt

Key is

BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is

EA3DCFFA 463099CA

X = BlockEncrypt(Key, X) is

F0781291 15A9A8E8

temp is

70F9F85E 350177E5

B228D49C 6374BBB6 EA3DCFFA 463099CA F0781291 15A9A8E8

requested_bits is

70 F9F85E35

0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115

seed_material is

70 F9F85E35

0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115

Update

provided_data is

70 F9F85E35

0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115

While loop

Key is

00 0000000 0000000 0000000 0000000 0000000

V is

00000000 00000001

Block #1

Blockin 0000000 00000001

Blockout 166B40B4 4ABA4BD6

output_block is

166B40B4 4ABA4BD6

temp is

166B40B4 4ABA4BD6

While loop

Key is

00 0000000 0000000 0000000 0000000 0000000

V is

00000000 00000002

Block #1

Blockin 0000000 00000002

Blockout 06E7EA22 CE92708F

output_block is

06E7EA22 CE92708F

temp is

166B40B4 4ABA4BD6 06E7EA22 CE92708F

While loop

Key is

00 0000000 0000000 0000000 0000000 0000000

V is

00000000 00000003

Block #1

Blockin 0000000 0000003
Blockout 4EB190C9 A2FA169C

output_block is

4EB190C9 A2FA169C

temp is

166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C

While loop

Key is

00 0000000 0000000 0000000 0000000 0000000

V is

00000000 00000004

Block #1

Blockin 0000000 0000004
Blockout D2FD8867 D50D2DFE

output_block is

D2FD8867 D50D2DFE

temp is

166B40B4 4ABA4BD6

06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE

```
temp XOR provided_data is
          66 92B8EA7F
BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4 CA8F5622 859AF6C0
```

```
Key is
66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4
```

```
V is
CA8F5622 859AF6C0
```

First call to Generate

```
*****
```

CTR_DRBG_Generate

```
requested_number_of_bits = 128
```

```
additional_input is <empty>
```

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

```
*****
```

CTR_DRBG_Reseed

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

```
additional_input is <empty>
```

Block_Cipher_df

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

number_of_bits_to_return = 232

S is

0000001D 0000001D 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000 0000001D 0000001D 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000

temp is

B435EC36 31249E3D

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000 0000001D 0000001D 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000

temp is

B435EC36 31249E3D A735CE05 7E609075

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000 0000001D 0000001D 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000

temp is

B435EC36 31249E3D A735CE05 7E609075 CA6920F2 1DF7CB3D

BCC

IV is

00000003 00000000

IV || S is

00000003 00000000 0000001D 0000001D 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C800000

temp is

B435EC36 31249E3D
A735CE05 7E609075 CA6920F2 1DF7CB3D 6547CE54 BA8A17A5

Key is

B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D

X is

F7CB3D65 47CE54BA

Block #1

Blockin F7CB3D65 47CE54BA

Blockout 7D3F6CAF 387E4C9A

BlockEncrypt

Key is

B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D

X is

F7CB3D65 47CE54BA

X = BlockEncrypt(Key, X) is

7D3F6CAF 387E4C9A

temp is

7D3F6CAF 387E4C9A

Block #1

Blockin 7D3F6CAF 387E4C9A

Blockout 1A5787D4 81378C06

BlockEncrypt

Key is

B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D

X is

7D3F6CAF 387E4C9A

X = BlockEncrypt(Key, X) is

1A5787D4 81378C06

temp is

7D3F6CAF 387E4C9A 1A5787D4 81378C06

Block #1

Blockin 1A5787D4 81378C06

Blockout C409511D DB736F2D

BlockEncrypt

Key is

B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D

X is

1A5787D4 81378C06

X = BlockEncrypt(Key, X) is

C409511D DB736F2D

temp is

7D3F6CAF 387E4C9A 1A5787D4 81378C06 C409511D DB736F2D

Block #1

Blockin C409511D DB736F2D

Blockout D4CB361F 4C1392A0

BlockEncrypt

Key is

B4 35EC3631 249E3DA7 35CE057E 609075CA 6920F21D

X is

C409511D DB736F2D

X = BlockEncrypt(Key, X) is

D4CB361F 4C1392A0

temp is

7D3F6CAF 387E4C9A

1A5787D4 81378C06 C409511D DB736F2D D4CB361F 4C1392A0

requested_bits is

7D 3F6CAF38

7E4C9A1A 5787D481 378C06C4 09511DDB 736F2DD4 CB361F4C

Update

provided_data is

7D 3F6CAF38

7E4C9A1A 5787D481 378C06C4 09511DDB 736F2DD4 CB361F4C

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C1

Block #1

Blockin CA8F5622 859AF6C1

Blockout 760BED7D 92B083B1

output_block is

760BED7D 92B083B1

temp is

760BED7D 92B083B1

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C2

Block #1

Blockin CA8F5622 859AF6C2

Blockout 0AF31CF0 656081EB

output_block is

0AF31CF0 656081EB

temp is

760BED7D 92B083B1 0AF31CF0 656081EB

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C3

Block #1

Blockin CA8F5622 859AF6C3

Blockout 51D241F0 2DA51012

output_block is

51D241F0 2DA51012

temp is

760BED7D 92B083B1 0AF31CF0 656081EB 51D241F0 2DA51012

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C4

Block #1

Blockin CA8F5622 859AF6C4
Blockout AAF72BA5 971324B4

output_block is

AAF72BA5 971324B4

temp is

760BED7D 92B083B1

0AF31CF0 656081EB 51D241F0 2DA51012 AAF72BA5 971324B4

temp XOR provided_data is

0B 3481D2AA

CECF2B10 A49B24E4 570DED95 DB10EDF6 D67F3F7E 3C1DBADB

Key is

0B 3481D2AA CECF2B10 A49B24E4 570DED95 DB10EDF6

V is

D67F3F7E 3C1DBADB

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is <empty>

Block #1

Blockin D67F3F7E 3C1DBADC
Blockout 64983055 D014550B

Block #1

Blockin D67F3F7E 3C1DBADD
Blockout 39DE699E 43130B64

Update

provided_data is
00 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is
0B 3481D2AA CECF2B10 A49B24E4 570DED95 DB10EDF6

V is

D67F3F7E 3C1DBADE

Block #1
Blockin D67F3F7E 3C1DBADE
Blockout 9895D584 68F52888

output_block is
9895D584 68F52888

temp is

9895D584 68F52888

While loop

Key is
0B 3481D2AA CECF2B10 A49B24E4 570DED95 DB10EDF6

V is

D67F3F7E 3C1DBADF

Block #1
Blockin D67F3F7E 3C1DBADF
Blockout 90E0C91A FE19D323

output_block is
90E0C91A FE19D323

temp is
9895D584 68F52888 90E0C91A FE19D323

While loop

Key is
0B 3481D2AA CECF2B10 A49B24E4 570DED95 DB10EDF6

V is
D67F3F7E 3C1DBAE0

Block #1
Blockin D67F3F7E 3C1DBAE0
Blockout FD2B846F 724CC5D6

output_block is
FD2B846F 724CC5D6

temp is
9895D584 68F52888 90E0C91A FE19D323 FD2B846F 724CC5D6

While loop

Key is
0B 3481D2AA CECF2B10 A49B24E4 570DED95 DB10EDF6

V is

D67F3F7E 3C1DBAE1

Block #1

Blockin D67F3F7E 3C1DBAE1

Blockout 5F04A5D3 31851A8D

output_block is

5F04A5D3 31851A8D

temp is

9895D584 68F52888

90E0C91A FE19D323 FD2B846F 724CC5D6 5F04A5D3 31851A8D

temp XOR provided_data is

98 95D58468

F5288890 E0C91AFE 19D323FD 2B846F72 4CC5D65F 04A5D331

Key is

98 95D58468 F5288890 E0C91AFE 19D323FD 2B846F72

V is

4CC5D65F 04A5D331

rnd_val is

64983055 D014550B 39DE699E 43130B64

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is <empty>

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

entropy_input is
C0 C1C2C3C4
C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBD**C**

additional_input is <empty>

Block_Cipher_df

input_str is
C0 C1C2C3C4
C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBD**C**

number_of_bits_to_return = 232

S is

0000001D 0000001D C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000

temp is

75D864A6 B6D27B8E

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000

temp is

75D864A6 B6D27B8E F1B88BC4 D95D7412

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000

temp is

75D864A6 B6D27B8E F1B88BC4 D95D7412 DA1D4B49 3894DD64

BCC

IV is

00000003 00000000

IV || S is

00000003 00000000 0000001D 0000001D C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DC800000

temp is
75D864A6 B6D27B8E
F1B88BC4 D95D7412 DA1D4B49 3894DD64 1F27605F F6EAC071

Key is
75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938

X is
94DD641F 27605FF6

Block #1
Blockin 94DD641F 27605FF6
Blockout 1A1AD191 C4A0E7D1

BlockEncrypt
Key is
75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938

X is
94DD641F 27605FF6

X = BlockEncrypt(Key, X) is
1A1AD191 C4A0E7D1

temp is
1A1AD191 C4A0E7D1

Block #1
Blockin 1A1AD191 C4A0E7D1
Blockout EA461812 450132A6

BlockEncrypt

Key is

75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938

X is

1A1AD191 C4A0E7D1

X = BlockEncrypt(Key, X) is

EA461812 450132A6

temp is

1A1AD191 C4A0E7D1 EA461812 450132A6

Block #1

Blockin EA461812 450132A6

Blockout A84F5E05 D0A53DBD

BlockEncrypt

Key is

75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938

X is

EA461812 450132A6

X = BlockEncrypt(Key, X) is

A84F5E05 D0A53DBD

temp is

1A1AD191 C4A0E7D1 EA461812 450132A6 A84F5E05 D0A53DBD

Block #1

Blockin A84F5E05 D0A53DBD

Blockout BCDC595B A4B22114

BlockEncrypt

Key is

75 D864A6B6 D27B8EF1 B88BC4D9 5D7412DA 1D4B4938

X is

A84F5E05 D0A53DBD

X = BlockEncrypt(Key, X) is

BCDC595B A4B22114

temp is

1A1AD191 C4A0E7D1

EA461812 450132A6 A84F5E05 D0A53DBD BCDC595B A4B22114

requested_bits is

1A 1AD191C4

A0E7D1EA 46181245 0132A6A8 4F5E05D0 A53DBDBC DC595BA4

Update

provided_data is

1A 1AD191C4

A0E7D1EA 46181245 0132A6A8 4F5E05D0 A53DBDBC DC595BA4

While loop

Key is

98 95D58468 F5288890 E0C91AFE 19D323FD 2B846F72

V is

4CC5D65F 04A5D332

Block #1
Blockin 4CC5D65F 04A5D332
Blockout F72FD288 19F8D378

output_block is
F72FD288 19F8D378

temp is
F72FD288 19F8D378

While loop

Key is
98 95D58468 F5288890 E0C91AFE 19D323FD 2B846F72

V is
4CC5D65F 04A5D333

Block #1
Blockin 4CC5D65F 04A5D333
Blockout 97C5D167 6B2377A3

output_block is
97C5D167 6B2377A3

temp is
F72FD288 19F8D378 97C5D167 6B2377A3

While loop

Key is
98 95D58468 F5288890 E0C91AFE 19D323FD 2B846F72

V is
4CC5D65F 04A5D334

Block #1
Blockin 4CC5D65F 04A5D334
Blockout 10A2DCAC ED13843B

output_block is
10A2DCAC ED13843B

temp is
F72FD288 19F8D378 97C5D167 6B2377A3 10A2DCAC ED13843B

While loop

Key is
98 95D58468 F5288890 E0C91AFE 19D323FD 2B846F72

V is
4CC5D65F 04A5D335

Block #1
Blockin 4CC5D65F 04A5D335
Blockout AF0C7BB0 5CAE9CA7

output_block is
AF0C7BB0 5CAE9CA7

temp is
F72FD288 19F8D378
97C5D167 6B2377A3 10A2DCAC ED13843B AF0C7BB0 5CAE9CA7

temp XOR provided_data is
ED 350319DD
5834A97D 83C9752E 224505B8 ED82A93D B6B98613 D022EBF8

Key is
ED 350319DD 5834A97D 83C9752E 224505B8 ED82A93D

V is

B6B98613 D022EBF8

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is <empty>

Block #1

Blockin B6B98613 D022EBF9

Blockout 035FDDA8 582A2214

Block #1

Blockin B6B98613 D022EBFA

Blockout EC722C41 0A8D95D3

Update

provided_data is

00 00000000

00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

ED 350319DD 5834A97D 83C9752E 224505B8 ED82A93D

V is

B6B98613 D022EBFB

Block #1

Blockin B6B98613 D022EBFB

Blockout 1AB79F3A 952A33CF

output_block is
1AB79F3A 952A33CF

temp is
1AB79F3A 952A33CF

While loop

Key is
ED 350319DD 5834A97D 83C9752E 224505B8 ED82A93D

V is
B6B98613 D022EBFC

Block #1
Blockin B6B98613 D022EBFC
Blockout 35BEA654 602509AC

output_block is
35BEA654 602509AC

temp is
1AB79F3A 952A33CF 35BEA654 602509AC

While loop

Key is
ED 350319DD 5834A97D 83C9752E 224505B8 ED82A93D

V is
B6B98613 D022EBFD

Block #1

Blockin B6B98613 D022EBFD
Blockout 8D121E67 D0FED235

output_block is
8D121E67 D0FED235

temp is
1AB79F3A 952A33CF 35BEA654 602509AC 8D121E67 D0FED235

While loop

Key is
ED 350319DD 5834A97D 83C9752E 224505B8 ED82A93D

V is

B6B98613 D022EBFE

Block #1
Blockin B6B98613 D022EBFE
Blockout 84BC5D0B 6C5410EA

output_block is
84BC5D0B 6C5410EA

temp is
1AB79F3A 952A33CF
35BEA654 602509AC 8D121E67 D0FED235 84BC5D0B 6C5410EA

temp XOR provided_data is
1A B79F3A95
2A33CF35 BEA65460 2509AC8D 121E67D0 FED23584 BC5D0B6C

Key is
1A B79F3A95 2A33CF35 BEA65460 2509AC8D 121E67D0

V is

FED23584 BC5D0B6C

rnd_val is
035FDDA8 582A2214 EC722C41 0A8D95D3

#####

CTR_DRBG

Requested Security Strength = 112

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

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

EntropyInput2 (for Reseed2) =
C0 C1C2C3C4
C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBD**C**

Nonce =
202122 23242526

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

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

AdditionalInput2 =
A0 A1A2A3A4
A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC

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

```
*****
```

CTR_DRBG_Instantiate_algorithm - with derivation function

entropy_input is

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

nonce is

```
202122 23242526
```

personal_str is

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

prediction_resistance_flag = "PredictionResistance"

```
-----
```

Block_Cipher_df

input_str is

```
    00 01020304 05060708 090A0B0C 0D0E0F10  
11121314 15161718 191A1B1C 20212223 24252640 41424344  
45464748 494A4B4C 4D4E4F50 51525354 55565758 595A5B5C
```

number_of_bits_to_return = 232

S is

```
    00000041 0000001D  
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617  
18191A1B 1C202122 23242526 40414243 44454647 48494A4B  
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000
```

```
-----
```

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000 00000041 0000001D
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C202122 23242526 40414243 44454647 48494A4B
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000

temp is

BF5C8905 7D02B0A6

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000 00000041 0000001D
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C202122 23242526 40414243 44454647 48494A4B
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000

temp is

BF5C8905 7D02B0A6 77FE7647 E9554668

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000 00000041 0000001D
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617

18191A1B 1C202122 23242526 40414243 44454647 48494A4B
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000

temp is
BF5C8905 7D02B0A6 77FE7647 E9554668 AE4D8DE0 DB992E46

BCC

IV is
00000003 00000000

IV || S is
00000003 00000000 00000041 0000001D
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C202122 23242526 40414243 44454647 48494A4B
4C4D4E4F 50515253 54555657 58595A5B 5C800000 00000000

temp is
BF5C8905 7D02B0A6
77FE7647 E9554668 AE4D8DE0 DB992E46 83E1389F 33A1E91F

Key is
BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is
992E4683 E1389F33

Block #1
Blockin 992E4683 E1389F33
Blockout 70F9F85E 350177E5

BlockEncrypt

Key is
BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is
992E4683 E1389F33

X = BlockEncrypt(Key, X) is
70F9F85E 350177E5

temp is
70F9F85E 350177E5

Block #1
Blockin 70F9F85E 350177E5
Blockout B228D49C 6374BBB6

BlockEncrypt

Key is
BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is
70F9F85E 350177E5

X = BlockEncrypt(Key, X) is
B228D49C 6374BBB6

temp is
70F9F85E 350177E5 B228D49C 6374BBB6

Block #1
Blockin B228D49C 6374BBB6
Blockout EA3DCFFA 463099CA

BlockEncrypt

Key is

BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is

B228D49C 6374BBB6

X = BlockEncrypt(Key, X) is

EA3DCFFA 463099CA

temp is

70F9F85E 350177E5 B228D49C 6374BBB6 EA3DCFFA 463099CA

Block #1

Blockin EA3DCFFA 463099CA

Blockout F0781291 15A9A8E8

BlockEncrypt

Key is

BF 5C89057D 02B0A677 FE7647E9 554668AE 4D8DE0DB

X is

EA3DCFFA 463099CA

X = BlockEncrypt(Key, X) is

F0781291 15A9A8E8

temp is

70F9F85E 350177E5

B228D49C 6374BBB6 EA3DCFFA 463099CA F0781291 15A9A8E8

requested_bits is

70 F9F85E35

0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115

seed_material is
70 F9F85E35
0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115

Update

provided_data is
70 F9F85E35
0177E5B2 28D49C63 74BBB6EA 3DCFFA46 3099CAF0 78129115

While loop

Key is
00 0000000 0000000 0000000 0000000 0000000

V is
00000000 00000001

Block #1
Blockin 00000000 00000001
Blockout 166B40B4 4ABA4BD6

output_block is
166B40B4 4ABA4BD6

temp is
166B40B4 4ABA4BD6

While loop

Key is
00 0000000 0000000 0000000 0000000 0000000

V is

00000000 00000002

Block #1

Blockin 00000000 00000002
Blockout 06E7EA22 CE92708F

output_block is

06E7EA22 CE92708F

temp is

166B40B4 4ABA4BD6 06E7EA22 CE92708F

While loop

Key is

00 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000003

Block #1

Blockin 00000000 00000003
Blockout 4EB190C9 A2FA169C

output_block is

4EB190C9 A2FA169C

temp is

166B40B4 4ABA4BD6 06E7EA22 CE92708F 4EB190C9 A2FA169C

While loop

Key is

00 0000000 0000000 0000000 0000000 0000000

V is

00000000 00000004

Block #1

Blockin 00000000 00000004

Blockout D2FD8867 D50D2DFE

output_block is

D2FD8867 D50D2DFE

temp is

166B40B4 4ABA4BD6

06E7EA22 CE92708F 4EB190C9 A2FA169C D2FD8867 D50D2DFE

temp XOR provided_data is

66 92B8EA7F

BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4 CA8F5622 859AF6C0

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C0

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is

60 61626364

65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

entropy_input is

80 81828384

85868788 898A8B8C 8D8E8F90 91929394 95969798 999A9B9C

additional_input is

60 61626364

65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C

Block_Cipher_df

input_str is

8081 82838485 86878889

8A8B8C8D 8E8F9091 92939495 96979899 9A9B9C60 61626364

65666768 696A6B6C 6D6E6F70 71727374 75767778 797A7B7C

number_of_bits_to_return = 232

S is

0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F

90919293 94959697 98999A9B 9C606162 63646566 6768696A

6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000

BCC

IV is

00000000 00000000

IV || S is

00000000 00000000

0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C606162 63646566 6768696A
6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000

temp is

58B3B0F6 8DD4432B

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000

0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C606162 63646566 6768696A
6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000

temp is

58B3B0F6 8DD4432B FE91AF80 FC822A3B

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000

0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C606162 63646566 6768696A
6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000

temp is

58B3B0F6 8DD4432B FE91AF80 FC822A3B 16D6D0E6 185F1A8D

BCC

IV is

00000003 00000000

IV || S is

00000003 00000000

0000003A 0000001D 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C606162 63646566 6768696A
6B6C6D6E 6F707172 73747576 7778797A 7B7C8000 00000000

temp is

58B3B0F6 8DD4432B

FE91AF80 FC822A3B 16D6D0E6 185F1A8D 6A2FC76E 4B22E671

Key is

58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618

X is

5F1A8D6A 2FC76E4B

Block #1

Blockin 5F1A8D6A 2FC76E4B

Blockout 8C09C342 0E2573AD

BlockEncrypt

Key is

58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618

X is

5F1A8D6A 2FC76E4B

X = BlockEncrypt(Key, X) is
8C09C342 0E2573AD

temp is
8C09C342 0E2573AD

Block #1
Blockin 8C09C342 0E2573AD
Blockout 6112E91C 0CAD6C1C

BlockEncrypt

Key is
58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618

X is
8C09C342 0E2573AD

X = BlockEncrypt(Key, X) is
6112E91C 0CAD6C1C

temp is
8C09C342 0E2573AD 6112E91C 0CAD6C1C

Block #1
Blockin 6112E91C 0CAD6C1C
Blockout 164907D9 2BF94019

BlockEncrypt

Key is
58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618

X is

6112E91C 0CAD6C1C

X = BlockEncrypt(Key, X) is
164907D9 2BF94019

temp is
8C09C342 0E2573AD 6112E91C 0CAD6C1C 164907D9 2BF94019

Block #1
Blockin 164907D9 2BF94019
Blockout 1E666F08 6A5CDA45

BlockEncrypt

Key is
58 B3B0F68D D4432BFE 91AF80FC 822A3B16 D6D0E618

X is
164907D9 2BF94019

X = BlockEncrypt(Key, X) is
1E666F08 6A5CDA45

temp is
8C09C342 0E2573AD
6112E91C 0CAD6C1C 164907D9 2BF94019 1E666F08 6A5CDA45

requested_bits is
8C 09C3420E
2573AD61 12E91C0C AD6C1C16 4907D92B F940191E 666F086A

Update

provided_data is

8C 09C3420E
2573AD61 12E91C0C AD6C1C16 4907D92B F940191E 666F086A

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C1

Block #1

Blockin CA8F5622 859AF6C1

Blockout 760BED7D 92B083B1

output_block is

760BED7D 92B083B1

temp is

760BED7D 92B083B1

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C2

Block #1

Blockin CA8F5622 859AF6C2

Blockout 0AF31CF0 656081EB

output_block is

0AF31CF0 656081EB

temp is

760BED7D 92B083B1 0AF31CF0 656081EB

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C3

Block #1

Blockin CA8F5622 859AF6C3

Blockout 51D241F0 2DA51012

output_block is

51D241F0 2DA51012

temp is

760BED7D 92B083B1 0AF31CF0 656081EB 51D241F0 2DA51012

While loop

Key is

66 92B8EA7F BB3C33B4 CF3EBEAD E6CB39A4 8C5F33E4

V is

CA8F5622 859AF6C4

Block #1

Blockin CA8F5622 859AF6C4

Blockout AAF72BA5 971324B4

output_block is
AAF72BA5 971324B4

temp is
760BED7D 92B083B1
0AF31CF0 656081EB 51D241F0 2DA51012 AAF72BA5 971324B4

temp XOR provided_data is
FA 022E3F9C
95F01C6B E1F5EC69 CDEDF747 9B462906 5C500BB4 9144ADFD

Key is
FA 022E3F9C 95F01C6B E1F5EC69 CDEDF747 9B462906

V is
5C500BB4 9144ADFD

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is <empty>

Block #1
Blockin 5C500BB4 9144ADFE
Blockout A29C1A8C 42FBC562

Block #1
Blockin 5C500BB4 9144ADFF
Blockout D7D1DBA7 DC541FFE

Update

provided_data is
00 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

FA 022E3F9C 95F01C6B E1F5EC69 CDEDF747 9B462906

V is

5C500BB4 9144AE00

Block #1

Blockin 5C500BB4 9144AE00

Blockout 7B6D52C6 92B78B5E

output_block is

7B6D52C6 92B78B5E

temp is

7B6D52C6 92B78B5E

While loop

Key is

FA 022E3F9C 95F01C6B E1F5EC69 CDEDF747 9B462906

V is

5C500BB4 9144AE01

Block #1

Blockin 5C500BB4 9144AE01

Blockout 0308AE1A D67FDE94

output_block is

0308AE1A D67FDE94

temp is

7B6D52C6 92B78B5E 0308AE1A D67FDE94

While loop

Key is

FA 022E3F9C 95F01C6B E1F5EC69 CDED747 9B462906

V is

5C500BB4 9144AE02

Block #1

Blockin 5C500BB4 9144AE02

Blockout 85499C53 54CC8C48

output_block is

85499C53 54CC8C48

temp is

7B6D52C6 92B78B5E 0308AE1A D67FDE94 85499C53 54CC8C48

While loop

Key is

FA 022E3F9C 95F01C6B E1F5EC69 CDED747 9B462906

V is

5C500BB4 9144AE03

Block #1

Blockin 5C500BB4 9144AE03

Blockout 75283B3B 6F13FD25

output_block is

75283B3B 6F13FD25

temp is

7B6D52C6 92B78B5E
0308AE1A D67FDE94 85499C53 54CC8C48 75283B3B 6F13FD25

temp XOR provided_data is

7B 6D52C692
B78B5E03 08AE1AD6 7FDE9485 499C5354 CC8C4875 283B3B6F

Key is

7B 6D52C692 B78B5E03 08AE1AD6 7FDE9485 499C5354

V is

CC8C4875 283B3B6F

rnd_val is

A29C1A8C 42FBC562 D7D1DBA7 DC541FFE

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is

A0 A1A2A3A4
A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

entropy_input is

C0 C1C2C3C4
C5C6C7C8 C9CACBCC CDCECFD0 D1D2D3D4 D5D6D7D8 D9DADBDC

additional_input is
A0 A1A2A3A4
A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC

Block_Cipher_df

input_str is
C0C1 C2C3C4C5 C6C7C8C9
CACBCCCD CECFD0D1 D2D3D4D5 D6D7D8D9 DADBDCA0 A1A2A3A4
A5A6A7A8 A9AAABAC ADAEAFB0 B1B2B3B4 B5B6B7B8 B9BABBBC

number_of_bits_to_return = 232

S is
0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBBC8000 00000000

BCC

IV is
00000000 00000000

IV || S is
00000000 00000000
0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBBC8000 00000000

temp is
D9863A5A 51A096BD

BCC

IV is

00000001 00000000

IV || S is

00000001 00000000

0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBBC8000 00000000

temp is

D9863A5A 51A096BD F2424B3F 81E02A6A

BCC

IV is

00000002 00000000

IV || S is

00000002 00000000

0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBBBC8000 00000000

temp is

D9863A5A 51A096BD F2424B3F 81E02A6A 451263CA 7D8B9E2A

BCC

IV is

00000003 00000000

IV || S is

00000003 00000000

0000003A 0000001D C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCA0A1A2 A3A4A5A6 A7A8A9AA
ABACADAE AFB0B1B2 B3B4B5B6 B7B8B9BA BBC8000 00000000

temp is

D9863A5A 51A096BD
F2424B3F 81E02A6A 451263CA 7D8B9E2A 7BDA3AEE 6EF73C33

Key is

D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D

X is

8B9E2A7B DA3AEE6E

Block #1

Blockin 8B9E2A7B DA3AEE6E
Blockout B1161FE3 3849916E

BlockEncrypt

Key is

D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D

X is

8B9E2A7B DA3AEE6E

X = BlockEncrypt(Key, X) is

B1161FE3 3849916E

temp is

B1161FE3 3849916E

Block #1

Blockin B1161FE3 3849916E

Blockout F1F20C6E 141630BE

BlockEncrypt

Key is

D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D

X is

B1161FE3 3849916E

X = BlockEncrypt(Key, X) is

F1F20C6E 141630BE

temp is

B1161FE3 3849916E F1F20C6E 141630BE

Block #1

Blockin F1F20C6E 141630BE

Blockout 20E312AC 5E3EDC6E

BlockEncrypt

Key is

D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D

X is

F1F20C6E 141630BE

X = BlockEncrypt(Key, X) is

20E312AC 5E3EDC6E

temp is

B1161FE3 3849916E F1F20C6E 141630BE 20E312AC 5E3EDC6E

Block #1
Blockin 20E312AC 5E3EDC6E
Blockout 7E5A819E D1AC80D7

BlockEncrypt

Key is
D9 863A5A51 A096BDF2 424B3F81 E02A6A45 1263CA7D

X is

20E312AC 5E3EDC6E

X = BlockEncrypt(Key, X) is
7E5A819E D1AC80D7

temp is

B1161FE3 3849916E
F1F20C6E 141630BE 20E312AC 5E3EDC6E 7E5A819E D1AC80D7

requested_bits is

B1 161FE338
49916EF1 F20C6E14 1630BE20 E312AC5E 3EDC6E7E 5A819ED1

Update

provided_data is
B1 161FE338
49916EF1 F20C6E14 1630BE20 E312AC5E 3EDC6E7E 5A819ED1

While loop

Key is
7B 6D52C692 B78B5E03 08AE1AD6 7FDE9485 499C5354

V is

CC8C4875 283B3B70

Block #1

Blockin CC8C4875 283B3B70

Blockout 329590B9 A8D9D6A2

output_block is

329590B9 A8D9D6A2

temp is

329590B9 A8D9D6A2

While loop

Key is

7B 6D52C692 B78B5E03 08AE1AD6 7FDE9485 499C5354

V is

CC8C4875 283B3B71

Block #1

Blockin CC8C4875 283B3B71

Blockout 8F259854 CFA4C60B

output_block is

8F259854 CFA4C60B

temp is

329590B9 A8D9D6A2 8F259854 CFA4C60B

While loop

Key is

7B 6D52C692 B78B5E03 08AE1AD6 7FDE9485 499C5354

V is

CC8C4875 283B3B72

Block #1

Blockin CC8C4875 283B3B72

Blockout E98501FA E0C5B9A4

output_block is

E98501FA E0C5B9A4

temp is

329590B9 A8D9D6A2 8F259854 CFA4C60B E98501FA E0C5B9A4

While loop

Key is

7B 6D52C692 B78B5E03 08AE1AD6 7FDE9485 499C5354

V is

CC8C4875 283B3B73

Block #1

Blockin CC8C4875 283B3B73

Blockout BAA36330 5349000E

output_block is

BAA36330 5349000E

temp is

329590B9 A8D9D6A2

8F259854 CFA4C60B E98501FA E0C5B9A4 BAA36330 5349000E

temp XOR provided_data is

83 838F5A90

9047CC7E D7943ADB B2F6B5C9 661356BE FB65CAC4 F9E2AE82

Key is

83 838F5A90 9047CC7E D7943ADB B2F6B5C9 661356BE

V is

FB65CAC4 F9E2AE82

CTR_DRBG_Generate

requested_number_of_bits = 128

additional_input is <empty>

Block #1

Blockin FB65CAC4 F9E2AE83

Blockout 0BDA66B0 49429061

Block #1

Blockin FB65CAC4 F9E2AE84

Blockout C013E422 8C2F44C6

Update

provided_data is

00 00000000

00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

83 838F5A90 9047CC7E D7943ADB B2F6B5C9 661356BE

V is

FB65CAC4 F9E2AE85

Block #1
Blockin FB65CAC4 F9E2AE85
Blockout BA356571 5D258747

output_block is
BA356571 5D258747

temp is
BA356571 5D258747

While loop

Key is
83 838F5A90 9047CC7E D7943ADB B2F6B5C9 661356BE

V is
FB65CAC4 F9E2AE86

Block #1
Blockin FB65CAC4 F9E2AE86
Blockout A6E2CEBA 632C9DD2

output_block is
A6E2CEBA 632C9DD2

temp is
BA356571 5D258747 A6E2CEBA 632C9DD2

While loop

Key is
83 838F5A90 9047CC7E D7943ADB B2F6B5C9 661356BE

V is

FB65CAC4 F9E2AE87

Block #1

Blockin FB65CAC4 F9E2AE87

Blockout B66272C0 A231A14B

output_block is

B66272C0 A231A14B

temp is

BA356571 5D258747 A6E2CEBA 632C9DD2 B66272C0 A231A14B

While loop

Key is

83 838F5A90 9047CC7E D7943ADB B2F6B5C9 661356BE

V is

FB65CAC4 F9E2AE88

Block #1

Blockin FB65CAC4 F9E2AE88

Blockout DFCC9637 A4B325C9

output_block is

DFCC9637 A4B325C9

temp is

BA356571 5D258747

A6E2CEBA 632C9DD2 B66272C0 A231A14B DFCC9637 A4B325C9

temp XOR provided_data is

BA 3565715D

258747A6 E2CEBA63 2C9DD2B6 6272C0A2 31A14BDF CC9637A4

Key is
BA 3565715D 258747A6 E2CEBA63 2C9DD2B6 6272C0A2

V is
31A14BDF CC9637A4

rnd_val is
0BDA66B0 49429061 C013E422 8C2F44C6

#####

CTR_DRBG

Requested Security Strength = 128

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

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

EntropyInput2 (for Reseed2) =
C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7

Nonce =
20212223 24252627

PersonalizationString = <empty>

AdditionalInput = <empty>

#####

CTR_DRBG_Instantiate_algorithm - with derivation function

entropy_input is

00010203 04050607

08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F

nonce is

20212223 24252627

personal_str is <empty>

prediction_resistance_flag = "No PredictionResistance"

Block_Cipher_df

input_str is

00010203 04050607 08090A0B 0C0D0E0F

10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627

number_of_bits_to_return = 256

S is

00000028 00000020 00010203 04050607

08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F

20212223 24252627 80000000 00000000 00000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000

00000000 00000000 00000028 00000020 00010203 04050607

08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F

20212223 24252627 80000000 00000000 00000000 00000000

temp is

834EBAD8 5C601126 1D1D9DF4 C42A1544

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000
00000000 00000000 00000028 00000020 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 80000000 00000000 00000000 00000000

temp is

834EBAD8 5C601126
1D1D9DF4 C42A1544 8EA249C1 226F0474 F3C55519 CB3677D2

Key is

834EBAD8 5C601126 1D1D9DF4 C42A1544

X is

8EA249C1 226F0474 F3C55519 CB3677D2

BlockEncrypt

Key is

834EBAD8 5C601126 1D1D9DF4 C42A1544

X is

8EA249C1 226F0474 F3C55519 CB3677D2

X = BlockEncrypt(Key, X) is
B8823BC4 F3AFBB6B A0373C69 BC49E2F6

temp is
B8823BC4 F3AFBB6B A0373C69 BC49E2F6

BlockEncrypt

Key is
834EBAD8 5C601126 1D1D9DF4 C42A1544

X is
B8823BC4 F3AFBB6B A0373C69 BC49E2F6

X = BlockEncrypt(Key, X) is
560EDE12 D8335B64 F5647FA0 A644162B

temp is
B8823BC4 F3AFBB6B
A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

requested_bits is
B8823BC4 F3AFBB6B
A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

seed_material is
B8823BC4 F3AFBB6B
A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

Update

provided_data is
B8823BC4 F3AFBB6B

A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

While loop

Key is

00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is

58E2FCCE FA7E3061 367F1D57 A4E7455A

temp is

58E2FCCE FA7E3061 367F1D57 A4E7455A

While loop

Key is

00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

0388DACE 60B6A392 F328C2B9 71B2FE78

temp is

58E2FCCE FA7E3061

367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is

E060C70A 09D18B0A

9648213E 18AEA7AC 558604DC B885F8F6 064CBD19 D7F6E853

Key is

E060C70A 09D18B0A 9648213E 18AEA7AC

V is

558604DC B885F8F6 064CBD19 D7F6E853

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

E060C70A 09D18B0A 9648213E 18AEA7AC

V is

558604DC B885F8F6 064CBD19 D7F6E856

output_block is

06EFCAB8 8D90354C 705D9E1A 6597070D

temp is

06EFCAB8 8D90354C 705D9E1A 6597070D

While loop

Key is

E060C70A 09D18B0A 9648213E 18AEA7AC

V is

558604DC B885F8F6 064CBD19 D7F6E857

output_block is

EFCC61E1 D29E976B 28E06845 E4E31B55

temp is

06EFCAB8 8D90354C

705D9E1A 6597070D EFCC61E1 D29E976B 28E06845 E4E31B55

temp XOR provided_data is

06EFCAB8 8D90354C

705D9E1A 6597070D EFCC61E1 D29E976B 28E06845 E4E31B55

Key is

06EFCAB8 8D90354C 705D9E1A 6597070D

V is

EFCC61E1 D29E976B 28E06845 E4E31B55

rnd_val is

8CF59C8C F6888B96

EB1C1E3E 79D82387 AF08A9E5 FF75E23F 1FBCD455 9B6B997E

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

06EFCAB8 8D90354C 705D9E1A 6597070D

V is

EFCC61E1 D29E976B 28E06845 E4E31B58

output_block is

666D019E CB5C9650 0BA95E80 57F9E1B9

temp is

666D019E CB5C9650 0BA95E80 57F9E1B9

While loop

Key is

06EFCAB8 8D90354C 705D9E1A 6597070D

V is

EFCC61E1 D29E976B 28E06845 E4E31B59

output_block is

D6E7980D 821EF067 2874863C 4F086FE3

temp is

666D019E CB5C9650

0BA95E80 57F9E1B9 D6E7980D 821EF067 2874863C 4F086FE3

temp XOR provided_data is

666D019E CB5C9650

0BA95E80 57F9E1B9 D6E7980D 821EF067 2874863C 4F086FE3

Key is

666D019E CB5C9650 0BA95E80 57F9E1B9

V is

D6E7980D 821EF067 2874863C 4F086FE3

rnd_val is

69CDEF91 2C692D61

B1DA4C05 146B52EB 7B8849BD 87937835 328254EC 25A9180E

#####

CTR_DRBG

Requested Security Strength = 128

prediction_resistance_flag = "NOT ENABLED"

EntropyInput =

00010203 04050607

08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F

EntropyInput1 (for Reseed1) =

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

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

Nonce =
20212223 24252627

PersonalizationString = <empty>

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

AdditionalInput2 =
A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

#####

CTR_DRBG_Instantiate_algorithm - with derivation function

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

nonce is
20212223 24252627

personal_str is <empty>

prediction_resistance_flag = "No PredictionResistance"

Block_Cipher_df

input_str is

00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627

number_of_bits_to_return = 256

S is

00000028 00000020 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 80000000 00000000 00000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000028 00000020 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 80000000 00000000 00000000 00000000

temp is

834EBAD8 5C601126 1D1D9DF4 C42A1544

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000
00000000 00000000 00000028 00000020 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F

