

#####

Block Cipher Modes of Operation

CCM Mode for Authentication and Confidentiality

#####

CCM-AES128

Example #1

Tlen = 32
Nlen = 56
Alen = 64
Plen = 32

Encrypt-Generate

K is
40414243 44454647 48494A4B 4C4D4E4F
N is
10111213 141516
A is
00010203 04050607
P is
20212223

B
4F101112 13141516 00000000 00000004
00080001 02030405 06070000 00000000
20212223 00000000 00000000 00000000

Compute the Mac

Block #1
Plaintext
4F101112 13141516 00000000 00000004
InputBlock 4F101112 13141516 00000000 00000004
OutputBlock 2AD239BB 229B8FB4 6E308F5B C7409B88
Block #2
Plaintext
00080001 02030405 06070000 00000000
InputBlock 2ADA39BA 20988BB1 68378F5B C7409B88
OutputBlock 2E3B9553 0AD7C902 68CAF2C5 97C49292
Block #3
Plaintext
20212223 00000000 00000000 00000000
InputBlock 0E1AB770 0AD7C902 68CAF2C5 97C49292
OutputBlock 6084341B 32042BF0 00B4B799 5553A3C5

T
6084341B

Compute S0

Block #1
InputBlock 07101112 13141516 00000000 00000000
OutputBlock 2D281146 10676C26 32BAD748 559A679A
Text-In 6084341B 00000000 00000000 00000000
Text-Out 4DAC255D 10676C26 32BAD748 559A679A

Compute S1..Sn

Block #1
InputBlock 07101112 13141516 00000000 00000001
OutputBlock 51432378 E474B339 71318484 103CDDFB
Text-In 20212223 8F010000 00010000 0028F9FF
Text-Out 7162015B 6B75B339 71308484 10142404

C is
7162015B 4DAC255D

Decrypt-Verify

Compute S0..Sn

Block #1
InputBlock 07101112 13141516 00000000 00000000
OutputBlock 2D281146 10676C26 32BAD748 559A679A
Text-In 4DAC255D 00000000 00000000 00000000
Text-Out 6084341B 10676C26 32BAD748 559A679A
Block #2
InputBlock 07101112 13141516 00000000 00000001
OutputBlock 51432378 E474B339 71318484 103CDDFB
Text-In 7162015B 00000000 00000000 00000000
Text-Out 20212223 E474B339 71318484 103CDDFB

P
20212223

T
6084341B

B
4F101112 13141516 00000000 00000004
00080001 02030405 06070000 00000000
20212223 00000000 00000000 00000000

Verify the Mac

```

Block #1
  Plaintext
  4F101112 13141516 00000000 00000004
  InputBlock   4F101112 13141516 00000000 00000004
  OutputBlock  2AD239BB 229B8FB4 6E308F5B C7409B88
Block #2
  Plaintext
  00080001 02030405 06070000 00000000
  InputBlock   2ADA39BA 20988BB1 68378F5B C7409B88
  OutputBlock  2E3B9553 0AD7C902 68CAF2C5 97C49292
Block #3
  Plaintext
  20212223 00000000 00000000 00000000
  InputBlock   0E1AB770 0AD7C902 68CAF2C5 97C49292
  OutputBlock  6084341B 32042BF0 00B4B799 5553A3C5

```

```

-----
Mac
  6084341B

```

```

Mac'
  6084341B

```

```

-----
The Mac verifies

```

```

P is
  20212223

```

```

=====
Example #2

```

```

Tlen = 48
Nlen = 64
Alen = 128
Plen = 128
-----

```

```

Encrypt-Generate

```

```

K is
  40414243 44454647 48494A4B 4C4D4E4F
N is
  10111213 14151617
A is
  00010203 04050607 08090A0B 0C0D0E0F
P is
  20212223 24252627 28292A2B 2C2D2E2F

```

```

-----
B
  56101112 13141516 17000000 00000010
  00100001 02030405 06070809 0A0B0C0D
  0E0F0000 00000000 00000000 00000000
  20212223 24252627 28292A2B 2C2D2E2F

```

Compute the Mac

Block #1
 Plaintext
 56101112 13141516 17000000 00000010
 InputBlock 56101112 13141516 17000000 00000010
 OutputBlock 14DF069C ABD1BCDA B1FC1B76 2CA942CA

Block #2
 Plaintext
 00100001 02030405 06070809 0A0B0C0D
 InputBlock 14CF069D A9D2B8DF B7FB137F 26A24EC7
 OutputBlock 46CFDF4B 2B2B0FF9 41F67E31 0699D812

Block #3
 Plaintext
 0E0F0000 00000000 00000000 00000000
 InputBlock 48C0DF4B 2B2B0FF9 41F67E31 0699D812
 OutputBlock 8E3A0218 5B01A7A1 CCB79832 A65E188A

Block #4
 Plaintext
 20212223 24252627 28292A2B 2C2D2E2F
 InputBlock AE1B203B 7F248186 E49EB219 8A7336A5
 OutputBlock 7F479FFC A464322B FE2D4F45 A8D8BA24

T
7F479FFC A464

Compute S0

Block #1
 InputBlock 06101112 13141516 17000000 00000000
 OutputBlock 6081D043 08A97DCC 20CDCC60 BF947B78
 Text-In 7F479FFC A4640000 00000000 00000000
 Text-Out 1FC64FBF ACCD7DCC 20CDCC60 BF947B78

Compute S1..Sn

Block #1
 InputBlock 06101112 13141516 17000000 00000001
 OutputBlock F280D2C3 75CF7945 20335DB9 2B107712
 Text-In 20212223 24252627 28292A2B 2C2D2E2F
 Text-Out D2A1F0E0 51EA5F62 081A7792 073D593D