20212223 24252627 80000000 00000000 00000000 00000000

temp is

834EBAD8 5C601126

1D1D9DF4 C42A1544 8EA249C1 226F0474 F3C55519 CB3677D2

Key is

834EBAD8 5C601126 1D1D9DF4 C42A1544

X is

8EA249C1 226F0474 F3C55519 CB3677D2

BlockEncrypt

Key is

834EBAD8 5C601126 1D1D9DF4 C42A1544

X is

8EA249C1 226F0474 F3C55519 CB3677D2

X = BlockEncrypt(Key, X) is

B8823BC4 F3AFBB6B A0373C69 BC49E2F6

temp is

B8823BC4 F3AFBB6B A0373C69 BC49E2F6

BlockEncrypt

Key is

834EBAD8 5C601126 1D1D9DF4 C42A1544

X is

B8823BC4 F3AFBB6B A0373C69 BC49E2F6

X = BlockEncrypt(Key, X) is

560EDE12 D8335B64 F5647FA0 A644162B

temp is

B8823BC4 F3AFBB6B
A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

requested_bits is

B8823BC4 F3AFBB6B
A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

seed_material is

B8823BC4 F3AFBB6B
A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

Update

provided_data is

B8823BC4 F3AFBB6B
A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

While loop

Key is

00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is

58E2FCCE FA7E3061 367F1D57 A4E7455A

temp is

58E2FCCE FA7E3061 367F1D57 A4E7455A

While loop

Key is

00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

0388DACE 60B6A392 F328C2B9 71B2FE78

temp is

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

temp XOR provided_data is

E060C70A 09D18B0A
9648213E 18AEA7AC 558604DC B885F8F6 064CBD19 D7F6E853

Key is

E060C70A 09D18B0A 9648213E 18AEA7AC

V is

558604DC B885F8F6 064CBD19 D7F6E853

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is

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

additional_input <> NULL, process appropriately

Block_Cipher_df

input_str is

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

number_of_bits_to_return = 256

S is

00000020 00000020 60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000000 00000000
00000020 00000020 60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000

temp is

1E28FC96 A28B1550 8D8FC557 2B37CD4A

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000

00000020 00000020 60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000

temp is

1E28FC96 A28B1550

8D8FC557 2B37CD4A 857D7807 8DB171BF 8894073D E0C07B85

Key is

1E28FC96 A28B1550 8D8FC557 2B37CD4A

X is

857D7807 8DB171BF 8894073D E0C07B85

BlockEncrypt

Key is

1E28FC96 A28B1550 8D8FC557 2B37CD4A

X is

857D7807 8DB171BF 8894073D E0C07B85

X = BlockEncrypt(Key, X) is

C9172CDC 185A4A36 9E62578A F8F7C107

temp is

C9172CDC 185A4A36 9E62578A F8F7C107

BlockEncrypt

Key is

1E28FC96 A28B1550 8D8FC557 2B37CD4A

X is

C9172CDC 185A4A36 9E62578A F8F7C107

X = BlockEncrypt(Key, X) is

62DC9AD4 254F6BE9 0497C56E DE6C9AA5

temp is

C9172CDC 185A4A36

9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5

requested_bits is

C9172CDC 185A4A36

9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5

Update

provided_data is

C9172CDC 185A4A36

9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5

While loop

Key is

E060C70A 09D18B0A 9648213E 18AEA7AC

V is

558604DC B885F8F6 064CBD19 D7F6E854

output_block is
8CF59C8C F6888B96 EB1C1E3E 79D82387

temp is
8CF59C8C F6888B96 EB1C1E3E 79D82387

While loop

Key is
E060C70A 09D18B0A 9648213E 18AEA7AC

V is
558604DC B885F8F6 064CBD19 D7F6E855

output_block is
AF08A9E5 FF75E23F 1FBCD455 9B6B997E

temp is
8CF59C8C F6888B96
EB1C1E3E 79D82387 AF08A9E5 FF75E23F 1FBCD455 9B6B997E

temp XOR provided_data is
45E2B050 EED2C1A0
757E49B4 812FE280 CDD43331 DA3A89D6 1B2B113B 450703DB

Key is
45E2B050 EED2C1A0 757E49B4 812FE280

V is
CDD43331 DA3A89D6 1B2B113B 450703DB

Update

provided_data is

C9172CDC 185A4A36
9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5

While loop

Key is

45E2B050 EED2C1A0 757E49B4 812FE280

V is

CDD43331 DA3A89D6 1B2B113B 450703DE

output_block is

DD30431A 73450CF7 CB2BE2DC 06B9F4AE

temp is

DD30431A 73450CF7 CB2BE2DC 06B9F4AE

While loop

Key is

45E2B050 EED2C1A0 757E49B4 812FE280

V is

CDD43331 DA3A89D6 1B2B113B 450703DF

output_block is

F66934E9 C07C869A D456AEB6 CCEAFFC6

temp is

DD30431A 73450CF7

CB2BE2DC 06B9F4AE F66934E9 C07C869A D456AEB6 CCEAFFC6

```
temp XOR provided_data is
    14276FC6 6B1F46C1
    5549B556 FE4E35A9 94B5AE3D E533ED73 D0C16BD8 12866563
```

```
Key is
    14276FC6 6B1F46C1 5549B556 FE4E35A9
```

```
V is
    94B5AE3D E533ED73 D0C16BD8 12866563
```

```
rnd_val is
    E8C74A4B 7BFFB53B
    EB80E78C A86BB6DF 70E2032A EB473E0D D54D2339 CEFCE9D0
```

Second call to Generate

```
*****
```

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is
 A0A1A2A3 A4A5A6A7
 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

additional_input <> NULL, process appropriately

Block_Cipher_df

input_str is
 A0A1A2A3 A4A5A6A7
 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

number_of_bits_to_return = 256

S is

00000020 00000020 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000000 00000000
00000020 00000020 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000

temp is

2A2E34C4 CF921C78 51C82FB6 11B3AD80

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000
00000020 00000020 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000

temp is

2A2E34C4 CF921C78

51C82FB6 11B3AD80 AF942BCE FE572E5A 0ABD1E75 F20EC649

Key is

2A2E34C4 CF921C78 51C82FB6 11B3AD80

X is

AF942BCE FE572E5A 0ABD1E75 F20EC649

BlockEncrypt

Key is

2A2E34C4 CF921C78 51C82FB6 11B3AD80

X is

AF942BCE FE572E5A 0ABD1E75 F20EC649

X = BlockEncrypt(Key, X) is

83D41C94 8108B4D5 1B5D2980 046BD7F4

temp is

83D41C94 8108B4D5 1B5D2980 046BD7F4

BlockEncrypt

Key is

2A2E34C4 CF921C78 51C82FB6 11B3AD80

X is

83D41C94 8108B4D5 1B5D2980 046BD7F4

X = BlockEncrypt(Key, X) is

A6A7B2A0 DD3DD0C6 123C4186 842C1270

temp is

83D41C94 8108B4D5

1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270

requested_bits is
83D41C94 8108B4D5
1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270

Update

provided_data is
83D41C94 8108B4D5
1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270

While loop

Key is
14276FC6 6B1F46C1 5549B556 FE4E35A9

V is
94B5AE3D E533ED73 D0C16BD8 12866564

output_block is
05F50BB2 529B7C91 BBD09DD8 58C7CA6A

temp is
05F50BB2 529B7C91 BBD09DD8 58C7CA6A

While loop

Key is
14276FC6 6B1F46C1 5549B556 FE4E35A9

V is
94B5AE3D E533ED73 D0C16BD8 12866565

output_block is
ACC0BF92 8CBD5A5F 7E9876CD D9CC2C40

temp is
05F50BB2 529B7C91
BBD09DD8 58C7CA6A ACC0BF92 8CBD5A5F 7E9876CD D9CC2C40

temp XOR provided_data is
86211726 D393C844
A08DB458 5CAC1D9E 0A670D32 51808A99 6CA4374B 5DE03E30

Key is
86211726 D393C844 A08DB458 5CAC1D9E

V is
0A670D32 51808A99 6CA4374B 5DE03E30

Update

provided_data is
83D41C94 8108B4D5
1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270

While loop

Key is
86211726 D393C844 A08DB458 5CAC1D9E

V is
0A670D32 51808A99 6CA4374B 5DE03E33

output_block is

F252A225 68371777 1DB64C49 EF80EAAC

temp is

F252A225 68371777 1DB64C49 EF80EAAC

While loop

Key is

86211726 D393C844 A08DB458 5CAC1D9E

V is

0A670D32 51808A99 6CA4374B 5DE03E34

output_block is

A4B5046C 96296D2C 0E9714AC 958FFE2

temp is

F252A225 68371777

1DB64C49 EF80EAAC A4B5046C 96296D2C 0E9714AC 958FFE2

temp XOR provided_data is

7186BEB1 E93FA3A2

06EB65C9 EBEB3D58 0212B6CC 4B14BDEA 1CAB552A 11A3ED92

Key is

7186BEB1 E93FA3A2 06EB65C9 EBEB3D58

V is

0212B6CC 4B14BDEA 1CAB552A 11A3ED92

rnd_val is

26B3F823 B4DBAFC2

3B141375 E10B3AEB 7A0B5DEF 1C7D760B 6F827D01 ECD17AC7

```
#####
```

CTR_DRBG

Requested Security Strength = 128

prediction_resistance_flag = "NOT ENABLED"

EntropyInput =

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

EntropyInput1 (for Reseed1) =

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

EntropyInput2 (for Reseed2) =

```
C0C1C2C3 C4C5C6C7  
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
```

Nonce =

```
20212223 24252627
```

PersonalizationString =

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

AdditionalInput = <empty>

```
#####
```

```
*****
```

CTR_DRBG_Instantiate_algorithm - with derivation function

entropy_input is

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

nonce is

```
20212223 24252627
```

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

prediction_resistance_flag = "No PredictionResistance"

Block_Cipher_df

input_str is
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 40414243 44454647
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F

number_of_bits_to_return = 256

S is
00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000

BCC

IV is
00000000 00000000 00000000 00000000

IV || S is
00000000 00000000 00000000 00000000
00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000

temp is
C4C14823 AE157968 6F2C4676 8030DE37

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000
00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000

temp is

C4C14823 AE157968

6F2C4676 8030DE37 95EC1158 E6CD251C 577C6047 EBFFB5FE

Key is

C4C14823 AE157968 6F2C4676 8030DE37

X is

95EC1158 E6CD251C 577C6047 EBFFB5FE

BlockEncrypt

Key is

C4C14823 AE157968 6F2C4676 8030DE37

X is

95EC1158 E6CD251C 577C6047 EBFFB5FE

X = BlockEncrypt(Key, X) is

C2659E6A EFBB0DFB 2096A598 CC1C509F

temp is

C2659E6A EFBB0DFB 2096A598 CC1C509F

BlockEncrypt

Key is

C4C14823 AE157968 6F2C4676 8030DE37

X is

C2659E6A EFBB0DFB 2096A598 CC1C509F

X = BlockEncrypt(Key, X) is

D926A4C1 E62F8936 D419709D 6124946A

temp is

C2659E6A EFBB0DFB
2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

requested_bits is

C2659E6A EFBB0DFB
2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

seed_material is

C2659E6A EFBB0DFB
2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

Update

provided_data is

C2659E6A EFBB0DFB
2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

While loop

Key is

00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is

58E2FCCE FA7E3061 367F1D57 A4E7455A

temp is

58E2FCCE FA7E3061 367F1D57 A4E7455A

While loop

Key is

00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

0388DACE 60B6A392 F328C2B9 71B2FE78

temp is

58E2FCCE FA7E3061

367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is

9A8762A4 15C53D9A

16E9B8CF 68FB15C5 DAAE7E0F 86992AA4 2731B224 10966A12

Key is

9A8762A4 15C53D9A 16E9B8CF 68FB15C5

V is

DAAE7E0F 86992AA4 2731B224 10966A12

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

9A8762A4 15C53D9A 16E9B8CF 68FB15C5

V is

DAAE7E0F 86992AA4 2731B224 10966A15

output_block is

74723E58 EE02C39B 247A781A 780DC1AE

temp is

74723E58 EE02C39B 247A781A 780DC1AE

While loop

Key is

9A8762A4 15C53D9A 16E9B8CF 68FB15C5

V is

DAAE7E0F 86992AA4 2731B224 10966A16

output_block is

EAF09A38 8B7E7D0A BA59FDED 97C93019

temp is

74723E58 EE02C39B

247A781A 780DC1AE EAF09A38 8B7E7D0A BA59FDED 97C93019

temp XOR provided_data is

74723E58 EE02C39B

247A781A 780DC1AE EAF09A38 8B7E7D0A BA59FDED 97C93019

Key is

74723E58 EE02C39B 247A781A 780DC1AE

V is

EAF09A38 8B7E7D0A BA59FDED 97C93019

rnd_val is

18FDEFBD C43D7A36

D5D6D862 205765D1 D701C9F2 37007030 DF1B8E70 EE4EEE29

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

74723E58 EE02C39B 247A781A 780DC1AE

V is

EAF09A38 8B7E7D0A BA59FDED 97C9301C

output_block is

7913991A 10063ACE DB602FDB 00AD2197

temp is

7913991A 10063ACE DB602FDB 00AD2197

While loop

Key is

74723E58 EE02C39B 247A781A 780DC1AE

V is

EAF09A38 8B7E7D0A BA59FDED 97C9301D

output_block is

F472A839 C98EE0A4 B7C5571C 6FDFF7D7

temp is

7913991A 10063ACE

DB602FDB 00AD2197 F472A839 C98EE0A4 B7C5571C 6FDFF7D7

temp XOR provided_data is

7913991A 10063ACE

DB602FDB 00AD2197 F472A839 C98EE0A4 B7C5571C 6FDFF7D7

Key is

7913991A 10063ACE DB602FDB 00AD2197

V is

F472A839 C98EE0A4 B7C5571C 6FDFF7D7

rnd_val is

9888F1D3 8BB1CCE3

1B363AA1 BD9B3961 6876C30D EE1FF0B7 BD8C4C44 1715C833

#####

CTR_DRBG

Requested Security Strength = 128

prediction_resistance_flag = "NOT ENABLED"

EntropyInput =

00010203 04050607

08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F

EntropyInput1 (for Reseed1) =

80818283 84858687

88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F

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

Nonce =
20212223 24252627

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

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

AdditionalInput2 =
A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

#####

CTR_DRBG_Instantiate_algorithm - with derivation function

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

nonce is
20212223 24252627

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

```
prediction_resistance_flag = "No PredictionResistance"
```

```
-----  
Block_Cipher_df
```

```
input_str is  
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617  
18191A1B 1C1D1E1F 20212223 24252627 40414243 44454647  
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
```

```
number_of_bits_to_return = 256
```

```
S is
```

```
00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F  
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627  
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657  
58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000
```

```
-----
```

```
BCC
```

```
IV is
```

```
00000000 00000000 00000000 00000000
```

```
IV || S is
```

```
00000000 00000000 00000000 00000000  
00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F  
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627  
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657  
58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000
```

```
temp is
```

```
C4C14823 AE157968 6F2C4676 8030DE37
```

```
-----
```

```
BCC
```

```
IV is
```

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000
00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000

temp is

C4C14823 AE157968
6F2C4676 8030DE37 95EC1158 E6CD251C 577C6047 EBFFB5FE

Key is

C4C14823 AE157968 6F2C4676 8030DE37

X is

95EC1158 E6CD251C 577C6047 EBFFB5FE

BlockEncrypt

Key is

C4C14823 AE157968 6F2C4676 8030DE37

X is

95EC1158 E6CD251C 577C6047 EBFFB5FE

X = BlockEncrypt(Key, X) is

C2659E6A EFBB0DFB 2096A598 CC1C509F

temp is

C2659E6A EFBB0DFB 2096A598 CC1C509F

BlockEncrypt

Key is

C4C14823 AE157968 6F2C4676 8030DE37

X is

C2659E6A EFBB0DFB 2096A598 CC1C509F

X = BlockEncrypt(Key, X) is

D926A4C1 E62F8936 D419709D 6124946A

temp is

C2659E6A EFBB0DFB

2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

requested_bits is

C2659E6A EFBB0DFB

2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

seed_material is

C2659E6A EFBB0DFB

2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

Update

provided_data is

C2659E6A EFBB0DFB

2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

While loop

Key is

00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is

58E2FCCE FA7E3061 367F1D57 A4E7455A

temp is

58E2FCCE FA7E3061 367F1D57 A4E7455A

While loop

Key is

00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

0388DACE 60B6A392 F328C2B9 71B2FE78

temp is

58E2FCCE FA7E3061

367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is

9A8762A4 15C53D9A

16E9B8CF 68FB15C5 DAAE7E0F 86992AA4 2731B224 10966A12

Key is

9A8762A4 15C53D9A 16E9B8CF 68FB15C5

V is

DAAE7E0F 86992AA4 2731B224 10966A12

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is

60616263 64656667

68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F

additional_input <> NULL, process appropriately

Block_Cipher_df

input_str is

60616263 64656667

68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F

number_of_bits_to_return = 256

S is

00000020 00000020 60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000000 00000000

00000020 00000020 60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000

temp is
1E28FC96 A28B1550 8D8FC557 2B37CD4A

BCC

IV is
00000001 00000000 00000000 00000000

IV || S is
00000001 00000000 00000000 00000000
00000020 00000020 60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000

temp is
1E28FC96 A28B1550
8D8FC557 2B37CD4A 857D7807 8DB171BF 8894073D E0C07B85

Key is
1E28FC96 A28B1550 8D8FC557 2B37CD4A

X is
857D7807 8DB171BF 8894073D E0C07B85

BlockEncrypt

Key is
1E28FC96 A28B1550 8D8FC557 2B37CD4A

X is
857D7807 8DB171BF 8894073D E0C07B85

X = BlockEncrypt(Key, X) is
C9172CDC 185A4A36 9E62578A F8F7C107

temp is
C9172CDC 185A4A36 9E62578A F8F7C107

BlockEncrypt

Key is
1E28FC96 A28B1550 8D8FC557 2B37CD4A

X is
C9172CDC 185A4A36 9E62578A F8F7C107

X = BlockEncrypt(Key, X) is
62DC9AD4 254F6BE9 0497C56E DE6C9AA5

temp is
C9172CDC 185A4A36
9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5

requested_bits is
C9172CDC 185A4A36
9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5

Update

provided_data is
C9172CDC 185A4A36
9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5

While loop

Key is

9A8762A4 15C53D9A 16E9B8CF 68FB15C5

V is

DAAE7E0F 86992AA4 2731B224 10966A13

output_block is

18FDEFBD C43D7A36 D5D6D862 205765D1

temp is

18FDEFBD C43D7A36 D5D6D862 205765D1

While loop

Key is

9A8762A4 15C53D9A 16E9B8CF 68FB15C5

V is

DAAE7E0F 86992AA4 2731B224 10966A14

output_block is

D701C9F2 37007030 DF1B8E70 EE4EEE29

temp is

18FDEFBD C43D7A36

D5D6D862 205765D1 D701C9F2 37007030 DF1B8E70 EE4EEE29

temp XOR provided_data is

D1EAC361 DC673000

4BB48FE8 D8A0A4D6 B5DD5326 124F1BD9 DB8C4B1E 3022748C

Key is

D1EAC361 DC673000 4BB48FE8 D8A0A4D6

V is
B5DD5326 124F1BD9 DB8C4B1E 3022748C

Update

provided_data is
C9172CDC 185A4A36
9E62578A F8F7C107 62DC9AD4 254F6BE9 0497C56E DE6C9AA5

While loop

Key is
D1EAC361 DC673000 4BB48FE8 D8A0A4D6

V is
B5DD5326 124F1BD9 DB8C4B1E 3022748F

output_block is
298D1882 F782A51E 7EBE2F26 C13E7517

temp is
298D1882 F782A51E 7EBE2F26 C13E7517

While loop

Key is
D1EAC361 DC673000 4BB48FE8 D8A0A4D6

V is
B5DD5326 124F1BD9 DB8C4B1E 30227490

output_block is

0CAEDD35 C87769FE D159CE86 E15868C2

temp is

298D1882 F782A51E

7EBE2F26 C13E7517 0CAEDD35 C87769FE D159CE86 E15868C2

temp XOR provided_data is

E09A345E EFD8EF28

E0DC78AC 39C9B410 6E7247E1 ED380217 D5CE0BE8 3F34F267

Key is

E09A345E EFD8EF28 E0DC78AC 39C9B410

V is

6E7247E1 ED380217 D5CE0BE8 3F34F267

rnd_val is

526CFB7F F19B8485

D6283F06 7A4CB832 77A736E8 45E423AE 0A363E91 A9D95F3B

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is

A0A1A2A3 A4A5A6A7

A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

additional_input <> NULL, process appropriately

Block_Cipher_df

input_str is

A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

number_of_bits_to_return = 256

S is

00000020 00000020 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000000 00000000
00000020 00000020 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000

temp is

2A2E34C4 CF921C78 51C82FB6 11B3AD80

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000
00000020 00000020 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000

temp is
2A2E34C4 CF921C78
51C82FB6 11B3AD80 AF942BCE FE572E5A 0ABD1E75 F20EC649

Key is
2A2E34C4 CF921C78 51C82FB6 11B3AD80

X is
AF942BCE FE572E5A 0ABD1E75 F20EC649

BlockEncrypt

Key is
2A2E34C4 CF921C78 51C82FB6 11B3AD80

X is
AF942BCE FE572E5A 0ABD1E75 F20EC649

X = BlockEncrypt(Key, X) is
83D41C94 8108B4D5 1B5D2980 046BD7F4

temp is
83D41C94 8108B4D5 1B5D2980 046BD7F4

BlockEncrypt

Key is
2A2E34C4 CF921C78 51C82FB6 11B3AD80

X is
83D41C94 8108B4D5 1B5D2980 046BD7F4

X = BlockEncrypt(Key, X) is
A6A7B2A0 DD3DD0C6 123C4186 842C1270

temp is
83D41C94 8108B4D5
1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270

requested_bits is
83D41C94 8108B4D5
1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270

Update

provided_data is
83D41C94 8108B4D5
1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270

While loop

Key is
E09A345E EFD8EF28 E0DC78AC 39C9B410

V is
6E7247E1 ED380217 D5CE0BE8 3F34F268

output_block is
83C9B360 C168810E 431507FE 9793CADF

temp is
83C9B360 C168810E 431507FE 9793CADF

While loop

Key is

E09A345E EFD8EF28 E0DC78AC 39C9B410

V is

6E7247E1 ED380217 D5CE0BE8 3F34F269

output_block is

D3CEB5C1 7CF87AE1 69B8CB71 8E05FBB5

temp is

83C9B360 C168810E

431507FE 9793CADF D3CEB5C1 7CF87AE1 69B8CB71 8E05FBB5

temp XOR provided_data is

001DAFF4 406035DB

58482E7E 93F81D2B 75690761 A1C5AA27 7B848AF7 0A29E9C5

Key is

001DAFF4 406035DB 58482E7E 93F81D2B

V is

75690761 A1C5AA27 7B848AF7 0A29E9C5

Update

provided_data is

83D41C94 8108B4D5

1B5D2980 046BD7F4 A6A7B2A0 DD3DD0C6 123C4186 842C1270

While loop

Key is

001DAFF4 406035DB 58482E7E 93F81D2B

V is

75690761 A1C5AA27 7B848AF7 0A29E9C8

output_block is

2FD18B98 5F49C724 52E634A3 D7CE864C

temp is

2FD18B98 5F49C724 52E634A3 D7CE864C

While loop

Key is

001DAFF4 406035DB 58482E7E 93F81D2B

V is

75690761 A1C5AA27 7B848AF7 0A29E9C9

output_block is

9F216599 6645B418 D44FA297 E6A01492

temp is

2FD18B98 5F49C724

52E634A3 D7CE864C 9F216599 6645B418 D44FA297 E6A01492

temp XOR provided_data is

AC05970C DE4173F1

49BB1D23 D3A551B8 3986D739 BB7864DE C673E311 628C06E2

Key is

AC05970C DE4173F1 49BB1D23 D3A551B8

V is

3986D739 BB7864DE C673E311 628C06E2

rnd_val is

FDDF99A0 8490FF79
55D79C2F 8C372418 38813579 4C18B3D6 31E37B85 0FF5EB0F

#####

CTR_DRBG

Requested Security Strength = 128

prediction_resistance_flag = "ENABLED"

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

EntropyInput1 (for Reseed1) =

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

EntropyInput2 (for Reseed2) =

C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF

Nonce =

20212223 24252627

PersonalizationString = <empty>

AdditionalInput = <empty>

#####

CTR_DRBG_Instantiate_algorithm - with derivation function

entropy_input is

00010203 04050607

08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F

nonce is

20212223 24252627

personal_str is <empty>

prediction_resistance_flag = "PredictionResistance"

Block_Cipher_df

input_str is

00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627

number_of_bits_to_return = 256

S is

00000028 00000020 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 80000000 00000000 00000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000028 00000020 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 80000000 00000000 00000000 00000000

temp is

834EBAD8 5C601126 1D1D9DF4 C42A1544

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000

00000000 00000000 00000028 00000020 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 80000000 00000000 00000000 00000000

temp is

834EBAD8 5C601126

1D1D9DF4 C42A1544 8EA249C1 226F0474 F3C55519 CB3677D2

Key is

834EBAD8 5C601126 1D1D9DF4 C42A1544

X is

8EA249C1 226F0474 F3C55519 CB3677D2

BlockEncrypt

Key is

834EBAD8 5C601126 1D1D9DF4 C42A1544

X is

8EA249C1 226F0474 F3C55519 CB3677D2

X = BlockEncrypt(Key, X) is

B8823BC4 F3AFBB6B A0373C69 BC49E2F6

temp is

B8823BC4 F3AFBB6B A0373C69 BC49E2F6

BlockEncrypt

Key is

834EBAD8 5C601126 1D1D9DF4 C42A1544

X is

B8823BC4 F3AFBB6B A0373C69 BC49E2F6

X = BlockEncrypt(Key, X) is

560EDE12 D8335B64 F5647FA0 A644162B

temp is

B8823BC4 F3AFBB6B

A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

requested_bits is

B8823BC4 F3AFBB6B

A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

seed_material is

B8823BC4 F3AFBB6B

A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

Update

provided_data is

B8823BC4 F3AFBB6B

A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

While loop

Key is

00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is

58E2FCCE FA7E3061 367F1D57 A4E7455A

temp is

58E2FCCE FA7E3061 367F1D57 A4E7455A

While loop

Key is

00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

0388DACE 60B6A392 F328C2B9 71B2FE78

temp is

58E2FCCE FA7E3061

367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is

E060C70A 09D18B0A

9648213E 18AEA7AC 558604DC B885F8F6 064CBD19 D7F6E853

Key is

E060C70A 09D18B0A 9648213E 18AEA7AC

V is

558604DC B885F8F6 064CBD19 D7F6E853

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

entropy_input is

80818283 84858687

88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F

additional_input is <empty>

Block_Cipher_df

input_str is

80818283 84858687

88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F

number_of_bits_to_return = 256

S is

00000020 00000020 80818283 84858687 88898A8B 8C8D8E8F

90919293 94959697 98999A9B 9C9D9E9F 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000000 00000000

00000020 00000020 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F 80000000 00000000

temp is

6689B2EA B8B5547F E46D8E0B 6AD94B8C

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000

00000020 00000020 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F 80000000 00000000

temp is

6689B2EA B8B5547F
E46D8E0B 6AD94B8C 4578F39E C865C2E4 EADB493B A265794F

Key is

6689B2EA B8B5547F E46D8E0B 6AD94B8C

X is

4578F39E C865C2E4 EADB493B A265794F

BlockEncrypt

Key is

6689B2EA B8B5547F E46D8E0B 6AD94B8C

X is

4578F39E C865C2E4 EADB493B A265794F

X = BlockEncrypt(Key, X) is

E8B2120B 0673C751 090997D6 BEAC637D

temp is

E8B2120B 0673C751 090997D6 BEAC637D

BlockEncrypt

Key is

6689B2EA B8B5547F E46D8E0B 6AD94B8C

X is

E8B2120B 0673C751 090997D6 BEAC637D

X = BlockEncrypt(Key, X) is

79D7CA26 C10FEE1F EAC1E952 46CC5005

temp is

E8B2120B 0673C751

090997D6 BEAC637D 79D7CA26 C10FEE1F EAC1E952 46CC5005

requested_bits is

E8B2120B 0673C751

090997D6 BEAC637D 79D7CA26 C10FEE1F EAC1E952 46CC5005

Update

provided_data is
E8B2120B 0673C751
090997D6 BEAC637D 79D7CA26 C10FEE1F EAC1E952 46CC5005

While loop

Key is
E060C70A 09D18B0A 9648213E 18AEA7AC

V is
558604DC B885F8F6 064CBD19 D7F6E854

output_block is
8CF59C8C F6888B96 EB1C1E3E 79D82387

temp is
8CF59C8C F6888B96 EB1C1E3E 79D82387

While loop

Key is
E060C70A 09D18B0A 9648213E 18AEA7AC

V is
558604DC B885F8F6 064CBD19 D7F6E855

output_block is
AF08A9E5 FF75E23F 1FBCD455 9B6B997E

temp is

8CF59C8C F6888B96
EB1C1E3E 79D82387 AF08A9E5 FF75E23F 1FB CD455 9B6B997E

temp XOR provided_data is

64478E87 F0FB4CC7
E21589E8 C77440FA D6DF63C3 3E7A0C20 F57D3D07 DDA7C97B

Key is

64478E87 F0FB4CC7 E21589E8 C77440FA

V is

D6DF63C3 3E7A0C20 F57D3D07 DDA7C97B

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

64478E87 F0FB4CC7 E21589E8 C77440FA

V is

D6DF63C3 3E7A0C20 F57D3D07 DDA7C97E

output_block is
77FA8FD1 623711DB C4F78811 94359692

temp is
77FA8FD1 623711DB C4F78811 94359692

While loop

Key is
64478E87 F0FB4CC7 E21589E8 C77440FA

V is
D6DF63C3 3E7A0C20 F57D3D07 DDA7C97F

output_block is
3ED2ABE4 23A82FB0 DDD70D6D 2DB30EB3

temp is
77FA8FD1 623711DB
C4F78811 94359692 3ED2ABE4 23A82FB0 DDD70D6D 2DB30EB3

temp XOR provided_data is
77FA8FD1 623711DB
C4F78811 94359692 3ED2ABE4 23A82FB0 DDD70D6D 2DB30EB3

Key is
77FA8FD1 623711DB C4F78811 94359692

V is
3ED2ABE4 23A82FB0 DDD70D6D 2DB30EB3

rnd_val is
BFF4B85D 68C84529

```
F24F69F9 ACF1756E 29BA648D DEB825C2 25FA32BA 490EF4A9
```

```
Second call to Generate
```

```
*****
```

```
CTR_DRBG_Generate
```

```
requested_number_of_bits = 256
```

```
additional_input is <empty>
```

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

```
*****
```

```
CTR_DRBG_Reseed
```

```
entropy_input is
```

```
C0C1C2C3 C4C5C6C7  
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED
```

```
additional_input is <empty>
```

```
Block_Cipher_df
```

```
input_str is
```

```
C0C1C2C3 C4C5C6C7  
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED
```

```
number_of_bits_to_return = 256
```

```
S is
```

```
00000020 00000020 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF  
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED 80000000 00000000
```

```
BCC
```

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000000 00000000
00000020 00000020 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF 80000000 00000000

temp is

72571427 A62CFFB3 105AA38D 4C701D8A

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000
00000020 00000020 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF 80000000 00000000

temp is

72571427 A62CFFB3
105AA38D 4C701D8A E90056D7 6C2480EE 096C3B48 059FD3F7

Key is

72571427 A62CFFB3 105AA38D 4C701D8A

X is

E90056D7 6C2480EE 096C3B48 059FD3F7

BlockEncrypt

Key is

72571427 A62CFFB3 105AA38D 4C701D8A

X is

E90056D7 6C2480EE 096C3B48 059FD3F7

X = BlockEncrypt(Key, X) is

ACEF0D4B 113B12C1 4E45C0A0 A9574DE6

temp is

ACEF0D4B 113B12C1 4E45C0A0 A9574DE6

BlockEncrypt

Key is

72571427 A62CFFB3 105AA38D 4C701D8A

X is

ACEF0D4B 113B12C1 4E45C0A0 A9574DE6

X = BlockEncrypt(Key, X) is

F20CF416 9FEF3831 76A7C304 F0066E66

temp is

ACEF0D4B 113B12C1

4E45C0A0 A9574DE6 F20CF416 9FEF3831 76A7C304 F0066E66

requested_bits is

ACEF0D4B 113B12C1

4E45C0A0 A9574DE6 F20CF416 9FEF3831 76A7C304 F0066E66

Update

provided_data is

ACEF0D4B 113B12C1
4E45C0A0 A9574DE6 F20CF416 9FEF3831 76A7C304 F0066E66

While loop

Key is

77FA8FD1 623711DB C4F78811 94359692

V is

3ED2ABE4 23A82FB0 DDD70D6D 2DB30EB4

output_block is

77B20847 D584D9C7 BF91AAAB 087F4615

temp is

77B20847 D584D9C7 BF91AAAB 087F4615

While loop

Key is

77FA8FD1 623711DB C4F78811 94359692

V is

3ED2ABE4 23A82FB0 DDD70D6D 2DB30EB5

output_block is

F31E70A8 B9ADF9A6 95229D64 BA9848AD

temp is

77B20847 D584D9C7

BF91AAAB 087F4615 F31E70A8 B9ADF9A6 95229D64 BA9848AD

temp XOR provided_data is
DB5D050C C4BFCB06
F1D46A0B A1280BF3 011284BE 2642C197 E3855E60 4A9E26CB

Key is
DB5D050C C4BFCB06 F1D46A0B A1280BF3

V is
011284BE 2642C197 E3855E60 4A9E26CB

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is
00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is
DB5D050C C4BFCB06 F1D46A0B A1280BF3

V is
011284BE 2642C197 E3855E60 4A9E26CE

output_block is
10A46DA7 3E72179C 696C3AFA A43474EC

temp is

10A46DA7 3E72179C 696C3AFA A43474EC

While loop

Key is

DB5D050C C4BFCB06 F1D46A0B A1280BF3

V is

011284BE 2642C197 E3855E60 4A9E26CF

output_block is

1CC0B5E0 56F167A8 8939447B 19C054F5

temp is

10A46DA7 3E72179C
696C3AFA A43474EC 1CC0B5E0 56F167A8 8939447B 19C054F5

temp XOR provided_data is

10A46DA7 3E72179C
696C3AFA A43474EC 1CC0B5E0 56F167A8 8939447B 19C054F5

Key is

10A46DA7 3E72179C 696C3AFA A43474EC

V is

1CC0B5E0 56F167A8 8939447B 19C054F5

rnd_val is

9BD26351 37A52AF7
D0FCBEFE FB97EA93 A0F4C438 BD98956C 0DACB04F 15EE25B3

#####

CTR_DRBG

Requested Security Strength = 128

prediction_resistance_flag = "ENABLED"

EntropyInput =

00010203 04050607

08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F

EntropyInput1 (for Reseed1) =

80818283 84858687

88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F

EntropyInput2 (for Reseed2) =

C0C1C2C3 C4C5C6C7

C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7

Nonce =

20212223 24252627

PersonalizationString = <empty>

AdditionalInput1 =

60616263 64656667

68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F

AdditionalInput2 =

A0A1A2A3 A4A5A6A7

A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

#####

CTR_DRBG_Instantiate_algorithm - with derivation function

entropy_input is

00010203 04050607

08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F

nonce is

20212223 24252627

personal_str is <empty>

prediction_resistance_flag = "PredictionResistance"

Block_Cipher_df

input_str is

00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627

number_of_bits_to_return = 256

S is

00000028 00000020 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 80000000 00000000 00000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000028 00000020 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 80000000 00000000 00000000 00000000

temp is

834EBAD8 5C601126 1D1D9DF4 C42A1544

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000
00000000 00000000 00000028 00000020 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 80000000 00000000 00000000 00000000

temp is

834EBAD8 5C601126

1D1D9DF4 C42A1544 8EA249C1 226F0474 F3C55519 CB3677D2

Key is

834EBAD8 5C601126 1D1D9DF4 C42A1544

X is

8EA249C1 226F0474 F3C55519 CB3677D2

BlockEncrypt

Key is

834EBAD8 5C601126 1D1D9DF4 C42A1544

X is

8EA249C1 226F0474 F3C55519 CB3677D2

X = BlockEncrypt(Key, X) is

B8823BC4 F3AFBB6B A0373C69 BC49E2F6

temp is
B8823BC4 F3AFBB6B A0373C69 BC49E2F6

BlockEncrypt

Key is
834EBAD8 5C601126 1D1D9DF4 C42A1544

X is
B8823BC4 F3AFBB6B A0373C69 BC49E2F6

X = BlockEncrypt(Key, X) is
560EDE12 D8335B64 F5647FA0 A644162B

temp is
B8823BC4 F3AFBB6B
A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

requested_bits is
B8823BC4 F3AFBB6B
A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

seed_material is
B8823BC4 F3AFBB6B
A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

Update

provided_data is
B8823BC4 F3AFBB6B
A0373C69 BC49E2F6 560EDE12 D8335B64 F5647FA0 A644162B

While loop

Key is

00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is

58E2FCCE FA7E3061 367F1D57 A4E7455A

temp is

58E2FCCE FA7E3061 367F1D57 A4E7455A

While loop

Key is

00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

0388DACE 60B6A392 F328C2B9 71B2FE78

temp is

58E2FCCE FA7E3061

367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is

E060C70A 09D18B0A

9648213E 18AEA7AC 558604DC B885F8F6 064CBD19 D7F6E853

Key is

E060C70A 09D18B0A 9648213E 18AEA7AC

V is

558604DC B885F8F6 064CBD19 D7F6E853

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is

60616263 64656667

68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

entropy_input is

80818283 84858687

88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F

additional_input is

60616263 64656667

68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F

Block_Cipher_df

input_str is

80818283 84858687 88898A8B 8C8D8E8F

90919293 94959697 98999A9B 9C9D9E9F 60616263 64656667

68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F

number_of_bits_to_return = 256

S is

00000040 00000020
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
98999A9B 9C9D9E9F 60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000000 00000000 00000040 00000020
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
98999A9B 9C9D9E9F 60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000

temp is

EBE472ED 18D7D72C A576D5D0 4F951FF2

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000040 00000020
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
98999A9B 9C9D9E9F 60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000

temp is

EBE472ED 18D7D72C
A576D5D0 4F951FF2 E1753FDA 28CA0A50 0C8D0BE0 F45D9C20

Key is
EBE472ED 18D7D72C A576D5D0 4F951FF2

X is
E1753FDA 28CA0A50 0C8D0BE0 F45D9C20

BlockEncrypt

Key is
EBE472ED 18D7D72C A576D5D0 4F951FF2

X is
E1753FDA 28CA0A50 0C8D0BE0 F45D9C20

X = BlockEncrypt(Key, X) is
C1F7BD08 F11F831D FFE48696 8B706115

temp is
C1F7BD08 F11F831D FFE48696 8B706115

BlockEncrypt

Key is
EBE472ED 18D7D72C A576D5D0 4F951FF2

X is
C1F7BD08 F11F831D FFE48696 8B706115

X = BlockEncrypt(Key, X) is
7D71F428 FC13B31C 0AB3A4BB 7FA41524

temp is

C1F7BD08 F11F831D
FFE48696 8B706115 7D71F428 FC13B31C 0AB3A4BB 7FA41524

requested_bits is

C1F7BD08 F11F831D
FFE48696 8B706115 7D71F428 FC13B31C 0AB3A4BB 7FA41524

Update

provided_data is

C1F7BD08 F11F831D
FFE48696 8B706115 7D71F428 FC13B31C 0AB3A4BB 7FA41524

While loop

Key is

E060C70A 09D18B0A 9648213E 18AEA7AC

V is

558604DC B885F8F6 064CBD19 D7F6E854

output_block is

8CF59C8C F6888B96 EB1C1E3E 79D82387

temp is

8CF59C8C F6888B96 EB1C1E3E 79D82387

While loop

Key is

E060C70A 09D18B0A 9648213E 18AEA7AC

V is

558604DC B885F8F6 064CBD19 D7F6E855

output_block is

AF08A9E5 FF75E23F 1FBCD455 9B6B997E

temp is

8CF59C8C F6888B96

EB1C1E3E 79D82387 AF08A9E5 FF75E23F 1FBCD455 9B6B997E

temp XOR provided_data is

4D022184 0797088B

14F898A8 F2A84292 D2795DCD 03665123 150F70EE E4CF8C5A

Key is

4D022184 0797088B 14F898A8 F2A84292

V is

D2795DCD 03665123 150F70EE E4CF8C5A

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

4D022184 0797088B 14F898A8 F2A84292

V is

D2795DCD 03665123 150F70EE E4CF8C5D

output_block is

B3AAF086 5F3A5014 E5D54C6A 47184F14

temp is

B3AAF086 5F3A5014 E5D54C6A 47184F14

While loop

Key is

4D022184 0797088B 14F898A8 F2A84292

V is

D2795DCD 03665123 150F70EE E4CF8C5E

output_block is

213CABA6 26EB614F 28A2E5AD 17BAFE2B

temp is

B3AAF086 5F3A5014

E5D54C6A 47184F14 213CABA6 26EB614F 28A2E5AD 17BAFE2B

temp XOR provided_data is

B3AAF086 5F3A5014

E5D54C6A 47184F14 213CABA6 26EB614F 28A2E5AD 17BAFE2B

Key is

B3AAF086 5F3A5014 E5D54C6A 47184F14

V is

213CABA6 26EB614F 28A2E5AD 17BAFE2B

rnd_val is

4573AC8B BB33D7CC
4DBEF3EE DF6EAЕ74 8B536C3A 1082CEE4 948CDB51 C83A7F9C

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is

A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAЕAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

entropy_input is

C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF

additional_input is

A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAЕAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

Block_Cipher_df

input_str is

C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDFA0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

number_of_bits_to_return = 256

S is

00000040 00000020
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
D8D9DADB DCDDDEDFA0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000000 00000040 00000020
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
D8D9DADB DCDDDEDFA0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000

temp is

F57B5902 0636E7E2 20EDB29F 6EBCC72D

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000 00000040 00000020
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7

D8D9DADB DCDDDED F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000

temp is

F57B5902 0636E7E2
20EDB29F 6EBCC72D DFA80B3D A0FFF2E7 E81EE4ED 18CDECA6

Key is

F57B5902 0636E7E2 20EDB29F 6EBCC72D

X is

DFA80B3D A0FFF2E7 E81EE4ED 18CDECA6

BlockEncrypt

Key is

F57B5902 0636E7E2 20EDB29F 6EBCC72D

X is

DFA80B3D A0FFF2E7 E81EE4ED 18CDECA6

X = BlockEncrypt(Key, X) is

DC4290C1 50AD02F0 B68092DA E2472F86

temp is

DC4290C1 50AD02F0 B68092DA E2472F86

BlockEncrypt

Key is

F57B5902 0636E7E2 20EDB29F 6EBCC72D

X is

DC4290C1 50AD02F0 B68092DA E2472F86

X = BlockEncrypt(Key, X) is

AF2B9220 9762D534 4076FF12 D162E485

temp is

DC4290C1 50AD02F0

B68092DA E2472F86 AF2B9220 9762D534 4076FF12 D162E485

requested_bits is

DC4290C1 50AD02F0

B68092DA E2472F86 AF2B9220 9762D534 4076FF12 D162E485

Update

provided_data is

DC4290C1 50AD02F0

B68092DA E2472F86 AF2B9220 9762D534 4076FF12 D162E485

While loop

Key is

B3AAF086 5F3A5014 E5D54C6A 47184F14

V is

213CABA6 26EB614F 28A2E5AD 17BAFE2C

output_block is

0A8E9ACF 2A4D283A 1BD44054 BBD51AC4

temp is

0A8E9ACF 2A4D283A 1BD44054 BBD51AC4

While loop

Key is

B3AAF086 5F3A5014 E5D54C6A 47184F14

V is

213CABA6 26EB614F 28A2E5AD 17BAFE2D

output_block is

D01DDA32 A4A752B2 AA21023F F30180D0

temp is

0A8E9ACF 2A4D283A

1BD44054 BBD51AC4 D01DDA32 A4A752B2 AA21023F F30180D0

temp XOR provided_data is

D6CC0A0E 7AE02ACA

AD54D28E 59923542 7F364812 33C58786 EA57FD2D 22636455

Key is

D6CC0A0E 7AE02ACA AD54D28E 59923542

V is

7F364812 33C58786 EA57FD2D 22636455

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is
00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

While loop

Key is
D6CC0A0E 7AE02ACA AD54D28E 59923542

V is

7F364812 33C58786 EA57FD2D 22636458

output_block is

89DE75C8 E0A4BCBA 0DD270E1 87E93EC7

temp is

89DE75C8 E0A4BCBA 0DD270E1 87E93EC7

While loop

Key is
D6CC0A0E 7AE02ACA AD54D28E 59923542

V is

7F364812 33C58786 EA57FD2D 22636459

output_block is

60B0D047 81606A14 BE1FE576 8405D9D1

temp is

89DE75C8 E0A4BCBA
0DD270E1 87E93EC7 60B0D047 81606A14 BE1FE576 8405D9D1

```
temp XOR provided_data is
          89DE75C8 E0A4BCBA
 0DD270E1 87E93EC7 60B0D047 81606A14 BE1FE576 8405D9D1
```

```
Key is
          89DE75C8 E0A4BCBA 0DD270E1 87E93EC7
```

```
V is
          60B0D047 81606A14 BE1FE576 8405D9D1
```

```
rnd_val is
          99C628CD D87BD8C2
 F1FE443A A7F761DA 16886436 32632335 4DA6311F FF5BC678
```

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

CTR_DRBG

Requested Security Strength = 128

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

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

```
EntropyInput2 (for Reseed2) =
          C0C1C2C3 C4C5C6C7
 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7
```

```
Nonce =
          20212223 24252627
```

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

```
AdditionalInput = <empty>
```

```
#####
*****
```

```
CTR_DRBG_Instantiate_algorithm - with derivation function
```

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

```
nonce is
        20212223 24252627
```

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

```
prediction_resistance_flag = "PredictionResistance"
```

```
-----
```

```
Block_Cipher_df
```

```
input_str is
        00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
        18191A1B 1C1D1E1F 20212223 24252627 40414243 44454647
        48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
```

```
number_of_bits_to_return = 256
```

```
S is
```

```
00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000
```

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000000 00000000
00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000

temp is

C4C14823 AE157968 6F2C4676 8030DE37

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000
00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000

temp is

C4C14823 AE157968

6F2C4676 8030DE37 95EC1158 E6CD251C 577C6047 EBFFB5FE

Key is

C4C14823 AE157968 6F2C4676 8030DE37

X is

95EC1158 E6CD251C 577C6047 EBFFB5FE

BlockEncrypt

Key is

C4C14823 AE157968 6F2C4676 8030DE37

X is

95EC1158 E6CD251C 577C6047 EBFFB5FE

X = BlockEncrypt(Key, X) is

C2659E6A EFBB0DFB 2096A598 CC1C509F

temp is

C2659E6A EFBB0DFB 2096A598 CC1C509F

BlockEncrypt

Key is

C4C14823 AE157968 6F2C4676 8030DE37

X is

C2659E6A EFBB0DFB 2096A598 CC1C509F

X = BlockEncrypt(Key, X) is

D926A4C1 E62F8936 D419709D 6124946A

temp is

C2659E6A EFBB0DFB

2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

requested_bits is
C2659E6A EFBB0DFB
2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

seed_material is
C2659E6A EFBB0DFB
2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

Update

provided_data is
C2659E6A EFBB0DFB
2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

While loop

Key is
00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000001

output_block is
58E2FCCE FA7E3061 367F1D57 A4E7455A

temp is
58E2FCCE FA7E3061 367F1D57 A4E7455A

While loop

Key is

00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

0388DACE 60B6A392 F328C2B9 71B2FE78

temp is

58E2FCCE FA7E3061

367F1D57 A4E7455A 0388DACE 60B6A392 F328C2B9 71B2FE78

temp XOR provided_data is

9A8762A4 15C53D9A

16E9B8CF 68FB15C5 DAAE7E0F 86992AA4 2731B224 10966A12

Key is

9A8762A4 15C53D9A 16E9B8CF 68FB15C5

V is

DAAE7E0F 86992AA4 2731B224 10966A12

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

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

additional_input is <empty>

Block_Cipher_df

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

number_of_bits_to_return = 256

S is
00000020 00000020 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F 80000000 00000000

BCC

IV is
00000000 00000000 00000000 00000000

IV || S is
00000000 00000000 00000000 00000000
00000020 00000020 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F 80000000 00000000

temp is
6689B2EA B8B5547F E46D8E0B 6AD94B8C

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000
00000020 00000020 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F 80000000 00000000

temp is

6689B2EA B8B5547F
E46D8E0B 6AD94B8C 4578F39E C865C2E4 EADB493B A265794F

Key is

6689B2EA B8B5547F E46D8E0B 6AD94B8C

X is

4578F39E C865C2E4 EADB493B A265794F

BlockEncrypt

Key is

6689B2EA B8B5547F E46D8E0B 6AD94B8C

X is

4578F39E C865C2E4 EADB493B A265794F

X = BlockEncrypt(Key, X) is

E8B2120B 0673C751 090997D6 BEAC637D

temp is

E8B2120B 0673C751 090997D6 BEAC637D

BlockEncrypt

Key is

6689B2EA B8B5547F E46D8E0B 6AD94B8C

X is

E8B2120B 0673C751 090997D6 BEAC637D

X = BlockEncrypt(Key, X) is

79D7CA26 C10FEE1F EAC1E952 46CC5005

temp is

E8B2120B 0673C751
090997D6 BEAC637D 79D7CA26 C10FEE1F EAC1E952 46CC5005

requested_bits is

E8B2120B 0673C751
090997D6 BEAC637D 79D7CA26 C10FEE1F EAC1E952 46CC5005

Update

provided_data is

E8B2120B 0673C751
090997D6 BEAC637D 79D7CA26 C10FEE1F EAC1E952 46CC5005

While loop

Key is

9A8762A4 15C53D9A 16E9B8CF 68FB15C5

V is

DAAE7E0F 86992AA4 2731B224 10966A13

output_block is

18FDEFBD C43D7A36 D5D6D862 205765D1

temp is

18FDEFBD C43D7A36 D5D6D862 205765D1

While loop

Key is

9A8762A4 15C53D9A 16E9B8CF 68FB15C5

V is

DAAE7E0F 86992AA4 2731B224 10966A14

output_block is

D701C9F2 37007030 DF1B8E70 EE4EEE29

temp is

18FDEFBD C43D7A36

D5D6D862 205765D1 D701C9F2 37007030 DF1B8E70 EE4EEE29

temp XOR provided_data is

F04FFDB6 C24EBD67

DCDF4FB4 9EFB06AC AED603D4 F60F9E2F 35DA6722 A882BE2C

Key is

F04FFDB6 C24EBD67 DCDF4FB4 9EFB06AC

V is

AED603D4 F60F9E2F 35DA6722 A882BE2C

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

F04FFDB6 C24EBD67 DCDF4FB4 9EFB06AC

V is

AED603D4 F60F9E2F 35DA6722 A882BE2F

output_block is

30F4A36C EEC8FB06 461F757F 9FFF5865

temp is

30F4A36C EEC8FB06 461F757F 9FFF5865

While loop

Key is

F04FFDB6 C24EBD67 DCDF4FB4 9EFB06AC

V is

AED603D4 F60F9E2F 35DA6722 A882BE30

output_block is

7E1FC53A 8D9322D2 6F1A255B 2A19CEEB

temp is

30F4A36C EEC8FB06
461F757F 9FFF5865 7E1FC53A 8D9322D2 6F1A255B 2A19CEEB

temp XOR provided_data is

30F4A36C EEC8FB06
461F757F 9FFF5865 7E1FC53A 8D9322D2 6F1A255B 2A19CEEB

Key is

30F4A36C EEC8FB06 461F757F 9FFF5865

V is

7E1FC53A 8D9322D2 6F1A255B 2A19CEEB

rnd_val is

F324104E 2FA14F79
D8AA60DF 06B93B3B C1573249 58F0A7EE 1E193677 A70E0250

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

entropy_input is

C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF

additional_input is <empty>

Block_Cipher_df

input_str is

C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF

number_of_bits_to_return = 256

S is

00000020 00000020 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000000 00000000
00000020 00000020 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF 80000000 00000000

temp is

72571427 A62CFFB3 105AA38D 4C701D8A

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000
00000020 00000020 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF 80000000 00000000

temp is

72571427 A62CFFB3
105AA38D 4C701D8A E90056D7 6C2480EE 096C3B48 059FD3F7

Key is

72571427 A62CFFB3 105AA38D 4C701D8A

X is

E90056D7 6C2480EE 096C3B48 059FD3F7

BlockEncrypt

Key is

72571427 A62CFFB3 105AA38D 4C701D8A

X is

E90056D7 6C2480EE 096C3B48 059FD3F7

X = BlockEncrypt(Key, X) is

ACEF0D4B 113B12C1 4E45C0A0 A9574DE6

temp is

ACEF0D4B 113B12C1 4E45C0A0 A9574DE6

BlockEncrypt

Key is

72571427 A62CFFB3 105AA38D 4C701D8A

X is

ACEF0D4B 113B12C1 4E45C0A0 A9574DE6

X = BlockEncrypt(Key, X) is

F20CF416 9FEF3831 76A7C304 F0066E66

temp is

ACEF0D4B 113B12C1

4E45C0A0 A9574DE6 F20CF416 9FEF3831 76A7C304 F0066E66

requested_bits is

ACEF0D4B 113B12C1

4E45C0A0 A9574DE6 F20CF416 9FEF3831 76A7C304 F0066E66

Update

provided_data is

ACEF0D4B 113B12C1

4E45C0A0 A9574DE6 F20CF416 9FEF3831 76A7C304 F0066E66

While loop

Key is

30F4A36C EEC8FB06 461F757F 9FFF5865

V is

7E1FC53A 8D9322D2 6F1A255B 2A19CEEC

output_block is

0083F230 2AA6069D 85CA5D62 7B134697

temp is

0083F230 2AA6069D 85CA5D62 7B134697

While loop

Key is

30F4A36C EEC8FB06 461F757F 9FFF5865

V is

7E1FC53A 8D9322D2 6F1A255B 2A19CEED

output_block is

900DBA47 8EB2A67A 54CC49AD FACCE41F

temp is

0083F230 2AA6069D

85CA5D62 7B134697 900DBA47 8EB2A67A 54CC49AD FACCE41F

temp XOR provided_data is

AC6CFF7B 3B9D145C

CB8F9DC2 D2440B71 62014E51 115D9E4B 226B8AA9 0ACA8A79

Key is

AC6CFF7B 3B9D145C CB8F9DC2 D2440B71

V is

62014E51 115D9E4B 226B8AA9 0ACA8A79

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is
00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000

While loop

Key is
AC6CFF7B 3B9D145C CB8F9DC2 D2440B71

V is

62014E51 115D9E4B 226B8AA9 0ACA8A7C

output_block is

561A1088 01412E20 882B0B5A 682EC41D

temp is

561A1088 01412E20 882B0B5A 682EC41D

While loop

Key is
AC6CFF7B 3B9D145C CB8F9DC2 D2440B71

V is

62014E51 115D9E4B 226B8AA9 0ACA8A7D

output_block is

C972133D 67C2B62C 74196869 30001E57

temp is

561A1088 01412E20

882B0B5A 682EC41D C972133D 67C2B62C 74196869 30001E57

temp XOR provided_data is

561A1088 01412E20

882B0B5A 682EC41D C972133D 67C2B62C 74196869 30001E57

Key is

561A1088 01412E20 882B0B5A 682EC41D

V is

C972133D 67C2B62C 74196869 30001E57

rnd_val is

78F4C840 134F40DC

001BFAD3 A90B5EF4 DEBDBFAC 3CFDF0CD 69A89DC4 FD34713F

#####

CTR_DRBG

Requested Security Strength = 128

prediction_resistance_flag = "ENABLED"

EntropyInput =

00010203 04050607

08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F

EntropyInput1 (for Reseed1) =

80818283 84858687

88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F

EntropyInput2 (for Reseed2) =

C0C1C2C3 C4C5C6C7

C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF

Nonce =

20212223 24252627

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

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

```
AdditionalInput2 =
    A0A1A2A3 A4A5A6A7
    A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
```

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

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

```
CTR_DRBG_Instantiate_algorithm - with derivation function
```

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

```
nonce is
    20212223 24252627
```

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

```
prediction_resistance_flag = "PredictionResistance"
```

```
-----
```

```
Block_Cipher_df
```

```
input_str is
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
```

```
number_of_bits_to_return = 256
```

S is

```
00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F  
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627  
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657  
58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000
```

BCC

IV is

```
00000000 00000000 00000000 00000000
```

IV || S is

```
00000000 00000000 00000000 00000000  
00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F  
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627  
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657  
58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000
```

temp is

```
C4C14823 AE157968 6F2C4676 8030DE37
```

BCC

IV is

```
00000001 00000000 00000000 00000000
```

IV || S is

```
00000001 00000000 00000000 00000000  
00000048 00000020 00010203 04050607 08090A0B 0C0D0E0F  
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627  
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657  
58595A5B 5C5D5E5F 80000000 00000000 00000000 00000000
```

temp is

C4C14823 AE157968
6F2C4676 8030DE37 95EC1158 E6CD251C 577C6047 EBFFB5FE

Key is

C4C14823 AE157968 6F2C4676 8030DE37

X is

95EC1158 E6CD251C 577C6047 EBFFB5FE

BlockEncrypt

Key is

C4C14823 AE157968 6F2C4676 8030DE37

X is

95EC1158 E6CD251C 577C6047 EBFFB5FE

X = BlockEncrypt(Key, X) is

C2659E6A EFBB0DFB 2096A598 CC1C509F

temp is

C2659E6A EFBB0DFB 2096A598 CC1C509F

BlockEncrypt

Key is

C4C14823 AE157968 6F2C4676 8030DE37

X is

C2659E6A EFBB0DFB 2096A598 CC1C509F

X = BlockEncrypt(Key, X) is
D926A4C1 E62F8936 D419709D 6124946A

temp is
C2659E6A EFBB0DFB
2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

requested_bits is
C2659E6A EFBB0DFB
2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

seed_material is
C2659E6A EFBB0DFB
2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

Update

provided_data is
C2659E6A EFBB0DFB
2096A598 CC1C509F D926A4C1 E62F8936 D419709D 6124946A

While loop

Key is
00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000001

output_block is
58E2FCCE FA7E3061 367F1D57 A4E7455A

temp is
58E2FCCE FA7E3061 367F1D57 A4E7455A

While loop

Key is
00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000002

output_block is
0388DACE 60B6A392 F328C2B9 71B2FE78

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

temp XOR provided_data is
9A8762A4 15C53D9A
16E9B8CF 68FB15C5 DAAE7E0F 86992AA4 2731B224 10966A12

Key is
9A8762A4 15C53D9A 16E9B8CF 68FB15C5

V is
DAAE7E0F 86992AA4 2731B224 10966A12

First call to Generate

CTR_DRBG_Generate

```
requested_number_of_bits = 256  
  
additional_input is  
60616263 64656667  
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
```

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

CTR_DRBG_Reseed

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

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

Block_Cipher_df

```
input_str is  
80818283 84858687 88898A8B 8C8D8E8F  
90919293 94959697 98999A9B 9C9D9E9F 60616263 64656667  
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
```

number_of_bits_to_return = 256

S is
00000040 00000020
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
98999A9B 9C9D9E9F 60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000000 00000000 00000040 00000020
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
98999A9B 9C9D9E9F 60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000

temp is

E8E472ED 18D7D72C A576D5D0 4F951FF2

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000 00000040 00000020
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
98999A9B 9C9D9E9F 60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80000000 00000000

temp is

E8E472ED 18D7D72C
A576D5D0 4F951FF2 E1753FDA 28CA0A50 0C8D0BE0 F45D9C20

Key is

E8E472ED 18D7D72C A576D5D0 4F951FF2

X is

E1753FDA 28CA0A50 0C8D0BE0 F45D9C20

BlockEncrypt

Key is

EBE472ED 18D7D72C A576D5D0 4F951FF2

X is

E1753FDA 28CA0A50 0C8D0BE0 F45D9C20

X = BlockEncrypt(Key, X) is

C1F7BD08 F11F831D FFE48696 8B706115

temp is

C1F7BD08 F11F831D FFE48696 8B706115

BlockEncrypt

Key is

EBE472ED 18D7D72C A576D5D0 4F951FF2

X is

C1F7BD08 F11F831D FFE48696 8B706115

X = BlockEncrypt(Key, X) is

7D71F428 FC13B31C 0AB3A4BB 7FA41524

temp is

C1F7BD08 F11F831D

FFE48696 8B706115 7D71F428 FC13B31C 0AB3A4BB 7FA41524

requested_bits is

C1F7BD08 F11F831D

FFE48696 8B706115 7D71F428 FC13B31C 0AB3A4BB 7FA41524

Update

provided_data is

C1F7BD08 F11F831D
FFE48696 8B706115 7D71F428 FC13B31C 0AB3A4BB 7FA41524

While loop

Key is

9A8762A4 15C53D9A 16E9B8CF 68FB15C5

V is

DAAE7E0F 86992AA4 2731B224 10966A13

output_block is

18FDEFBD C43D7A36 D5D6D862 205765D1

temp is

18FDEFBD C43D7A36 D5D6D862 205765D1

While loop

Key is

9A8762A4 15C53D9A 16E9B8CF 68FB15C5

V is

DAAE7E0F 86992AA4 2731B224 10966A14

output_block is

D701C9F2 37007030 DF1B8E70 EE4EEE29

temp is

18FDEFBD C43D7A36

D5D6D862 205765D1 D701C9F2 37007030 DF1B8E70 EE4EEE29

temp XOR provided_data is
D90A52B5 3522F92B
2A325EF4 AB2704C4 AA703DDA CB13C32C D5A82ACB 91EAFB0D

Key is
D90A52B5 3522F92B 2A325EF4 AB2704C4

V is
AA703DDA CB13C32C D5A82ACB 91EAFB0D

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is
00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is
D90A52B5 3522F92B 2A325EF4 AB2704C4

V is
AA703DDA CB13C32C D5A82ACB 91EAFB10

output_block is
19ED3F6B 4C63004C 8E48DDF5 E8389046

temp is

19ED3F6B 4C63004C 8E48DDF5 E8389046

While loop

Key is

D90A52B5 3522F92B 2A325EF4 AB2704C4

V is

AA703DDA CB13C32C D5A82ACB 91EAFB11

output_block is

B51A544A 9C38D15D 30944D92 C709A151

temp is

19ED3F6B 4C63004C

8E48DDF5 E8389046 B51A544A 9C38D15D 30944D92 C709A151

temp XOR provided_data is

19ED3F6B 4C63004C

8E48DDF5 E8389046 B51A544A 9C38D15D 30944D92 C709A151

Key is

19ED3F6B 4C63004C 8E48DDF5 E8389046

V is

B51A544A 9C38D15D 30944D92 C709A151

rnd_val is

87D6BDA1 9F461BF0

B4E1D5BC 87A265A4 AE118AF2 8AB3D8E9 62827B79 08C76279

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is

A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

entropy_input is

C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7

additional_input is

A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

Block_Cipher_df

input_str is

C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7 A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

number_of_bits_to_return = 256

S is

00000040 00000020
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
D8D9DADB DCDDDED7 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000000 00000000 00000040 00000020
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
D8D9DADB DCDDDEF A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000

temp is

F57B5902 0636E7E2 20EDB29F 6EBCC72D

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000 00000040 00000020
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
D8D9DADB DCDDDEF A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF 80000000 00000000

temp is

F57B5902 0636E7E2

20EDB29F 6EBCC72D DFA80B3D A0FFF2E7 E81EE4ED 18CDECA6

Key is

F57B5902 0636E7E2 20EDB29F 6EBCC72D

X is

DFA80B3D A0FFF2E7 E81EE4ED 18CDECA6

BlockEncrypt

Key is

F57B5902 0636E7E2 20EDB29F 6EBCC72D

X is

DFA80B3D A0FFF2E7 E81EE4ED 18CDECA6

X = BlockEncrypt(Key, X) is

DC4290C1 50AD02F0 B68092DA E2472F86

temp is

DC4290C1 50AD02F0 B68092DA E2472F86

BlockEncrypt

Key is

F57B5902 0636E7E2 20EDB29F 6EBCC72D

X is

DC4290C1 50AD02F0 B68092DA E2472F86

X = BlockEncrypt(Key, X) is

AF2B9220 9762D534 4076FF12 D162E485

temp is

DC4290C1 50AD02F0

B68092DA E2472F86 AF2B9220 9762D534 4076FF12 D162E485

requested_bits is
DC4290C1 50AD02F0
B68092DA E2472F86 AF2B9220 9762D534 4076FF12 D162E485

Update

provided_data is
DC4290C1 50AD02F0
B68092DA E2472F86 AF2B9220 9762D534 4076FF12 D162E485

While loop

Key is
19ED3F6B 4C63004C 8E48DDF5 E8389046

V is

B51A544A 9C38D15D 30944D92 C709A152

output_block is

DB89FDDE 2A4C1124 BE15D236 18668BE6

temp is

DB89FDDE 2A4C1124 BE15D236 18668BE6

While loop

Key is
19ED3F6B 4C63004C 8E48DDF5 E8389046

V is

B51A544A 9C38D15D 30944D92 C709A153

output_block is
F10F36FD 869D45CB 2FA79450 F27B30FF

temp is
DB89FDFE 2A4C1124
BE15D236 18668BE6 F10F36FD 869D45CB 2FA79450 F27B30FF

temp XOR provided_data is
07CB6D3F 7AE113D4
089540EC FA21A460 5E24A4DD 11FF90FF 6FD16B42 2319D47A

Key is
07CB6D3F 7AE113D4 089540EC FA21A460

V is
5E24A4DD 11FF90FF 6FD16B42 2319D47A

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is
00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is
07CB6D3F 7AE113D4 089540EC FA21A460

V is

5E24A4DD 11FF90FF 6FD16B42 2319D47D

output_block is

E7950365 FE7156AA 4A8E253B 03021DE4

temp is

E7950365 FE7156AA 4A8E253B 03021DE4

While loop

Key is

07CB6D3F 7AE113D4 089540EC FA21A460

V is

5E24A4DD 11FF90FF 6FD16B42 2319D47E

output_block is

54C4DAE2 D0160479 C7C5529F 376DA9A7

temp is

E7950365 FE7156AA

4A8E253B 03021DE4 54C4DAE2 D0160479 C7C5529F 376DA9A7

temp XOR provided_data is

E7950365 FE7156AA

4A8E253B 03021DE4 54C4DAE2 D0160479 C7C5529F 376DA9A7

Key is

E7950365 FE7156AA 4A8E253B 03021DE4

V is

54C4DAE2 D0160479 C7C5529F 376DA9A7

```
rnd_val is
    2D59B89D C71C48D6
    C327A7E2 C4328ECE AF85FB5F 8EE00226 1B0FC412 90ECE29F
#####
CTR_DRBG
    Requested Security Strength = 192
    prediction_resistance_flag = "NOT ENABLED"
    EntropyInput =
        00010203 04050607 08090A0B 0C0D0E0F
        10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627

    EntropyInput1 (for Reseed1) =
        80818283 84858687 88898A8B 8C8D8E8F
        90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7

    EntropyInput2 (for Reseed2) =
        C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
        D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7

    Nonce =
        20212223 24252627 28292A2B

    PersonalizationString = <empty>
    AdditionalInput = <empty>
#####
*****
```

CTR_DRBG_Instantiate_algorithm - with derivation function

```
entropy_input is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
```

nonce is

20212223 24252627 28292A2B

personal_str is <empty>

prediction_resistance_flag = "No PredictionResistance"

Block_Cipher_df

input_str is

00010203

04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B
1C1D1E1F 20212223 24252627 20212223 24252627 28292A2B

number_of_bits_to_return = 320

S is

00000034 00000028 00010203 04050607

08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 80000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000

00000000 00000000 00000034 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 80000000

temp is

2D64B3D8 692984AD B6FBBA41 F69E74E1

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000

00000000 00000000 00000034 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 80000000

temp is

2D64B3D8 692984AD

B6FBBA41 F69E74E1 72DAEE1D 75EFF1E 66616F2E 9F91BC31

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000

00000000 00000000 00000034 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 80000000

temp is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E
66616F2E 9F91BC31 C6ADE98F EB96A83C A6F71BF5 BCE6944D

Key is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

X is
66616F2E 9F91BC31 C6ADE98F EB96A83C

BlockEncrypt

Key is
2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

X is
66616F2E 9F91BC31 C6ADE98F EB96A83C

X = BlockEncrypt(Key, X) is
45EBC7A3 4CB5BFDB A58CBFCC A756DDCB

temp is
45EBC7A3 4CB5BFDB A58CBFCC A756DDCB

BlockEncrypt

Key is
2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

X is
45EBC7A3 4CB5BFDB A58CBFCC A756DDCB

X = BlockEncrypt(Key, X) is
7150F160 187803C2 0380FB02 636C8E59

temp is
45EBC7A3 4CB5BFDB
A58CBFCC A756DDCB 7150F160 187803C2 0380FB02 636C8E59

BlockEncrypt

Key is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

X is

7150F160 187803C2 0380FB02 636C8E59

X = BlockEncrypt(Key, X) is

B1A94E9C C2360559 9C002E3A 221F5C21

temp is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB 7150F160 187803C2
0380FB02 636C8E59 B1A94E9C C2360559 9C002E3A 221F5C21

requested_bits is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559

seed_material is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559

Update

provided_data is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559

While loop

Key is

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is

CD33B28A C773F74B A00ED1F3 12572435

temp is

CD33B28A C773F74B A00ED1F3 12572435

While loop

Key is

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

98E7247C 07F0FE41 1C267E43 84B0F600

temp is

CD33B28A C773F74B

A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600

While loop

Key is

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000003

output_block is
2A3493E6 6235EE67 DEECCD2F 3B393BD8

temp is
CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8

temp XOR provided_data is
88D87529 8BC64890 05826E3F B501F9FE
E9B7D51C 1F88FD83 1FA68541 E7DC7859 9B9DDD7A A003EB3E

Key is
88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83

V is
1FA68541 E7DC7859 9B9DDD7A A003EB3E

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

While loop

Key is

88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83

V is

1FA68541 E7DC7859 9B9DDD7A A003EB41

output_block is

FC55C88D AFA06880 F2C73C08 1E8FA294

temp is

FC55C88D AFA06880 F2C73C08 1E8FA294

While loop

Key is

88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83

V is

1FA68541 E7DC7859 9B9DDD7A A003EB42

output_block is

DBE69237 CDB6EF72 96CE3A7B 114703B2

temp is

FC55C88D AFA06880

F2C73C08 1E8FA294 DBE69237 CDB6EF72 96CE3A7B 114703B2

While loop

Key is

88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83

V is

1FA68541 E7DC7859 9B9DDD7A A003EB43

output_block is

8810183A 1A7C9CFC 14560D9C 4FE75670

temp is

FC55C88D AFA06880 F2C73C08 1E8FA294 DBE69237 CDB6EF72
96CE3A7B 114703B2 8810183A 1A7C9CFC 14560D9C 4FE75670

temp XOR provided_data is

FC55C88D AFA06880 F2C73C08 1E8FA294
DBE69237 CDB6EF72 96CE3A7B 114703B2 8810183A 1A7C9CFC

Key is

FC55C88D AFA06880 F2C73C08 1E8FA294 DBE69237 CDB6EF72

V is

96CE3A7B 114703B2 8810183A 1A7C9CFC

rnd_val is

1A646BB1 D38BD2AE
A30CF5C5 D812A624 B50D3ECA 99E508B2 5B5448A8 B96C0F2E

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

While loop

Key is
FC55C88D AFA06880 F2C73C08 1E8FA294 DBE69237 CDB6EF72

V is

96CE3A7B 114703B2 8810183A 1A7C9CFF

output_block is

2F3BBFBBD 6D63C6B1 84E68CEC CC43AD6D

temp is

2F3BBFBBD 6D63C6B1 84E68CEC CC43AD6D

While loop

Key is
FC55C88D AFA06880 F2C73C08 1E8FA294 DBE69237 CDB6EF72

V is

96CE3A7B 114703B2 8810183A 1A7C9D00

output_block is

DF160344 BF7E8318 E7D017F5 94D5C087

temp is

2F3BBFBBD 6D63C6B1
84E68CEC CC43AD6D DF160344 BF7E8318 E7D017F5 94D5C087

While loop

Key is

FC55C88D AFA06880 F2C73C08 1E8FA294 DBE69237 CDB6EF72

V is

96CE3A7B 114703B2 8810183A 1A7C9D01

output_block is

DEDEBD95 523BD30A DC046C03 94AC5E42

temp is

2F3BBFBBD 6D63C6B1 84E68CEC CC43AD6D DF160344 BF7E8318
E7D017F5 94D5C087 DEDEBD95 523BD30A DC046C03 94AC5E42

temp XOR provided_data is

2F3BBFBBD 6D63C6B1 84E68CEC CC43AD6D
DF160344 BF7E8318 E7D017F5 94D5C087 DEDEBD95 523BD30A

Key is

2F3BBFBBD 6D63C6B1 84E68CEC CC43AD6D DF160344 BF7E8318

V is

E7D017F5 94D5C087 DEDEBD95 523BD30A

rnd_val is

0920CB32 A773E0FF
4BBBBF90A CB1D7044 E15B629A FB3C7F9F E26673E3 E7BE4727

#####

CTR_DRBG

Requested Security Strength = 192

```
prediction_resistance_flag = "NOT ENABLED"
EntropyInput =
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
```

```
EntropyInput1 (for Reseed1) =
    80818283 84858687 88898A8B 8C8D8E8F
    90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
```

```
EntropyInput2 (for Reseed2) =
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
    D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7 E0E1E2E3 E4E5E6E7
```

```
Nonce =
    20212223 24252627 28292A2B
```

```
PersonalizationString = <empty>
```

```
AdditionalInput1 =
    60616263 64656667 68696A6B 6C6D6E6F
    70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687
```

```
AdditionalInput2 =
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
    B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7
```

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

```
*****
```

```
CTR_DRBG_Instantiate_algorithm - with derivation function
```

```
entropy_input is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
```

```
nonce is
    20212223 24252627 28292A2B
```

```
personal_str is <empty>  
prediction_resistance_flag = "No PredictionResistance"  
-----
```

Block_Cipher_df

```
input_str is  
00010203  
04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B  
1C1D1E1F 20212223 24252627 20212223 24252627 28292A2B
```

number_of_bits_to_return = 320

```
S is  
00000034 00000028 00010203 04050607  
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F  
20212223 24252627 20212223 24252627 28292A2B 80000000
```

BCC

IV is
00000000 00000000 00000000 00000000

IV || S is
00000000 00000000
00000000 00000000 00000034 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 80000000

```
temp is  
2D64B3D8 692984AD B6FBBA41 F69E74E1
```

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000

00000000 00000000 00000034 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 80000000

temp is

2D64B3D8 692984AD

B6FBBA41 F69E74E1 72DAEE1D 75EFF1E 66616F2E 9F91BC31

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000

00000000 00000000 00000034 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 80000000

temp is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

66616F2E 9F91BC31 C6ADE98F EB96A83C A6F71BF5 BCE6944D

Key is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

X is

66616F2E 9F91BC31 C6ADE98F EB96A83C

BlockEncrypt

Key is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

X is

66616F2E 9F91BC31 C6ADE98F EB96A83C

X = BlockEncrypt(Key, X) is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB

temp is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB

BlockEncrypt

Key is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

X is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB

X = BlockEncrypt(Key, X) is

7150F160 187803C2 0380FB02 636C8E59

temp is

45EBC7A3 4CB5BFDB

A58CBFCC A756DDCB 7150F160 187803C2 0380FB02 636C8E59

BlockEncrypt

Key is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFFF1E

X is

7150F160 187803C2 0380FB02 636C8E59

X = BlockEncrypt(Key, X) is

B1A94E9C C2360559 9C002E3A 221F5C21

temp is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB 7150F160 187803C2
0380FB02 636C8E59 B1A94E9C C2360559 9C002E3A 221F5C21

requested_bits is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559

seed_material is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559

Update

provided_data is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559

While loop

Key is

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is
CD33B28A C773F74B A00ED1F3 12572435

temp is
CD33B28A C773F74B A00ED1F3 12572435

While loop

Key is
00000000 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000002

output_block is
98E7247C 07F0FE41 1C267E43 84B0F600

temp is
CD33B28A C773F74B
A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600

While loop

Key is
00000000 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000003

output_block is
2A3493E6 6235EE67 DEECCD2F 3B393BD8

```
temp is
CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8
```

```
temp XOR provided_data is
88D87529 8BC64890 05826E3F B501F9FE
E9B7D51C 1F88FD83 1FA68541 E7DC7859 9B9DDD7A A003EB3E
```

```
Key is
88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83
```

```
V is
1FA68541 E7DC7859 9B9DDD7A A003EB3E
```

```
First call to Generate
```

```
*****
```

```
CTR_DRBG_Generate
```

```
requested_number_of_bits = 256
```

```
additional_input is
60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687
```

```
additional_input <> NULL, process appropriately
```

```
Block_Cipher_df
```

```
input_str is
60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687
```

```
number_of_bits_to_return = 320
```

```
S is
```

00000028 00000028 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 80000000 00000000 00000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000
00000000 00000000 00000028 00000028 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 80000000 00000000 00000000 00000000

temp is

E5460ACC 5126F932 D56D1A29 1FC4A2A2

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000
00000000 00000000 00000028 00000028 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 80000000 00000000 00000000 00000000

temp is

E5460ACC 5126F932
D56D1A29 1FC4A2A2 280D9844 33D9A0F7 BE003DAF 2996B5CF

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000

00000000 00000000 00000028 00000028 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 80000000 00000000 00000000 00000000

temp is

E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7
BE003DAF 2996B5CF 5AD5C453 7046B98F C143E7B2 F9A465C4

Key is

E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7

X is

BE003DAF 2996B5CF 5AD5C453 7046B98F

BlockEncrypt

Key is

E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7

X is

BE003DAF 2996B5CF 5AD5C453 7046B98F

X = BlockEncrypt(Key, X) is

A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C

temp is

A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C

BlockEncrypt

Key is

E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7

X is

A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C

X = BlockEncrypt(Key, X) is

3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1

temp is

A2F76A3A 0305FCDE

2DB7FA2D ED8DE90C 3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1

BlockEncrypt

Key is

E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7

X is

3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1

X = BlockEncrypt(Key, X) is

B2AA5CA0 E45067DE 84D9D2FA FDA512C9

temp is

A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C 3E877DE5 FA752EB7

2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE 84D9D2FA FDA512C9

requested_bits is

A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C

3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE

Update

provided_data is

A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C
3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE

While loop

Key is

88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83

V is

1FA68541 E7DC7859 9B9DDD7A A003EB3F

output_block is

1A646BB1 D38BD2AE A30CF5C5 D812A624

temp is

1A646BB1 D38BD2AE A30CF5C5 D812A624

While loop

Key is

88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83

V is

1FA68541 E7DC7859 9B9DDD7A A003EB40

output_block is

B50D3ECA 99E508B2 5B5448A8 B96C0F2E

temp is

1A646BB1 D38BD2AE
A30CF5C5 D812A624 B50D3ECA 99E508B2 5B5448A8 B96C0F2E

While loop

Key is

88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83

V is

1FA68541 E7DC7859 9B9DDD7A A003EB41

output_block is

FC55C88D AFA06880 F2C73C08 1E8FA294

temp is

1A646BB1 D38BD2AE A30CF5C5 D812A624 B50D3ECA 99E508B2
5B5448A8 B96C0F2E FC55C88D AFA06880 F2C73C08 1E8FA294

temp XOR provided_data is

B893018B D08E2E70 8EBB0FE8 359F4F28
8B8A432F 63902605 7428740C 3EDBCCDF 4EFF942D 4BF00F5E

Key is

B893018B D08E2E70 8EBB0FE8 359F4F28 8B8A432F 63902605

V is

7428740C 3EDBCCDF 4EFF942D 4BF00F5E

Update

provided_data is

A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C
3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE

While loop

Key is

B893018B D08E2E70 8EBB0FE8 359F4F28 8B8A432F 63902605

V is

7428740C 3EDBCCDF 4EFF942D 4BF00F61

output_block is

E346B483 9677B724 7BE0AAB3 B1B969CA

temp is

E346B483 9677B724 7BE0AAB3 B1B969CA

While loop

Key is

B893018B D08E2E70 8EBB0FE8 359F4F28 8B8A432F 63902605

V is

7428740C 3EDBCCDF 4EFF942D 4BF00F62

output_block is

B13C2105 AE36F9F1 27ECBD37 E72AB845

temp is

E346B483 9677B724

7BE0AAB3 B1B969CA B13C2105 AE36F9F1 27ECBD37 E72AB845

While loop

Key is

B893018B D08E2E70 8EBB0FE8 359F4F28 8B8A432F 63902605

V is

7428740C 3EDBCCDF 4EFF942D 4BF00F63

output_block is

30C645C9 C33C3CA7 C827ACB0 825A11CF

temp is

E346B483 9677B724 7BE0AAB3 B1B969CA B13C2105 AE36F9F1
27ECBD37 E72AB845 30C645C9 C33C3CA7 C827ACB0 825A11CF

temp XOR provided_data is

41B1DEB9 95724BFA 5657509E 5C3480C6
8FBB5CE0 5443D746 08908193 609D7BB4 826C1969 276C5B79

Key is

41B1DEB9 95724BFA 5657509E 5C3480C6 8FBB5CE0 5443D746

V is

08908193 609D7BB4 826C1969 276C5B79

rnd_val is

6157D6C6 22896303
FE8E748C 18F2CE2E DF5C8A30 B8BBC26F D44C683D 7B150A97

Second call to Generate

CTR_DRBG_Generate

```
requested_number_of_bits = 256  
  
additional_input is  
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF  
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7
```

```
additional_input <> NULL, process appropriately
```

```
Block_Cipher_df
```

```
input_str is  
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF  
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7
```

```
number_of_bits_to_return = 320
```

```
S is
```

```
00000028 00000028 A0A1A2A3 A4A5A6A7  
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF  
C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000
```

```
BCC
```

```
IV is
```

```
00000000 00000000 00000000 00000000
```

```
IV || S is
```

```
00000000 00000000 00000028 00000028 A0A1A2A3 A4A5A6A7  
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF  
C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000
```

```
temp is
```

```
0DEF5001 1B1229C8 3DD880BE E398BDD8
```