C is
D2A1F0E0 51EA5F62 081A7792 073D593D
1FC64FBF ACCD

Decrypt-Verify

Compute S0..Sn

Block #1
InputBlock 06101112 13141516 17000000 00000000
OutputBlock 6081D043 08A97DCC 20CDCC60 BF947B78
Text-In 1FC64FBF ACCD00C0 03000000 00000500
Text-Out 7F479FFC A4647D0C 23CDCC60 BF947E78

Block #2
InputBlock 06101112 13141516 17000000 00000001
OutputBlock F280D2C3 75CF7945 20335DB9 2B107712
Text-In D2A1F0E0 51EA5F62 081A7792 073D593D
Text-Out 20212223 24252627 28292A2B 2C2D2E2F

P
20212223 24252627 28292A2B 2C2D2E2F

T
7F479FFC A464

B
56101112 13141516 17000000 00000010
00100001 02030405 06070809 0A0B0C0D
0E0F0000 00000000 00000000 00000000
20212223 24252627 28292A2B 2C2D2E2F

Verify the Mac

Block #1
Plaintext
56101112 13141516 17000000 00000010
InputBlock 56101112 13141516 17000000 00000010
OutputBlock 14DF069C ABD1BCDA B1FC1B76 2CA942CA

Block #2
Plaintext
00100001 02030405 06070809 0A0B0C0D
InputBlock 14CF069D A9D2B8DF B7FB137F 26A24EC7
OutputBlock 46CFDF4B 2B2B0FF9 41F67E31 0699D812

Block #3
Plaintext
0E0F0000 00000000 00000000 00000000
InputBlock 48C0DF4B 2B2B0FF9 41F67E31 0699D812
OutputBlock 8E3A0218 5B01A7A1 CCB79832 A65E188A

Block #4
Plaintext
20212223 24252627 28292A2B 2C2D2E2F
InputBlock AE1B203B 7F248186 E49EB219 8A7336A5
OutputBlock 7F479FFC A464322B FE2D4F45 A8D8BA24

Mac
7F479FFC A464

Mac'
7F479FFC A464

The Mac verifies

P is
20212223 24252627 28292A2B 2C2D2E2F

=====
Example #3

Tlen = 64
Nlen = 96
Alen = 160
Plen = 192

Encrypt-Generate

K is
40414243 44454647 48494A4B 4C4D4E4F
N is
10111213 14151617 18191A1B
A is
00010203 04050607 08090A0B 0C0D0E0F
10111213
P is
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637

B
5A101112 13141516 1718191A 1B000018
00140001 02030405 06070809 0A0B0C0D
0E0F1011 12130000 00000000 00000000
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 00000000 00000000

Compute the Mac

Block #1
Plaintext
5A101112 13141516 1718191A 1B000018
InputBlock 5A101112 13141516 1718191A 1B000018
OutputBlock A72F566C FDF02E0C C9FD2E5A 7EC8DC2D
Block #2
Plaintext
00140001 02030405 06070809 0A0B0C0D
InputBlock A73B566D FFF32A09 CFFA2653 74C3D020
OutputBlock C1429ED7 C76185E3 D1B720B1 4CE8BF82
Block #3
Plaintext
0E0F1011 12130000 00000000 00000000
InputBlock CF4D8EC6 D57285E3 D1B720B1 4CE8BF82
OutputBlock A9509E3B 58CCA9C4 D855BE30 8A60F2D1
Block #4
Plaintext

```
20212223 24252627 28292A2B 2C2D2E2F
InputBlock 8971BC18 7CE98FE3 F07C941B A64DDCFE
OutputBlock 8F634EB8 2AC15581 490194CD F74B711E
Block #5
Plaintext
30313233 34353637 00000000 00000000
InputBlock BF527C8B 1EF463B6 490194CD F74B711E
OutputBlock 67C99240 C7D51048 B4C9BCEC 10AE0215
```

T
67C99240 C7D51048

Compute S0

```
Block #1
InputBlock 02101112 13141516 1718191A 1B000000
OutputBlock 2F8A00BB 06658919 C3A040A6 EAED1A7F
Text-In 67C99240 C7D51048 00000000 00000000
Text-Out 484392FB C1B09951 C3A040A6 EAED1A7F
-----
```

Compute S1..Sn

```
Block #1
InputBlock 02101112 13141516 1718191A 1B000001
OutputBlock C393238A D1923C5D B335C0C7 E1BAC924
Text-In 20212223 24252627 28292A2B 2C2D2E2F
Text-Out E3B201A9 F5B71A7A 9B1CEAEC CD97E70B
Block #2
InputBlock 02101112 13141516 1718191A 1B000002
OutputBlock 514798EA 9077BC92 6C22EBEF 2AC732DC
Text-In 30313233 34353637 00E4BCA5 90010000
Text-Out 6176AAD9 A4428AA5 6CC6574A BAC632DC
-----
```

C is
E3B201A9 F5B71A7A 9B1CEAEC CD97E70B
6176AAD9 A4428AA5 484392FB C1B09951

Decrypt-Verify

Compute S0..Sn

```
Block #1
InputBlock 02101112 13141516 1718191A 1B000000
OutputBlock 2F8A00BB 06658919 C3A040A6 EAED1A7F
Text-In 484392FB C1B09951 0400EAEC CD97E70B
Text-Out 67C99240 C7D51048 C7A0AA4A 277AFD74
Block #2
InputBlock 02101112 13141516 1718191A 1B000001
OutputBlock C393238A D1923C5D B335C0C7 E1BAC924
Text-In E3B201A9 F5B71A7A 9B1CEAEC CD97E70B
Text-Out 20212223 24252627 28292A2B 2C2D2E2F
Block #3
```