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000

00000000 00000000 00000028 00000028 A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000

temp is

0DEF5001 1B1229C8

3DD880BE E398BDD8 61E3855F 743C9876 6CCEDC9B 90C1461E

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000

00000000 00000000 00000028 00000028 A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000

temp is

0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876

6CCEDC9B 90C1461E 92B6D6BA 30B91657 85E11146 2B2050F1

Key is

0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876

X is

6CCEDC9B 90C1461E 92B6D6BA 30B91657

BlockEncrypt

Key is

0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876

X is

6CCEDC9B 90C1461E 92B6D6BA 30B91657

X = BlockEncrypt(Key, X) is

1F2069F0 C00F3158 44CF0216 2913FC35

temp is

1F2069F0 C00F3158 44CF0216 2913FC35

BlockEncrypt

Key is

0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876

X is

1F2069F0 C00F3158 44CF0216 2913FC35

X = BlockEncrypt(Key, X) is

F485B9DC 9EFDA069 E47E7C8D 674FECE1

temp is

1F2069F0 C00F3158

44CF0216 2913FC35 F485B9DC 9EFDA069 E47E7C8D 674FECE1

BlockEncrypt

Key is
0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876

X is
F485B9DC 9EFDA069 E47E7C8D 674FECE1

X = BlockEncrypt(Key, X) is
3AB17BE9 025A1ACE F7E2A934 A3DDFD0B

temp is
1F2069F0 C00F3158 44CF0216 2913FC35 F485B9DC 9EFDA069
E47E7C8D 674FECE1 3AB17BE9 025A1ACE F7E2A934 A3DDFD0B

requested_bits is
1F2069F0 C00F3158 44CF0216 2913FC35
F485B9DC 9EFDA069 E47E7C8D 674FECE1 3AB17BE9 025A1ACE

Update

provided_data is
1F2069F0 C00F3158 44CF0216 2913FC35
F485B9DC 9EFDA069 E47E7C8D 674FECE1 3AB17BE9 025A1ACE

While loop

Key is
41B1DEB9 95724BFA 5657509E 5C3480C6 8FBB5CE0 5443D746

V is
08908193 609D7BB4 826C1969 276C5B7A

output_block is
D982D885 7401F676 F76F9E47 923C805D

temp is

D982D885 7401F676 F76F9E47 923C805D

While loop

Key is

41B1DEB9 95724BFA 5657509E 5C3480C6 8FBB5CE0 5443D746

V is

08908193 609D7BB4 826C1969 276C5B7B

output_block is

100F2574 62B6A6D6 0DEFE841 138AA5F7

temp is

D982D885 7401F676

F76F9E47 923C805D 100F2574 62B6A6D6 0DEFE841 138AA5F7

While loop

Key is

41B1DEB9 95724BFA 5657509E 5C3480C6 8FBB5CE0 5443D746

V is

08908193 609D7BB4 826C1969 276C5B7C

output_block is

D5D8AE6E 3D66D253 B4C1824D F6736A5C

temp is

D982D885 7401F676 F76F9E47 923C805D 100F2574 62B6A6D6

0DEFE841 138AA5F7 D5D8AE6E 3D66D253 B4C1824D F6736A5C

temp XOR provided_data is
C6A2B175 B40EC72E B3A09C51 BB2F7C68
E48A9CA8 FC4B06BF E99194CC 74C54916 EF69D587 3F3CC89D

Key is
C6A2B175 B40EC72E B3A09C51 BB2F7C68 E48A9CA8 FC4B06BF

V is
E99194CC 74C54916 EF69D587 3F3CC89D

Update

provided_data is
1F2069F0 C00F3158 44CF0216 2913FC35
F485B9DC 9EFDA069 E47E7C8D 674FECE1 3AB17BE9 025A1ACE

While loop

Key is
C6A2B175 B40EC72E B3A09C51 BB2F7C68 E48A9CA8 FC4B06BF

V is
E99194CC 74C54916 EF69D587 3F3CC8A0

output_block is
6426D45A 9387D0FD EA65286E 3B751CEF

temp is
6426D45A 9387D0FD EA65286E 3B751CEF

While loop

Key is

C6A2B175 B40EC72E B3A09C51 BB2F7C68 E48A9CA8 FC4B06BF

V is

E99194CC 74C54916 EF69D587 3F3CC8A1

output_block is

5CA13272 687E3828 0C24DBA3 36344980

temp is

6426D45A 9387D0FD

EA65286E 3B751CEF 5CA13272 687E3828 0C24DBA3 36344980

While loop

Key is

C6A2B175 B40EC72E B3A09C51 BB2F7C68 E48A9CA8 FC4B06BF

V is

E99194CC 74C54916 EF69D587 3F3CC8A2

output_block is

AE880B7B 64CD81C1 1920D6B3 8112D7DE

temp is

6426D45A 9387D0FD EA65286E 3B751CEF 5CA13272 687E3828

0C24DBA3 36344980 AE880B7B 64CD81C1 1920D6B3 8112D7DE

temp XOR provided_data is

7B06BDAA 5388E1A5 AEAA2A78 1266E0DA

A8248BAE F6839841 E85AA72E 517BA561 94397092 66979B0F

Key is

7B06BDAA 5388E1A5 AEAA2A78 1266E0DA A8248BAE F6839841

V is

E85AA72E 517BA561 94397092 66979B0F

rnd_val is

1F6DBD50 693817A1
9EF22622 3AB727E1 67158848 35CA0C5B 3B46D570 B4DD975A

#####

CTR_DRBG

Requested Security Strength = 192

prediction_resistance_flag = "NOT ENABLED"

EntropyInput =

00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627

EntropyInput1 (for Reseed1) =

80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7

EntropyInput2 (for Reseed2) =

C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDFF E0E1E2E3 E4E5E6E7

Nonce =

20212223 24252627 28292A2B

PersonalizationString =

40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667

AdditionalInput = <empty>

#####

CTR_DRBG_Instantiate_algorithm - with derivation function

entropy_input is

00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627

nonce is

20212223 24252627 28292A2B

personal_str is

40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667

prediction_resistance_flag = "No PredictionResistance"

Block_Cipher_df

input_str is

00010203 04050607 08090A0B 0C0D0E0F 10111213
14151617 18191A1B 1C1D1E1F 20212223 24252627 20212223
24252627 28292A2B 40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667

number_of_bits_to_return = 320

S is

0000005C 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 40414243
44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
5C5D5E5F 60616263 64656667 80000000 00000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000

00000000 00000000 0000005C 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 40414243
44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
5C5D5E5F 60616263 64656667 80000000 00000000 00000000

temp is

883662C0 53AC837C 186A91D7 0C5398FA

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000

00000000 00000000 0000005C 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 40414243
44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
5C5D5E5F 60616263 64656667 80000000 00000000 00000000

temp is

883662C0 53AC837C

186A91D7 0C5398FA 9028263E F8303EE6 F7658E84 1E8EDDB4

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000000	00000000	0000005C	00000028	00010203	04050607
08090A0B	0C0D0E0F	10111213	14151617	18191A1B	1C1D1E1F
20212223	24252627	20212223	24252627	28292A2B	40414243
44454647	48494A4B	4C4D4E4F	50515253	54555657	58595A5B
5C5D5E5F	60616263	64656667	80000000	00000000	00000000

temp is

883662C0	53AC837C	186A91D7	0C5398FA	9028263E	F8303EE6
F7658E84	1E8EDDB4	BA630844	25877431	5143AC1F	156049EB

Key is

883662C0	53AC837C	186A91D7	0C5398FA	9028263E	F8303EE6
----------	----------	----------	----------	----------	----------

X is

F7658E84	1E8EDDB4	BA630844	25877431
----------	----------	----------	----------

BlockEncrypt

Key is

883662C0	53AC837C	186A91D7	0C5398FA	9028263E	F8303EE6
----------	----------	----------	----------	----------	----------

X is

F7658E84	1E8EDDB4	BA630844	25877431
----------	----------	----------	----------

X = BlockEncrypt(Key, X) is

AC49318E	F0FA3331	F54CFB30	6C9B7B15
----------	----------	----------	----------

temp is

AC49318E	F0FA3331	F54CFB30	6C9B7B15
----------	----------	----------	----------

BlockEncrypt

Key is

883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6

X is

AC49318E F0FA3331 F54CFB30 6C9B7B15

X = BlockEncrypt(Key, X) is

9334B962 5E62F257 2431DA7D 0A5F7534

temp is

AC49318E F0FA3331
F54CFB30 6C9B7B15 9334B962 5E62F257 2431DA7D 0A5F7534

BlockEncrypt

Key is

883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6

X is

9334B962 5E62F257 2431DA7D 0A5F7534

X = BlockEncrypt(Key, X) is

B22E0E89 FF0FF392 A7CECDBE 5A4E766F

temp is

AC49318E F0FA3331 F54CFB30 6C9B7B15 9334B962 5E62F257
2431DA7D 0A5F7534 B22E0E89 FF0FF392 A7CECDBE 5A4E766F

requested_bits is

AC49318E F0FA3331 F54CFB30 6C9B7B15
9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392

seed_material is
AC49318E F0FA3331 F54CFB30 6C9B7B15
9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392

Update

provided_data is
AC49318E F0FA3331 F54CFB30 6C9B7B15
9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392

While loop

Key is
00000000 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000001

output_block is
CD33B28A C773F74B A00ED1F3 12572435

temp is
CD33B28A C773F74B A00ED1F3 12572435

While loop

Key is
00000000 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000002

output_block is
98E7247C 07F0FE41 1C267E43 84B0F600

temp is
CD33B28A C773F74B
A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600

While loop

Key is
00000000 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000003

output_block is
2A3493E6 6235EE67 DEECCD2F 3B393BD8

temp is
CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8

temp XOR provided_data is
617A8304 3789C47A 55422AC3 7ECC5F20
0BD39D1E 59920C16 3817A43E 8EEF8334 981A9D6F 9D3A1DF5

Key is
617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

V is
3817A43E 8EEF8334 981A9D6F 9D3A1DF5

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

While loop

Key is

617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

V is

3817A43E 8EEF8334 981A9D6F 9D3A1DF8

output_block is

6C0BA382 122A6E1E BEB51820 656D3D45

temp is

6C0BA382 122A6E1E BEB51820 656D3D45

While loop

Key is

617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

V is

3817A43E 8EEF8334 981A9D6F 9D3A1DF9

output_block is

B0B4DA3A EDAF317E 1A823DC4 D0A03B6C

temp is

6C0BA382 122A6E1E

BEB51820 656D3D45 B0B4DA3A EDAF317E 1A823DC4 D0A03B6C

While loop

Key is

617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

V is

3817A43E 8EEF8334 981A9D6F 9D3A1DFA

output_block is

2CE4F489 BB227382 A4FBC53E ACD12025

temp is

6C0BA382 122A6E1E BEB51820 656D3D45 B0B4DA3A EDAF317E

1A823DC4 D0A03B6C 2CE4F489 BB227382 A4FBC53E ACD12025

temp XOR provided_data is

6C0BA382 122A6E1E BEB51820 656D3D45

B0B4DA3A EDAF317E 1A823DC4 D0A03B6C 2CE4F489 BB227382

Key is

6C0BA382 122A6E1E BEB51820 656D3D45 B0B4DA3A EDAF317E

V is

1A823DC4 D0A03B6C 2CE4F489 BB227382

rnd_val is

E231244B 3235B085
C8160442 4357E852 01E3828B 5C455686 79A5555F 867AAC8C

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

While loop

Key is

6C0BA382 122A6E1E BEB51820 656D3D45 B0B4DA3A EDAF317E

V is

1A823DC4 D0A03B6C 2CE4F489 BB227385

output_block is

BC0C07EA E35CBFBF 88E428FC F551504C

temp is

BC0C07EA E35CBFBF 88E428FC F551504C

While loop

Key is

6C0BA382 122A6E1E BEB51820 656D3D45 B0B4DA3A EDAF317E

V is

1A823DC4 D0A03B6C 2CE4F489 BB227386

output_block is

9CC98126 B9758E67 FB830F34 233D1F68

temp is

BC0C07EA E35CBFBF

88E428FC F551504C 9CC98126 B9758E67 FB830F34 233D1F68

While loop

Key is

6C0BA382 122A6E1E BEB51820 656D3D45 B0B4DA3A EDAF317E

V is

1A823DC4 D0A03B6C 2CE4F489 BB227387

output_block is

46937CEF 28E4A716 11760A28 05C7ABA8

temp is

BC0C07EA E35CBFBF 88E428FC F551504C 9CC98126 B9758E67

FB830F34 233D1F68 46937CEF 28E4A716 11760A28 05C7ABA8

temp XOR provided_data is

BC0C07EA E35CBFBF 88E428FC F551504C

9CC98126 B9758E67 FB830F34 233D1F68 46937CEF 28E4A716

Key is
BC0C07EA E35CBFBF 88E428FC F551504C 9CC98126 B9758E67

V is
FB830F34 233D1F68 46937CEF 28E4A716

rnd_val is
DD0F7BC CADADA3
1A676522 59CE569A 271DD85C F66C3D6A 7E9FAED6 1F38D219

#####

CTR_DRBG

Requested Security Strength = 192

prediction_resistance_flag = "NOT ENABLED"
EntropyInput =
00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627

EntropyInput1 (for Reseed1) =
80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7

EntropyInput2 (for Reseed2) =
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7 E0E1E2E3 E4E5E6E7

Nonce =
20212223 24252627 28292A2B

PersonalizationString =
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667

```
AdditionalInput1 =
    60616263 64656667 68696A6B 6C6D6E6F
    70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687
```

```
AdditionalInput2 =
    A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
    B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7
```

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

```
*****
```

```
CTR_DRBG_Instantiate_algorithm - with derivation function
```

```
entropy_input is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
```

```
nonce is
```

```
20212223 24252627 28292A2B
```

```
personal_str is
```

```
    40414243 44454647 48494A4B 4C4D4E4F
    50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667
```

```
prediction_resistance_flag = "No PredictionResistance"
```

```
-----
```

```
Block_Cipher_df
```

```
input_str is
    00010203 04050607 08090A0B 0C0D0E0F 10111213
    14151617 18191A1B 1C1D1E1F 20212223 24252627 20212223
    24252627 28292A2B 40414243 44454647 48494A4B 4C4D4E4F
    50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667
```

```
number_of_bits_to_return = 320
```

```
S is
```

0000005C 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 40414243
44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
5C5D5E5F 60616263 64656667 80000000 00000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000

00000000 00000000 0000005C 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 40414243
44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
5C5D5E5F 60616263 64656667 80000000 00000000 00000000

temp is

883662C0 53AC837C 186A91D7 0C5398FA

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000

00000000 00000000 0000005C 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 40414243
44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
5C5D5E5F 60616263 64656667 80000000 00000000 00000000

temp is

883662C0 53AC837C
186A91D7 0C5398FA 9028263E F8303EE6 F7658E84 1E8EDDB4

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000

00000000 00000000 0000005C 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 40414243
44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
5C5D5E5F 60616263 64656667 80000000 00000000 00000000

temp is

883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6
F7658E84 1E8EDDB4 BA630844 25877431 5143AC1F 156049EB

Key is

883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6

X is

F7658E84 1E8EDDB4 BA630844 25877431

BlockEncrypt

Key is

883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6

X is

F7658E84 1E8EDDB4 BA630844 25877431

X = BlockEncrypt(Key, X) is
AC49318E F0FA3331 F54CFB30 6C9B7B15

temp is
AC49318E F0FA3331 F54CFB30 6C9B7B15

BlockEncrypt

Key is
883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6

X is
AC49318E F0FA3331 F54CFB30 6C9B7B15

X = BlockEncrypt(Key, X) is
9334B962 5E62F257 2431DA7D 0A5F7534

temp is
AC49318E F0FA3331
F54CFB30 6C9B7B15 9334B962 5E62F257 2431DA7D 0A5F7534

BlockEncrypt

Key is
883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6

X is
9334B962 5E62F257 2431DA7D 0A5F7534

X = BlockEncrypt(Key, X) is
B22E0E89 FF0FF392 A7CECDBE 5A4E766F

temp is
AC49318E F0FA3331 F54CFB30 6C9B7B15 9334B962 5E62F257
2431DA7D 0A5F7534 B22E0E89 FF0FF392 A7CECDBE 5A4E766F

requested_bits is
AC49318E F0FA3331 F54CFB30 6C9B7B15
9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392

seed_material is
AC49318E F0FA3331 F54CFB30 6C9B7B15
9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392

Update

provided_data is
AC49318E F0FA3331 F54CFB30 6C9B7B15
9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392

While loop

Key is
00000000 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000001

output_block is
CD33B28A C773F74B A00ED1F3 12572435

temp is
CD33B28A C773F74B A00ED1F3 12572435

While loop

Key is

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

98E7247C 07F0FE41 1C267E43 84B0F600

temp is

CD33B28A C773F74B

A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600

While loop

Key is

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000003

output_block is

2A3493E6 6235EE67 DEECCD2F 3B393BD8

temp is

CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41

1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8

temp XOR provided_data is

617A8304 3789C47A 55422AC3 7ECC5F20

0BD39D1E 59920C16 3817A43E 8EEF8334 981A9D6F 9D3A1DF5

Key is
617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

V is
3817A43E 8EEF8334 981A9D6F 9D3A1DF5

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is
60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687

additional_input <> NULL, process appropriately

Block_Cipher_df

input_str is
60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687

number_of_bits_to_return = 320

S is
00000028 00000028 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 80000000 00000000 00000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000

00000000 00000000 00000028 00000028 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 80000000 00000000 00000000 00000000

temp is

E5460ACC 5126F932 D56D1A29 1FC4A2A2

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000

00000000 00000000 00000028 00000028 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 80000000 00000000 00000000 00000000

temp is

E5460ACC 5126F932

D56D1A29 1FC4A2A2 280D9844 33D9A0F7 BE003DAF 2996B5CF

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000

00000000 00000000 00000028 00000028 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F

80818283 84858687 80000000 00000000 00000000 00000000

temp is

E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7
BE003DAF 2996B5CF 5AD5C453 7046B98F C143E7B2 F9A465C4

Key is

E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7

X is

BE003DAF 2996B5CF 5AD5C453 7046B98F

BlockEncrypt

Key is

E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7

X is

BE003DAF 2996B5CF 5AD5C453 7046B98F

X = BlockEncrypt(Key, X) is

A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C

temp is

A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C

BlockEncrypt

Key is

E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7

X is

A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C

X = BlockEncrypt(Key, X) is

3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1

temp is

A2F76A3A 0305FCDE

2DB7FA2D ED8DE90C 3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1

BlockEncrypt

Key is

E5460ACC 5126F932 D56D1A29 1FC4A2A2 280D9844 33D9A0F7

X is

3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1

X = BlockEncrypt(Key, X) is

B2AA5CA0 E45067DE 84D9D2FA FDA512C9

temp is

A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C 3E877DE5 FA752EB7
2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE 84D9D2FA FDA512C9

requested_bits is

A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C

3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE

Update

provided_data is

A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C

3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE

While loop

Key is

617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

V is

3817A43E 8EEF8334 981A9D6F 9D3A1DF6

output_block is

E231244B 3235B085 C8160442 4357E852

temp is

E231244B 3235B085 C8160442 4357E852

While loop

Key is

617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

V is

3817A43E 8EEF8334 981A9D6F 9D3A1DF7

output_block is

01E3828B 5C455686 79A5555F 867AAC8C

temp is

E231244B 3235B085

C8160442 4357E852 01E3828B 5C455686 79A5555F 867AAC8C

While loop

Key is
617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

V is
3817A43E 8EEF8334 981A9D6F 9D3A1DF8

output_block is
6C0BA382 122A6E1E BEB51820 656D3D45

temp is
E231244B 3235B085 C8160442 4357E852 01E3828B 5C455686
79A5555F 867AAC8C 6C0BA382 122A6E1E BEB51820 656D3D45

temp XOR provided_data is
40C64E71 31304C5B E5A1FE6F AEDA015E
3F64FF6E A6307831 56D969FB 01CD6F7D DEA1FF22 F67A09C0

Key is
40C64E71 31304C5B E5A1FE6F AEDA015E 3F64FF6E A6307831

V is
56D969FB 01CD6F7D DEA1FF22 F67A09C0

Update

provided_data is
A2F76A3A 0305FCDE 2DB7FA2D ED8DE90C
3E877DE5 FA752EB7 2F7C3CA4 87B7C3F1 B2AA5CA0 E45067DE

While loop

Key is
40C64E71 31304C5B E5A1FE6F AEDA015E 3F64FF6E A6307831

V is

56D969FB 01CD6F7D DEA1FF22 F67A09C3

output_block is

DEBD9695 37A6430F 0DB95ED7 3201DBE2

temp is

DEBD9695 37A6430F 0DB95ED7 3201DBE2

While loop

Key is

40C64E71 31304C5B E5A1FE6F AEDA015E 3F64FF6E A6307831

V is

56D969FB 01CD6F7D DEA1FF22 F67A09C4

output_block is

EFBE2871 482A39AB 25F35788 F9A81DA9

temp is

DEBD9695 37A6430F

0DB95ED7 3201DBE2 EFBE2871 482A39AB 25F35788 F9A81DA9

While loop

Key is

40C64E71 31304C5B E5A1FE6F AEDA015E 3F64FF6E A6307831

V is

56D969FB 01CD6F7D DEA1FF22 F67A09C5

output_block is

C720524A D46F4281 57BEFC8B 39800846

temp is

DEBD9695 37A6430F 0DB95ED7 3201DBE2 EFBE2871 482A39AB
25F35788 F9A81DA9 C720524A D46F4281 57BEFC8B 39800846

temp XOR provided_data is

7C4AFCAF 34A3BFD1 200EA4FA DF8C32EE
D1395594 B25F171C 0A8F6B2C 7E1FDE58 758A0EEA 303F255F

Key is

7C4AFCAF 34A3BFD1 200EA4FA DF8C32EE D1395594 B25F171C

V is

0A8F6B2C 7E1FDE58 758A0EEA 303F255F

rnd_val is

242D0B6B 9598779C
5CF5A50E DFD61C2C 95D383BC 493AC202 845FAC96 D276C092

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is

A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7

additional_input <> NULL, process appropriately

Block_Cipher_df
input_str is
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7

number_of_bits_to_return = 320

S is
00000028 00000028 A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000

BCC

IV is
00000000 00000000 00000000 00000000

IV || S is
00000000 00000000
00000000 00000000 00000028 00000028 A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000

temp is
0DEF5001 1B1229C8 3DD880BE E398BDD8

BCC

IV is
00000001 00000000 00000000 00000000

IV || S is
00000001 00000000
00000000 00000000 00000028 00000028 A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000

temp is

0DEF5001 1B1229C8

3DD880BE E398BDD8 61E3855F 743C9876 6CCEDC9B 90C1461E

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000

00000000 00000000 00000028 00000028 A0A1A2A3 A4A5A6A7

A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

C0C1C2C3 C4C5C6C7 80000000 00000000 00000000 00000000

temp is

0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876

6CCEDC9B 90C1461E 92B6D6BA 30B91657 85E11146 2B2050F1

Key is

0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876

X is

6CCEDC9B 90C1461E 92B6D6BA 30B91657

BlockEncrypt

Key is

0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876

X is

6CCEDC9B 90C1461E 92B6D6BA 30B91657

X = BlockEncrypt(Key, X) is

1F2069F0 C00F3158 44CF0216 2913FC35

temp is

1F2069F0 C00F3158 44CF0216 2913FC35

BlockEncrypt

Key is

0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876

X is

1F2069F0 C00F3158 44CF0216 2913FC35

X = BlockEncrypt(Key, X) is

F485B9DC 9EFDA069 E47E7C8D 674FECE1

temp is

1F2069F0 C00F3158

44CF0216 2913FC35 F485B9DC 9EFDA069 E47E7C8D 674FECE1

BlockEncrypt

Key is

0DEF5001 1B1229C8 3DD880BE E398BDD8 61E3855F 743C9876

X is

F485B9DC 9EFDA069 E47E7C8D 674FECE1

X = BlockEncrypt(Key, X) is

3AB17BE9 025A1ACE F7E2A934 A3DDFD0B

temp is

1F2069F0 C00F3158 44CF0216 2913FC35 F485B9DC 9EFDA069
E47E7C8D 674FECE1 3AB17BE9 025A1ACE F7E2A934 A3DDFD0B

requested_bits is

1F2069F0 C00F3158 44CF0216 2913FC35
F485B9DC 9EFDA069 E47E7C8D 674FECE1 3AB17BE9 025A1ACE

Update

provided_data is

1F2069F0 C00F3158 44CF0216 2913FC35
F485B9DC 9EFDA069 E47E7C8D 674FECE1 3AB17BE9 025A1ACE

While loop

Key is

7C4AFCAF 34A3BFD1 200EA4FA DF8C32EE D1395594 B25F171C

V is

0A8F6B2C 7E1FDE58 758A0EEA 303F2560

output_block is

8494CE15 4602C729 EC414D3A 6A177D89

temp is

8494CE15 4602C729 EC414D3A 6A177D89

While loop

Key is
7C4AFCAF 34A3BFD1 200EA4FA DF8C32EE D1395594 B25F171C

V is
0A8F6B2C 7E1FDE58 758A0EEA 303F2561

output_block is
0CDD1884 9A3CE775 6D0AE053 FF341BEB

temp is
8494CE15 4602C729
EC414D3A 6A177D89 0CDD1884 9A3CE775 6D0AE053 FF341BEB

While loop

Key is
7C4AFCAF 34A3BFD1 200EA4FA DF8C32EE D1395594 B25F171C

V is
0A8F6B2C 7E1FDE58 758A0EEA 303F2562

output_block is
8DFBC57C 8F8C72CA 81E88545 88E0EE64

temp is
8494CE15 4602C729 EC414D3A 6A177D89 0CDD1884 9A3CE775
6D0AE053 FF341BEB 8DFBC57C 8F8C72CA 81E88545 88E0EE64

temp XOR provided_data is
9BB4A7E5 860DF671 A88E4F2C 430481BC
F858A158 04C1471C 89749CDE 987BF70A B74ABE95 8DD66804

Key is
9BB4A7E5 860DF671 A88E4F2C 430481BC F858A158 04C1471C

V is

89749CDE 987BF70A B74ABE95 8DD66804

Update

provided_data is

1F2069F0 C00F3158 44CF0216 2913FC35
F485B9DC 9EFDA069 E47E7C8D 674FECE1 3AB17BE9 025A1ACE

While loop

Key is

9BB4A7E5 860DF671 A88E4F2C 430481BC F858A158 04C1471C

V is

89749CDE 987BF70A B74ABE95 8DD66807

output_block is

D05FC7BA 4F2B0E54 F0C3387A 1D51F568

temp is

D05FC7BA 4F2B0E54 F0C3387A 1D51F568

While loop

Key is

9BB4A7E5 860DF671 A88E4F2C 430481BC F858A158 04C1471C

V is

89749CDE 987BF70A B74ABE95 8DD66808

output_block is
CB8871EC 046141F1 135D52C7 27DBB8F3

temp is
D05FC7BA 4F2B0E54
F0C3387A 1D51F568 CB8871EC 046141F1 135D52C7 27DBB8F3

While loop

Key is
9BB4A7E5 860DF671 A88E4F2C 430481BC F858A158 04C1471C

V is
89749CDE 987BF70A B74ABE95 8DD66809

output_block is
6344C16B 719DEC7B 32A06AF0 44E269C7

temp is
D05FC7BA 4F2B0E54 F0C3387A 1D51F568 CB8871EC 046141F1
135D52C7 27DBB8F3 6344C16B 719DEC7B 32A06AF0 44E269C7

temp XOR provided_data is
CF7FAE4A 8F243F0C B40C3A6C 3442095D
3F0DC830 9A9CE198 F7232E4A 40945412 59F5BA82 73C7F6B5

Key is
CF7FAE4A 8F243F0C B40C3A6C 3442095D 3F0DC830 9A9CE198

V is
F7232E4A 40945412 59F5BA82 73C7F6B5

rnd_val is
D2892F04 52967041
4F098DA2 6684CB1E 9460F3A6 ED58BFC8 383A300B DAF284AD

```
#####
```

CTR_DRBG

Requested Security Strength = 192

```
prediction_resistance_flag = "ENABLED"  
EntropyInput =  
    00010203 04050607 08090A0B 0C0D0E0F  
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
```

```
EntropyInput1 (for Reseed1) =  
    80818283 84858687 88898A8B 8C8D8E8F  
    90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
```

```
EntropyInput2 (for Reseed2) =  
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF  
    D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7
```

```
Nonce =  
    20212223 24252627 28292A2B
```

PersonalizationString = <empty>

AdditionalInput = <empty>

```
#####
```

```
*****
```

CTR_DRBG_Instantiate_algorithm - with derivation function

```
entropy_input is  
    00010203 04050607 08090A0B 0C0D0E0F  
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
```

```
nonce is  
    20212223 24252627 28292A2B
```

```
personal_str is <empty>  
prediction_resistance_flag = "PredictionResistance"
```

Block_Cipher_df

```
input_str is  
00010203  
04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B  
1C1D1E1F 20212223 24252627 20212223 24252627 28292A2B
```

```
number_of_bits_to_return = 320
```

```
S is  
00000034 00000028 00010203 04050607  
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F  
20212223 24252627 20212223 24252627 28292A2B 80000000
```

BCC

```
IV is  
00000000 00000000 00000000 00000000
```

```
IV || S is  
00000000 00000000  
00000000 00000000 00000034 00000028 00010203 04050607  
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F  
20212223 24252627 20212223 24252627 28292A2B 80000000
```

```
temp is  
2D64B3D8 692984AD B6FBBA41 F69E74E1
```

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000

00000000 00000000 00000034 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 80000000

temp is

2D64B3D8 692984AD

B6FBBA41 F69E74E1 72DAEE1D 75EFF1E 66616F2E 9F91BC31

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000

00000000 00000000 00000034 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 80000000

temp is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

66616F2E 9F91BC31 C6ADE98F EB96A83C A6F71BF5 BCE6944D

Key is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

X is

66616F2E 9F91BC31 C6ADE98F EB96A83C

BlockEncrypt

Key is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

X is

66616F2E 9F91BC31 C6ADE98F EB96A83C

X = BlockEncrypt(Key, X) is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB

temp is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB

BlockEncrypt

Key is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

X is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB

X = BlockEncrypt(Key, X) is

7150F160 187803C2 0380FB02 636C8E59

temp is

45EBC7A3 4CB5BFDB

A58CBFCC A756DDCB 7150F160 187803C2 0380FB02 636C8E59

BlockEncrypt

Key is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFFF1E

X is

7150F160 187803C2 0380FB02 636C8E59

X = BlockEncrypt(Key, X) is

B1A94E9C C2360559 9C002E3A 221F5C21

temp is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB 7150F160 187803C2
0380FB02 636C8E59 B1A94E9C C2360559 9C002E3A 221F5C21

requested_bits is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559

seed_material is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559

Update

provided_data is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559

While loop

Key is

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is
CD33B28A C773F74B A00ED1F3 12572435

temp is
CD33B28A C773F74B A00ED1F3 12572435

While loop

Key is
00000000 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000002

output_block is
98E7247C 07F0FE41 1C267E43 84B0F600

temp is
CD33B28A C773F74B
A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600

While loop

Key is
00000000 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000003

output_block is
2A3493E6 6235EE67 DEECCD2F 3B393BD8

```
temp is
CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8
```

```
temp XOR provided_data is
88D87529 8BC64890 05826E3F B501F9FE
E9B7D51C 1F88FD83 1FA68541 E7DC7859 9B9DDD7A A003EB3E
```

```
Key is
88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83
```

```
V is
1FA68541 E7DC7859 9B9DDD7A A003EB3E
```

First call to Generate

```
*****
```

CTR_DRBG_Generate

```
requested_number_of_bits = 256
```

```
additional_input is <empty>
```

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

```
*****
```

CTR_DRBG_Reseed

```
entropy_input is
```

```
80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
```

```
additional_input is <empty>
```

Block_Cipher_df

input_str is
80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7

number_of_bits_to_return = 320

S is
00000028 00000028 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 80000000 00000000 00000000 00000000

BCC

IV is
00000000 00000000 00000000 00000000

IV || S is
00000000 00000000
00000000 00000000 00000028 00000028 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 80000000 00000000 00000000 00000000

temp is
D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD

BCC

IV is
00000001 00000000 00000000 00000000

IV || S is
00000001 00000000
00000000 00000000 00000028 00000028 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 80000000 00000000 00000000 00000000

temp is

D4DC3DD9 64EB0CA9
AFB81ED4 D728EACD D598A470 CD085CAD 313F0704 00084980

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000
00000000 00000000 00000028 00000028 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 80000000 00000000 00000000 00000000

temp is

D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD
313F0704 00084980 E8128432 2968C4EB 2EA63668 13E2E7E3

Key is

D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD

X is

313F0704 00084980 E8128432 2968C4EB

BlockEncrypt

Key is

D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD

X is

313F0704 00084980 E8128432 2968C4EB

X = BlockEncrypt(Key, X) is
ECE25874 66228E78 6B45F5AA E1E7407B

temp is
ECE25874 66228E78 6B45F5AA E1E7407B

BlockEncrypt

Key is
D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD

X is
ECE25874 66228E78 6B45F5AA E1E7407B

X = BlockEncrypt(Key, X) is
C500EB8B 6D8EAD20 9217569B C032FAF6

temp is
ECE25874 66228E78
6B45F5AA E1E7407B C500EB8B 6D8EAD20 9217569B C032FAF6

BlockEncrypt

Key is
D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD

X is
C500EB8B 6D8EAD20 9217569B C032FAF6

X = BlockEncrypt(Key, X) is
8DCC82DB 4927187D 79D87935 70CCFCBC

temp is
ECE25874 66228E78 6B45F5AA E1E7407B C500EB8B 6D8EAD20
9217569B C032FAF6 8DCC82DB 4927187D 79D87935 70CCFCBC

requested_bits is
ECE25874 66228E78 6B45F5AA E1E7407B
C500EB8B 6D8EAD20 9217569B C032FAF6 8DCC82DB 4927187D

Update

provided_data is
ECE25874 66228E78 6B45F5AA E1E7407B
C500EB8B 6D8EAD20 9217569B C032FAF6 8DCC82DB 4927187D

While loop

Key is
88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83

V is
1FA68541 E7DC7859 9B9DDD7A A003EB3F

output_block is
1A646BB1 D38BD2AE A30CF5C5 D812A624

temp is
1A646BB1 D38BD2AE A30CF5C5 D812A624

While loop

Key is
88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83

V is

1FA68541 E7DC7859 9B9DDD7A A003EB40

output_block is

B50D3ECA 99E508B2 5B5448A8 B96C0F2E

temp is

1A646BB1 D38BD2AE

A30CF5C5 D812A624 B50D3ECA 99E508B2 5B5448A8 B96C0F2E

While loop

Key is

88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83

V is

1FA68541 E7DC7859 9B9DDD7A A003EB41

output_block is

FC55C88D AFA06880 F2C73C08 1E8FA294

temp is

1A646BB1 D38BD2AE A30CF5C5 D812A624 B50D3ECA 99E508B2

5B5448A8 B96C0F2E FC55C88D AFA06880 F2C73C08 1E8FA294

temp XOR provided_data is

F68633C5 B5A95CD6 C849006F 39F5E65F

700DD541 F46BA592 C9431E33 795EF5D8 71994A56 E68770FD

Key is

F68633C5 B5A95CD6 C849006F 39F5E65F 700DD541 F46BA592

V is

C9431E33 795EF5D8 71994A56 E68770FD

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

While loop

Key is

F68633C5 B5A95CD6 C849006F 39F5E65F 700DD541 F46BA592

V is

C9431E33 795EF5D8 71994A56 E6877100

output_block is

C122A362 565F8A65 E4F497AF 6EBEB1F1

temp is

C122A362 565F8A65 E4F497AF 6EBEB1F1

While loop

Key is

F68633C5 B5A95CD6 C849006F 39F5E65F 700DD541 F46BA592

V is

C9431E33 795EF5D8 71994A56 E6877101

output_block is

001B843D 50205A56 8F09BEAE A5FF5ECD

temp is

C122A362 565F8A65

E4F497AF 6EBEB1F1 001B843D 50205A56 8F09BEAE A5FF5ECD

While loop

Key is

F68633C5 B5A95CD6 C849006F 39F5E65F 700DD541 F46BA592

V is

C9431E33 795EF5D8 71994A56 E6877102

output_block is

0D3723AF 116550F7 B0D762A6 354F8AC7

temp is

C122A362 565F8A65 E4F497AF 6EBEB1F1 001B843D 50205A56

8F09BEAE A5FF5ECD 0D3723AF 116550F7 B0D762A6 354F8AC7

temp XOR provided_data is

C122A362 565F8A65 E4F497AF 6EBEB1F1

001B843D 50205A56 8F09BEAE A5FF5ECD 0D3723AF 116550F7

Key is

C122A362 565F8A65 E4F497AF 6EBEB1F1 001B843D 50205A56

V is

8F09BEAE A5FF5ECD 0D3723AF 116550F7

rnd_val is

D1C68E36 9E5AE5CF

B6564317 13DC972E 54B87DA6 326D0D49 D1C11653 70049FDB

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

entropy_input is

C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7 E0E1E2E3 E4E5E6E7

additional_input is <empty>

Block_Cipher_df

input_str is

C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7 E0E1E2E3 E4E5E6E7

number_of_bits_to_return = 320

S is

00000028 00000028 C0C1C2C3 C4C5C6C7

C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7

E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000028 00000028 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000

temp is

98316F8D C09A27EA 960FDB96 D22C96D3

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000000 00000000 00000028 00000028 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000

temp is

98316F8D C09A27EA
960FDB96 D22C96D3 C95E08EF DAB3E081 BDA51061 F9619651

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000
00000000 00000000 00000028 00000028 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000

temp is

98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081
BDA51061 F9619651 191D1E83 B09E52F5 1D6A9C00 B4889F28

Key is

98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081

X is

BDA51061 F9619651 191D1E83 B09E52F5

BlockEncrypt

Key is

98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081

X is

BDA51061 F9619651 191D1E83 B09E52F5

X = BlockEncrypt(Key, X) is

60C2CB2F DB52737D 19692CF5 E74AC177

temp is

60C2CB2F DB52737D 19692CF5 E74AC177

BlockEncrypt

Key is

98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081

X is

60C2CB2F DB52737D 19692CF5 E74AC177

X = BlockEncrypt(Key, X) is

F94540C2 F7FCE903 859505EA BF87DB61

temp is

60C2CB2F DB52737D

19692CF5 E74AC177 F94540C2 F7FCE903 859505EA BF87DB61

BlockEncrypt

Key is

98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081

X is

F94540C2 F7FCE903 859505EA BF87DB61

X = BlockEncrypt(Key, X) is

9FA75BC1 074138FE 9811C2BC F2A688DF

temp is

60C2CB2F DB52737D 19692CF5 E74AC177 F94540C2 F7FCE903

859505EA BF87DB61 9FA75BC1 074138FE 9811C2BC F2A688DF

requested_bits is

60C2CB2F DB52737D 19692CF5 E74AC177

F94540C2 F7FCE903 859505EA BF87DB61 9FA75BC1 074138FE

Update

provided_data is

60C2CB2F DB52737D 19692CF5 E74AC177
F94540C2 F7FCE903 859505EA BF87DB61 9FA75BC1 074138FE

While loop

Key is

C122A362 565F8A65 E4F497AF 6EBEB1F1 001B843D 50205A56

V is

8F09BEAE A5FF5ECD 0D3723AF 116550F8

output_block is

F9D4CFFA 99A2A750 F2EDAD7E 802EEFCE

temp is

F9D4CFFA 99A2A750 F2EDAD7E 802EEFCE

While loop

Key is

C122A362 565F8A65 E4F497AF 6EBEB1F1 001B843D 50205A56

V is

8F09BEAE A5FF5ECD 0D3723AF 116550F9

output_block is

392BBCB4 09BB6C04 74E28DA4 473F2CAF

temp is

F9D4CFFA 99A2A750

F2EDAD7E 802EEFCE 392BBCB4 09BB6C04 74E28DA4 473F2CAF

While loop

Key is

C122A362 565F8A65 E4F497AF 6EBEB1F1 001B843D 50205A56

V is

8F09BEAE A5FF5ECD 0D3723AF 116550FA

output_block is

D2175CBF 4AA9238E B659F6F3 467B046A

temp is

F9D4CFFA 99A2A750 F2EDAD7E 802EEFCE 392BBCB4 09BB6C04

74E28DA4 473F2CAF D2175CBF 4AA9238E B659F6F3 467B046A

temp XOR provided_data is

991604D5 42F0D42D EB84818B 67642EB9

C06EFC76 FE478507 F177884E F8B8F7CE 4DB0077E 4DE81B70

Key is

991604D5 42F0D42D EB84818B 67642EB9 C06EFC76 FE478507

V is

F177884E F8B8F7CE 4DB0077E 4DE81B70

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

While loop

Key is

991604D5 42F0D42D EB84818B 67642EB9 C06EFC76 FE478507

V is

F177884E F8B8F7CE 4DB0077E 4DE81B73

output_block is

621A3370 C857E028 253B3C45 D1E67351

temp is

621A3370 C857E028 253B3C45 D1E67351

While loop

Key is

991604D5 42F0D42D EB84818B 67642EB9 C06EFC76 FE478507

V is

F177884E F8B8F7CE 4DB0077E 4DE81B74

output_block is

FA2EC31E DC76F7FF 6BA1806A F804F591

temp is

621A3370 C857E028

253B3C45 D1E67351 FA2EC31E DC76F7FF 6BA1806A F804F591

While loop

Key is

991604D5 42F0D42D EB84818B 67642EB9 C06EFC76 FE478507

V is

F177884E F8B8F7CE 4DB0077E 4DE81B75

output_block is

AFC28095 D1B1505A 119E138B 76A9400A

temp is

621A3370 C857E028 253B3C45 D1E67351 FA2EC31E DC76F7FF

6BA1806A F804F591 AFC28095 D1B1505A 119E138B 76A9400A

temp XOR provided_data is

621A3370 C857E028 253B3C45 D1E67351

FA2EC31E DC76F7FF 6BA1806A F804F591 AFC28095 D1B1505A

Key is

621A3370 C857E028 253B3C45 D1E67351 FA2EC31E DC76F7FF

V is

6BA1806A F804F591 AFC28095 D1B1505A

rnd_val is

615A2637 1F46583E

A33ED757 09D0EE55 5C62EC04 433648A7 C62FD43D 2764D52F

#####

CTR_DRBG

Requested Security Strength = 192

prediction_resistance_flag = "ENABLED"

EntropyInput =

00010203 04050607 08090A0B 0C0D0E0F

10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627

EntropyInput1 (for Reseed1) =

80818283 84858687 88898A8B 8C8D8E8F

90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7

EntropyInput2 (for Reseed2) =

C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7 E0E1E2E3 E4E5E6E7

Nonce =

20212223 24252627 28292A2B

PersonalizationString = <empty>

AdditionalInput1 =

60616263 64656667 68696A6B 6C6D6E6F

70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687

AdditionalInput2 =

A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF

B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7

#####

CTR_DRBG_Instantiate_algorithm - with derivation function

entropy_input is

00010203 04050607 08090A0B 0C0D0E0F

10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627

nonce is

20212223 24252627 28292A2B

personal_str is <empty>

prediction_resistance_flag = "PredictionResistance"

Block_Cipher_df

input_str is

00010203

04050607 08090A0B 0C0D0E0F 10111213 14151617 18191A1B
1C1D1E1F 20212223 24252627 20212223 24252627 28292A2B

number_of_bits_to_return = 320

S is

00000034 00000028 00010203 04050607

08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 80000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000

00000000 00000000 00000034 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 80000000

temp is

2D64B3D8 692984AD B6FBBA41 F69E74E1

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000

00000000 00000000 00000034 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 80000000

temp is

2D64B3D8 692984AD

B6FBBA41 F69E74E1 72DAEE1D 75EFF1E 66616F2E 9F91BC31

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000

00000000 00000000 00000034 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 80000000

temp is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E
66616F2E 9F91BC31 C6ADE98F EB96A83C A6F71BF5 BCE6944D

Key is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

X is
66616F2E 9F91BC31 C6ADE98F EB96A83C

BlockEncrypt

Key is
2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

X is
66616F2E 9F91BC31 C6ADE98F EB96A83C

X = BlockEncrypt(Key, X) is
45EBC7A3 4CB5BFDB A58CBFCC A756DDCB

temp is
45EBC7A3 4CB5BFDB A58CBFCC A756DDCB

BlockEncrypt

Key is
2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

X is
45EBC7A3 4CB5BFDB A58CBFCC A756DDCB

X = BlockEncrypt(Key, X) is
7150F160 187803C2 0380FB02 636C8E59

temp is
45EBC7A3 4CB5BFDB
A58CBFCC A756DDCB 7150F160 187803C2 0380FB02 636C8E59

BlockEncrypt

Key is

2D64B3D8 692984AD B6FBBA41 F69E74E1 72DAEE1D 75EFF1E

X is

7150F160 187803C2 0380FB02 636C8E59

X = BlockEncrypt(Key, X) is

B1A94E9C C2360559 9C002E3A 221F5C21

temp is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB 7150F160 187803C2
0380FB02 636C8E59 B1A94E9C C2360559 9C002E3A 221F5C21

requested_bits is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559

seed_material is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559

Update

provided_data is

45EBC7A3 4CB5BFDB A58CBFCC A756DDCB
7150F160 187803C2 0380FB02 636C8E59 B1A94E9C C2360559

While loop

Key is

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is

CD33B28A C773F74B A00ED1F3 12572435

temp is

CD33B28A C773F74B A00ED1F3 12572435

While loop

Key is

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

98E7247C 07F0FE41 1C267E43 84B0F600

temp is

CD33B28A C773F74B

A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600

While loop

Key is

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000003

```
output_block is  
2A3493E6 6235EE67 DEECCD2F 3B393BD8
```

```
temp is  
CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41  
1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8
```

```
temp XOR provided_data is  
88D87529 8BC64890 05826E3F B501F9FE  
E9B7D51C 1F88FD83 1FA68541 E7DC7859 9B9DDD7A A003EB3E
```

```
Key is  
88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83
```

```
V is  
1FA68541 E7DC7859 9B9DDD7A A003EB3E
```

```
First call to Generate
```

```
*****
```

```
CTR_DRBG_Generate
```

```
requested_number_of_bits = 256
```

```
additional_input is  
60616263 64656667 68696A6B 6C6D6E6F  
70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687
```

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

```
*****
```

```
CTR_DRBG_Reseed
```

```
entropy_input is  
80818283 84858687 88898A8B 8C8D8E8F  
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
```

additional_input is
60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687

Block_Cipher_df

input_str is
80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687

number_of_bits_to_return = 320

S is
00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000

BCC

IV is
00000000 00000000 00000000 00000000

IV || S is
00000000 00000000 00000000 00000000
00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000

temp is
FA46944A 0BDDB5EF A60EFAFE B9574E97

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000
00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000

temp is

FA46944A 0BDBB5EF
A60EFAFE B9574E97 A1E88E07 AFFCD4EC E8EB2D2C ED3E4283

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000 00000000 00000000
00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000

temp is

FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC
E8EB2D2C ED3E4283 8D8520E1 65EB3BDE BFAABC51 C44420CE

Key is

FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC

X is
E8EB2D2C ED3E4283 8D8520E1 65EB3BDE

BlockEncrypt

Key is
FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC

X is
E8EB2D2C ED3E4283 8D8520E1 65EB3BDE

X = BlockEncrypt(Key, X) is
D6D201B9 33F0FA92 A953C84C B739185C

temp is
D6D201B9 33F0FA92 A953C84C B739185C

BlockEncrypt

Key is
FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC

X is
D6D201B9 33F0FA92 A953C84C B739185C

X = BlockEncrypt(Key, X) is
5F353217 EFC411AD 5CD15D92 B481BEEF

temp is
D6D201B9 33F0FA92
A953C84C B739185C 5F353217 EFC411AD 5CD15D92 B481BEEF

BlockEncrypt

Key is

FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC

X is

5F353217 EFC411AD 5CD15D92 B481BEEF

X = BlockEncrypt(Key, X) is

7BDD58F3 8FD4827B 7A57A0F1 55ED8D8E

temp is

D6D201B9 33F0FA92 A953C84C B739185C 5F353217 EFC411AD
5CD15D92 B481BEEF 7BDD58F3 8FD4827B 7A57A0F1 55ED8D8E

requested_bits is

D6D201B9 33F0FA92 A953C84C B739185C
5F353217 EFC411AD 5CD15D92 B481BEEF 7BDD58F3 8FD4827B

Update

provided_data is

D6D201B9 33F0FA92 A953C84C B739185C
5F353217 EFC411AD 5CD15D92 B481BEEF 7BDD58F3 8FD4827B

While loop

Key is

88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83

V is

1FA68541 E7DC7859 9B9DDD7A A003EB3F

output_block is

1A646BB1 D38BD2AE A30CF5C5 D812A624

temp is

1A646BB1 D38BD2AE A30CF5C5 D812A624

While loop

Key is

88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83

V is

1FA68541 E7DC7859 9B9DDD7A A003EB40

output_block is

B50D3ECA 99E508B2 5B5448A8 B96C0F2E

temp is

1A646BB1 D38BD2AE

A30CF5C5 D812A624 B50D3ECA 99E508B2 5B5448A8 B96C0F2E

While loop

Key is

88D87529 8BC64890 05826E3F B501F9FE E9B7D51C 1F88FD83

V is

1FA68541 E7DC7859 9B9DDD7A A003EB41

output_block is

FC55C88D AFA06880 F2C73C08 1E8FA294

temp is
1A646BB1 D38BD2AE A30CF5C5 D812A624 B50D3ECA 99E508B2
5B5448A8 B96C0F2E FC55C88D AFA06880 F2C73C08 1E8FA294

temp XOR provided_data is
CCB66A08 E07B283C 0A5F3D89 6F2BBE78
EA380CDD 7621191F 0785153A 0DEDDB1C1 8788907E 2074EAFB

Key is
CCB66A08 E07B283C 0A5F3D89 6F2BBE78 EA380CDD 7621191F

V is
0785153A 0DEDDB1C1 8788907E 2074EAFB

CTR_DRBG_Generate

requested_number_of_bits = 256
additional_input is <empty>

Update

provided_data is
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

While loop

Key is
CCB66A08 E07B283C 0A5F3D89 6F2BBE78 EA380CDD 7621191F

V is

0785153A 0DEDDB1C1 8788907E 2074EAFE

output_block is
30DDEC5F 10795E1A 725319A0 DBF33FE5

temp is
30DDEC5F 10795E1A 725319A0 DBF33FE5

While loop

Key is
CCB66A08 E07B283C 0A5F3D89 6F2BBE78 EA380CDD 7621191F

V is
0785153A 0DEDDB1C1 8788907E 2074EAFF

output_block is
88C0ADCB 131B96B1 66AB4857 3E84F77C

temp is
30DDEC5F 10795E1A
725319A0 DBF33FE5 88C0ADCB 131B96B1 66AB4857 3E84F77C

While loop

Key is
CCB66A08 E07B283C 0A5F3D89 6F2BBE78 EA380CDD 7621191F

V is
0785153A 0DEDDB1C1 8788907E 2074EB00

output_block is
34709B9D 03C5D50D 60F4BE8A C3A926E8

```
temp is
30DDEC5F 10795E1A 725319A0 DBF33FE5 88C0ADCB 131B96B1
66AB4857 3E84F77C 34709B9D 03C5D50D 60F4BE8A C3A926E8
```

```
temp XOR provided_data is
30DDEC5F 10795E1A 725319A0 DBF33FE5
88C0ADCB 131B96B1 66AB4857 3E84F77C 34709B9D 03C5D50D
```

```
Key is
30DDEC5F 10795E1A 725319A0 DBF33FE5 88C0ADCB 131B96B1
```

```
V is
66AB4857 3E84F77C 34709B9D 03C5D50D
```

```
rnd_val is
85C9EBEB 01415602
991037DC B4E75C58 FF1638B6 98519565 25BA9FD2 BAB2F5DC
```

```
Second call to Generate
```

```
*****
```

```
CTR_DRBG_Generate
```

```
requested_number_of_bits = 256
```

```
additional_input is
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7
```

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

```
*****
```

```
CTR_DRBG_Reseed
```

```
entropy_input is
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
```

D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED F E0E1E2E3 E4E5E6E7

additional_input is

A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7

Block_Cipher_df

input_str is

C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED F
E0E1E2E3 E4E5E6E7 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7

number_of_bits_to_return = 320

S is

00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED F E0E1E2E3 E4E5E6E7
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000000 00000000
00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED F E0E1E2E3 E4E5E6E7
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000

temp is

E7ABCDD0 A6525584 7CEC9281 848F4138

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000
00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7 E0E1E2E3 E4E5E6E7
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000

temp is

E7ABCDD0 A6525584

7CEC9281 848F4138 55A14C04 0528CE89 199791EC 6E93B3E6

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000 00000000 00000000
00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7 E0E1E2E3 E4E5E6E7
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000

temp is

E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89

199791EC 6E93B3E6 62B20794 F25B3684 1E0EBF28 4BD7EB51

Key is
E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89

X is
199791EC 6E93B3E6 62B20794 F25B3684

BlockEncrypt

Key is
E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89

X is
199791EC 6E93B3E6 62B20794 F25B3684

X = BlockEncrypt(Key, X) is
F1BF2700 8A0E046B 826E30EF E8E34AA7

temp is
F1BF2700 8A0E046B 826E30EF E8E34AA7

BlockEncrypt

Key is
E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89

X is
F1BF2700 8A0E046B 826E30EF E8E34AA7

X = BlockEncrypt(Key, X) is
BA2F6BC3 8CCDDBF2 31973B03 F26077D0

temp is
F1BF2700 8A0E046B

826E30EF E8E34AA7 BA2F6BC3 8CCDDBF2 31973B03 F26077D0

BlockEncrypt

Key is

E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89

X is

BA2F6BC3 8CCDDBF2 31973B03 F26077D0

X = BlockEncrypt(Key, X) is

442C7DA9 71F60F2D E8F43156 CAC4AB30

temp is

F1BF2700 8A0E046B 826E30EF E8E34AA7 BA2F6BC3 8CCDDBF2
31973B03 F26077D0 442C7DA9 71F60F2D E8F43156 CAC4AB30

requested_bits is

F1BF2700 8A0E046B 826E30EF E8E34AA7
BA2F6BC3 8CCDDBF2 31973B03 F26077D0 442C7DA9 71F60F2D

Update

provided_data is

F1BF2700 8A0E046B 826E30EF E8E34AA7
BA2F6BC3 8CCDDBF2 31973B03 F26077D0 442C7DA9 71F60F2D

While loop

Key is

30DDEC5F 10795E1A 725319A0 DBF33FE5 88C0ADCB 131B96B1

V is

66AB4857 3E84F77C 34709B9D 03C5D50E

output_block is

C0C92B2B 9EA1D51B CB8E6E98 6D802515

temp is

C0C92B2B 9EA1D51B CB8E6E98 6D802515

While loop

Key is

30DDEC5F 10795E1A 725319A0 DBF33FE5 88C0ADCB 131B96B1

V is

66AB4857 3E84F77C 34709B9D 03C5D50F

output_block is

CC0E6B41 8D60E816 8DCEFBF8 C5416257

temp is

C0C92B2B 9EA1D51B

CB8E6E98 6D802515 CC0E6B41 8D60E816 8DCEFBF8 C5416257

While loop

Key is

30DDEC5F 10795E1A 725319A0 DBF33FE5 88C0ADCB 131B96B1

V is

66AB4857 3E84F77C 34709B9D 03C5D510

output_block is

13DE1FA1 45BC29D4 ED919153 5367F330

temp is
C0C92B2B 9EA1D51B CB8E6E98 6D802515 CC0E6B41 8D60E816
8DCEFBF8 C5416257 13DE1FA1 45BC29D4 ED919153 5367F330

temp XOR provided_data is
31760C2B 14AFD170 49E05E77 85636FB2
76210082 01AD33E4 BC59C0FB 37211587 57F26208 344A26F9

Key is
31760C2B 14AFD170 49E05E77 85636FB2 76210082 01AD33E4

V is
BC59C0FB 37211587 57F26208 344A26F9

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

While loop

Key is
31760C2B 14AFD170 49E05E77 85636FB2 76210082 01AD33E4

V is

BC59C0FB 37211587 57F26208 344A26FC

output_block is

53F2BFC5 E663EA33 20A6EB96 DD4D07E0

temp is

53F2BFC5 E663EA33 20A6EB96 DD4D07E0

While loop

Key is

31760C2B 14AFD170 49E05E77 85636FB2 76210082 01AD33E4

V is

BC59C0FB 37211587 57F26208 344A26FD

output_block is

D5E8B942 B093FDE7 6264FFB5 EE0E948F

temp is

53F2BFC5 E663EA33

20A6EB96 DD4D07E0 D5E8B942 B093FDE7 6264FFB5 EE0E948F

While loop

Key is

31760C2B 14AFD170 49E05E77 85636FB2 76210082 01AD33E4

V is

BC59C0FB 37211587 57F26208 344A26FE

output_block is

A29DC07B 6BC4CC60 A32F4C28 E8ACAD8D

temp is

53F2BFC5 E663EA33 20A6EB96 DD4D07E0 D5E8B942 B093FDE7
6264FFB5 EE0E948F A29DC07B 6BC4CC60 A32F4C28 E8ACAD8D

temp XOR provided_data is

53F2BFC5 E663EA33 20A6EB96 DD4D07E0
D5E8B942 B093FDE7 6264FFB5 EE0E948F A29DC07B 6BC4CC60

Key is

53F2BFC5 E663EA33 20A6EB96 DD4D07E0 D5E8B942 B093FDE7

V is

6264FFB5 EE0E948F A29DC07B 6BC4CC60

rnd_val is

52D60B92 95D030CD
5DF0740F 6298F7FB 0BCE9363 56179511 4A3C3FAF 3782C843

#####

CTR_DRBG

Requested Security Strength = 192

prediction_resistance_flag = "ENABLED"

EntropyInput =
00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627

EntropyInput1 (for Reseed1) =

80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7

EntropyInput2 (for Reseed2) =

C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7 E0E1E2E3 E4E5E6E7

```
Nonce =
20212223 24252627 28292A2B
```

```
PersonalizationString =
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667
```

```
AdditionalInput = <empty>
```

```
#####
*****
```

```
CTR_DRBG_Instantiate_algorithm - with derivation function
```

```
entropy_input is
00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
```

```
nonce is
20212223 24252627 28292A2B
```

```
personal_str is
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667
```

```
prediction_resistance_flag = "PredictionResistance"
```

```
-----
```

```
Block_Cipher_df
```

```
input_str is
00010203 04050607 08090A0B 0C0D0E0F 10111213
14151617 18191A1B 1C1D1E1F 20212223 24252627 20212223
24252627 28292A2B 40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667
```

number_of_bits_to_return = 320

S is

```
0000005C 00000028 00010203 04050607  
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F  
20212223 24252627 20212223 24252627 28292A2B 40414243  
44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B  
5C5D5E5F 60616263 64656667 80000000 00000000 00000000
```

BCC

IV is

```
00000000 00000000 00000000 00000000
```

IV || S is

```
00000000 00000000 0000005C 00000028 00010203 04050607  
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F  
20212223 24252627 20212223 24252627 28292A2B 40414243  
44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B  
5C5D5E5F 60616263 64656667 80000000 00000000 00000000
```

temp is

```
883662C0 53AC837C 186A91D7 0C5398FA
```

BCC

IV is

```
00000001 00000000 00000000 00000000
```

IV || S is

```
00000000 00000000 0000005C 00000028 00010203 04050607  
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F  
20212223 24252627 20212223 24252627 28292A2B 40414243  
44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B  
5C5D5E5F 60616263 64656667 80000000 00000000 00000000
```

temp is

883662C0 53AC837C
186A91D7 0C5398FA 9028263E F8303EE6 F7658E84 1E8EDDB4

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000
00000000 00000000 0000005C 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 40414243
44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
5C5D5E5F 60616263 64656667 80000000 00000000 00000000

temp is

883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6
F7658E84 1E8EDDB4 BA630844 25877431 5143AC1F 156049EB

Key is

883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6

X is

F7658E84 1E8EDDB4 BA630844 25877431

BlockEncrypt

Key is

883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6

X is

F7658E84 1E8EDDB4 BA630844 25877431

X = BlockEncrypt(Key, X) is

AC49318E F0FA3331 F54CFB30 6C9B7B15

temp is

AC49318E F0FA3331 F54CFB30 6C9B7B15

BlockEncrypt

Key is

883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6

X is

AC49318E F0FA3331 F54CFB30 6C9B7B15

X = BlockEncrypt(Key, X) is

9334B962 5E62F257 2431DA7D 0A5F7534

temp is

AC49318E F0FA3331
F54CFB30 6C9B7B15 9334B962 5E62F257 2431DA7D 0A5F7534

BlockEncrypt

Key is

883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6

X is

9334B962 5E62F257 2431DA7D 0A5F7534

X = BlockEncrypt(Key, X) is
B22E0E89 FF0FF392 A7CECDBE 5A4E766F

temp is
AC49318E F0FA3331 F54CFB30 6C9B7B15 9334B962 5E62F257
2431DA7D 0A5F7534 B22E0E89 FF0FF392 A7CECDBE 5A4E766F

requested_bits is
AC49318E F0FA3331 F54CFB30 6C9B7B15
9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392

seed_material is
AC49318E F0FA3331 F54CFB30 6C9B7B15
9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392

Update

provided_data is
AC49318E F0FA3331 F54CFB30 6C9B7B15
9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392

While loop

Key is
00000000 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000001

output_block is
CD33B28A C773F74B A00ED1F3 12572435

temp is
CD33B28A C773F74B A00ED1F3 12572435

While loop

Key is

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

98E7247C 07F0FE41 1C267E43 84B0F600

temp is

CD33B28A C773F74B

A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600

While loop

Key is

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000003

output_block is

2A3493E6 6235EE67 DEECCD2F 3B393BD8

temp is

CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41

1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8

temp XOR provided_data is

617A8304 3789C47A 55422AC3 7ECC5F20

```
0BD39D1E 59920C16 3817A43E 8EEF8334 981A9D6F 9D3A1DF5
```

```
Key is  
617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16
```

```
V is  
3817A43E 8EEF8334 981A9D6F 9D3A1DF5
```

```
-----  
First call to Generate
```

```
*****
```

```
CTR_DRBG_Generate
```

```
requested_number_of_bits = 256
```

```
additional_input is <empty>
```

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

```
*****
```

```
CTR_DRBG_Reseed
```

```
entropy_input is
```

```
80818283 84858687 88898A8B 8C8D8E8F
```

```
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
```

```
additional_input is <empty>
```

```
-----
```

```
Block_Cipher_df
```

```
input_str is
```

```
80818283 84858687 88898A8B 8C8D8E8F
```

```
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
```

```
number_of_bits_to_return = 320
```

S is

00000028	00000028	80818283	84858687		
88898A8B	8C8D8E8F	90919293	94959697	98999A9B	9C9D9E9F
A0A1A2A3	A4A5A6A7	80000000	00000000	00000000	00000000

BCC

IV is

00000000	00000000	00000000	00000000
----------	----------	----------	----------

IV || S is

00000000	00000000	00000028	00000028	80818283	84858687
88898A8B	8C8D8E8F	90919293	94959697	98999A9B	9C9D9E9F
A0A1A2A3	A4A5A6A7	80000000	00000000	00000000	00000000

temp is

D4DC3DD9	64EB0CA9	AFB81ED4	D728EACD
----------	----------	----------	----------

BCC

IV is

00000001	00000000	00000000	00000000
----------	----------	----------	----------

IV || S is

00000000	00000000	00000028	00000028	80818283	84858687
88898A8B	8C8D8E8F	90919293	94959697	98999A9B	9C9D9E9F
A0A1A2A3	A4A5A6A7	80000000	00000000	00000000	00000000

temp is

D4DC3DD9	64EB0CA9				
AFB81ED4	D728EACD	D598A470	CD085CAD	313F0704	00084980

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000

00000000 00000000 00000028 00000028 80818283 84858687

88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F

A0A1A2A3 A4A5A6A7 80000000 00000000 00000000 00000000

temp is

D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD

313F0704 00084980 E8128432 2968C4EB 2EA63668 13E2E7E3

Key is

D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD

X is

313F0704 00084980 E8128432 2968C4EB

BlockEncrypt

Key is

D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD

X is

313F0704 00084980 E8128432 2968C4EB

X = BlockEncrypt(Key, X) is

ECE25874 66228E78 6B45F5AA E1E7407B

temp is

ECE25874 66228E78 6B45F5AA E1E7407B

BlockEncrypt

Key is

D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD

X is

ECE25874 66228E78 6B45F5AA E1E7407B

X = BlockEncrypt(Key, X) is

C500EB8B 6D8EAD20 9217569B C032FAF6

temp is

ECE25874 66228E78

6B45F5AA E1E7407B C500EB8B 6D8EAD20 9217569B C032FAF6

BlockEncrypt

Key is

D4DC3DD9 64EB0CA9 AFB81ED4 D728EACD D598A470 CD085CAD

X is

C500EB8B 6D8EAD20 9217569B C032FAF6

X = BlockEncrypt(Key, X) is

8DCC82DB 4927187D 79D87935 70CCFCBC

temp is

ECE25874 66228E78 6B45F5AA E1E7407B C500EB8B 6D8EAD20

9217569B C032FAF6 8DCC82DB 4927187D 79D87935 70CCFCBC

requested_bits is

ECE25874 66228E78 6B45F5AA E1E7407B
C500EB8B 6D8EAD20 9217569B C032FAF6 8DCC82DB 4927187D

Update

provided_data is
ECE25874 66228E78 6B45F5AA E1E7407B
C500EB8B 6D8EAD20 9217569B C032FAF6 8DCC82DB 4927187D

While loop

Key is
617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

V is
3817A43E 8EEF8334 981A9D6F 9D3A1DF6

output_block is
E231244B 3235B085 C8160442 4357E852

temp is
E231244B 3235B085 C8160442 4357E852

While loop

Key is
617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

V is
3817A43E 8EEF8334 981A9D6F 9D3A1DF7

output_block is

01E3828B 5C455686 79A5555F 867AAC8C

temp is

E231244B 3235B085

C8160442 4357E852 01E3828B 5C455686 79A5555F 867AAC8C

While loop

Key is

617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

V is

3817A43E 8EEF8334 981A9D6F 9D3A1DF8

output_block is

6C0BA382 122A6E1E BEB51820 656D3D45

temp is

E231244B 3235B085 C8160442 4357E852 01E3828B 5C455686

79A5555F 867AAC8C 6C0BA382 122A6E1E BEB51820 656D3D45

temp XOR provided_data is

0ED37C3F 54173EFD A353F1E8 A2B0A829

C4E36900 31CBFBAA6 EBB203C4 4648567A E1C72159 5B0D7663

Key is

0ED37C3F 54173EFD A353F1E8 A2B0A829 C4E36900 31CBFBAA6

V is

EBB203C4 4648567A E1C72159 5B0D7663

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

While loop

Key is

0ED37C3F 54173EFD A353F1E8 A2B0A829 C4E36900 31CBFBA6

V is

EBB203C4 4648567A E1C72159 5B0D7666

output_block is

941C5910 4692AC61 74F5BD51 9BF44FAA

temp is

941C5910 4692AC61 74F5BD51 9BF44FAA

While loop

Key is

0ED37C3F 54173EFD A353F1E8 A2B0A829 C4E36900 31CBFBA6

V is

EBB203C4 4648567A E1C72159 5B0D7667

output_block is

37677E3E BA575D06 97D13841 1E0E3088

temp is

941C5910 4692AC61

74F5BD51 9BF44FAA 37677E3E BA575D06 97D13841 1E0E3088

While loop

Key is

0ED37C3F 54173EFD A353F1E8 A2B0A829 C4E36900 31CBFBAA

V is

EBB203C4 4648567A E1C72159 5B0D7668

output_block is

8FCDC0E7 22EE559B 7967A230 92EF728F

temp is

941C5910 4692AC61 74F5BD51 9BF44FAA 37677E3E BA575D06

97D13841 1E0E3088 8FCDC0E7 22EE559B 7967A230 92EF728F

temp XOR provided_data is

941C5910 4692AC61 74F5BD51 9BF44FAA

37677E3E BA575D06 97D13841 1E0E3088 8FCDC0E7 22EE559B

Key is

941C5910 4692AC61 74F5BD51 9BF44FAA 37677E3E BA575D06

V is

97D13841 1E0E3088 8FCDC0E7 22EE559B

rnd_val is

F780D4A2 C25CF8EE

7407D948 EC0B724A 4235D8B2 0E650813 92755CA7 912AD7C0

Second call to Generate

```
*****
```

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Generate FAILED: Reseed is required

```
*****
```

CTR_DRBG_Reseed

entropy_input is

C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7 E0E1E2E3 E4E5E6E7

additional_input is <empty>

Block_Cipher_df

input_str is

C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7 E0E1E2E3 E4E5E6E7

number_of_bits_to_return = 320

S is

00000028 00000028 C0C1C2C3 C4C5C6C7

C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7

E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000

00000000 00000000 00000028 00000028 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000

temp is

98316F8D C09A27EA 960FDB96 D22C96D3

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000

00000000 00000000 00000028 00000028 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000

temp is

98316F8D C09A27EA

960FDB96 D22C96D3 C95E08EF DAB3E081 BDA51061 F9619651

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000

00000000 00000000 00000028 00000028 C0C1C2C3 C4C5C6C7

C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED
E0E1E2E3 E4E5E6E7 80000000 00000000 00000000 00000000

temp is
98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081
BDA51061 F9619651 191D1E83 B09E52F5 1D6A9C00 B4889F28

Key is
98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081

X is
BDA51061 F9619651 191D1E83 B09E52F5

BlockEncrypt

Key is
98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081

X is
BDA51061 F9619651 191D1E83 B09E52F5

X = BlockEncrypt(Key, X) is
60C2CB2F DB52737D 19692CF5 E74AC177

temp is
60C2CB2F DB52737D 19692CF5 E74AC177

BlockEncrypt

Key is
98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081

X is

60C2CB2F DB52737D 19692CF5 E74AC177

X = BlockEncrypt(Key, X) is

F94540C2 F7FCE903 859505EA BF87DB61

temp is

60C2CB2F DB52737D

19692CF5 E74AC177 F94540C2 F7FCE903 859505EA BF87DB61

BlockEncrypt

Key is

98316F8D C09A27EA 960FDB96 D22C96D3 C95E08EF DAB3E081

X is

F94540C2 F7FCE903 859505EA BF87DB61

X = BlockEncrypt(Key, X) is

9FA75BC1 074138FE 9811C2BC F2A688DF

temp is

60C2CB2F DB52737D 19692CF5 E74AC177 F94540C2 F7FCE903

859505EA BF87DB61 9FA75BC1 074138FE 9811C2BC F2A688DF

requested_bits is

60C2CB2F DB52737D 19692CF5 E74AC177

F94540C2 F7FCE903 859505EA BF87DB61 9FA75BC1 074138FE

Update

provided_data is

60C2CB2F DB52737D 19692CF5 E74AC177

F94540C2 F7FCE903 859505EA BF87DB61 9FA75BC1 074138FE

While loop

Key is

941C5910 4692AC61 74F5BD51 9BF44FAA 37677E3E BA575D06

V is

97D13841 1E0E3088 8FCDC0E7 22EE559C

output_block is

78F91B65 6FB3D42E C4B48E70 4F34BCE9

temp is

78F91B65 6FB3D42E C4B48E70 4F34BCE9

While loop

Key is

941C5910 4692AC61 74F5BD51 9BF44FAA 37677E3E BA575D06

V is

97D13841 1E0E3088 8FCDC0E7 22EE559D

output_block is

10A6A43B D0D2A7AC 70C91188 E109F0C0

temp is

78F91B65 6FB3D42E

C4B48E70 4F34BCE9 10A6A43B D0D2A7AC 70C91188 E109F0C0

While loop

Key is

941C5910 4692AC61 74F5BD51 9BF44FAA 37677E3E BA575D06

V is

97D13841 1E0E3088 8FCDC0E7 22EE559E

output_block is

D6093035 63CD146C C94F91E8 D38A18F7

temp is

78F91B65 6FB3D42E C4B48E70 4F34BCE9 10A6A43B D0D2A7AC
70C91188 E109F0C0 D6093035 63CD146C C94F91E8 D38A18F7

temp XOR provided_data is

183BD04A B4E1A753 DDDDA285 A87E7D9E
E9E3E4F9 272E4EAF F55C1462 5E8E2BA1 49AE6BF4 648C2C92

Key is

183BD04A B4E1A753 DDDDA285 A87E7D9E E9E3E4F9 272E4EAF

V is

F55C1462 5E8E2BA1 49AE6BF4 648C2C92

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

183BD04A B4E1A753 DDDDA285 A87E7D9E E9E3E4F9 272E4EAF

V is

F55C1462 5E8E2BA1 49AE6BF4 648C2C95

output_block is

2FFD9DF2 057D5F9F 704B48CE 890646ED

temp is

2FFD9DF2 057D5F9F 704B48CE 890646ED

While loop

Key is

183BD04A B4E1A753 DDDDA285 A87E7D9E E9E3E4F9 272E4EAF

V is

F55C1462 5E8E2BA1 49AE6BF4 648C2C96

output_block is

BFEAB396 648A7FC4 CA995C6F DAC51E3E

temp is

2FFD9DF2 057D5F9F

704B48CE 890646ED BFEAB396 648A7FC4 CA995C6F DAC51E3E

While loop

Key is

183BD04A B4E1A753 DDDDA285 A87E7D9E E9E3E4F9 272E4EAF

V is

F55C1462 5E8E2BA1 49AE6BF4 648C2C97

output_block is

0F6B301A C1AC316E 2E4CBA0D 04A47306

temp is

2FFD9DF2 057D5F9F 704B48CE 890646ED BFEAB396 648A7FC4
CA995C6F DAC51E3E 0F6B301A C1AC316E 2E4CBA0D 04A47306

temp XOR provided_data is

2FFD9DF2 057D5F9F 704B48CE 890646ED BFEAB396 648A7FC4
CA995C6F DAC51E3E 0F6B301A C1AC316E

Key is

2FFD9DF2 057D5F9F 704B48CE 890646ED BFEAB396 648A7FC4

V is

CA995C6F DAC51E3E 0F6B301A C1AC316E

rnd_val is

BA14617F 915BA964
CB79276B DADC840C 14B631BB D1A59097 054FA6DF F863B238

#####

CTR_DRBG

Requested Security Strength = 192

prediction_resistance_flag = "ENABLED"

EntropyInput =

00010203 04050607 08090A0B 0C0D0E0F

10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627

EntropyInput1 (for Reseed1) =
80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7

EntropyInput2 (for Reseed2) =
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7 E0E1E2E3 E4E5E6E7

Nonce =
20212223 24252627 28292A2B

PersonalizationString =
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667

AdditionalInput1 =
60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687

AdditionalInput2 =
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7

#####

CTR_DRBG_Instantiate_algorithm - with derivation function

entropy_input is
00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627

nonce is
20212223 24252627 28292A2B

```
personal_str is
    40414243 44454647 48494A4B 4C4D4E4F
    50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667
```

```
prediction_resistance_flag = "PredictionResistance"
```

```
-----  
Block_Cipher_df
```

```
input_str is
    00010203 04050607 08090A0B 0C0D0E0F 10111213
    14151617 18191A1B 1C1D1E1F 20212223 24252627 20212223
    24252627 28292A2B 40414243 44454647 48494A4B 4C4D4E4F
    50515253 54555657 58595A5B 5C5D5E5F 60616263 64656667
```

```
number_of_bits_to_return = 320
```

```
S is
    0000005C 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 40414243
    44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
    5C5D5E5F 60616263 64656667 80000000 00000000 00000000
```

```
-----
```

```
BCC
```

```
IV is
```

```
00000000 00000000 00000000 00000000
```

```
IV || S is
```

```
00000000 00000000 0000005C 00000028 00010203 04050607
    08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
    20212223 24252627 20212223 24252627 28292A2B 40414243
    44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
    5C5D5E5F 60616263 64656667 80000000 00000000 00000000
```

temp is
883662C0 53AC837C 186A91D7 0C5398FA

BCC

IV is
00000001 00000000 00000000 00000000

IV || S is
00000001 00000000
00000000 00000000 0000005C 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 40414243
44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
5C5D5E5F 60616263 64656667 80000000 00000000 00000000

temp is
883662C0 53AC837C
186A91D7 0C5398FA 9028263E F8303EE6 F7658E84 1E8EDDB4

BCC

IV is
00000002 00000000 00000000 00000000

IV || S is
00000002 00000000
00000000 00000000 0000005C 00000028 00010203 04050607
08090A0B 0C0D0E0F 10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 20212223 24252627 28292A2B 40414243
44454647 48494A4B 4C4D4E4F 50515253 54555657 58595A5B
5C5D5E5F 60616263 64656667 80000000 00000000 00000000

temp is
883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6
F7658E84 1E8EDDB4 BA630844 25877431 5143AC1F 156049EB

Key is
883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6

X is
F7658E84 1E8EDDB4 BA630844 25877431

BlockEncrypt

Key is
883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6

X is
F7658E84 1E8EDDB4 BA630844 25877431

X = BlockEncrypt(Key, X) is
AC49318E F0FA3331 F54CFB30 6C9B7B15

temp is
AC49318E F0FA3331 F54CFB30 6C9B7B15

BlockEncrypt

Key is
883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6

X is
AC49318E F0FA3331 F54CFB30 6C9B7B15

X = BlockEncrypt(Key, X) is
9334B962 5E62F257 2431DA7D 0A5F7534

temp is

AC49318E F0FA3331

F54CFB30 6C9B7B15 9334B962 5E62F257 2431DA7D 0A5F7534

BlockEncrypt

Key is

883662C0 53AC837C 186A91D7 0C5398FA 9028263E F8303EE6

X is

9334B962 5E62F257 2431DA7D 0A5F7534

X = BlockEncrypt(Key, X) is

B22E0E89 FF0FF392 A7CECDBE 5A4E766F

temp is

AC49318E F0FA3331 F54CFB30 6C9B7B15 9334B962 5E62F257

2431DA7D 0A5F7534 B22E0E89 FF0FF392 A7CECDBE 5A4E766F

requested_bits is

AC49318E F0FA3331 F54CFB30 6C9B7B15

9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392

seed_material is

AC49318E F0FA3331 F54CFB30 6C9B7B15

9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392

Update

provided_data is

AC49318E F0FA3331 F54CFB30 6C9B7B15

9334B962 5E62F257 2431DA7D 0A5F7534 B22E0E89 FF0FF392

While loop

Key is

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is

CD33B28A C773F74B A00ED1F3 12572435

temp is

CD33B28A C773F74B A00ED1F3 12572435

While loop

Key is

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

98E7247C 07F0FE41 1C267E43 84B0F600

temp is

CD33B28A C773F74B

A00ED1F3 12572435 98E7247C 07F0FE41 1C267E43 84B0F600

While loop

Key is
00000000 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000003

output_block is
2A3493E6 6235EE67 DEECCD2F 3B393BD8

temp is
CD33B28A C773F74B A00ED1F3 12572435 98E7247C 07F0FE41
1C267E43 84B0F600 2A3493E6 6235EE67 DEECCD2F 3B393BD8

temp XOR provided_data is
617A8304 3789C47A 55422AC3 7ECC5F20
0BD39D1E 59920C16 3817A43E 8EEF8334 981A9D6F 9D3A1DF5

Key is
617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

V is
3817A43E 8EEF8334 981A9D6F 9D3A1DF5

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is
60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

entropy_input is
80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7

additional_input is
60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687

Block_Cipher_df

input_str is
80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 60616263 64656667 68696A6B 6C6D6E6F
70717273 74757677 78797A7B 7C7D7E7F 80818283 84858687

number_of_bits_to_return = 320

S is
00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000

BCC

IV is
00000000 00000000 00000000 00000000

IV || S is
00000000 00000000 00000000 00000000
00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7

60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000

temp is

FA46944A 0BDBB5EF A60EFAFE B9574E97

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000
00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000

temp is

FA46944A 0BDBB5EF
A60EFAFE B9574E97 A1E88E07 AFFCD4EC E8EB2D2C ED3E4283

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000 00000000 00000000
00000050 00000028 80818283 84858687 88898A8B 8C8D8E8F
90919293 94959697 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
78797A7B 7C7D7E7F 80818283 84858687 80000000 00000000

temp is

FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC
E8EB2D2C ED3E4283 8D8520E1 65EB3BDE BFAABC51 C44420CE