InputBlock 02101112 13141516 1718191A 1B000002
OutputBlock 514798EA 9077BC92 6C22EBEF 2AC732DC
Text-In 6176AAD9 A4428AA5 0200CC60 BF947E78
Text-Out 30313233 34353637 6E22278F 95534CA4

P

20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637

T

67C99240 C7D51048

B

5A101112 13141516 1718191A 1B000018
00140001 02030405 06070809 0A0B0C0D
0E0F1011 12130000 00000000 00000000
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 00000000 00000000

Verify the Mac

Block #1

Plaintext
5A101112 13141516 1718191A 1B000018
InputBlock 5A101112 13141516 1718191A 1B000018
OutputBlock A72F566C FDF02E0C C9FD2E5A 7EC8DC2D

Block #2

Plaintext
00140001 02030405 06070809 0A0B0C0D
InputBlock A73B566D FFF32A09 CFFA2653 74C3D020
OutputBlock C1429ED7 C76185E3 D1B720B1 4CE8BF82

Block #3

Plaintext
0E0F1011 12130000 00000000 00000000
InputBlock CF4D8EC6 D57285E3 D1B720B1 4CE8BF82
OutputBlock A9509E3B 58CCA9C4 D855BE30 8A60F2D1

Block #4

Plaintext
20212223 24252627 28292A2B 2C2D2E2F
InputBlock 8971BC18 7CE98FE3 F07C941B A64DDCFE
OutputBlock 8F634EB8 2AC15581 490194CD F74B711E

Block #5

Plaintext
30313233 34353637 00000000 00000000
InputBlock BF527C8B 1EF463B6 490194CD F74B711E
OutputBlock 67C99240 C7D51048 B4C9BCEC 10AE0215

Mac

67C99240 C7D51048

Mac'

67C99240 C7D51048

The Mac verifies

P is
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637

=====

Example #4

Tlen = 32
Nlen = 56
Alen = 0
Plen = 512

Encrypt-Generate

K is
40414243 44454647 48494A4B 4C4D4E4F
N is
10111213 141516
A is
<empty>
P is
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F

B
0F101112 13141516 00000000 00000040
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F

Compute the Mac

Block #1
Plaintext
0F101112 13141516 00000000 00000040
InputBlock 0F101112 13141516 00000000 00000040
OutputBlock 9099080E C6CB2EC8 73619985 E6730968

Block #2
Plaintext
20212223 24252627 28292A2B 2C2D2E2F
InputBlock B0B82A2D E2EE08EF 5B48B3AE CA5E2747
OutputBlock 4525F5C6 77448BAE BAA23474 08C70281

Block #3
Plaintext
30313233 34353637 38393A3B 3C3D3E3F
InputBlock 7514C7F5 4371BD99 829B0E4F 34FA3CBE
OutputBlock EDDAF750 798E9FA6 CB46F761 152A3F48

```

Block #4
  Plaintext
  40414243 44454647 4849A4B 4C4D4E4F
  InputBlock  AD9BB513 3DCBD9E1 830FBD2A 59677107
  OutputBlock  CEC248C2 19848C54 9CB0F3F6 E8447086
Block #5
  Plaintext
  50515253 54555657 58595A5B 5C5D5E5F
  InputBlock  9E931A91 4DD1DA03 C4E9A9AD B4192ED9
  OutputBlock  EB43741A 0291B7ED 97883FA0 267464D0

```

```

T
  EB43741A

```

Compute S0

```

Block #1
  InputBlock  07101112 13141516 00000000 00000000
  OutputBlock 2D281146 10676C26 32BAD748 559A679A
  Text-In     EB43741A 00000000 00000000 00000000
  Text-Out    C66B655C 10676C26 32BAD748 559A679A

```

Compute S1..Sn

```

Block #1
  InputBlock  07101112 13141516 00000000 00000001
  OutputBlock 51432378 E474B339 71318484 103CDDFB
  Text-In     20212223 24252627 28292A2B 2C2D2E2F
  Text-Out    7162015B C051951E 5918AEAF 3C11F3D4
Block #2
  InputBlock  07101112 13141516 00000000 00000002
  OutputBlock 9C070DBE 6F5FC5E4 5159013F CE719016
  Text-In     30313233 34353637 38393A3B 3C3D3E3F
  Text-Out    AC363F8D 5B6AF3D3 69603B04 F24CAE29
Block #3
  InputBlock  07101112 13141516 00000000 00000003
  OutputBlock D60F6D68 BD965704 BF6C6D85 61F94CA5
  Text-In     40414243 44454647 4849A4B 4C4D4E4F
  Text-Out    964E2F2B F9D31143 F72527CE 2DB402EA
Block #4
  InputBlock  07101112 13141516 00000000 00000004
  OutputBlock E7375C19 44E5D8D5 7E3C4D96 AA5F39A6
  Text-In     50515253 54555657 58595A5B 5C5D5E5F
  Text-Out    B7660E4A 10B08E82 266517CD F60267F9

```

C is

```

7162015B C051951E 5918AEAF 3C11F3D4
AC363F8D 5B6AF3D3 69603B04 F24CAE29
964E2F2B F9D31143 F72527CE 2DB402EA
B7660E4A 10B08E82 266517CD F60267F9
C66B655C