Key is
FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC

X is
E8EB2D2C ED3E4283 8D8520E1 65EB3BDE

BlockEncrypt

Key is
FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC

X is
E8EB2D2C ED3E4283 8D8520E1 65EB3BDE

X = BlockEncrypt(Key, X) is
D6D201B9 33F0FA92 A953C84C B739185C

temp is
D6D201B9 33F0FA92 A953C84C B739185C

BlockEncrypt

Key is
FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC

X is
D6D201B9 33F0FA92 A953C84C B739185C

X = BlockEncrypt(Key, X) is
5F353217 EFC411AD 5CD15D92 B481BEEF

temp is
D6D201B9 33F0FA92
A953C84C B739185C 5F353217 EFC411AD 5CD15D92 B481BEEF

BlockEncrypt

Key is
FA46944A 0BDBB5EF A60EFAFE B9574E97 A1E88E07 AFFCD4EC

X is
5F353217 EFC411AD 5CD15D92 B481BEEF

X = BlockEncrypt(Key, X) is
7BDD58F3 8FD4827B 7A57A0F1 55ED8D8E

temp is
D6D201B9 33F0FA92 A953C84C B739185C 5F353217 EFC411AD
5CD15D92 B481BEEF 7BDD58F3 8FD4827B 7A57A0F1 55ED8D8E

requested_bits is
D6D201B9 33F0FA92 A953C84C B739185C
5F353217 EFC411AD 5CD15D92 B481BEEF 7BDD58F3 8FD4827B

Update

provided_data is
D6D201B9 33F0FA92 A953C84C B739185C
5F353217 EFC411AD 5CD15D92 B481BEEF 7BDD58F3 8FD4827B

While loop

Key is

617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

V is

3817A43E 8EEF8334 981A9D6F 9D3A1DF6

output_block is

E231244B 3235B085 C8160442 4357E852

temp is

E231244B 3235B085 C8160442 4357E852

While loop

Key is

617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

V is

3817A43E 8EEF8334 981A9D6F 9D3A1DF7

output_block is

01E3828B 5C455686 79A5555F 867AAC8C

temp is

E231244B 3235B085

C8160442 4357E852 01E3828B 5C455686 79A5555F 867AAC8C

While loop

Key is

617A8304 3789C47A 55422AC3 7ECC5F20 0BD39D1E 59920C16

V is

3817A43E 8EEF8334 981A9D6F 9D3A1DF8

output_block is

6C0BA382 122A6E1E BEB51820 656D3D45

temp is

E231244B 3235B085 C8160442 4357E852 01E3828B 5C455686
79A5555F 867AAC8C 6C0BA382 122A6E1E BEB51820 656D3D45

temp XOR provided_data is

34E325F2 01C54A17 6145CC0E F46EF00E
5ED6B09C B381472B 257408CD 32FB1263 17D6FB71 9DFEEC65

Key is

34E325F2 01C54A17 6145CC0E F46EF00E 5ED6B09C B381472B

V is

257408CD 32FB1263 17D6FB71 9DFEEC65

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000

While loop

Key is

34E325F2 01C54A17 6145CC0E F46EF00E 5ED6B09C B381472B

V is

257408CD 32FB1263 17D6FB71 9DFEEC68

output_block is

A8E263CA 208C8E9C 14A130E7 86501B95

temp is

A8E263CA 208C8E9C 14A130E7 86501B95

While loop

Key is

34E325F2 01C54A17 6145CC0E F46EF00E 5ED6B09C B381472B

V is

257408CD 32FB1263 17D6FB71 9DFEEC69

output_block is

C8BFE1A5 73158D8E DBAA41D2 AEBC2648

temp is

A8E263CA 208C8E9C

14A130E7 86501B95 C8BFE1A5 73158D8E DBAA41D2 AEBC2648

While loop

Key is

34E325F2 01C54A17 6145CC0E F46EF00E 5ED6B09C B381472B

V is

257408CD 32FB1263 17D6FB71 9DFEEC6A

output_block is

3FC73970 BB89187C 0A48CD51 23703346

temp is

A8E263CA 208C8E9C 14A130E7 86501B95 C8BFE1A5 73158D8E
DBAA41D2 AEBD2648 3FC73970 BB89187C 0A48CD51 23703346

temp XOR provided_data is

A8E263CA 208C8E9C 14A130E7 86501B95
C8BFE1A5 73158D8E DBAA41D2 AEBD2648 3FC73970 BB89187C

Key is

A8E263CA 208C8E9C 14A130E7 86501B95 C8BFE1A5 73158D8E

V is

DBAA41D2 AEBD2648 3FC73970 BB89187C

rnd_val is

01AFE09F 7BA5D683
8BCAB837 75F9C286 E6132674 06560F2C 069DB758 98DE5D3F

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is

A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

entropy_input is

C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7

additional_input is

A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7

Block_Cipher_df

input_str is

C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7

number_of_bits_to_return = 320

S is

00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000000 00000000

00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED F E0E1E2E3 E4E5E6E7
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000

temp is

E7ABCDD0 A6525584 7CEC9281 848F4138

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000
00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED F E0E1E2E3 E4E5E6E7
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000

temp is

E7ABCDD0 A6525584
7CEC9281 848F4138 55A14C04 0528CE89 199791EC 6E93B3E6

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000 00000000 00000000
00000050 00000028 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED F E0E1E2E3 E4E5E6E7
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 80000000 00000000

temp is
E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89
199791EC 6E93B3E6 62B20794 F25B3684 1E0EBF28 4BD7EB51

Key is
E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89

X is
199791EC 6E93B3E6 62B20794 F25B3684

BlockEncrypt

Key is
E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89

X is
199791EC 6E93B3E6 62B20794 F25B3684

X = BlockEncrypt(Key, X) is
F1BF2700 8A0E046B 826E30EF E8E34AA7

temp is
F1BF2700 8A0E046B 826E30EF E8E34AA7

BlockEncrypt

Key is
E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89

X is
F1BF2700 8A0E046B 826E30EF E8E34AA7

```
X = BlockEncrypt(Key, X) is  
    BA2F6BC3 8CCDBBF2 31973B03 F26077D0
```

```
temp is  
    F1BF2700 8A0E046B  
    826E30EF E8E34AA7 BA2F6BC3 8CCDBBF2 31973B03 F26077D0
```

```
BlockEncrypt
```

```
Key is  
    E7ABCDD0 A6525584 7CEC9281 848F4138 55A14C04 0528CE89
```

```
X is
```

```
    BA2F6BC3 8CCDBBF2 31973B03 F26077D0
```

```
X = BlockEncrypt(Key, X) is  
    442C7DA9 71F60F2D E8F43156 CAC4AB30
```

```
temp is
```

```
    F1BF2700 8A0E046B 826E30EF E8E34AA7 BA2F6BC3 8CCDBBF2  
    31973B03 F26077D0 442C7DA9 71F60F2D E8F43156 CAC4AB30
```

```
requested_bits is
```

```
    F1BF2700 8A0E046B 826E30EF E8E34AA7  
    BA2F6BC3 8CCDBBF2 31973B03 F26077D0 442C7DA9 71F60F2D
```

```
Update
```

```
provided_data is
```

```
    F1BF2700 8A0E046B 826E30EF E8E34AA7  
    BA2F6BC3 8CCDBBF2 31973B03 F26077D0 442C7DA9 71F60F2D
```

While loop

Key is

A8E263CA 208C8E9C 14A130E7 86501B95 C8BFE1A5 73158D8E

V is

DBAA41D2 AEBD2648 3FC73970 BB89187D

output_block is

42BFE34F 5E9BB3D3A F3687CD7 1E272A79

temp is

42BFE34F 5E9BB3D3A F3687CD7 1E272A79

While loop

Key is

A8E263CA 208C8E9C 14A130E7 86501B95 C8BFE1A5 73158D8E

V is

DBAA41D2 AEBD2648 3FC73970 BB89187E

output_block is

0D1E7656 27674349 A90BCAA4 593E524A

temp is

42BFE34F 5E9BB3D3A

F3687CD7 1E272A79 0D1E7656 27674349 A90BCAA4 593E524A

While loop

Key is

A8E263CA 208C8E9C 14A130E7 86501B95 C8BFE1A5 73158D8E

V is

DBAA41D2 AEBD2648 3FC73970 BB89187F

output_block is

09EEBE39 A6D92E93 5BDDA9B4 85228F47

temp is

42BFE34F 5E9BBD3A F3687CD7 1E272A79 0D1E7656 27674349
A90BCAA4 593E524A 09EEBE39 A6D92E93 5BDDA9B4 85228F47

temp XOR provided_data is

B300C44F D495B951 71064C38 F6C460DE
B7311D95 ABAA98BB 989CF1A7 AB5E259A 4DC2C390 D72F21BE

Key is

B300C44F D495B951 71064C38 F6C460DE B7311D95 ABAA98BB

V is

989CF1A7 AB5E259A 4DC2C390 D72F21BE

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

B300C44F D495B951 71064C38 F6C460DE B7311D95 ABAA98BB

V is

989CF1A7 AB5E259A 4DC2C390 D72F21C1

output_block is

DB8BD973 74F50B22 666645C0 BA1B793F

temp is

DB8BD973 74F50B22 666645C0 BA1B793F

While loop

Key is

B300C44F D495B951 71064C38 F6C460DE B7311D95 ABAA98BB

V is

989CF1A7 AB5E259A 4DC2C390 D72F21C2

output_block is

E4CB777D 0C8A7763 32537E93 15B9A355

temp is

DB8BD973 74F50B22

666645C0 BA1B793F E4CB777D 0C8A7763 32537E93 15B9A355

While loop

Key is

B300C44F D495B951 71064C38 F6C460DE B7311D95 ABAA98BB

V is

989CF1A7 AB5E259A 4DC2C390 D72F21C3

output_block is

6C7A241D 6EC6C460 218F1E3B 355A264B

temp is

DB8BD973 74F50B22 666645C0 BA1B793F E4CB777D 0C8A7763
32537E93 15B9A355 6C7A241D 6EC6C460 218F1E3B 355A264B

temp XOR provided_data is

DB8BD973 74F50B22 666645C0 BA1B793F
E4CB777D 0C8A7763 32537E93 15B9A355 6C7A241D 6EC6C460

Key is

DB8BD973 74F50B22 666645C0 BA1B793F E4CB777D 0C8A7763

V is

32537E93 15B9A355 6C7A241D 6EC6C460

rnd_val is

28730443 3D9D7301
8DB647F8 459775BD 4EB52AF0 85D764AF A52D1DEE D8DACCDD

#####

CTR_DRBG

Requested Security Strength = 256

prediction_resistance_flag = "NOT ENABLED"

EntropyInput =

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

```
EntropyInput1 (for Reseed1) =
 80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
 98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
```

```
EntropyInput2 (for Reseed2) =
 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
 D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
```

```
Nonce =
 20212223 24252627 28292A2B 2C2D2E2F
```

```
PersonalizationString = <empty>
```

```
AdditionalInput = <empty>
```

```
#####
*****
```

```
*****
```

```
CTR_DRBG_Instantiate_algorithm - with derivation function
```

```
entropy_input is
 00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
 18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
```

```
nonce is
```

```
20212223 24252627 28292A2B 2C2D2E2F
```

```
personal_str is <empty>
```

```
prediction_resistance_flag = "No PredictionResistance"
```

```
-----
```

```
Block_Cipher_df
```

```
input_str is
 00010203 04050607 08090A0B 0C0D0E0F
 10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
 28292A2B 2C2D2E2F 20212223 24252627 28292A2B 2C2D2E2F
```

number_of_bits_to_return = 384

S is

00000040	00000030				
00010203	04050607	08090A0B	0C0D0E0F	10111213	14151617
18191A1B	1C1D1E1F	20212223	24252627	28292A2B	2C2D2E2F
20212223	24252627	28292A2B	2C2D2E2F	80000000	00000000

BCC

IV is

00000000	00000000	00000000	00000000
----------	----------	----------	----------

IV || S is

00000000	00000000	00000000	00000000	00000040	00000030
00010203	04050607	08090A0B	0C0D0E0F	10111213	14151617
18191A1B	1C1D1E1F	20212223	24252627	28292A2B	2C2D2E2F
20212223	24252627	28292A2B	2C2D2E2F	80000000	00000000

temp is

4BC4520F	E87668A3	A2CE3DCB	5F564BA9
----------	----------	----------	----------

BCC

IV is

00000001	00000000	00000000	00000000
----------	----------	----------	----------

IV || S is

00000001	00000000	00000000	00000000	00000040	00000030
00010203	04050607	08090A0B	0C0D0E0F	10111213	14151617
18191A1B	1C1D1E1F	20212223	24252627	28292A2B	2C2D2E2F
20212223	24252627	28292A2B	2C2D2E2F	80000000	00000000

temp is

4BC4520F	E87668A3
----------	----------

A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000 00000000 00000000 00000040 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000

temp is

4BC4520F E87668A3 A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB
9C275423 0F4E6DC4 8283F162 52D8520F D651F481 64D42EC9

Key is

4BC4520F E87668A3
A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is

8283F162 52D8520F D651F481 64D42EC9

BlockEncrypt

Key is

4BC4520F E87668A3
A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is

8283F162 52D8520F D651F481 64D42EC9

X = BlockEncrypt(Key, X) is
DF1F3CA3 8349478C CDFE738A 222E0645

temp is
DF1F3CA3 8349478C CDFE738A 222E0645

BlockEncrypt

Key is
4BC4520F E87668A3
A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is
DF1F3CA3 8349478C CDFE738A 222E0645

X = BlockEncrypt(Key, X) is
494008AD CEFBE237 13596A7E AE41BBCD

temp is
DF1F3CA3 8349478C
CDFE738A 222E0645 494008AD CEFBE237 13596A7E AE41BBCD

BlockEncrypt

Key is
4BC4520F E87668A3
A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is
494008AD CEFBE237 13596A7E AE41BBCD

X = BlockEncrypt(Key, X) is
C66368D7 8DA21092 840E23C8 995CE6D2

temp is
DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

requested_bits is
DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

seed_material is
DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

Update

provided_data is
DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

While loop

Key is
00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000001

output_block is
530F8AFB C74536B9 A963B4F1 C4CB738B

temp is
530F8AFB C74536B9 A963B4F1 C4CB738B

While loop

Key is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

CEA7403D 4D606B6E 074EC5D3 BAF39D18

temp is

530F8AFB C74536B9
A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18

While loop

Key is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000003

output_block is

726003CA 37A62A74 D1A2F58E 7506358E

temp is

530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E

temp XOR provided_data is

```
8C10B658 440C7135 649DC77B E6E575CE 87E74890 839B8959  
1417AFAD 14B226D5 B4036B1D BA043AE6 55ACD646 EC5AD35C
```

Key is

```
8C10B658 440C7135  
649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5
```

V is

```
B4036B1D BA043AE6 55ACD646 EC5AD35C
```

First call to Generate

```
*****
```

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

```
00000000 00000000 00000000 00000000 00000000 00000000  
00000000 00000000 00000000 00000000 00000000 00000000
```

While loop

Key is

```
8C10B658 440C7135  
649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5
```

V is

```
B4036B1D BA043AE6 55ACD646 EC5AD35F
```

output_block is
68F2F51A 364601AF 9533C864 F25DA997

temp is
68F2F51A 364601AF 9533C864 F25DA997

While loop

Key is
8C10B658 440C7135
649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5

V is
B4036B1D BA043AE6 55ACD646 EC5AD360

output_block is
7D095ACE B5DE8DA2 333C4085 8D88DE5B

temp is
68F2F51A 364601AF
9533C864 F25DA997 7D095ACE B5DE8DA2 333C4085 8D88DE5B

While loop

Key is
8C10B658 440C7135
649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5

V is
B4036B1D BA043AE6 55ACD646 EC5AD361

output_block is
33B6B005 72CE4C19 9D0284FA 8BADA00B

temp is
68F2F51A 364601AF 9533C864 F25DA997 7D095ACE B5DE8DA2
333C4085 8D88DE5B 33B6B005 72CE4C19 9D0284FA 8BADA00B

temp XOR provided_data is
68F2F51A 364601AF 9533C864 F25DA997 7D095ACE B5DE8DA2
333C4085 8D88DE5B 33B6B005 72CE4C19 9D0284FA 8BADA00B

Key is
68F2F51A 364601AF
9533C864 F25DA997 7D095ACE B5DE8DA2 333C4085 8D88DE5B

V is
33B6B005 72CE4C19 9D0284FA 8BADA00B

rnd_val is
E686DD55 F758FD91
BA7CB726 FE0B573A 180AB674 39FFBDDE 5EC28FB3 7A16A53B

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

68F2F51A 364601AF
9533C864 F25DA997 7D095ACE B5DE8DA2 333C4085 8D88DE5B

V is

33B6B005 72CE4C19 9D0284FA 8BADA00E

output_block is

54789912 FE730A2F 836836F4 DA7246F6

temp is

54789912 FE730A2F 836836F4 DA7246F6

While loop

Key is

68F2F51A 364601AF
9533C864 F25DA997 7D095ACE B5DE8DA2 333C4085 8D88DE5B

V is

33B6B005 72CE4C19 9D0284FA 8BADA00F

output_block is

C52195FF 4AD1D913 8E38D01E FB037FEF

temp is

54789912 FE730A2F
836836F4 DA7246F6 C52195FF 4AD1D913 8E38D01E FB037FEF

While loop

Key is

68F2F51A 364601AF
9533C864 F25DA997 7D095ACE B5DE8DA2 333C4085 8D88DE5B

V is

33B6B005 72CE4C19 9D0284FA 8BADA010

output_block is

659CE64A 4923FB20 CAFB265F 1004328E

temp is

54789912 FE730A2F 836836F4 DA7246F6 C52195FF 4AD1D913
8E38D01E FB037FEF 659CE64A 4923FB20 CAFB265F 1004328E

temp XOR provided_data is

54789912 FE730A2F 836836F4 DA7246F6 C52195FF 4AD1D913
8E38D01E FB037FEF 659CE64A 4923FB20 CAFB265F 1004328E

Key is

54789912 FE730A2F
836836F4 DA7246F6 C52195FF 4AD1D913 8E38D01E FB037FEF

V is

659CE64A 4923FB20 CAFB265F 1004328E

rnd_val is

8DA6CC59 E703CED0
7D58D96E 5B6D7836 C3259973 5B734F88 C1A73B53 C7A6D82E

#####

CTR_DRBG

Requested Security Strength = 256

prediction_resistance_flag = "NOT ENABLED"

```
EntropyInput =
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
```

```
EntropyInput1 (for Reseed1) =
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
```

```
EntropyInput2 (for Reseed2) =
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
D8D9DADB DCDDDEF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
```

```
Nonce =
20212223 24252627 28292A2B 2C2D2E2F
```

```
PersonalizationString = <empty>
```

```
AdditionalInput1 =
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F
```

```
AdditionalInput2 =
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
```

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

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

```
CTR_DRBG_Instantiate_algorithm - with derivation function
```

```
entropy_input is
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
```

```
nonce is
20212223 24252627 28292A2B 2C2D2E2F
```

```
personal_str is <empty>  
prediction_resistance_flag = "No PredictionResistance"
```

Block_Cipher_df

```
input_str is  
00010203 04050607 08090A0B 0C0D0E0F  
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627  
28292A2B 2C2D2E2F 20212223 24252627 28292A2B 2C2D2E2F
```

```
number_of_bits_to_return = 384
```

S is

```
00000040 00000030  
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617  
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F  
20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000
```

BCC

IV is

```
00000000 00000000 00000000 00000000
```

IV || S is

```
00000000 00000000 00000000 00000000 00000040 00000030  
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617  
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F  
20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000
```

temp is

```
4BC4520F E87668A3 A2CE3DCB 5F564BA9
```

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000040 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000

temp is

4BC4520F E87668A3
A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000 00000000 00000040 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000

temp is

4BC4520F E87668A3 A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB
9C275423 0F4E6DC4 8283F162 52D8520F D651F481 64D42EC9

Key is

4BC4520F E87668A3
A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is

8283F162 52D8520F D651F481 64D42EC9

BlockEncrypt

Key is

4BC4520F E87668A3
A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is

8283F162 52D8520F D651F481 64D42EC9

X = BlockEncrypt(Key, X) is

DF1F3CA3 8349478C CDFE738A 222E0645

temp is

DF1F3CA3 8349478C CDFE738A 222E0645

BlockEncrypt

Key is

4BC4520F E87668A3
A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is

DF1F3CA3 8349478C CDFE738A 222E0645

X = BlockEncrypt(Key, X) is

494008AD CEFBE237 13596A7E AE41BBCD

temp is

DF1F3CA3 8349478C
CDFE738A 222E0645 494008AD CEFBE237 13596A7E AE41BBCD

BlockEncrypt

Key is

4BC4520F E87668A3
A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is

494008AD CEFBE237 13596A7E AE41BBCD

X = BlockEncrypt(Key, X) is

C66368D7 8DA21092 840E23C8 995CE6D2

temp is

DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

requested_bits is

DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

seed_material is

DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

Update

provided_data is

DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

While loop

Key is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is

530F8AFB C74536B9 A963B4F1 C4CB738B

temp is

530F8AFB C74536B9 A963B4F1 C4CB738B

While loop

Key is

00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

CEA7403D 4D606B6E 074EC5D3 BAF39D18

temp is

530F8AFB C74536B9

A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18

While loop

Key is

00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000003

output_block is

726003CA 37A62A74 D1A2F58E 7506358E

temp is

530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E

temp XOR provided_data is

8C10B658 440C7135 649DC77B E6E575CE 87E74890 839B8959
1417AFAD 14B226D5 B4036B1D BA043AE6 55ACD646 EC5AD35C

Key is

8C10B658 440C7135
649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5

V is

B4036B1D BA043AE6 55ACD646 EC5AD35C

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is

60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F

additional_input <> NULL, process appropriately

Block_Cipher_df

input_str is
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F

number_of_bits_to_return = 384

S is

00000030 00000030 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000
00000000 00000000 00000030 00000030 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

temp is

DE8D1951 762E5557 CFAE1170 EEF4B933

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000
00000000 00000000 00000030 00000030 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

temp is

DE8D1951 762E5557
CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000
00000000 00000000 00000030 00000030 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

temp is

DE8D1951 762E5557 CFAE1170 EEF4B933 F9C0BD35 6D5244B9
158CEE79 08C40855 6254BE89 B2960465 D4879231 3E993E48

Key is

DE8D1951 762E5557
CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855

X is

6254BE89 B2960465 D4879231 3E993E48

BlockEncrypt

Key is

DE8D1951 762E5557
CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855

X is

6254BE89 B2960465 D4879231 3E993E48

X = BlockEncrypt(Key, X) is

4D8C89E0 1B308B59 E99AE0AD 702902F8

temp is

4D8C89E0 1B308B59 E99AE0AD 702902F8

BlockEncrypt

Key is

DE8D1951 762E5557

CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855

X is

4D8C89E0 1B308B59 E99AE0AD 702902F8

X = BlockEncrypt(Key, X) is

249768D0 97B4C73B CCFCD763 CD5AC761

temp is

4D8C89E0 1B308B59

E99AE0AD 702902F8 249768D0 97B4C73B CCFCD763 CD5AC761

BlockEncrypt

Key is

DE8D1951 762E5557

CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855

X is

249768D0 97B4C73B CCFCD763 CD5AC761

X = BlockEncrypt(Key, X) is
9267624C 0952CA7B A8ACDFCC E2A669D5

temp is
4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
CCFC763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5

requested_bits is
4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
CCFC763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5

Update

provided_data is
4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
CCFC763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5

While loop

Key is
8C10B658 440C7135
649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5

V is
B4036B1D BA043AE6 55ACD646 EC5AD35D

output_block is
E686DD55 F758FD91 BA7CB726 FE0B573A

temp is
E686DD55 F758FD91 BA7CB726 FE0B573A

While loop

Key is

8C10B658 440C7135
649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5

V is

B4036B1D BA043AE6 55ACD646 EC5AD35E

output_block is

180AB674 39FFBDDE 5EC28FB3 7A16A53B

temp is

E686DD55 F758FD91
BA7CB726 FE0B573A 180AB674 39FFBDDE 5EC28FB3 7A16A53B

While loop

Key is

8C10B658 440C7135
649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5

V is

B4036B1D BA043AE6 55ACD646 EC5AD35F

output_block is

68F2F51A 364601AF 9533C864 F25DA997

temp is

E686DD55 F758FD91 BA7CB726 FE0B573A 180AB674 39FFBDDE
5EC28FB3 7A16A53B 68F2F51A 364601AF 9533C864 F25DA997

temp XOR provided_data is

AB0A54B5 EC6876C8 53E6578B 8E2255C2 3C9DDEA4 AE4B7AC5
923E58D0 B74C625A FA959756 3F14CBD4 3D9F17A8 10FBC042

Key is

AB0A54B5 EC6876C8
53E6578B 8E2255C2 3C9DDEA4 AE4B7AC5 923E58D0 B74C625A

V is

FA959756 3F14CBD4 3D9F17A8 10FBC042

Update

provided_data is

4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
CCFC763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5

While loop

Key is

AB0A54B5 EC6876C8
53E6578B 8E2255C2 3C9DDEA4 AE4B7AC5 923E58D0 B74C625A

V is

FA959756 3F14CBD4 3D9F17A8 10FBC045

output_block is

C66418B2 D26BFCC0 74F6B220 09C389BE

temp is

C66418B2 D26BFCC0 74F6B220 09C389BE

While loop

Key is

AB0A54B5 EC6876C8
53E6578B 8E2255C2 3C9DDEA4 AE4B7AC5 923E58D0 B74C625A

V is

FA959756 3F14CBD4 3D9F17A8 10FBC046

output_block is

6A0A2310 DE0CCE9E 05AA0F03 C83D8AFF

temp is

C66418B2 D26BFCC0
74F6B220 09C389BE 6A0A2310 DE0CCE9E 05AA0F03 C83D8AFF

While loop

Key is

AB0A54B5 EC6876C8
53E6578B 8E2255C2 3C9DDEA4 AE4B7AC5 923E58D0 B74C625A

V is

FA959756 3F14CBD4 3D9F17A8 10FBC047

output_block is

4CA3EC53 574253AC E3F17918 B3B50877

temp is

C66418B2 D26BFCC0 74F6B220 09C389BE 6A0A2310 DE0CCE9E
05AA0F03 C83D8AFF 4CA3EC53 574253AC E3F17918 B3B50877

temp XOR provided_data is

8BE89152 C95B7799 9D6C528D 79EA8B46 4E9D4BC0 49B809A5
C956D860 05674D9E DEC48E1F 5E1099D7 4B5DA6D4 511361A2

Key is

8BE89152 C95B7799

9D6C528D 79EA8B46 4E9D4BC0 49B809A5 C956D860 05674D9E

V is

DEC48E1F 5E1099D7 4B5DA6D4 511361A2

rnd_val is

498D25F7 124327CD
FEBAF7F0 1559AFF8 4813F609 74BA5BD8 96C0CD5F 88BA5E32

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is

A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

additional_input <> NULL, process appropriately

Block_Cipher_df

input_str is

A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

number_of_bits_to_return = 384

S is

00000030 00000030 A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000

00000000 00000000 00000030 00000030 A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

temp is

BC61575C 5D4B8037 C9E380B9 3E376057

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000

00000000 00000000 00000030 00000030 A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

temp is

BC61575C 5D4B8037

C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000000	00000000	00000030	00000030	A0A1A2A3	A4A5A6A7
00000000	00000000	00000030	00000030	A8A9AAAB	ACADAEAF
B0B1B2B3	B4B5B6B7	B8B9BABB	BCBDBEBF	C0C1C2C3	C4C5C6C7
C8C9CACB	CCCDCECF	80000000	00000000	C0C1C2C3	C4C5C6C7

temp is

BC61575C	5D4B8037	C9E380B9	3E376057	2C0B3606	11252C52
85BDEC6C	567C9B5A	F6259D1D	3848CC93	296E04B5	AD60A97F

Key is

BC61575C	5D4B8037				
C9E380B9	3E376057	2C0B3606	11252C52	85BDEC6C	567C9B5A

X is

F6259D1D	3848CC93	296E04B5	AD60A97F
----------	----------	----------	----------

BlockEncrypt

Key is

BC61575C	5D4B8037				
C9E380B9	3E376057	2C0B3606	11252C52	85BDEC6C	567C9B5A

X is

F6259D1D	3848CC93	296E04B5	AD60A97F
----------	----------	----------	----------

X = BlockEncrypt(Key, X) is

FBD01F35	7D143F63	0DC0E7F9	B48DAC71
----------	----------	----------	----------

temp is

FBD01F35	7D143F63	0DC0E7F9	B48DAC71
----------	----------	----------	----------

BlockEncrypt

Key is

BC61575C 5D4B8037
C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A

X is

FBD01F35 7D143F63 0DC0E7F9 B48DAC71

X = BlockEncrypt(Key, X) is

440CD750 A626DDB6 7744FD19 DFA9D223

temp is

FBD01F35 7D143F63
0DC0E7F9 B48DAC71 440CD750 A626DDB6 7744FD19 DFA9D223

BlockEncrypt

Key is

BC61575C 5D4B8037
C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A

X is

440CD750 A626DDB6 7744FD19 DFA9D223

X = BlockEncrypt(Key, X) is

FB21DE23 A5E64CE0 712FE847 AF490C39

temp is

FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6
7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39

requested_bits is

FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6
7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39

Update

provided_data is
FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6
7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39

While loop

Key is

8BE89152 C95B7799
9D6C528D 79EA8B46 4E9D4BC0 49B809A5 C956D860 05674D9E

V is

DEC48E1F 5E1099D7 4B5DA6D4 511361A3

output_block is

DCA0E245 D8F0260D 9DDAB936 54755CA0

temp is

DCA0E245 D8F0260D 9DDAB936 54755CA0

While loop

Key is

8BE89152 C95B7799
9D6C528D 79EA8B46 4E9D4BC0 49B809A5 C956D860 05674D9E

V is

DEC48E1F 5E1099D7 4B5DA6D4 511361A4

output_block is

82EDC0CF 4B852CCE 877A1669 CD904C99

temp is

DCA0E245 D8F0260D
9DDAB936 54755CA0 82EDC0CF 4B852CCE 877A1669 CD904C99

While loop

Key is

8BE89152 C95B7799
9D6C528D 79EA8B46 4E9D4BC0 49B809A5 C956D860 05674D9E

V is

DEC48E1F 5E1099D7 4B5DA6D4 511361A5

output_block is

050B4A10 6405F911 1D600B2C AD9634CC

temp is

DCA0E245 D8F0260D 9DDAB936 54755CA0 82EDC0CF 4B852CCE
877A1669 CD904C99 050B4A10 6405F911 1D600B2C AD9634CC

temp XOR provided_data is

2770FD70 A5E4196E 901A5ECF E0F8F0D1 C6E1179F EDA3F178
F03EEB70 12399EBA FE2A9433 C1E3B5F1 6C4FE36B 02DF38F5

Key is

2770FD70 A5E4196E
901A5ECF E0F8F0D1 C6E1179F EDA3F178 F03EEB70 12399EBA

V is

FE2A9433 C1E3B5F1 6C4FE36B 02DF38F5

Update

provided_data is
FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6
7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39

While loop

Key is

2770FD70 A5E4196E
901A5ECF E0F8F0D1 C6E1179F EDA3F178 F03EEB70 12399EBA

V is

FE2A9433 C1E3B5F1 6C4FE36B 02DF38F8

output_block is

B0B737AF E2DDCB5C 9DBF368E 333CA850

temp is

B0B737AF E2DDCB5C 9DBF368E 333CA850

While loop

Key is

2770FD70 A5E4196E
901A5ECF E0F8F0D1 C6E1179F EDA3F178 F03EEB70 12399EBA

V is

FE2A9433 C1E3B5F1 6C4FE36B 02DF38F9

output_block is

8B3EB1AA 3B9DEBFA 903BD057 130CC025

temp is

B0B737AF E2DDCB5C

9DBF368E 333CA850 8B3EB1AA 3B9DEBFA 903BD057 130CC025

While loop

Key is

2770FD70 A5E4196E
901A5ECF E0F8F0D1 C6E1179F EDA3F178 F03EEB70 12399EBA

V is

FE2A9433 C1E3B5F1 6C4FE36B 02DF38FA

output_block is

524C2048 99A54528 C304AE71 1F5A57DF

temp is

B0B737AF E2DDCB5C 9DBF368E 333CA850 8B3EB1AA 3B9DEBFA
903BD057 130CC025 524C2048 99A54528 C304AE71 1F5A57DF

temp XOR provided_data is

4B67289A 9FC9F43F 907FD177 87B10421 CF3266FA 9DBB364C
E77F2D4E CCA51206 A96DFE6B 3C4309C8 B22B4636 B0135BE6

Key is

4B67289A 9FC9F43F
907FD177 87B10421 CF3266FA 9DBB364C E77F2D4E CCA51206

V is

A96DFE6B 3C4309C8 B22B4636 B0135BE6

rnd_val is

81DAAF98 00C34FF0
A104E51D 87E36F5B 17EB14B9 ABC5064C ADDA976E C4F77D34

#####

CTR_DRBG

Requested Security Strength = 256

```
prediction_resistance_flag = "NOT ENABLED"  
EntropyInput =  
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617  
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
```

```
EntropyInput1 (for Reseed1) =  
    80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697  
    98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
```

```
EntropyInput2 (for Reseed2) =  
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7  
    D8D9DADB DCDDDED F E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
```

```
Nonce =  
    20212223 24252627 28292A2B 2C2D2E2F
```

```
PersonalizationString =  
    40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657  
    58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F
```

AdditionalInput = <empty>

#####

CTR_DRBG_Instantiate_algorithm - with derivation function

```
entropy_input is  
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617  
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
```

```
nonce is  
    20212223 24252627 28292A2B 2C2D2E2F
```

```
personal_str is
    40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
    58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F
```

```
prediction_resistance_flag = "No PredictionResistance"
```

```
-----
```

```
Block_Cipher_df
```

```
input_str is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
    28292A2B 2C2D2E2F 20212223 24252627 28292A2B 2C2D2E2F
    40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
    58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F
```

```
number_of_bits_to_return = 384
```

```
S is
```

```
    00000070 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
    60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000
```

```
-----
```

```
BCC
```

```
IV is
```

```
    00000000 00000000 00000000 00000000
```

```
IV || S is
```

```
    00000000 00000000 00000000 00000000 00000070 00000030
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
    20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
    48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
    60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000
```

temp is

8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000 00000070 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000

temp is

8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000 00000000 00000000 00000070 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000

temp is

8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08 A13B6B8D A420CCBC

43CF57C7 F3A7C718 2B4B429F EDFD2D2D 937CA4B4 71B86606

Key is

8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

X is

2B4B429F EDFD2D2D 937CA4B4 71B86606

BlockEncrypt

Key is

8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

X is

2B4B429F EDFD2D2D 937CA4B4 71B86606

X = BlockEncrypt(Key, X) is

31D82952 CBF4754A 1354F1A9 184841B4

temp is

31D82952 CBF4754A 1354F1A9 184841B4

BlockEncrypt

Key is

8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

X is

31D82952 CBF4754A 1354F1A9 184841B4

```
X = BlockEncrypt(Key, X) is  
    C0812181 C179FD79 547E5367 AB8C9FA4
```

```
temp is  
    31D82952 CBF4754A  
    1354F1A9 184841B4 C0812181 C179FD79 547E5367 AB8C9FA4
```

```
BlockEncrypt
```

```
Key is  
    8A0B0FB5 AA3FA8FD  
    4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718
```

```
X is  
    C0812181 C179FD79 547E5367 AB8C9FA4
```

```
X = BlockEncrypt(Key, X) is  
    51223D14 E89B833F 62FC5EF8 0034A200
```

```
temp is  
    31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79  
    547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200
```

```
requested_bits is  
    31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79  
    547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200
```

```
seed_material is  
    31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79  
    547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200
```

```
Update
```

provided_data is
31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200

While loop

Key is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is

530F8AFB C74536B9 A963B4F1 C4CB738B

temp is

530F8AFB C74536B9 A963B4F1 C4CB738B

While loop

Key is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

CEA7403D 4D606B6E 074EC5D3 BAF39D18

temp is

530F8AFB C74536B9

A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18

While loop

Key is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000003

output_block is

726003CA 37A62A74 D1A2F58E 7506358E

temp is

530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E

temp XOR provided_data is

62D7A3A9 0CB143F3 BA374558 DC83323F 0E2661BC 8C199617
533096B4 117F02BC 23423EDE DF3DA94B B35EAB76 7532978E

Key is

62D7A3A9 0CB143F3
BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is

23423EDE DF3DA94B B35EAB76 7532978E

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

62D7A3A9 0CB143F3
BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is

23423EDE DF3DA94B B35EAB76 75329791

output_block is

40A4397E 72F15782 98F8B8FB 54A8BAD1

temp is

40A4397E 72F15782 98F8B8FB 54A8BAD1

While loop

Key is

62D7A3A9 0CB143F3
BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is

23423EDE DF3DA94B B35EAB76 75329792

output_block is
6526C8ED 91619BBF 3F3FEEA1 5FCB3AF5

temp is
40A4397E 72F15782
98F8B8FB 54A8BAD1 6526C8ED 91619BBF 3F3FEEA1 5FCB3AF5

While loop

Key is
62D7A3A9 0CB143F3
BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is
23423EDE DF3DA94B B35EAB76 75329793

output_block is
E901923A FE17A74F 53B00B2F 3E5148B5

temp is
40A4397E 72F15782 98F8B8FB 54A8BAD1 6526C8ED 91619BBF
3F3FEEA1 5FCB3AF5 E901923A FE17A74F 53B00B2F 3E5148B5

temp XOR provided_data is
40A4397E 72F15782 98F8B8FB 54A8BAD1 6526C8ED 91619BBF
3F3FEEA1 5FCB3AF5 E901923A FE17A74F 53B00B2F 3E5148B5

Key is
40A4397E 72F15782
98F8B8FB 54A8BAD1 6526C8ED 91619BBF 3F3FEEA1 5FCB3AF5

V is
E901923A FE17A74F 53B00B2F 3E5148B5

rnd_val is

99BB703C DD820609
903F1241 EA856E27 A54C2B75 EEA7775B 68093FCD 47B52E7F

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

40A4397E 72F15782
98F8B8FB 54A8BAD1 6526C8ED 91619BBF 3F3FEEA1 5FCB3AF5

V is

E901923A FE17A74F 53B00B2F 3E5148B8

output_block is

97308A02 E0455DC1 73380181 249766FC

temp is

97308A02 E0455DC1 73380181 249766FC

While loop

Key is

40A4397E 72F15782
98F8B8FB 54A8BAD1 6526C8ED 91619BBF 3F3FEEA1 5FCB3AF5

V is

E901923A FE17A74F 53B00B2F 3E5148B9

output_block is

79B62BE6 8C41B2F2 748E07E0 E4D0AF8B

temp is

97308A02 E0455DC1
73380181 249766FC 79B62BE6 8C41B2F2 748E07E0 E4D0AF8B

While loop

Key is

40A4397E 72F15782
98F8B8FB 54A8BAD1 6526C8ED 91619BBF 3F3FEEA1 5FCB3AF5

V is

E901923A FE17A74F 53B00B2F 3E5148BA

output_block is

D0938581 D7C44751 1FF4F5C9 00972CE0

temp is

97308A02 E0455DC1 73380181 249766FC 79B62BE6 8C41B2F2
748E07E0 E4D0AF8B D0938581 D7C44751 1FF4F5C9 00972CE0

```
temp XOR provided_data is  
97308A02 E0455DC1 73380181 249766FC 79B62BE6 8C41B2F2  
748E07E0 E4D0AF8B D0938581 D7C44751 1FF4F5C9 00972CE0
```

Key is

```
97308A02 E0455DC1  
73380181 249766FC 79B62BE6 8C41B2F2 748E07E0 E4D0AF8B
```

V is

```
D0938581 D7C44751 1FF4F5C9 00972CE0
```

rnd_val is

```
BB2A0F5F 0CA6D306  
34BA6068 EB94AAE8 701437DB 7223A1B5 AFE87715 47DA3CEE
```

```
#####
```

CTR_DRBG

Requested Security Strength = 256

```
prediction_resistance_flag = "NOT ENABLED"  
EntropyInput =  
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617  
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
```

```
EntropyInput1 (for Reseed1) =  
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697  
98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
```

```
EntropyInput2 (for Reseed2) =  
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7  
D8D9DADB DCDDDED7 E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
```

Nonce =

```
20212223 24252627 28292A2B 2C2D2E2F
```

PersonalizationString =

```
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657  
58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F
```

```
AdditionalInput1 =  
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677  
78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F
```

```
AdditionalInput2 =  
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7  
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
```

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

```
*****
```

```
CTR_DRBG_Instantiate_algorithm - with derivation function
```

```
entropy_input is  
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617  
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
```

```
nonce is
```

```
20212223 24252627 28292A2B 2C2D2E2F
```

```
personal_str is
```

```
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657  
58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F
```

```
prediction_resistance_flag = "No PredictionResistance"
```

```
-----
```

```
Block_Cipher_df
```

```
input_str is  
00010203 04050607 08090A0B 0C0D0E0F  
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627  
28292A2B 2C2D2E2F 20212223 24252627 28292A2B 2C2D2E2F  
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657  
58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F
```

```
number_of_bits_to_return = 384
```