```

Decrypt-Verify

Compute S0..Sn

Block #1
InputBlock 07101112 13141516 00000000 00000000
OutputBlock 2D281146 10676C26 32BAD748 559A679A
Text-In C66B655C 13141516 00000000 00000040
Text-Out EB43741A 03737930 32BAD748 559A67DA
Block #2
InputBlock 07101112 13141516 00000000 00000001
OutputBlock 51432378 E474B339 71318484 103CDDFB
Text-In 7162015B C051951E 5918AEAF 3C11F3D4
Text-Out 20212223 24252627 28292A2B 2C2D2E2F
Block #3
InputBlock 07101112 13141516 00000000 00000002
OutputBlock 9C070DBE 6F5FC5E4 5159013F CE719016
Text-In AC363F8D 5B6AF3D3 69603B04 F24CAE29
Text-Out 30313233 34353637 38393A3B 3C3D3E3F
Block #4
InputBlock 07101112 13141516 00000000 00000003
OutputBlock D60F6D68 BD965704 BF6C6D85 61F94CA5
Text-In 964E2F2B F9D31143 F72527CE 2DB402EA
Text-Out 40414243 44454647 48494A4B 4C4D4E4F
Block #5
InputBlock 07101112 13141516 00000000 00000004
OutputBlock E7375C19 44E5D8D5 7E3C4D96 AA5F39A6
Text-In B7660E4A 10B08E82 266517CD F60267F9
Text-Out 50515253 54555657 58595A5B 5C5D5E5F

P
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F

T
EB43741A

B
0F101112 13141516 00000000 00000040
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F

Verify the Mac

Block #1
Plaintext
0F101112 13141516 00000000 00000040
InputBlock 0F101112 13141516 00000000 00000040
OutputBlock 9099080E C6CB2EC8 73619985 E6730968
Block #2
Plaintext

```
20212223 24252627 28292A2B 2C2D2E2F
InputBlock  B0B82A2D E2EE08EF 5B48B3AE CA5E2747
OutputBlock 4525F5C6 77448BAE BAA23474 08C70281
Block #3
Plaintext
30313233 34353637 38393A3B 3C3D3E3F
InputBlock  7514C7F5 4371BD99 829B0E4F 34FA3CBE
OutputBlock EDDAF750 798E9FA6 CB46F761 152A3F48
Block #4
Plaintext
40414243 44454647 48494A4B 4C4D4E4F
InputBlock  AD9BB513 3DCBD9E1 830FBD2A 59677107
OutputBlock CEC248C2 19848C54 9CB0F3F6 E8447086
Block #5
Plaintext
50515253 54555657 58595A5B 5C5D5E5F
InputBlock  9E931A91 4DD1DA03 C4E9A9AD B4192ED9
OutputBlock EB43741A 0291B7ED 97883FA0 267464D0
```

```
-----
Mac
EB43741A
```

```
Mac'
EB43741A
```

```
-----
The Mac verifies
```

```
P is
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F
```

```
=====
Example #5
```

```
Tlen = 32
Nlen = 56
Alen = 512
Plen = 0
-----
```

```
Encrypt-Generate
```

```
K is
40414243 44454647 48494A4B 4C4D4E4F
N is
10111213 141516
A is
00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
P is
<empty>
```

B

4F101112 13141516 00000000 00000000
00400001 02030405 06070809 0A0B0C0D
0E0F1011 12131415 16171819 1A1B1C1D
1E1F2021 22232425 26272829 2A2B2C2D
2E2F3031 32333435 36373839 3A3B3C3D
3E3F0000 00000000 00000000 00000000

Compute the Mac

Block #1

Plaintext

4F101112 13141516 00000000 00000000
InputBlock 4F101112 13141516 00000000 00000000
OutputBlock D5B7B9A9 D8A531A5 3DDC9151 7E069F61

Block #2

Plaintext

00400001 02030405 06070809 0A0B0C0D
InputBlock D5F7B9A8 DAA635A0 3BDB9958 740D936C
OutputBlock F1772540 CF3CF000 6EEE02D A4573703

Block #3

Plaintext

0E0F1011 12131415 16171819 1A1B1C1D
InputBlock FF783551 DD2FE415 78F9A834 BE4C2B1E
OutputBlock 7695F384 BADF4806 74190DA1 5E44DB68

Block #4

Plaintext

1E1F2021 22232425 26272829 2A2B2C2D
InputBlock 688AD3A5 98FC6C23 523E2588 746FF745
OutputBlock F1609045 D4CACF1F 6F6158D9 54461EA5

Block #5

Plaintext

2E2F3031 32333435 36373839 3A3B3C3D
InputBlock DF4FA074 E6F9FB2A 595660E0 6E7D2298
OutputBlock 2DE1F91A 1EC05368 B24669E4 899AB13E

Block #6

Plaintext

3E3F0000 00000000 00000000 00000000
InputBlock 13DEF91A 1EC05368 B24669E4 899AB13E
OutputBlock C56832BE B146FF3B 35BA1761 C9C00D58

T

C56832BE

Compute S0

Block #1

InputBlock 07101112 13141516 00000000 00000000
OutputBlock 2D281146 10676C26 32BAD748 559A679A
Text-In C56832BE 00000000 00000000 00000000
Text-Out E84023F8 10676C26 32BAD748 559A679A

Compute S1..Sn

<empty payload>

C is
E84023F8

Decrypt-Verify

Compute S0..Sn

Block #1
InputBlock 07101112 13141516 00000000 00000000
OutputBlock 2D281146 10676C26 32BAD748 559A679A
Text-In E84023F8 030000C0 58595A5B 5C5D0700
Text-Out C56832BE 13676CE6 6AE38D13 09C7609A

P
<empty>

T
C56832BE

B
4F101112 13141516 00000000 00000000
00400001 02030405 06070809 0A0B0C0D
0E0F1011 12131415 16171819 1A1B1C1D
1E1F2021 22232425 26272829 2A2B2C2D
2E2F3031 32333435 36373839 3A3B3C3D
3E3F0000 00000000 00000000 00000000

Verify the Mac

Block #1
Plaintext
4F101112 13141516 00000000 00000000
InputBlock 4F101112 13141516 00000000 00000000
OutputBlock D5B7B9A9 D8A531A5 3DDC9151 7E069F61
Block #2
Plaintext
00400001 02030405 06070809 0A0B0C0D
InputBlock D5F7B9A8 DAA635A0 3BDB9958 740D936C
OutputBlock F1772540 CF3CF000 6EEE02D A4573703
Block #3
Plaintext
0E0F1011 12131415 16171819 1A1B1C1D
InputBlock FF783551 DD2FE415 78F9A834 BE4C2B1E
OutputBlock 7695F384 BADF4806 74190DA1 5E44DB68
Block #4

```
Plaintext
1E1F2021 22232425 26272829 2A2B2C2D
InputBlock   688AD3A5 98FC6C23 523E2588 746FF745
OutputBlock  F1609045 D4CACF1F 6F6158D9 54461EA5
Block #5
Plaintext
2E2F3031 32333435 36373839 3A3B3C3D
InputBlock   DF4FA074 E6F9FB2A 595660E0 6E7D2298
OutputBlock  2DE1F91A 1EC05368 B24669E4 899AB13E
Block #6
Plaintext
3E3F0000 00000000 00000000 00000000
InputBlock   13DEF91A 1EC05368 B24669E4 899AB13E
OutputBlock  C56832BE B146FF3B 35BA1761 C9C00D58
```

```
-----
Mac
C56832BE
```

```
Mac'
C56832BE
```

```
-----
The Mac verifies
```

```
P is
<empty>
```

```
=====
*****
#####
```

```
Block Cipher Modes of Operation
CCM Mode for Authentication and Confidentiality
```

```
#####
CCM-AES192
```

```
-----
Example #1
```

```
Tlen = 32
Nlen = 56
Alen = 64
Plen = 32
-----
```

```
Encrypt-Generate
```

```
K is
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657
N is
10111213 141516
A is
```

00010203 04050607

P is

20212223

B

4F101112 13141516 00000000 00000004
00080001 02030405 06070000 00000000
20212223 00000000 00000000 00000000

Compute the Mac

Block #1

Plaintext

4F101112 13141516 00000000 00000004

InputBlock 4F101112 13141516 00000000 00000004

OutputBlock 41010554 D3301B18 DA9BB4FD 48D9F733

Block #2

Plaintext

00080001 02030405 06070000 00000000

InputBlock 41090555 D1331F1D DC9CB4FD 48D9F733

OutputBlock 521A1567 B9C519DC B1FE866B C94D576A

Block #3

Plaintext

20212223 00000000 00000000 00000000

InputBlock 723B3744 B9C519DC B1FE866B C94D576A

OutputBlock 08C8A3CE 4D53E873 AC4338BC 70E01090

T

08C8A3CE

Compute S0

Block #1

InputBlock 07101112 13141516 00000000 00000000

OutputBlock C00B851B BC5508C7 DE9B8605 06CA6B84

Text-In 08C8A3CE 00000000 00000000 00000000

Text-Out C8C326D5 BC5508C7 DE9B8605 06CA6B84

Compute S1..Sn

Block #1

InputBlock 07101112 13141516 00000000 00000001

OutputBlock 38CF3513 D06C288F 6F81C3EE 1EEBB1B3

Text-In 20212223 24010000 00010000 0028F9FF

Text-Out 18EE1730 F46D288F 6F80C3EE 1EC3484C

C is

18EE1730 C8C326D5

Decrypt-Verify

Compute S0..Sn

Block #1
 InputBlock 07101112 13141516 00000000 00000000
 OutputBlock C00B851B BC5508C7 DE9B8605 06CA6B84
 Text-In C8C326D5 030000C0 0E0027CE 2DB402EA
 Text-Out 08C8A3CE BF550807 D09BA1CB 2B7E696E

Block #2
 InputBlock 07101112 13141516 00000000 00000001
 OutputBlock 38CF3513 D06C288F 6F81C3EE 1EEBB1B3
 Text-In 18EE1730 10B08E82 266517CD F6020500
 Text-Out 20212223 C0DCA60D 49E4D423 E8E9B4B3

P
20212223

T
08C8A3CE

B
 4F101112 13141516 00000000 00000004
 00080001 02030405 06070000 00000000
 20212223 00000000 00000000 00000000

Verify the Mac

Block #1
 Plaintext
 4F101112 13141516 00000000 00000004
 InputBlock 4F101112 13141516 00000000 00000004
 OutputBlock 41010554 D3301B18 DA9BB4FD 48D9F733

Block #2
 Plaintext
 00080001 02030405 06070000 00000000
 InputBlock 41090555 D1331F1D DC9CB4FD 48D9F733
 OutputBlock 521A1567 B9C519DC B1FE866B C94D576A

Block #3
 Plaintext
 20212223 00000000 00000000 00000000
 InputBlock 723B3744 B9C519DC B1FE866B C94D576A
 OutputBlock 08C8A3CE 4D53E873 AC4338BC 70E01090

Mac
08C8A3CE

Mac'
08C8A3CE

The Mac verifies

P is
20212223

=====

Example #2

Tlen = 48
Nlen = 64
Alen = 128
Plen = 128

Encrypt-Generate

K is
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657
N is
10111213 14151617
A is
00010203 04050607 08090A0B 0C0D0E0F
P is
20212223 24252627 28292A2B 2C2D2E2F

B
56101112 13141516 17000000 00000010
00100001 02030405 06070809 0A0B0C0D
0E0F0000 00000000 00000000 00000000
20212223 24252627 28292A2B 2C2D2E2F

Compute the Mac

Block #1
Plaintext
56101112 13141516 17000000 00000010
InputBlock 56101112 13141516 17000000 00000010
OutputBlock 9AF42EF5 A6120A84 A09BF8CB 87514EE0
Block #2
Plaintext
00100001 02030405 06070809 0A0B0C0D
InputBlock 9AE42EF4 A4110E81 A69CF4BF 8D5A42ED
OutputBlock 4B8CFC80 8B7F8CCC E11E180B 741BDF2A
Block #3
Plaintext
0E0F0000 00000000 00000000 00000000
InputBlock 4583FC80 8B7F8CCC E11E180B 741BDF2A
OutputBlock 1C5FA006 CF5154F4 FD6C1988 A26D89EC
Block #4
Plaintext
20212223 24252627 28292A2B 2C2D2E2F
InputBlock 3C7E8225 EB7472D3 D54533A3 8E40A7C3
OutputBlock CB70F475 C8E87078 58D54254 E1464C98