S is

```
00000070 00000030  
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617  
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F  
20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647  
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F  
60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000
```

BCC

IV is

```
00000000 00000000 00000000 00000000
```

IV || S is

```
00000000 00000000 00000000 00000000 00000070 00000030  
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617  
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F  
20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647  
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F  
60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000
```

temp is

```
8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08
```

BCC

IV is

```
00000001 00000000 00000000 00000000
```

IV || S is

```
00000001 00000000 00000000 00000070 00000030  
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617  
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
```

20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000

temp is

8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000 00000000 00000000 00000070 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000

temp is

8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08 A13B6B8D A420CCBC
43CF57C7 F3A7C718 2B4B429F EDFD2D2D 937CA4B4 71B86606

Key is

8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

X is

2B4B429F EDFD2D2D 937CA4B4 71B86606

BlockEncrypt

Key is

8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

X is

2B4B429F EDFD2D2D 937CA4B4 71B86606

X = BlockEncrypt(Key, X) is

31D82952 CBF4754A 1354F1A9 184841B4

temp is

31D82952 CBF4754A 1354F1A9 184841B4

BlockEncrypt

Key is

8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

X is

31D82952 CBF4754A 1354F1A9 184841B4

X = BlockEncrypt(Key, X) is

C0812181 C179FD79 547E5367 AB8C9FA4

temp is

31D82952 CBF4754A
1354F1A9 184841B4 C0812181 C179FD79 547E5367 AB8C9FA4

BlockEncrypt

Key is

8A0B0FB5 AA3FA8FD

4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

X is

C0812181 C179FD79 547E5367 AB8C9FA4

X = BlockEncrypt(Key, X) is

51223D14 E89B833F 62FC5EF8 0034A200

temp is

31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200

requested_bits is

31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200

seed_material is

31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200

Update

provided_data is

31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200

While loop

Key is

00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is
530F8AFB C74536B9 A963B4F1 C4CB738B

temp is
530F8AFB C74536B9 A963B4F1 C4CB738B

While loop

Key is
00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000002

output_block is
CEA7403D 4D606B6E 074EC5D3 BAF39D18

temp is
530F8AFB C74536B9
A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18

While loop

Key is
00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000003

output_block is

726003CA 37A62A74 D1A2F58E 7506358E

temp is

530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E

temp XOR provided_data is

62D7A3A9 0CB143F3 BA374558 DC83323F 0E2661BC 8C199617
533096B4 117F02BC 23423EDE DF3DA94B B35EAB76 7532978E

Key is

62D7A3A9 0CB143F3
BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is

23423EDE DF3DA94B B35EAB76 7532978E

First call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is

60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F

additional_input <> NULL, process appropriately

Block_Cipher_df

input_str is

60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F

number_of_bits_to_return = 384

S is

00000030 00000030 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000030 00000030 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

temp is

DE8D1951 762E5557 CFAE1170 EEF4B933

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000
00000000 00000000 00000030 00000030 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

temp is

DE8D1951 762E5557
CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000

00000000 00000000 00000030 00000030 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

temp is

DE8D1951 762E5557 CFAE1170 EEF4B933 F9C0BD35 6D5244B9
158CEE79 08C40855 6254BE89 B2960465 D4879231 3E993E48

Key is

DE8D1951 762E5557

CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855

X is

6254BE89 B2960465 D4879231 3E993E48

BlockEncrypt

Key is

DE8D1951 762E5557

CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855

X is

6254BE89 B2960465 D4879231 3E993E48

X = BlockEncrypt(Key, X) is
4D8C89E0 1B308B59 E99AE0AD 702902F8

temp is
4D8C89E0 1B308B59 E99AE0AD 702902F8

BlockEncrypt

Key is
DE8D1951 762E5557
CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855

X is
4D8C89E0 1B308B59 E99AE0AD 702902F8

X = BlockEncrypt(Key, X) is
249768D0 97B4C73B CCFCD763 CD5AC761

temp is
4D8C89E0 1B308B59
E99AE0AD 702902F8 249768D0 97B4C73B CCFCD763 CD5AC761

BlockEncrypt

Key is
DE8D1951 762E5557
CFAE1170 EEF4B933 F9C0BD35 6D5244B9 158CEE79 08C40855

X is
249768D0 97B4C73B CCFCD763 CD5AC761

X = BlockEncrypt(Key, X) is
9267624C 0952CA7B A8ACDFCC E2A669D5

temp is
4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
CCFC763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5

requested_bits is
4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
CCFC763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5

Update

provided_data is
4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
CCFC763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5

While loop

Key is
62D7A3A9 0CB143F3
BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is
23423EDE DF3DA94B B35EAB76 7532978F

output_block is
99BB703C DD820609 903F1241 EA856E27

temp is
99BB703C DD820609 903F1241 EA856E27

While loop

Key is

62D7A3A9 0CB143F3
BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is

23423EDE DF3DA94B B35EAB76 75329790

output_block is

A54C2B75 EEA7775B 68093FCD 47B52E7F

temp is

99BB703C DD820609
903F1241 EA856E27 A54C2B75 EEA7775B 68093FCD 47B52E7F

While loop

Key is

62D7A3A9 0CB143F3
BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is

23423EDE DF3DA94B B35EAB76 75329791

output_block is

40A4397E 72F15782 98F8B8FB 54A8BAD1

temp is

99BB703C DD820609 903F1241 EA856E27 A54C2B75 EEA7775B
68093FCD 47B52E7F 40A4397E 72F15782 98F8B8FB 54A8BAD1

temp XOR provided_data is

D437F9DC C6B28D50 79A5F2EC 9AAC6CDF 81DB43A5 7913B060
A4F5E8AE 8AEFE91E D2C35B32 7BA39DF9 30546737 B60ED304

Key is

D437F9DC C6B28D50

79A5F2EC 9AAC6CDF 81DB43A5 7913B060 A4F5E8AE 8AEFE91E

V is

D2C35B32 7BA39DF9 30546737 B60ED304

Update

provided_data is

4D8C89E0 1B308B59 E99AE0AD 702902F8 249768D0 97B4C73B
CCFC763 CD5AC761 9267624C 0952CA7B A8ACDFCC E2A669D5

While loop

Key is

D437F9DC C6B28D50

79A5F2EC 9AAC6CDF 81DB43A5 7913B060 A4F5E8AE 8AEFE91E

V is

D2C35B32 7BA39DF9 30546737 B60ED307

output_block is

94AC6E07 4D46CB0B 15C13188 C79E747F

temp is

94AC6E07 4D46CB0B 15C13188 C79E747F

While loop

Key is

D437F9DC C6B28D50

79A5F2EC 9AAC6CDF 81DB43A5 7913B060 A4F5E8AE 8AEFE91E

V is

D2C35B32 7BA39DF9 30546737 B60ED308

output_block is

26AE0E89 253EAFF2 A663DC6E 9347201D

temp is

94AC6E07 4D46CB0B

15C13188 C79E747F 26AE0E89 253EAFF2 A663DC6E 9347201D

While loop

Key is

D437F9DC C6B28D50

79A5F2EC 9AAC6CDF 81DB43A5 7913B060 A4F5E8AE 8AEFE91E

V is

D2C35B32 7BA39DF9 30546737 B60ED309

output_block is

67A42F29 2DFD819B 1A2BE5DD 18496C49

temp is

94AC6E07 4D46CB0B 15C13188 C79E747F 26AE0E89 253EAFF2

A663DC6E 9347201D 67A42F29 2DFD819B 1A2BE5DD 18496C49

temp XOR provided_data is

D920E7E7 56764052 FC5BD125 B7B77687 02396659 B28A68C9

6A9F0B0D 5E1DE77C F5C34D65 24AF4BE0 B2873A11 FAEF059C

Key is

D920E7E7 56764052

FC5BD125 B7B77687 02396659 B28A68C9 6A9F0B0D 5E1DE77C

V is

F5C34D65 24AF4BE0 B2873A11 FAEF059C

rnd_val is

47111E14 6562E9AA
2FB2A1B0 95D37A81 65AF8FC7 CA611D63 2BE7D4C1 45C83900

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is

A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

additional_input <> NULL, process appropriately

Block_Cipher_df

input_str is

A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

number_of_bits_to_return = 384

S is

00000030 00000030 A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000

00000000 00000000 00000030 00000030 A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

temp is

BC61575C 5D4B8037 C9E380B9 3E376057

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000

00000000 00000000 00000030 00000030 A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

temp is

BC61575C 5D4B8037

C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000

00000000 00000000 00000030 00000030 A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF

C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

temp is

BC61575C 5D4B8037 C9E380B9 3E376057 2C0B3606 11252C52
85BDEC6C 567C9B5A F6259D1D 3848CC93 296E04B5 AD60A97F

Key is

BC61575C 5D4B8037
C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A

X is

F6259D1D 3848CC93 296E04B5 AD60A97F

BlockEncrypt

Key is

BC61575C 5D4B8037
C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A

X is

F6259D1D 3848CC93 296E04B5 AD60A97F

X = BlockEncrypt(Key, X) is

FBD01F35 7D143F63 0DC0E7F9 B48DAC71

temp is

FBD01F35 7D143F63 0DC0E7F9 B48DAC71

BlockEncrypt

Key is

BC61575C 5D4B8037

C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A

X is

FBD01F35 7D143F63 0DC0E7F9 B48DAC71

X = BlockEncrypt(Key, X) is

440CD750 A626DDB6 7744FD19 DFA9D223

temp is

FBD01F35 7D143F63

0DC0E7F9 B48DAC71 440CD750 A626DDB6 7744FD19 DFA9D223

BlockEncrypt

Key is

BC61575C 5D4B8037

C9E380B9 3E376057 2C0B3606 11252C52 85BDEC6C 567C9B5A

X is

440CD750 A626DDB6 7744FD19 DFA9D223

X = BlockEncrypt(Key, X) is

FB21DE23 A5E64CE0 712FE847 AF490C39

temp is

FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6

7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39

requested_bits is

FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6

7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39

Update

provided_data is
FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6
7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39

While loop

Key is

D920E7E7 56764052
FC5BD125 B7B77687 02396659 B28A68C9 6A9F0B0D 5E1DE77C

V is

F5C34D65 24AF4BE0 B2873A11 FAEF059D

output_block is

39AEAB48 6D431EA6 FA729E7B 8DE7EEBC

temp is

39AEAB48 6D431EA6 FA729E7B 8DE7EEBC

While loop

Key is

D920E7E7 56764052
FC5BD125 B7B77687 02396659 B28A68C9 6A9F0B0D 5E1DE77C

V is

F5C34D65 24AF4BE0 B2873A11 FAEF059E

output_block is

2B974223 14E62662 B5292502 EF19F208

temp is

39AEAB48 6D431EA6

FA729E7B 8DE7EEBC 2B974223 14E62662 B5292502 EF19F208

While loop

Key is

D920E7E7 56764052

FC5BD125 B7B77687 02396659 B28A68C9 6A9F0B0D 5E1DE77C

V is

F5C34D65 24AF4BE0 B2873A11 FAEF059F

output_block is

5481D794 AEA9149 3D37E5F4 7344631E

temp is

39AEAB48 6D431EA6 FA729E7B 8DE7EEBC 2B974223 14E62662

B5292502 EF19F208 5481D794 AEA9149 3D37E5F4 7344631E

temp XOR provided_data is

C27EB47D 105721C5 F7B27982 396A42CD 6F9B9573 B2C0FBD4

C26DD81B 30B0202B AFA009B7 0B49DDA9 4C180DB3 DC0D6F27

Key is

C27EB47D 105721C5

F7B27982 396A42CD 6F9B9573 B2C0FBD4 C26DD81B 30B0202B

V is

AFA009B7 0B49DDA9 4C180DB3 DC0D6F27

Update

provided_data is

FBD01F35 7D143F63 0DC0E7F9 B48DAC71 440CD750 A626DDB6

7744FD19 DFA9D223 FB21DE23 A5E64CE0 712FE847 AF490C39

While loop

Key is

C27EB47D 105721C5
F7B27982 396A42CD 6F9B9573 B2C0FBD4 C26DD81B 30B0202B

V is

AFA009B7 0B49DDA9 4C180DB3 DC0D6F2A

output_block is

776A18C9 10E930E6 01A81AFA F27A254B

temp is

776A18C9 10E930E6 01A81AFA F27A254B

While loop

Key is

C27EB47D 105721C5
F7B27982 396A42CD 6F9B9573 B2C0FBD4 C26DD81B 30B0202B

V is

AFA009B7 0B49DDA9 4C180DB3 DC0D6F2B

output_block is

6249277E C60F443C CBD11B72 DCB63E6F

temp is

776A18C9 10E930E6
01A81AFA F27A254B 6249277E C60F443C CBD11B72 DCB63E6F

While loop

Key is

C27EB47D 105721C5
F7B27982 396A42CD 6F9B9573 B2C0FBD4 C26DD81B 30B0202B

V is

AFA009B7 0B49DDA9 4C180DB3 DC0D6F2C

output_block is

8FF0B81F D441A1C7 66FFCFD0 EFAFCA4D

temp is

776A18C9 10E930E6 01A81AFA F27A254B 6249277E C60F443C
CBD11B72 DCB63E6F 8FF0B81F D441A1C7 66FFCFD0 EFAFCA4D

temp XOR provided_data is

8CBA07FC 6DFD0F85 0C68FD03 46F7893A 2645F02E 6029998A
BC95E66B 031FEC4C 74D1663C 71A7ED27 17D02797 40E6C674

Key is

8CBA07FC 6DFD0F85
0C68FD03 46F7893A 2645F02E 6029998A BC95E66B 031FEC4C

V is

74D1663C 71A7ED27 17D02797 40E6C674

rnd_val is

98A28E3B 1BA363C9
DAF0F688 7A1CF52B 833D3354 D77A7C10 837DD63D D2E645F8

#####

CTR_DRBG

Requested Security Strength = 256

```
prediction_resistance_flag = "ENABLED"
EntropyInput =
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
```

```
EntropyInput1 (for Reseed1) =
    80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
    98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
```

```
EntropyInput2 (for Reseed2) =
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
    D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
```

```
Nonce =
    20212223 24252627 28292A2B 2C2D2E2F
```

```
PersonalizationString = <empty>
```

```
AdditionalInput = <empty>
```

```
#####
*****
```

```
*****
```

```
CTR_DRBG_Instantiate_algorithm - with derivation function
```

```
entropy_input is
    00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
    18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
```

```
nonce is
    20212223 24252627 28292A2B 2C2D2E2F
```

```
personal_str is <empty>
```

```
prediction_resistance_flag = "PredictionResistance"
```

```
-----
```

```
Block_Cipher_df
```

input_str is

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

number_of_bits_to_return = 384

S is

00000040 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000000 00000040 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000

temp is

4BC4520F E87668A3 A2CE3DCB 5F564BA9

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000000 00000040 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617

18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000

temp is

4BC4520F E87668A3
A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000 00000000 00000000 00000040 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000

temp is

4BC4520F E87668A3 A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB
9C275423 0F4E6DC4 8283F162 52D8520F D651F481 64D42EC9

Key is

4BC4520F E87668A3
A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is

8283F162 52D8520F D651F481 64D42EC9

BlockEncrypt

Key is

4BC4520F E87668A3

A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is

8283F162 52D8520F D651F481 64D42EC9

X = BlockEncrypt(Key, X) is

DF1F3CA3 8349478C CDFE738A 222E0645

temp is

DF1F3CA3 8349478C CDFE738A 222E0645

BlockEncrypt

Key is

4BC4520F E87668A3

A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is

DF1F3CA3 8349478C CDFE738A 222E0645

X = BlockEncrypt(Key, X) is

494008AD CEFBE237 13596A7E AE41BBCD

temp is

DF1F3CA3 8349478C

CDFE738A 222E0645 494008AD CEFBE237 13596A7E AE41BBCD

BlockEncrypt

Key is

4BC4520F E87668A3

A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is

494008AD CEFBE237 13596A7E AE41BBCD

X = BlockEncrypt(Key, X) is

C66368D7 8DA21092 840E23C8 995CE6D2

temp is

DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

requested_bits is

DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

seed_material is

DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

Update

provided_data is

DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

While loop

Key is

00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is

530F8AFB C74536B9 A963B4F1 C4CB738B

temp is

530F8AFB C74536B9 A963B4F1 C4CB738B

While loop

Key is

00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

CEA7403D 4D606B6E 074EC5D3 BAF39D18

temp is

530F8AFB C74536B9

A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18

While loop

Key is

00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000003

output_block is

726003CA 37A62A74 D1A2F58E 7506358E

```
temp is
530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E
```

```
temp XOR provided_data is
8C10B658 440C7135 649DC77B E6E575CE 87E74890 839B8959
1417AFAD 14B226D5 B4036B1D BA043AE6 55ACD646 EC5AD35C
```

Key is

```
8C10B658 440C7135
649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5
```

V is

```
B4036B1D BA043AE6 55ACD646 EC5AD35C
```

First call to Generate

```
*****
```

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Generate FAILED: Reseed is required

```
*****
```

CTR_DRBG_Reseed

entropy_input is
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEEF

additional_input is <empty>

Block_Cipher_df

input_str is
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697
98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF

number_of_bits_to_return = 384

S is
00000030 00000030 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000

BCC

IV is
00000000 00000000 00000000 00000000

IV || S is
00000000 00000000
00000000 00000000 00000030 00000030 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000

temp is
6808E8C2 37359B53 E4AC883F 8D22A1CA

BCC

IV is
00000001 00000000 00000000 00000000

IV || S is
00000001 00000000
00000000 00000000 00000030 00000030 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000

temp is
6808E8C2 37359B53
E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6

BCC

IV is
00000002 00000000 00000000 00000000

IV || S is
00000002 00000000
00000000 00000000 00000030 00000030 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000

temp is
6808E8C2 37359B53 E4AC883F 8D22A1CA DC9A2BCF C2C81F7F
F712FC22 E18D59F6 D870D670 2017B3B4 5327BDD3 E5D50B51

Key is
6808E8C2 37359B53
E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6

X is
D870D670 2017B3B4 5327BDD3 E5D50B51

BlockEncrypt

Key is
6808E8C2 37359B53
E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6

X is

D870D670 2017B3B4 5327BDD3 E5D50B51

X = BlockEncrypt(Key, X) is

F11E1D8A FE3197D7 A33A494B 9676DBF2

temp is

F11E1D8A FE3197D7 A33A494B 9676DBF2

BlockEncrypt

Key is

6808E8C2 37359B53

E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6

X is

F11E1D8A FE3197D7 A33A494B 9676DBF2

X = BlockEncrypt(Key, X) is

27E44756 CA44780C C36E0AA3 895C552E

temp is

F11E1D8A FE3197D7

A33A494B 9676DBF2 27E44756 CA44780C C36E0AA3 895C552E

BlockEncrypt

Key is

6808E8C2 37359B53

E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6

X is

27E44756 CA44780C C36E0AA3 895C552E

```
X = BlockEncrypt(Key, X) is  
    6301C157 C36F26C4 986874E7 698ECCFD
```

```
temp is  
    F11E1D8A FE3197D7 A33A494B 9676DBF2 27E44756 CA44780C  
    C36E0AA3 895C552E 6301C157 C36F26C4 986874E7 698ECCFD
```

```
requested_bits is  
    F11E1D8A FE3197D7 A33A494B 9676DBF2 27E44756 CA44780C  
    C36E0AA3 895C552E 6301C157 C36F26C4 986874E7 698ECCFD
```

Update

```
provided_data is  
    F11E1D8A FE3197D7 A33A494B 9676DBF2 27E44756 CA44780C  
    C36E0AA3 895C552E 6301C157 C36F26C4 986874E7 698ECCFD
```

While loop

```
Key is  
    8C10B658 440C7135  
    649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5
```

```
V is  
    B4036B1D BA043AE6 55ACD646 EC5AD35D
```

```
output_block is  
    E686DD55 F758FD91 BA7CB726 FE0B573A
```

```
temp is  
    E686DD55 F758FD91 BA7CB726 FE0B573A
```

While loop

Key is

8C10B658 440C7135
649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5

V is

B4036B1D BA043AE6 55ACD646 EC5AD35E

output_block is

180AB674 39FFBDDE 5EC28FB3 7A16A53B

temp is

E686DD55 F758FD91
BA7CB726 FE0B573A 180AB674 39FFBDDE 5EC28FB3 7A16A53B

While loop

Key is

8C10B658 440C7135
649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5

V is

B4036B1D BA043AE6 55ACD646 EC5AD35F

output_block is

68F2F51A 364601AF 9533C864 F25DA997

temp is

E686DD55 F758FD91 BA7CB726 FE0B573A 180AB674 39FFBDDE
5EC28FB3 7A16A53B 68F2F51A 364601AF 9533C864 F25DA997

temp XOR provided_data is

1798C0DF 09696A46 1946FE6D 687D8CC8 3FEEF122 F3BBC5F2

9DAC8510 F34AF015 0BF3344D F529276B 0D5BBC83 9BD3656A

Key is

1798C0DF 09696A46

1946FE6D 687D8CC8 3FEEF122 F3BBC5F2 9DAC8510 F34AF015

V is

0BF3344D F529276B 0D5BBC83 9BD3656A

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000 00000000 00000000 00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

1798C0DF 09696A46

1946FE6D 687D8CC8 3FEEF122 F3BBC5F2 9DAC8510 F34AF015

V is

0BF3344D F529276B 0D5BBC83 9BD3656D

output_block is

28BC65A8 6AB7C74E DF4BB872 87D34FBB

temp is
28BC65A8 6AB7C74E DF4BB872 87D34FBB

While loop

Key is
1798C0DF 09696A46
1946FE6D 687D8CC8 3FEEF122 F3BBC5F2 9DAC8510 F34AF015

V is

0BF3344D F529276B 0D5BBC83 9BD3656E

output_block is
8D6F16D7 B91B6ABB EE7B8886 5B0FC7BD

temp is
28BC65A8 6AB7C74E
DF4BB872 87D34FBB 8D6F16D7 B91B6ABB EE7B8886 5B0FC7BD

While loop

Key is
1798C0DF 09696A46
1946FE6D 687D8CC8 3FEEF122 F3BBC5F2 9DAC8510 F34AF015

V is

0BF3344D F529276B 0D5BBC83 9BD3656F

output_block is
B74611F3 9295A625 7C39984C 9C099B30

temp is
28BC65A8 6AB7C74E DF4BB872 87D34FBB 8D6F16D7 B91B6ABB
EE7B8886 5B0FC7BD B74611F3 9295A625 7C39984C 9C099B30

```
temp XOR provided_data is
    28BC65A8 6AB7C74E DF4BB872 87D34FBB 8D6F16D7 B91B6ABB
    EE7B8886 5B0FC7BD B74611F3 9295A625 7C39984C 9C099B30
```

Key is

```
    28BC65A8 6AB7C74E
    DF4BB872 87D34FBB 8D6F16D7 B91B6ABB EE7B8886 5B0FC7BD
```

V is

```
    B74611F3 9295A625 7C39984C 9C099B30
```

rnd_val is

```
    D1E9C737 B6EBAED7
    65A0D4E4 C6EAEBE2 67F5E919 3680FDFF A62F4865 B3F009EC
```

Second call to Generate

```
*****
```

CTR_DRBG_Generate

```
requested_number_of_bits = 256
```

```
additional_input is <empty>
```

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

```
*****
```

CTR_DRBG_Reseed

```
entropy_input is
```

```
    C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
    D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
```

```
additional_input is <empty>
```

Block_Cipher_df

input_str is
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF

number_of_bits_to_return = 384

S is

00000030 00000030 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000030 00000030 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000

temp is

F2977267 80DDB539 4AFDD5B8 CCC350C9

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000
00000000 00000000 00000030 00000030 C0C1C2C3 C4C5C6C7

C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000

temp is

F2977267 80DDB539
4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000
00000000 00000000 00000030 00000030 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000

temp is

F2977267 80DDB539 4AFDD5B8 CCC350C9 AA2EF303 87F07708
919EA794 06ADEF9B 31221A7E 3A0CE21C 54C7074E 0C011CA8

Key is

F2977267 80DDB539
4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B

X is

31221A7E 3A0CE21C 54C7074E 0C011CA8

BlockEncrypt

Key is

F2977267 80DDB539

4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B

X is

31221A7E 3A0CE21C 54C7074E 0C011CA8

X = BlockEncrypt(Key, X) is

AAA32C63 E6A3FED3 B6787677 D5867143

temp is

AAA32C63 E6A3FED3 B6787677 D5867143

BlockEncrypt

Key is

F2977267 80DDB539

4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B

X is

AAA32C63 E6A3FED3 B6787677 D5867143

X = BlockEncrypt(Key, X) is

F04E8A91 0E0A3F2F A7CDDD9B 8D03090C

temp is

AAA32C63 E6A3FED3

B6787677 D5867143 F04E8A91 0E0A3F2F A7CDDD9B 8D03090C

BlockEncrypt

Key is

F2977267 80DDB539

4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B

X is

F04E8A91 0E0A3F2F A7CDDD9B 8D03090C

X = BlockEncrypt(Key, X) is

E74B09AD 16BC3C53 457691EE BC770472

temp is

AAA32C63 E6A3FED3 B6787677 D5867143 F04E8A91 0E0A3F2F
A7CDDD9B 8D03090C E74B09AD 16BC3C53 457691EE BC770472

requested_bits is

AAA32C63 E6A3FED3 B6787677 D5867143 F04E8A91 0E0A3F2F
A7CDDD9B 8D03090C E74B09AD 16BC3C53 457691EE BC770472

Update

provided_data is

AAA32C63 E6A3FED3 B6787677 D5867143 F04E8A91 0E0A3F2F
A7CDDD9B 8D03090C E74B09AD 16BC3C53 457691EE BC770472

While loop

Key is

28BC65A8 6AB7C74E

DF4BB872 87D34FBB 8D6F16D7 B91B6ABB EE7B8886 5B0FC7BD

V is

B74611F3 9295A625 7C39984C 9C099B31

output_block is

7ECAD37E 8013E170 208C17FB 03A50642

temp is

7ECAD37E 8013E170 208C17FB 03A50642

While loop

Key is

28BC65A8 6AB7C74E
DF4BB872 87D34FBB 8D6F16D7 B91B6ABB EE7B8886 5B0FC7BD

V is

B74611F3 9295A625 7C39984C 9C099B32

output_block is

ED31FE00 EE996396 816BAF1B 7071AF4D

temp is

7ECAD37E 8013E170
208C17FB 03A50642 ED31FE00 EE996396 816BAF1B 7071AF4D

While loop

Key is

28BC65A8 6AB7C74E
DF4BB872 87D34FBB 8D6F16D7 B91B6ABB EE7B8886 5B0FC7BD

V is

B74611F3 9295A625 7C39984C 9C099B33

output_block is

35C0BF18 C24A77A2 20585DEB 469B94B6

temp is

7ECAD37E 8013E170 208C17FB 03A50642 ED31FE00 EE996396
816BAF1B 7071AF4D 35C0BF18 C24A77A2 20585DEB 469B94B6

```
temp XOR provided_data is  
D469FF1D 66B01FA3 96F4618C D6237701 1D7F7491 E0935CB9  
26A67280 FD72A641 D28BB6B5 D4F64BF1 652ECC05 FAEC90C4
```

Key is

```
D469FF1D 66B01FA3  
96F4618C D6237701 1D7F7491 E0935CB9 26A67280 FD72A641
```

V is

```
D28BB6B5 D4F64BF1 652ECC05 FAEC90C4
```

```
*****
```

CTR_DRBG_Generate

```
requested_number_of_bits = 256
```

```
additional_input is <empty>
```

```
-----
```

Update

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

```
-----
```

While loop

Key is

```
D469FF1D 66B01FA3  
96F4618C D6237701 1D7F7491 E0935CB9 26A67280 FD72A641
```

V is

```
D28BB6B5 D4F64BF1 652ECC05 FAEC90C7
```

output_block is

```
9659D767 B5C6A2BF 0F2D0368 D72322E0
```

temp is

9659D767 B5C6A2BF 0F2D0368 D72322E0

While loop

Key is

D469FF1D 66B01FA3

96F4618C D6237701 1D7F7491 E0935CB9 26A67280 FD72A641

V is

D28BB6B5 D4F64BF1 652ECC05 FAEC90C8

output_block is

2B75794A 587DC968 48AB97AE EBA2ED8D

temp is

9659D767 B5C6A2BF

0F2D0368 D72322E0 2B75794A 587DC968 48AB97AE EBA2ED8D

While loop

Key is

D469FF1D 66B01FA3

96F4618C D6237701 1D7F7491 E0935CB9 26A67280 FD72A641

V is

D28BB6B5 D4F64BF1 652ECC05 FAEC90C9

output_block is

C7B0D234 2F4275B4 28F8D432 2201BCC7

temp is

```
9659D767 B5C6A2BF 0F2D0368 D72322E0 2B75794A 587DC968  
48AB97AE EBA2ED8D C7B0D234 2F4275B4 28F8D432 2201BCC7
```

```
temp XOR provided_data is  
9659D767 B5C6A2BF 0F2D0368 D72322E0 2B75794A 587DC968  
48AB97AE EBA2ED8D C7B0D234 2F4275B4 28F8D432 2201BCC7
```

Key is

```
9659D767 B5C6A2BF  
0F2D0368 D72322E0 2B75794A 587DC968 48AB97AE EBA2ED8D
```

V is

```
C7B0D234 2F4275B4 28F8D432 2201BCC7
```

rnd_val is

```
259DC78C CFAEC421  
0C30AF81 5E4F75A5 662B7DA4 B41013BD C00302DF B6076492
```

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

CTR_DRBG

Requested Security Strength = 256

```
prediction_resistance_flag = "ENABLED"  
EntropyInput =  
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617  
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
```

```
EntropyInput1 (for Reseed1) =  
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697  
98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEEF
```

```
EntropyInput2 (for Reseed2) =  
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7  
D8D9DADB DCDDDED F E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
```

Nonce =

20212223 24252627 28292A2B 2C2D2E2F

PersonalizationString = <empty>

AdditionalInput1 =

60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F

AdditionalInput2 =

A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

#####

CTR_DRBG_Instantiate_algorithm - with derivation function

entropy_input is

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

nonce is

20212223 24252627 28292A2B 2C2D2E2F

personal_str is <empty>

prediction_resistance_flag = "PredictionResistance"

Block_Cipher_df

input_str is

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

number_of_bits_to_return = 384

S is

	00000040	00000030			
00010203	04050607	08090A0B	0C0D0E0F	10111213	14151617
18191A1B	1C1D1E1F	20212223	24252627	28292A2B	2C2D2E2F
20212223	24252627	28292A2B	2C2D2E2F	80000000	00000000

BCC

IV is

00000000	00000000	00000000	00000000
----------	----------	----------	----------

IV || S is

00000000	00000000	00000000	00000000	00000040	00000030
00010203	04050607	08090A0B	0C0D0E0F	10111213	14151617
18191A1B	1C1D1E1F	20212223	24252627	28292A2B	2C2D2E2F
20212223	24252627	28292A2B	2C2D2E2F	80000000	00000000

temp is

4BC4520F	E87668A3	A2CE3DCB	5F564BA9
----------	----------	----------	----------

BCC

IV is

00000001	00000000	00000000	00000000
----------	----------	----------	----------

IV || S is

00000001	00000000	00000000	00000000	00000040	00000030
00010203	04050607	08090A0B	0C0D0E0F	10111213	14151617
18191A1B	1C1D1E1F	20212223	24252627	28292A2B	2C2D2E2F
20212223	24252627	28292A2B	2C2D2E2F	80000000	00000000

temp is

4BC4520F	E87668A3				
A2CE3DCB	5F564BA9	5F84CA59	86AFC9CB	9C275423	0F4E6DC4

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000 00000000 00000000 00000040 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 80000000 00000000

temp is

4BC4520F E87668A3 A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB
9C275423 0F4E6DC4 8283F162 52D8520F D651F481 64D42EC9

Key is

4BC4520F E87668A3

A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is

8283F162 52D8520F D651F481 64D42EC9

BlockEncrypt

Key is

4BC4520F E87668A3

A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is

8283F162 52D8520F D651F481 64D42EC9

X = BlockEncrypt(Key, X) is

DF1F3CA3 8349478C CDFE738A 222E0645

temp is

DF1F3CA3 8349478C CDFE738A 222E0645

BlockEncrypt

Key is

4BC4520F E87668A3

A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is

DF1F3CA3 8349478C CDFE738A 222E0645

X = BlockEncrypt(Key, X) is

494008AD CEFBE237 13596A7E AE41BBCD

temp is

DF1F3CA3 8349478C

CDFE738A 222E0645 494008AD CEFBE237 13596A7E AE41BBCD

BlockEncrypt

Key is

4BC4520F E87668A3

A2CE3DCB 5F564BA9 5F84CA59 86AFC9CB 9C275423 0F4E6DC4

X is

494008AD CEFBE237 13596A7E AE41BBCD

X = BlockEncrypt(Key, X) is

C66368D7 8DA21092 840E23C8 995CE6D2

temp is

DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

requested_bits is

DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

seed_material is

DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

Update

provided_data is

DF1F3CA3 8349478C CDFE738A 222E0645 494008AD CEFBE237
13596A7E AE41BBCD C66368D7 8DA21092 840E23C8 995CE6D2

While loop

Key is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is

530F8AFB C74536B9 A963B4F1 C4CB738B

temp is

530F8AFB C74536B9 A963B4F1 C4CB738B

While loop

Key is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

CEA7403D 4D606B6E 074EC5D3 BAF39D18

temp is

530F8AFB C74536B9
A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18

While loop

Key is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000003

output_block is

726003CA 37A62A74 D1A2F58E 7506358E

temp is

530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E

temp XOR provided_data is

8C10B658 440C7135 649DC77B E6E575CE 87E74890 839B8959
1417AFAD 14B226D5 B4036B1D BA043AE6 55ACD646 EC5AD35C

Key is

```
8C10B658 440C7135  
649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5
```

V is

```
B4036B1D BA043AE6 55ACD646 EC5AD35C
```

First call to Generate

```
*****
```

CTR_DRBG_Generate

```
requested_number_of_bits = 256
```

```
additional_input is
```

```
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677  
78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F
```

Generate FAILED: Reseed is required

```
*****
```

CTR_DRBG_Reseed

```
entropy_input is
```

```
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697  
98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEEF
```

```
additional_input is
```

```
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677  
78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F
```

Block_Cipher_df

```
input_str is
```

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

98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677
78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F

number_of_bits_to_return = 384

S is

00000060 00000030 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000060 00000030 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

temp is

26006BB7 A0830E15 C03BA4E7 E5D71612

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000

00000000 00000000 00000060 00000030 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

temp is

26006BB7 A0830E15
C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000
00000000 00000000 00000060 00000030 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

temp is

26006BB7 A0830E15 C03BA4E7 E5D71612 8E403592 A555A544
8BB8CCFE B2A3F6D1 AEB21276 FE31F327 091B662A E7AEB81E

Key is

26006BB7 A0830E15
C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1

X is

AEB21276 FE31F327 091B662A E7AEB81E

BlockEncrypt

Key is

26006BB7 A0830E15
C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1

X is

AEB21276 FE31F327 091B662A E7AEB81E

X = BlockEncrypt(Key, X) is

D855085C 105ACC7B 757E459C B1895761

temp is

D855085C 105ACC7B 757E459C B1895761

BlockEncrypt

Key is

26006BB7 A0830E15
C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1

X is

D855085C 105ACC7B 757E459C B1895761

X = BlockEncrypt(Key, X) is

500B0067 10CD4AC5 E966A1E9 3EFF73E0

temp is

D855085C 105ACC7B
757E459C B1895761 500B0067 10CD4AC5 E966A1E9 3EFF73E0

BlockEncrypt

Key is

26006BB7 A0830E15
C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1

X is

500B0067 10CD4AC5 E966A1E9 3EFF73E0

X = BlockEncrypt(Key, X) is

64E59D80 71CD6888 B6F4DC40 58576A9C

temp is

D855085C 105ACC7B 757E459C B1895761 500B0067 10CD4AC5
E966A1E9 3EFF73E0 64E59D80 71CD6888 B6F4DC40 58576A9C

requested_bits is

D855085C 105ACC7B 757E459C B1895761 500B0067 10CD4AC5
E966A1E9 3EFF73E0 64E59D80 71CD6888 B6F4DC40 58576A9C

Update

provided_data is

D855085C 105ACC7B 757E459C B1895761 500B0067 10CD4AC5
E966A1E9 3EFF73E0 64E59D80 71CD6888 B6F4DC40 58576A9C

While loop

Key is

8C10B658 440C7135
649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5

V is

B4036B1D BA043AE6 55ACD646 EC5AD35D

output_block is

E686DD55 F758FD91 BA7CB726 FE0B573A

temp is

E686DD55 F758FD91 BA7CB726 FE0B573A

While loop

Key is

8C10B658 440C7135

649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5

V is

B4036B1D BA043AE6 55ACD646 EC5AD35E

output_block is

180AB674 39FFBDFE 5EC28FB3 7A16A53B

temp is

E686DD55 F758FD91

BA7CB726 FE0B573A 180AB674 39FFBDFE 5EC28FB3 7A16A53B

While loop

Key is

8C10B658 440C7135

649DC77B E6E575CE 87E74890 839B8959 1417AFAD 14B226D5

V is

B4036B1D BA043AE6 55ACD646 EC5AD35F

output_block is

68F2F51A 364601AF 9533C864 F25DA997

temp is
E686DD55 F758FD91 BA7CB726 FE0B573A 180AB674 39FFBDDE
5EC28FB3 7A16A53B 68F2F51A 364601AF 9533C864 F25DA997

temp XOR provided_data is
3ED3D509 E70231EA CF02F2BA 4F82005B 4801B613 2932F73B
B7A42E5A 44E9D6DB 0C17689A 478B6927 23C71424 AA0AC30B

Key is

3ED3D509 E70231EA
CF02F2BA 4F82005B 4801B613 2932F73B B7A42E5A 44E9D6DB

V is

0C17689A 478B6927 23C71424 AA0AC30B

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

3ED3D509 E70231EA
CF02F2BA 4F82005B 4801B613 2932F73B B7A42E5A 44E9D6DB

V is

0C17689A 478B6927 23C71424 AA0AC30E

output_block is

4CC7BBC C943D0EB 5B5A21C6 EA95EDD1

temp is

4CC7BBC C943D0EB 5B5A21C6 EA95EDD1

While loop

Key is

3ED3D509 E70231EA

CF02F2BA 4F82005B 4801B613 2932F73B B7A42E5A 44E9D6DB

V is

0C17689A 478B6927 23C71424 AA0AC30F

output_block is

08DF55C5 8FAF67CD 9E73B72E 01143BCE

temp is

4CC7BBC C943D0EB

5B5A21C6 EA95EDD1 08DF55C5 8FAF67CD 9E73B72E 01143BCE

While loop

Key is

3ED3D509 E70231EA

CF02F2BA 4F82005B 4801B613 2932F73B B7A42E5A 44E9D6DB

V is

0C17689A 478B6927 23C71424 AA0AC310

output_block is
6A179785 73C8AB48 15DA5329 D1B49C44

temp is
4CC7BBC C943D0EB 5B5A21C6 EA95EDD1 08DF55C5 8FAF67CD
9E73B72E 01143BCE 6A179785 73C8AB48 15DA5329 D1B49C44

temp XOR provided_data is
4CC7BBC C943D0EB 5B5A21C6 EA95EDD1 08DF55C5 8FAF67CD
9E73B72E 01143BCE 6A179785 73C8AB48 15DA5329 D1B49C44

Key is
4CC7BBC C943D0EB
5B5A21C6 EA95EDD1 08DF55C5 8FAF67CD 9E73B72E 01143BCE

V is
6A179785 73C8AB48 15DA5329 D1B49C44

rnd_val is
71BB3F9C 9CEAF4E6
C92A83EB 4C722501 0EE150AC 75E23F5F 77AD5073 EF24D88A

Second call to Generate

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAECF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

Generate FAILED: Reseed is required

CTR_DRBG_Reseed

entropy_input is
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF

additional_input is
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

Block_Cipher_df

input_str is
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

number_of_bits_to_return = 384

S is

00000060 00000030 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000060 00000030 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7