T
CB70F475 C8E8

Compute S0

Block #1
InputBlock 06101112 13141516 17000000 00000000
OutputBlock 9D99385D 628F5E77 0C92E77B 6C0206C4
Text-In CB70F475 C8E80000 00000000 00000000
Text-Out 56E9CC28 AA675E77 0C92E77B 6C0206C4

Compute S1..Sn

Block #1
InputBlock 06101112 13141516 17000000 00000001
OutputBlock 021394C3 B6646E89 5A109696 362250E4
Text-In 20212223 24252627 28292A2B 2C2D2E2F
Text-Out 2232B6E0 924148AE 7239BCBD 1A0F7ECB

C is
2232B6E0 924148AE 7239BCBD 1A0F7ECB
56E9CC28 AA67

Decrypt-Verify

Compute S0..Sn

Block #1
InputBlock 06101112 13141516 17000000 00000000
OutputBlock 9D99385D 628F5E77 0C92E77B 6C0206C4
Text-In 56E9CC28 AA6700C0 0D0017CD F6020500
Text-Out CB70F475 C8E85EB7 0192F0B6 9A0003C4
Block #2
InputBlock 06101112 13141516 17000000 00000001
OutputBlock 021394C3 B6646E89 5A109696 362250E4
Text-In 2232B6E0 924148AE 7239BCBD 1A0F7ECB
Text-Out 20212223 24252627 28292A2B 2C2D2E2F

P
20212223 24252627 28292A2B 2C2D2E2F

T
CB70F475 C8E8

B
56101112 13141516 17000000 00000010
00100001 02030405 06070809 0A0B0C0D

0E0F0000 00000000 00000000 00000000
20212223 24252627 28292A2B 2C2D2E2F

Verify the Mac

Block #1
Plaintext
56101112 13141516 17000000 00000010
InputBlock 56101112 13141516 17000000 00000010
OutputBlock 9AF42EF5 A6120A84 A09BFCB6 87514EE0
Block #2
Plaintext
00100001 02030405 06070809 0A0B0C0D
InputBlock 9AE42EF4 A4110E81 A69CF4BF 8D5A42ED
OutputBlock 4B8CFC80 8B7F8CCC E11E180B 741BDF2A
Block #3
Plaintext
0E0F0000 00000000 00000000 00000000
InputBlock 4583FC80 8B7F8CCC E11E180B 741BDF2A
OutputBlock 1C5FA006 CF5154F4 FD6C1988 A26D89EC
Block #4
Plaintext
20212223 24252627 28292A2B 2C2D2E2F
InputBlock 3C7E8225 EB7472D3 D54533A3 8E40A7C3
OutputBlock CB70F475 C8E87078 58D54254 E1464C98

Mac
CB70F475 C8E8

Mac'
CB70F475 C8E8

The Mac verifies

P is
20212223 24252627 28292A2B 2C2D2E2F

=====

Example #3

Tlen = 64
Nlen = 96
Alen = 160
Plen = 192

Encrypt-Generate

K is
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657
N is
10111213 14151617 18191A1B
A is

00010203 04050607 08090A0B 0C0D0E0F
10111213

P is

20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637

B

5A101112 13141516 1718191A 1B000018
00140001 02030405 06070809 0A0B0C0D
0E0F1011 12130000 00000000 00000000
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 00000000 00000000

Compute the Mac

Block #1

Plaintext

5A101112 13141516 1718191A 1B000018
InputBlock 5A101112 13141516 1718191A 1B000018
OutputBlock C4941769 35E08020 E5E2A33A A3AC831E

Block #2

Plaintext

00140001 02030405 06070809 0A0B0C0D
InputBlock C4801768 37E38425 E3E5AB33 A9A78F13
OutputBlock 3A0F3212 A3C1341E 8803BBF9 7EE3AF26

Block #3

Plaintext

0E0F1011 12130000 00000000 00000000
InputBlock 34002203 B1D2341E 8803BBF9 7EE3AF26
OutputBlock 7D481F1E E022C8CB C3BF2330 6E8BD185

Block #4

Plaintext

20212223 24252627 28292A2B 2C2D2E2F
InputBlock 5D693D3D C407EEEC EB96091B 42A6FFAA
OutputBlock 15414200 1B7575C7 2B6C7C12 50FEFDA8

Block #5

Plaintext

30313233 34353637 00000000 00000000
InputBlock 25707033 2F4043F0 2B6C7C12 50FEFDA8
OutputBlock 0BCD9057 7CDC251A E7C9EF4F C18B0BF8

T

0BCD9057 7CDC251A

Compute S0

Block #1

InputBlock 02101112 13141516 1718191A 1B000000
OutputBlock 49FBF905 2C83BC40 5C8AFAB3 20C91973
Text-In 0BCD9057 7CDC251A 00000000 00000000
Text-Out 42366952 505F995A 5C8AFAB3 20C91973

Compute S1..Sn

Block #1
InputBlock 02101112 13141516 1718191A 1B000001
OutputBlock A0A0134C FCB302F1 04CE4954 9564BB99
Text-In 20212223 24252627 28292A2B 2C2D2E2F
Text-Out 8081316F D89624D6 2CE7637F B94995B6
Block #2
InputBlock 02101112 13141516 1718191A 1B000002
OutputBlock 532D62E5 21B3E836 0D7BC2DE B6BD8500
Text-In 30313233 34353637 00E4BCA5 90010000
Text-Out 631C50D6 1586DE01 0D9F7E7B 26BC8500

C is
8081316F D89624D6 2CE7637F B94995B6
631C50D6 1586DE01 42366952 505F995A

Decrypt-Verify

Compute S0..Sn

Block #1
InputBlock 02101112 13141516 1718191A 1B000000
OutputBlock 49FBF905 2C83BC40 5C8AFAB3 20C91973
Text-In 42366952 505F995A 0C00637F B94995B6
Text-Out 0BCD9057 7CDC251A 508A99CC 99808CC5
Block #2
InputBlock 02101112 13141516 1718191A 1B000001
OutputBlock A0A0134C FCB302F1 04CE4954 9564BB99
Text-In 8081316F D89624D6 2CE7637F B94995B6
Text-Out 20212223 24252627 28292A2B 2C2D2E2F
Block #3
InputBlock 02101112 13141516 1718191A 1B000002
OutputBlock 532D62E5 21B3E836 0D7BC2DE B6BD8500
Text-In 631C50D6 1586DE01 0A002A2B 2C2D2E2F
Text-Out 30313233 34353637 077BE8F5 9A90AB2F

P
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637

T
0BCD9057 7CDC251A

B
5A101112 13141516 1718191A 1B000018
00140001 02030405 06070809 0A0B0C0D
0E0F1011 12130000 00000000 00000000
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 00000000 00000000

Verify the Mac

```

Block #1
  Plaintext
    5A101112 13141516 1718191A 1B000018
  InputBlock   5A101112 13141516 1718191A 1B000018
  OutputBlock  C4941769 35E08020 E5E2A33A A3AC831E
Block #2
  Plaintext
    00140001 02030405 06070809 0A0B0C0D
  InputBlock   C4801768 37E38425 E3E5AB33 A9A78F13
  OutputBlock  3A0F3212 A3C1341E 8803BBF9 7EE3AF26
Block #3
  Plaintext
    0E0F1011 12130000 00000000 00000000
  InputBlock   34002203 B1D2341E 8803BBF9 7EE3AF26
  OutputBlock  7D481F1E E022C8CB C3BF2330 6E8BD185
Block #4
  Plaintext
    20212223 24252627 28292A2B 2C2D2E2F
  InputBlock   5D693D3D C407EEEC EB96091B 42A6FFAA
  OutputBlock  15414200 1B7575C7 2B6C7C12 50FEFDA8
Block #5
  Plaintext
    30313233 34353637 00000000 00000000
  InputBlock   25707033 2F4043F0 2B6C7C12 50FEFDA8
  OutputBlock  0BCD9057 7CDC251A E7C9EF4F C18B0BFB

```

```

-----
Mac
  0BCD9057 7CDC251A

```

```

Mac'
  0BCD9057 7CDC251A

```

```

-----

```

The Mac verifies

```

P is
  20212223 24252627 28292A2B 2C2D2E2F
  30313233 34353637

```

```

=====

```

Example #4

```

Tlen = 32
Nlen = 56
Alen = 0
Plen = 512

```

```

-----

```

Encrypt-Generate

```

K is
  40414243 44454647 48494A4B 4C4D4E4F
  50515253 54555657
N is

```

10111213 141516

A is

<empty>

P is

20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F

B

0F101112 13141516 00000000 00000040
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F

Compute the Mac

Block #1

Plaintext

0F101112 13141516 00000000 00000040

InputBlock 0F101112 13141516 00000000 00000040

OutputBlock 7B02760B A35C4239 18471C8B DE51F837

Block #2

Plaintext

20212223 24252627 28292A2B 2C2D2E2F

InputBlock 5B235428 8779641E 306E36A0 F27CD618

OutputBlock B0E28591 1ECD50C9 D4B21E2A 0904F2B3

Block #3

Plaintext

30313233 34353637 38393A3B 3C3D3E3F

InputBlock 80D3B7A2 2AF866FE EC8B2411 3539CC8C

OutputBlock 4062B2D3 D4361CA6 AEC8DD6C 2F65B5D7

Block #4

Plaintext

40414243 44454647 48494A4B 4C4D4E4F

InputBlock 0023F090 90735AE1 E6819727 6328FB98

OutputBlock 43908C95 9B62B3CD EFD473EE 4B2B8D1D

Block #5

Plaintext

50515253 54555657 58595A5B 5C5D5E5F

InputBlock 13C1DEC6 CF37E59A B78D29B5 1776D342

OutputBlock 09C5AAA7 12ABE338 8331E506 99FB5C10

T

09C5AAA7

Compute S0

Block #1

InputBlock 07101112 13141516 00000000 00000000

OutputBlock C00B851B BC5508C7 DE9B8605 06CA6B84

Text-In 09C5AAA7 00000000 00000000 00000000

Text-Out C9CE2FBC BC5508C7 DE9B8605 06CA6B84

Compute S1..Sn

```
Block #1
  InputBlock  07101112 13141516 00000000 00000001
  OutputBlock 38CF3513 D06C288F 6F81C3EE 1EEBB1B3
  Text-In     20212223 24252627 28292A2B 2C2D2E2F
  Text-Out    18EE1730 F4490EA8 47A8E9C5 32C69F9C
Block #2
  InputBlock  07101112 13141516 00000000 00000002
  OutputBlock 3A62A86B 682B4D5D 62C023CF BDADB696
  Text-In     30313233 34353637 38393A3B 3C3D3E3F
  Text-Out    0A539A58 5C1E7B6A 5AF919F4 819088A9
Block #3
  InputBlock  07101112 13141516 00000000 00000003
  OutputBlock 2E977016 14DD9547 3634DC77 379D5DA4
  Text-In     40414243 44454647 48494A4B 4C4D4E4F
  Text-Out    6ED63255 5098D300 7E7D963C 7BD013EB
Block #4
  InputBlock  07101112 13141516 00000000 00000004
  OutputBlock 60272383 AF96CC5A ACFB30C4 17C313F2
  Text-In     50515253 54555657 58595A5B 5C5D5E5F
  Text-Out    307671D0 FBC39A0D F4A26A9F 4B9E4DAD
```