A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

temp is

A77C22F8 F701BD5D F0E36418 04462F38

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000
00000000 00000000 00000060 00000030 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

temp is

A77C22F8 F701BD5D
F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000
00000000 00000000 00000060 00000030 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

temp is
A77C22F8 F701BD5D F0E36418 04462F38 ACB4E9E8 00ABEB0E
18882C37 5360FFB3 46C9AE43 4389D41E 050AE515 E7C05BA3

Key is
A77C22F8 F701BD5D
F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3

X is
46C9AE43 4389D41E 050AE515 E7C05BA3

BlockEncrypt
Key is
A77C22F8 F701BD5D
F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3

X is
46C9AE43 4389D41E 050AE515 E7C05BA3

X = BlockEncrypt(Key, X) is
4462618D 4FA2FD6D 5B0312B1 A8BA3E8F

temp is
4462618D 4FA2FD6D 5B0312B1 A8BA3E8F

BlockEncrypt
Key is
A77C22F8 F701BD5D
F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3

X is

4462618D 4FA2FD6D 5B0312B1 A8BA3E8F

X = BlockEncrypt(Key, X) is

6909E1FF 1DF7D047 788FE17E 615BE531

temp is

4462618D 4FA2FD6D

5B0312B1 A8BA3E8F 6909E1FF 1DF7D047 788FE17E 615BE531

BlockEncrypt

Key is

A77C22F8 F701BD5D

F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3

X is

6909E1FF 1DF7D047 788FE17E 615BE531

X = BlockEncrypt(Key, X) is

7F99849D D5C2442E BB6CCCC9 4FBAB255

temp is

4462618D 4FA2FD6D 5B0312B1 A8BA3E8F 6909E1FF 1DF7D047

788FE17E 615BE531 7F99849D D5C2442E BB6CCCC9 4FBAB255

requested_bits is

4462618D 4FA2FD6D 5B0312B1 A8BA3E8F 6909E1FF 1DF7D047

788FE17E 615BE531 7F99849D D5C2442E BB6CCCC9 4FBAB255

Update

provided_data is

4462618D 4FA2FD6D 5B0312B1 A8BA3E8F 6909E1FF 1DF7D047
788FE17E 615BE531 7F99849D D5C2442E BB6CCCC9 4FBAB255

While loop

Key is

4CC7BBC C943D0EB
5B5A21C6 EA95EDD1 08DF55C5 8FAF67CD 9E73B72E 01143BCE

V is

6A179785 73C8AB48 15DA5329 D1B49C45

output_block is

24B048EA F05CAFE5 DD6F0FB2 286260F6

temp is

24B048EA F05CAFE5 DD6F0FB2 286260F6

While loop

Key is

4CC7BBC C943D0EB
5B5A21C6 EA95EDD1 08DF55C5 8FAF67CD 9E73B72E 01143BCE

V is

6A179785 73C8AB48 15DA5329 D1B49C46

output_block is

A70281B2 8D1F015B 274FC493 6887DC9D

temp is

24B048EA F05CAFE5
DD6F0FB2 286260F6 A70281B2 8D1F015B 274FC493 6887DC9D

While loop

Key is

4CC7BBC C943D0EB
5B5A21C6 EA95EDD1 08DF55C5 8FAF67CD 9E73B72E 01143BCE

V is

6A179785 73C8AB48 15DA5329 D1B49C47

output_block is

8086CDC5 A0997070 A038BD76 1C2627A6

temp is

24B048EA F05CAFE5 DD6F0FB2 286260F6 A70281B2 8D1F015B
274FC493 6887DC9D 8086CDC5 A0997070 A038BD76 1C2627A6

temp XOR provided_data is

60D22967 BFFE5288 866C1D03 80D85E79 CE0B604D 90E8D11C
5FC025ED 09DC39AC FF1F4958 755B345E 1B5471BF 539C95F3

Key is

60D22967 BFFE5288
866C1D03 80D85E79 CE0B604D 90E8D11C 5FC025ED 09DC39AC

V is

FF1F4958 755B345E 1B5471BF 539C95F3

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

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

While loop

Key is

```
60D22967 BFFE5288  
866C1D03 80D85E79 CE0B604D 90E8D11C 5FC025ED 09DC39AC
```

V is

```
FF1F4958 755B345E 1B5471BF 539C95F6
```

output_block is

```
9E56500A 6898B16D 6265BC60 CAF2705E
```

temp is

```
9E56500A 6898B16D 6265BC60 CAF2705E
```

While loop

Key is

```
60D22967 BFFE5288  
866C1D03 80D85E79 CE0B604D 90E8D11C 5FC025ED 09DC39AC
```

V is

```
FF1F4958 755B345E 1B5471BF 539C95F7
```

output_block is

```
1453470E D44D2883 B421447D 71F6176B
```

temp is

9E56500A 6898B16D
6265BC60 CAF2705E 1453470E D44D2883 B421447D 71F6176B

While loop

Key is

60D22967 BFFE5288
866C1D03 80D85E79 CE0B604D 90E8D11C 5FC025ED 09DC39AC

V is

FF1F4958 755B345E 1B5471BF 539C95F8

output_block is

4D0DC726 445D0DEC C1CD0D7C 41016C9B

temp is

9E56500A 6898B16D 6265BC60 CAF2705E 1453470E D44D2883
B421447D 71F6176B 4D0DC726 445D0DEC C1CD0D7C 41016C9B

temp XOR provided_data is

9E56500A 6898B16D 6265BC60 CAF2705E 1453470E D44D2883
B421447D 71F6176B 4D0DC726 445D0DEC C1CD0D7C 41016C9B

Key is

9E56500A 6898B16D
6265BC60 CAF2705E 1453470E D44D2883 B421447D 71F6176B

V is

4D0DC726 445D0DEC C1CD0D7C 41016C9B

rnd_val is

386DEBBB F091BBF0
502957B0 329938FB 836B82E5 94A2F5FD D5EB28D4 E35528F4

```
#####
```

CTR_DRBG

Requested Security Strength = 256

prediction_resistance_flag = "ENABLED"

EntropyInput =

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

EntropyInput1 (for Reseed1) =

```
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697  
98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
```

EntropyInput2 (for Reseed2) =

```
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7  
D8D9DADB DCDDDEDF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
```

Nonce =

```
20212223 24252627 28292A2B 2C2D2E2F
```

PersonalizationString =

```
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657  
58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F
```

AdditionalInput = <empty>

```
#####
```

```
*****
```

CTR_DRBG_Instantiate_algorithm - with derivation function

entropy_input is

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

nonce is

```
20212223 24252627 28292A2B 2C2D2E2F
```

```
personal_str is
    40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
    58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F
```

```
prediction_resistance_flag = "PredictionResistance"
```

```
-----  
Block_Cipher_df
```

```
input_str is
    00010203 04050607 08090A0B 0C0D0E0F
    10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
    28292A2B 2C2D2E2F 20212223 24252627 28292A2B 2C2D2E2F
    40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
    58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F
```

```
number_of_bits_to_return = 384
```

```
S is
```

```
    00000070 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000
```

```
-----
```

```
BCC
```

```
IV is
```

```
00000000 00000000 00000000 00000000
```

```
IV || S is
```

```
00000000 00000000 00000000 00000000 00000070 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
```

60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000

temp is

8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000 00000000 00000070 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000

temp is

8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000 00000000 00000000 00000070 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000

temp is
8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08 A13B6B8D A420CCBC
43CF57C7 F3A7C718 2B4B429F EDFD2D2D 937CA4B4 71B86606

Key is
8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

X is
2B4B429F EDFD2D2D 937CA4B4 71B86606

BlockEncrypt

Key is
8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

X is
2B4B429F EDFD2D2D 937CA4B4 71B86606

X = BlockEncrypt(Key, X) is
31D82952 CBF4754A 1354F1A9 184841B4

temp is
31D82952 CBF4754A 1354F1A9 184841B4

BlockEncrypt

Key is
8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

X is

31D82952 CBF4754A 1354F1A9 184841B4

X = BlockEncrypt(Key, X) is

C0812181 C179FD79 547E5367 AB8C9FA4

temp is

31D82952 CBF4754A

1354F1A9 184841B4 C0812181 C179FD79 547E5367 AB8C9FA4

BlockEncrypt

Key is

8A0B0FB5 AA3FA8FD

4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

X is

C0812181 C179FD79 547E5367 AB8C9FA4

X = BlockEncrypt(Key, X) is

51223D14 E89B833F 62FC5EF8 0034A200

temp is

31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79

547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200

requested_bits is

31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79

547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200

seed_material is

31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79

547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200

Update

provided_data is
31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200

While loop

Key is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000001

output_block is

530F8AFB C74536B9 A963B4F1 C4CB738B

temp is

530F8AFB C74536B9 A963B4F1 C4CB738B

While loop

Key is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

CEA7403D 4D606B6E 074EC5D3 BAF39D18

temp is

530F8AFB C74536B9
A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18

While loop

Key is

00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000003

output_block is

726003CA 37A62A74 D1A2F58E 7506358E

temp is

530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E
074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E

temp XOR provided_data is

62D7A3A9 0CB143F3 BA374558 DC83323F 0E2661BC 8C199617
533096B4 117F02BC 23423EDE DF3DA94B B35EAB76 7532978E

Key is

62D7A3A9 0CB143F3
BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is

23423EDE DF3DA94B B35EAB76 7532978E

First call to Generate

```
CTR_DRBG_Generate
```

```
    requested_number_of_bits = 256
```

```
    additional_input is <empty>
```

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

```
*****
```

```
CTR_DRBG_Reseed
```

```
    entropy_input is
```

```
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697  
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
```

```
    additional_input is <empty>
```

```
-----  
Block_Cipher_df
```

```
    input_str is
```

```
        80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697  
        98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
```

```
    number_of_bits_to_return = 384
```

```
S is
```

```
        00000030 00000030 80818283 84858687  
        88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F  
        A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000
```

```
-----  
BCC
```

```
IV is
```

```
        00000000 00000000 00000000 00000000
```

```
IV || S is
```

```
        00000000 00000000
```

00000000 00000000 00000030 00000030 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000

temp is

6808E8C2 37359B53 E4AC883F 8D22A1CA

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000
00000000 00000000 00000030 00000030 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000

temp is

6808E8C2 37359B53
E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000
00000000 00000000 00000030 00000030 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 80000000 00000000

temp is

6808E8C2 37359B53 E4AC883F 8D22A1CA DC9A2BCF C2C81F7F

F712FC22 E18D59F6 D870D670 2017B3B4 5327BDD3 E5D50B51

Key is

6808E8C2 37359B53
E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6

X is

D870D670 2017B3B4 5327BDD3 E5D50B51

BlockEncrypt

Key is

6808E8C2 37359B53
E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6

X is

D870D670 2017B3B4 5327BDD3 E5D50B51

X = BlockEncrypt(Key, X) is

F11E1D8A FE3197D7 A33A494B 9676DBF2

temp is

F11E1D8A FE3197D7 A33A494B 9676DBF2

BlockEncrypt

Key is

6808E8C2 37359B53
E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6

X is

F11E1D8A FE3197D7 A33A494B 9676DBF2

X = BlockEncrypt(Key, X) is
27E44756 CA44780C C36E0AA3 895C552E

temp is
F11E1D8A FE3197D7
A33A494B 9676DBF2 27E44756 CA44780C C36E0AA3 895C552E

BlockEncrypt

Key is
6808E8C2 37359B53
E4AC883F 8D22A1CA DC9A2BCF C2C81F7F F712FC22 E18D59F6

X is

27E44756 CA44780C C36E0AA3 895C552E

X = BlockEncrypt(Key, X) is
6301C157 C36F26C4 986874E7 698ECCFD

temp is
F11E1D8A FE3197D7 A33A494B 9676DBF2 27E44756 CA44780C
C36E0AA3 895C552E 6301C157 C36F26C4 986874E7 698ECCFD

requested_bits is
F11E1D8A FE3197D7 A33A494B 9676DBF2 27E44756 CA44780C
C36E0AA3 895C552E 6301C157 C36F26C4 986874E7 698ECCFD

Update

provided_data is
F11E1D8A FE3197D7 A33A494B 9676DBF2 27E44756 CA44780C
C36E0AA3 895C552E 6301C157 C36F26C4 986874E7 698ECCFD

While loop

Key is

62D7A3A9 0CB143F3
BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is

23423EDE DF3DA94B B35EAB76 7532978F

output_block is

99BB703C DD820609 903F1241 EA856E27

temp is

99BB703C DD820609 903F1241 EA856E27

While loop

Key is

62D7A3A9 0CB143F3
BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is

23423EDE DF3DA94B B35EAB76 75329790

output_block is

A54C2B75 EEA7775B 68093FCD 47B52E7F

temp is

99BB703C DD820609
903F1241 EA856E27 A54C2B75 EEA7775B 68093FCD 47B52E7F

While loop

Key is

62D7A3A9 0CB143F3
BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is

23423EDE DF3DA94B B35EAB76 75329791

output_block is

40A4397E 72F15782 98F8B8FB 54A8BAD1

temp is

99BB703C DD820609 903F1241 EA856E27 A54C2B75 EEA7775B
68093FCD 47B52E7F 40A4397E 72F15782 98F8B8FB 54A8BAD1

temp XOR provided_data is

68A56DB6 23B391DE 33055B0A 7CF3B5D5 82A86C23 24E30F57
AB67356E CEE97B51 23A5F829 B19E7146 0090CC1C 3D26762C

Key is

68A56DB6 23B391DE
33055B0A 7CF3B5D5 82A86C23 24E30F57 AB67356E CEE97B51

V is

23A5F829 B19E7146 0090CC1C 3D26762C

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is
00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is
68A56DB6 23B391DE
33055B0A 7CF3B5D5 82A86C23 24E30F57 AB67356E CEE97B51

V is

23A5F829 B19E7146 0090CC1C 3D26762F

output_block is

0C47A82D 2442216E A904EC72 E3BDF875

temp is

0C47A82D 2442216E A904EC72 E3BDF875

While loop

Key is
68A56DB6 23B391DE
33055B0A 7CF3B5D5 82A86C23 24E30F57 AB67356E CEE97B51

V is

23A5F829 B19E7146 0090CC1C 3D267630

output_block is

6ABE26CD 74DC1CD3 EC6084B1 C60B49E8

temp is

0C47A82D 2442216E
A904EC72 E3BDF875 6ABE26CD 74DC1CD3 EC6084B1 C60B49E8

While loop

Key is

68A56DB6 23B391DE
33055B0A 7CF3B5D5 82A86C23 24E30F57 AB67356E CEE97B51

V is

23A5F829 B19E7146 0090CC1C 3D267631

output_block is

5BF18BBA A9D36E9D A7C1A6B4 FB4ABC9D

temp is

0C47A82D 2442216E A904EC72 E3BDF875 6ABE26CD 74DC1CD3
EC6084B1 C60B49E8 5BF18BBA A9D36E9D A7C1A6B4 FB4ABC9D

temp XOR provided_data is

0C47A82D 2442216E A904EC72 E3BDF875 6ABE26CD 74DC1CD3
EC6084B1 C60B49E8 5BF18BBA A9D36E9D A7C1A6B4 FB4ABC9D

Key is

0C47A82D 2442216E
A904EC72 E3BDF875 6ABE26CD 74DC1CD3 EC6084B1 C60B49E8

V is

5BF18BBA A9D36E9D A7C1A6B4 FB4ABC9D

rnd_val is

1A2E3FEE 9056E98D
375525FD C2B63B95 B47CE51F CF594D80 4BD5A17F 2E01139B

Second call to Generate

```
*****
```

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Generate FAILED: Reseed is required

```
*****
```

CTR_DRBG_Reseed

entropy_input is

C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
D8D9DADB DCDDDED7 E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF

additional_input is <empty>

Block_Cipher_df

input_str is

C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
D8D9DADB DCDDDED7 E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF

number_of_bits_to_return = 384

S is

00000030 00000030 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED7
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000030 00000030 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000

temp is

F2977267 80DDB539 4AFDD5B8 CCC350C9

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000
00000000 00000000 00000030 00000030 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000

temp is

F2977267 80DDB539
4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000
00000000 00000000 00000030 00000030 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF 80000000 00000000

temp is
F2977267 80DDB539 4AFDD5B8 CCC350C9 AA2EF303 87F07708
919EA794 06ADEF9B 31221A7E 3A0CE21C 54C7074E 0C011CA8

Key is
F2977267 80DDB539
4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B

X is
31221A7E 3A0CE21C 54C7074E 0C011CA8

BlockEncrypt

Key is
F2977267 80DDB539
4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B

X is
31221A7E 3A0CE21C 54C7074E 0C011CA8

X = BlockEncrypt(Key, X) is
AAA32C63 E6A3FED3 B6787677 D5867143

temp is
AAA32C63 E6A3FED3 B6787677 D5867143

BlockEncrypt

Key is
F2977267 80DDB539
4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B

X is

AAA32C63 E6A3FED3 B6787677 D5867143

X = BlockEncrypt(Key, X) is

F04E8A91 0E0A3F2F A7CDDD9B 8D03090C

temp is

AAA32C63 E6A3FED3

B6787677 D5867143 F04E8A91 0E0A3F2F A7CDDD9B 8D03090C

BlockEncrypt

Key is

F2977267 80DDB539

4AFDD5B8 CCC350C9 AA2EF303 87F07708 919EA794 06ADEF9B

X is

F04E8A91 0E0A3F2F A7CDDD9B 8D03090C

X = BlockEncrypt(Key, X) is

E74B09AD 16BC3C53 457691EE BC770472

temp is

AAA32C63 E6A3FED3 B6787677 D5867143 F04E8A91 0E0A3F2F

A7CDDD9B 8D03090C E74B09AD 16BC3C53 457691EE BC770472

requested_bits is

AAA32C63 E6A3FED3 B6787677 D5867143 F04E8A91 0E0A3F2F

A7CDDD9B 8D03090C E74B09AD 16BC3C53 457691EE BC770472

Update

provided_data is

AAA32C63 E6A3FED3 B6787677 D5867143 F04E8A91 0E0A3F2F

A7CDDD9B 8D03090C E74B09AD 16BC3C53 457691EE BC770472

While loop

Key is

0C47A82D 2442216E
A904EC72 E3BDF875 6ABE26CD 74DC1CD3 EC6084B1 C60B49E8

V is

5BF18BBA A9D36E9D A7C1A6B4 FB4ABC9E

output_block is

AB18E1F1 ABEF409E 52DCDE30 3D02FC54

temp is

AB18E1F1 ABEF409E 52DCDE30 3D02FC54

While loop

Key is

0C47A82D 2442216E
A904EC72 E3BDF875 6ABE26CD 74DC1CD3 EC6084B1 C60B49E8

V is

5BF18BBA A9D36E9D A7C1A6B4 FB4ABC9F

output_block is

DE988F57 31C380F9 B32BA7C3 4C794DDB

temp is

AB18E1F1 ABEF409E
52DCDE30 3D02FC54 DE988F57 31C380F9 B32BA7C3 4C794DDB

While loop

Key is

0C47A82D 2442216E
A904EC72 E3BDF875 6ABE26CD 74DC1CD3 EC6084B1 C60B49E8

V is

5BF18BBA A9D36E9D A7C1A6B4 FB4ABC0

output_block is

88DBB237 E58E23BF E34A6BF4 592480D9

temp is

AB18E1F1 ABEF409E 52DCDE30 3D02FC54 DE988F57 31C380F9
B32BA7C3 4C794DDB 88DBB237 E58E23BF E34A6BF4 592480D9

temp XOR provided_data is

01BBCD92 4D4CBE4D E4A4A847 E8848D17 2ED605C6 3FC9BFD6
14E67A58 C17A44D7 6F90BB9A F3321FEC A63CFA1A E55384AB

Key is

01BBCD92 4D4CBE4D
E4A4A847 E8848D17 2ED605C6 3FC9BFD6 14E67A58 C17A44D7

V is

6F90BB9A F3321FEC A63CFA1A E55384AB

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

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

While loop

Key is

```
01BBCD92 4D4CBE4D  
E4A4A847 E8848D17 2ED605C6 3FC9BFD6 14E67A58 C17A44D7
```

V is

```
6F90BB9A F3321FEC A63CFA1A E55384AE
```

output_block is

```
A36C785C 712E59D1 2FDE205C 9A10BAE5
```

temp is

```
A36C785C 712E59D1 2FDE205C 9A10BAE5
```

While loop

Key is

```
01BBCD92 4D4CBE4D  
E4A4A847 E8848D17 2ED605C6 3FC9BFD6 14E67A58 C17A44D7
```

V is

```
6F90BB9A F3321FEC A63CFA1A E55384AF
```

output_block is

```
C0A4CA2F 0282977F 44D0F4A1 EC889D62
```

temp is

A36C785C 712E59D1
2FDE205C 9A10BAE5 C0A4CA2F 0282977F 44D0F4A1 EC889D62

While loop

Key is

01BBCD92 4D4CBE4D
E4A4A847 E8848D17 2ED605C6 3FC9BFD6 14E67A58 C17A44D7

V is

6F90BB9A F3321FEC A63CFA1A E55384B0

output_block is

CEC24BC1 DABE2F6E 459F14FD 869349FB

temp is

A36C785C 712E59D1 2FDE205C 9A10BAE5 C0A4CA2F 0282977F
44D0F4A1 EC889D62 CEC24BC1 DABE2F6E 459F14FD 869349FB

temp XOR provided_data is

A36C785C 712E59D1 2FDE205C 9A10BAE5 C0A4CA2F 0282977F
44D0F4A1 EC889D62 CEC24BC1 DABE2F6E 459F14FD 869349FB

Key is

A36C785C 712E59D1
2FDE205C 9A10BAE5 C0A4CA2F 0282977F 44D0F4A1 EC889D62

V is

CEC24BC1 DABE2F6E 459F14FD 869349FB

rnd_val is

601F9538 4F0D8594
6301D1EA CE8F645A 825CE38F 1E2565B0 C0C43944 8E9CA8AC

#####

CTR_DRBG

Requested Security Strength = 256

```
prediction_resistance_flag = "ENABLED"  
EntropyInput =  
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617  
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
```

```
EntropyInput1 (for Reseed1) =  
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697  
98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
```

```
EntropyInput2 (for Reseed2) =  
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7  
D8D9DADB DCDDDEF E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
```

```
Nonce =  
20212223 24252627 28292A2B 2C2D2E2F
```

```
PersonalizationString =  
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657  
58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F
```

```
AdditionalInput1 =  
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677  
78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F
```

```
AdditionalInput2 =  
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7  
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
```

#####

CTR_DRBG_Instantiate_algorithm - with derivation function

```
entropy_input is
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
```

```
nonce is
20212223 24252627 28292A2B 2C2D2E2F
```

```
personal_str is
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F
```

```
prediction_resistance_flag = "PredictionResistance"
```

Block_Cipher_df

```
input_str is
00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F 20212223 24252627
28292A2B 2C2D2E2F 20212223 24252627 28292A2B 2C2D2E2F
40414243 44454647 48494A4B 4C4D4E4F 50515253 54555657
58595A5B 5C5D5E5F 60616263 64656667 68696A6B 6C6D6E6F
```

```
number_of_bits_to_return = 384
```

```
S is
00000070 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000
```

BCC

```
IV is
00000000 00000000 00000000 00000000
```

IV || S is

```
00000000 00000000 00000000 00000000 00000070 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000
```

temp is

```
8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08
```

BCC

IV is

```
00000001 00000000 00000000 00000000
```

IV || S is

```
00000001 00000000 00000000 00000000 00000070 00000030
00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000
```

temp is

```
8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718
```

BCC

IV is

```
00000002 00000000 00000000 00000000
```

IV || S is

```
00000002 00000000 00000000 00000000 00000070 00000030
```

00010203 04050607 08090A0B 0C0D0E0F 10111213 14151617
18191A1B 1C1D1E1F 20212223 24252627 28292A2B 2C2D2E2F
20212223 24252627 28292A2B 2C2D2E2F 40414243 44454647
48494A4B 4C4D4E4F 50515253 54555657 58595A5B 5C5D5E5F
60616263 64656667 68696A6B 6C6D6E6F 80000000 00000000

temp is

8A0B0FB5 AA3FA8FD 4B9E8708 FACD2A08 A13B6B8D A420CCBC
43CF57C7 F3A7C718 2B4B429F EDFD2D2D 937CA4B4 71B86606

Key is

8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

X is

2B4B429F EDFD2D2D 937CA4B4 71B86606

BlockEncrypt

Key is

8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

X is

2B4B429F EDFD2D2D 937CA4B4 71B86606

X = BlockEncrypt(Key, X) is

31D82952 CBF4754A 1354F1A9 184841B4

temp is

31D82952 CBF4754A 1354F1A9 184841B4

BlockEncrypt

Key is

8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

X is

31D82952 CBF4754A 1354F1A9 184841B4

X = BlockEncrypt(Key, X) is

C0812181 C179FD79 547E5367 AB8C9FA4

temp is

31D82952 CBF4754A
1354F1A9 184841B4 C0812181 C179FD79 547E5367 AB8C9FA4

BlockEncrypt

Key is

8A0B0FB5 AA3FA8FD
4B9E8708 FACD2A08 A13B6B8D A420CCBC 43CF57C7 F3A7C718

X is

C0812181 C179FD79 547E5367 AB8C9FA4

X = BlockEncrypt(Key, X) is

51223D14 E89B833F 62FC5EF8 0034A200

temp is

31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200

requested_bits is

31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200

seed_material is
31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200

Update

provided_data is
31D82952 CBF4754A 1354F1A9 184841B4 C0812181 C179FD79
547E5367 AB8C9FA4 51223D14 E89B833F 62FC5EF8 0034A200

While loop

Key is
00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is
00000000 00000000 00000000 00000001

output_block is
530F8AFB C74536B9 A963B4F1 C4CB738B

temp is
530F8AFB C74536B9 A963B4F1 C4CB738B

While loop

Key is
00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000002

output_block is

CEA7403D 4D606B6E 074EC5D3 BAF39D18

temp is

530F8AFB C74536B9

A963B4F1 C4CB738B CEA7403D 4D606B6E 074EC5D3 BAF39D18

While loop

Key is

00000000 00000000

00000000 00000000 00000000 00000000 00000000 00000000

V is

00000000 00000000 00000000 00000003

output_block is

726003CA 37A62A74 D1A2F58E 7506358E

temp is

530F8AFB C74536B9 A963B4F1 C4CB738B CEA7403D 4D606B6E

074EC5D3 BAF39D18 726003CA 37A62A74 D1A2F58E 7506358E

temp XOR provided_data is

62D7A3A9 0CB143F3 BA374558 DC83323F 0E2661BC 8C199617

533096B4 117F02BC 23423EDE DF3DA94B B35EAB76 7532978E

Key is

62D7A3A9 0CB143F3

BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is

23423EDE DF3DA94B B35EAB76 7532978E

First call to Generate

```
*****
```

CTR_DRBG_Generate

```
requested_number_of_bits = 256
```

```
additional_input is
```

```
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677  
78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F
```

Generate FAILED: Reseed is required

```
*****
```

CTR_DRBG_Reseed

```
entropy_input is
```

```
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697  
98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF
```

```
additional_input is
```

```
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677  
78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F
```

Block_Cipher_df

```
input_str is
```

```
80818283 84858687 88898A8B 8C8D8E8F 90919293 94959697  
98999A9B 9C9D9E9F A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF  
60616263 64656667 68696A6B 6C6D6E6F 70717273 74757677  
78797A7B 7C7D7E7F 80818283 84858687 88898A8B 8C8D8E8F
```

```
number_of_bits_to_return = 384
```

```
S is
```

00000060 00000030 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000

00000000 00000000 00000060 00000030 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

temp is

26006BB7 A0830E15 C03BA4E7 E5D71612

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000

00000000 00000000 00000060 00000030 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

temp is

26006BB7 A0830E15
C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000

00000000 00000000 00000060 00000030 80818283 84858687
88898A8B 8C8D8E8F 90919293 94959697 98999A9B 9C9D9E9F
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF 60616263 64656667
68696A6B 6C6D6E6F 70717273 74757677 78797A7B 7C7D7E7F
80818283 84858687 88898A8B 8C8D8E8F 80000000 00000000

temp is

26006BB7 A0830E15 C03BA4E7 E5D71612 8E403592 A555A544
8BB8CCFE B2A3F6D1 AEB21276 FE31F327 091B662A E7AEB81E

Key is

26006BB7 A0830E15
C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1

X is

AEB21276 FE31F327 091B662A E7AEB81E

BlockEncrypt

Key is

26006BB7 A0830E15
C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1

X is

AEB21276 FE31F327 091B662A E7AEB81E

X = BlockEncrypt(Key, X) is

D855085C 105ACC7B 757E459C B1895761

temp is

D855085C 105ACC7B 757E459C B1895761

BlockEncrypt

Key is

26006BB7 A0830E15

C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1

X is

D855085C 105ACC7B 757E459C B1895761

X = BlockEncrypt(Key, X) is

500B0067 10CD4AC5 E966A1E9 3EFF73E0

temp is

D855085C 105ACC7B

757E459C B1895761 500B0067 10CD4AC5 E966A1E9 3EFF73E0

BlockEncrypt

Key is

26006BB7 A0830E15

C03BA4E7 E5D71612 8E403592 A555A544 8BB8CCFE B2A3F6D1

X is

500B0067 10CD4AC5 E966A1E9 3EFF73E0

X = BlockEncrypt(Key, X) is
64E59D80 71CD6888 B6F4DC40 58576A9C

temp is
D855085C 105ACC7B 757E459C B1895761 500B0067 10CD4AC5
E966A1E9 3EFF73E0 64E59D80 71CD6888 B6F4DC40 58576A9C

requested_bits is
D855085C 105ACC7B 757E459C B1895761 500B0067 10CD4AC5
E966A1E9 3EFF73E0 64E59D80 71CD6888 B6F4DC40 58576A9C

Update

provided_data is
D855085C 105ACC7B 757E459C B1895761 500B0067 10CD4AC5
E966A1E9 3EFF73E0 64E59D80 71CD6888 B6F4DC40 58576A9C

While loop

Key is
62D7A3A9 0CB143F3
BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is
23423EDE DF3DA94B B35EAB76 7532978F

output_block is
99BB703C DD820609 903F1241 EA856E27

temp is
99BB703C DD820609 903F1241 EA856E27

While loop

Key is

62D7A3A9 0CB143F3
BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is

23423EDE DF3DA94B B35EAB76 75329790

output_block is

A54C2B75 EEA7775B 68093FCD 47B52E7F

temp is

99BB703C DD820609
903F1241 EA856E27 A54C2B75 EEA7775B 68093FCD 47B52E7F

While loop

Key is

62D7A3A9 0CB143F3
BA374558 DC83323F 0E2661BC 8C199617 533096B4 117F02BC

V is

23423EDE DF3DA94B B35EAB76 75329791

output_block is

40A4397E 72F15782 98F8B8FB 54A8BAD1

temp is

99BB703C DD820609 903F1241 EA856E27 A54C2B75 EEA7775B
68093FCD 47B52E7F 40A4397E 72F15782 98F8B8FB 54A8BAD1

temp XOR provided_data is

41EE7860 CDD8CA72 E54157DD 5B0C3946 F5472B12 FE6A3D9E
816F9E24 794A5D9F 2441A4FE 033C3F0A 2E0C64BB 0CFFD04D

Key is

41EE7860 CDD8CA72
E54157DD 5B0C3946 F5472B12 FE6A3D9E 816F9E24 794A5D9F

V is

2441A4FE 033C3F0A 2E0C64BB 0CFFD04D

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

41EE7860 CDD8CA72
E54157DD 5B0C3946 F5472B12 FE6A3D9E 816F9E24 794A5D9F

V is

2441A4FE 033C3F0A 2E0C64BB 0CFFD050

output_block is

30B27377 DE24BD94 8F2037BC BA1BB65B

temp is

30B27377 DE24BD94 8F2037BC BA1BB65B

While loop

Key is

41EE7860 CDD8CA72

E54157DD 5B0C3946 F5472B12 FE6A3D9E 816F9E24 794A5D9F

V is

2441A4FE 033C3F0A 2E0C64BB 0CFFD051

output_block is

EAF4E2D2 46CFE777 0F27D16B 89069C3A

temp is

30B27377 DE24BD94

8F2037BC BA1BB65B EAF4E2D2 46CFE777 0F27D16B 89069C3A

While loop

Key is

41EE7860 CDD8CA72

E54157DD 5B0C3946 F5472B12 FE6A3D9E 816F9E24 794A5D9F

V is

2441A4FE 033C3F0A 2E0C64BB 0CFFD052

output_block is

0592090E A1D6CB56 93F23B12 1BB07AC2

temp is

30B27377 DE24BD94 8F2037BC BA1BB65B EAF4E2D2 46CFE777

0F27D16B 89069C3A 0592090E A1D6CB56 93F23B12 1BB07AC2

```
temp XOR provided_data is
 30B27377 DE24BD94 8F2037BC BA1BB65B EAF4E2D2 46CFE777
 0F27D16B 89069C3A 0592090E A1D6CB56 93F23B12 1BB07AC2
```

Key is

```
 30B27377 DE24BD94
 8F2037BC BA1BB65B EAF4E2D2 46CFE777 0F27D16B 89069C3A
```

V is

```
 0592090E A1D6CB56 93F23B12 1BB07AC2
```

rnd_val is

```
 EAE6BCE7 81807E52
 4D26605E A1980779 32D01EEB 445B9AC6 C5D99C10 1D29F46E
```

Second call to Generate

```
*****
```

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is

```
 A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
 B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF
```

Generate FAILED: Reseed is required

```
*****
```

CTR_DRBG_Reseed

entropy_input is

```
 C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
 D8D9DADB DCDDDED7 E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
```

additional_input is

A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

Block_Cipher_df

input_str is
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7
D8D9DADB DCDDDED F E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF
A0A1A2A3 A4A5A6A7 A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7
B8B9BABB BCBDBEBF C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF

number_of_bits_to_return = 384

S is

00000060 00000030 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED F
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

BCC

IV is

00000000 00000000 00000000 00000000

IV || S is

00000000 00000000 00000060 00000030 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDED F
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

temp is

A77C22F8 F701BD5D F0E36418 04462F38

BCC

IV is

00000001 00000000 00000000 00000000

IV || S is

00000001 00000000
00000000 00000000 00000060 00000030 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

temp is

A77C22F8 F701BD5D

F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3

BCC

IV is

00000002 00000000 00000000 00000000

IV || S is

00000002 00000000
00000000 00000000 00000060 00000030 C0C1C2C3 C4C5C6C7
C8C9CACB CCCDCECF D0D1D2D3 D4D5D6D7 D8D9DADB DCDDDEDF
E0E1E2E3 E4E5E6E7 E8E9EAEB ECEDEEEF A0A1A2A3 A4A5A6A7
A8A9AAAB ACADAEAF B0B1B2B3 B4B5B6B7 B8B9BABB BCBDBEBF
C0C1C2C3 C4C5C6C7 C8C9CACB CCCDCECF 80000000 00000000

temp is

A77C22F8 F701BD5D F0E36418 04462F38 ACB4E9E8 00ABEB0E
18882C37 5360FFB3 46C9AE43 4389D41E 050AE515 E7C05BA3

Key is
A77C22F8 F701BD5D
F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3

X is
46C9AE43 4389D41E 050AE515 E7C05BA3

BlockEncrypt

Key is
A77C22F8 F701BD5D
F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3

X is
46C9AE43 4389D41E 050AE515 E7C05BA3

X = BlockEncrypt(Key, X) is
4462618D 4FA2FD6D 5B0312B1 A8BA3E8F

temp is
4462618D 4FA2FD6D 5B0312B1 A8BA3E8F

BlockEncrypt

Key is
A77C22F8 F701BD5D
F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3

X is
4462618D 4FA2FD6D 5B0312B1 A8BA3E8F

X = BlockEncrypt(Key, X) is
6909E1FF 1DF7D047 788FE17E 615BE531

temp is

4462618D 4FA2FD6D
5B0312B1 A8BA3E8F 6909E1FF 1DF7D047 788FE17E 615BE531

BlockEncrypt

Key is

A77C22F8 F701BD5D
F0E36418 04462F38 ACB4E9E8 00ABEB0E 18882C37 5360FFB3

X is

6909E1FF 1DF7D047 788FE17E 615BE531

X = BlockEncrypt(Key, X) is

7F99849D D5C2442E BB6CCCC9 4FBAB255

temp is

4462618D 4FA2FD6D 5B0312B1 A8BA3E8F 6909E1FF 1DF7D047
788FE17E 615BE531 7F99849D D5C2442E BB6CCCC9 4FBAB255

requested_bits is

4462618D 4FA2FD6D 5B0312B1 A8BA3E8F 6909E1FF 1DF7D047
788FE17E 615BE531 7F99849D D5C2442E BB6CCCC9 4FBAB255

Update

provided_data is

4462618D 4FA2FD6D 5B0312B1 A8BA3E8F 6909E1FF 1DF7D047
788FE17E 615BE531 7F99849D D5C2442E BB6CCCC9 4FBAB255

While loop

Key is

30B27377 DE24BD94
8F2037BC BA1BB65B EAF4E2D2 46CFE777 0F27D16B 89069C3A

V is

0592090E A1D6CB56 93F23B12 1BB07AC3

output_block is

49724416 6965665C E658C814 AE95122A

temp is

49724416 6965665C E658C814 AE95122A

While loop

Key is

30B27377 DE24BD94
8F2037BC BA1BB65B EAF4E2D2 46CFE777 0F27D16B 89069C3A

V is

0592090E A1D6CB56 93F23B12 1BB07AC4

output_block is

DE01CB7F A3BD14EF 0F00EEFA 7DCA0699

temp is

49724416 6965665C
E658C814 AE95122A DE01CB7F A3BD14EF 0F00EEFA 7DCA0699

While loop

Key is

30B27377 DE24BD94
8F2037BC BA1BB65B EAF4E2D2 46CFE777 0F27D16B 89069C3A

V is

0592090E A1D6CB56 93F23B12 1BB07AC5

output_block is

21ADEF12 119A1B34 E5DF1581 62CC7F6E

temp is

49724416 6965665C E658C814 AE95122A DE01CB7F A3BD14EF
0F00EEFA 7DCA0699 21ADEF12 119A1B34 E5DF1581 62CC7F6E

temp XOR provided_data is

0D10259B 26C79B31 BD5BDA5 062F2CA5 B7082A80 BE4AC4A8
778F0F84 1C91E3A8 5E366B8F C4585F1A 5EB3D948 2D76CD3B

Key is

0D10259B 26C79B31
BD5BDA5 062F2CA5 B7082A80 BE4AC4A8 778F0F84 1C91E3A8

V is

5E366B8F C4585F1A 5EB3D948 2D76CD3B

CTR_DRBG_Generate

requested_number_of_bits = 256

additional_input is <empty>

Update

provided_data is

00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000 00000000 00000000

While loop

Key is

0D10259B 26C79B31
BD5BDAAS 062F2CA5 B7082A80 BE4AC4A8 778F0F84 1C91E3A8

V is

5E366B8F C4585F1A 5EB3D948 2D76CD3E

output_block is

A12D1656 186D2BC2 AF8837A1 F5F41C75

temp is

A12D1656 186D2BC2 AF8837A1 F5F41C75

While loop

Key is

0D10259B 26C79B31
BD5BDAAS 062F2CA5 B7082A80 BE4AC4A8 778F0F84 1C91E3A8

V is

5E366B8F C4585F1A 5EB3D948 2D76CD3F

output_block is

6832B24D 2F4EEB19 EFBD0618 14F0B45D

temp is

A12D1656 186D2BC2
AF8837A1 F5F41C75 6832B24D 2F4EEB19 EFBD0618 14F0B45D

While loop

Key is

0D10259B 26C79B31
BD5BDAAS 062F2CA5 B7082A80 BE4AC4A8 778F0F84 1C91E3A8

V is

5E366B8F C4585F1A 5EB3D948 2D76CD40

output_block is

DB10B248 786AD0CA EB9C1B03 60D2DF4C

temp is

A12D1656 186D2BC2 AF8837A1 F5F41C75 6832B24D 2F4EEB19
EFBD0618 14F0B45D DB10B248 786AD0CA EB9C1B03 60D2DF4C

temp XOR provided_data is

A12D1656 186D2BC2 AF8837A1 F5F41C75 6832B24D 2F4EEB19
EFBD0618 14F0B45D DB10B248 786AD0CA EB9C1B03 60D2DF4C

Key is

A12D1656 186D2BC2
AF8837A1 F5F41C75 6832B24D 2F4EEB19 EFBD0618 14F0B45D

V is

DB10B248 786AD0CA EB9C1B03 60D2DF4C

rnd_val is

738E99C9 5AF59519
AAD37FF3 D5180986 ADEBAB6E 95836725 097E50A8 D1D0BD28