C is

```
18EE1730 F4490EA8 47A8E9C5 32C69F9C
0A539A58 5C1E7B6A 5AF919F4 819088A9
6ED63255 5098D300 7E7D963C 7BD013EB
307671D0 FBC39A0D F4A26A9F 4B9E4DAD
C9CE2FBC
```

Decrypt-Verify

Compute S0..Sn

```
Block #1
  InputBlock  07101112 13141516 00000000 00000000
  OutputBlock C00B851B BC5508C7 DE9B8605 06CA6B84
  Text-In     C9CE2FBC 13141516 00000000 00000040
  Text-Out    09C5AAA7 AF411DD1 DE9B8605 06CA6BC4
Block #2
  InputBlock  07101112 13141516 00000000 00000001
  OutputBlock 38CF3513 D06C288F 6F81C3EE 1EEBB1B3
  Text-In     18EE1730 F4490EA8 47A8E9C5 32C69F9C
  Text-Out    20212223 24252627 28292A2B 2C2D2E2F
Block #3
  InputBlock  07101112 13141516 00000000 00000002
  OutputBlock 3A62A86B 682B4D5D 62C023CF BDADB696
  Text-In     0A539A58 5C1E7B6A 5AF919F4 819088A9
  Text-Out    30313233 34353637 38393A3B 3C3D3E3F
Block #4
  InputBlock  07101112 13141516 00000000 00000003
  OutputBlock 2E977016 14DD9547 3634DC77 379D5DA4
  Text-In     6ED63255 5098D300 7E7D963C 7BD013EB
```

Text-Out 40414243 44454647 48494A4B 4C4D4E4F
Block #5
InputBlock 07101112 13141516 00000000 00000004
OutputBlock 60272383 AF96CC5A ACFB30C4 17C313F2
Text-In 307671D0 FBC39A0D F4A26A9F 4B9E4DAD
Text-Out 50515253 54555657 58595A5B 5C5D5E5F

P
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F

T
09C5AAA7

B
0F101112 13141516 00000000 00000040
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F

Verify the Mac

Block #1
Plaintext
0F101112 13141516 00000000 00000040
InputBlock 0F101112 13141516 00000000 00000040
OutputBlock 7B02760B A35C4239 18471C8B DE51F837
Block #2
Plaintext
20212223 24252627 28292A2B 2C2D2E2F
InputBlock 5B235428 8779641E 306E36A0 F27CD618
OutputBlock B0E28591 1ECD50C9 D4B21E2A 0904F2B3
Block #3
Plaintext
30313233 34353637 38393A3B 3C3D3E3F
InputBlock 80D3B7A2 2AF866FE EC8B2411 3539CC8C
OutputBlock 4062B2D3 D4361CA6 AEC8DD6C 2F65B5D7
Block #4
Plaintext
40414243 44454647 48494A4B 4C4D4E4F
InputBlock 0023F090 90735AE1 E6819727 6328FB98
OutputBlock 43908C95 9B62B3CD EFD473EE 4B2B8D1D
Block #5
Plaintext
50515253 54555657 58595A5B 5C5D5E5F
InputBlock 13C1DEC6 CF37E59A B78D29B5 1776D342
OutputBlock 09C5AAA7 12ABE338 8331E506 99FB5C10

Mac
09C5AAA7

Mac'
09C5AAA7

The Mac verifies

P is
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F

=====

Example #5

Tlen = 32
Nlen = 56
Alen = 512
Plen = 0

Encrypt-Generate

K is
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657

N is
10111213 141516

A is
00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F

P is
<empty>

B
4F101112 13141516 00000000 00000000
00400001 02030405 06070809 0A0B0C0D
0E0F1011 12131415 16171819 1A1B1C1D
1E1F2021 22232425 26272829 2A2B2C2D
2E2F3031 32333435 36373839 3A3B3C3D
3E3F0000 00000000 00000000 00000000

Compute the Mac

Block #1
Plaintext
4F101112 13141516 00000000 00000000
InputBlock 4F101112 13141516 00000000 00000000
OutputBlock 9A092A11 7F2BD319 D45C4EF9 9FD0E8A9
Block #2
Plaintext

```

00400001 02030405 06070809 0A0B0C0D
InputBlock 9A492A10 7D28D71C D25B46F0 95DBE4A4
OutputBlock FACA8BA0 73669FD4 5CF43B42 7E3013F6
Block #3
Plaintext
0E0F1011 12131415 16171819 1A1B1C1D
InputBlock F4C59BB1 61758BC1 4AE3235B 642B0FEB
OutputBlock CEC60BC8 54B4DE20 C7D921EB 4A468269
Block #4
Plaintext
1E1F2021 22232425 26272829 2A2B2C2D
InputBlock D0D92BE9 7697FA05 E1FE09C2 606DAE44
OutputBlock AB7B4C27 CA1ECA3F A3109637 2558D66F
Block #5
Plaintext
2E2F3031 32333435 36373839 3A3B3C3D
InputBlock 85547C16 F82DFE0A 9527AE0E 1F63EA52
OutputBlock 0FFB328B 7D21D483 7E1F1636 2409C26F
Block #6
Plaintext
3E3F0000 00000000 00000000 00000000
InputBlock 31C4328B 7D21D483 7E1F1636 2409C26F
OutputBlock 31F0AF4C E0F62807 70F709E9 8671AD14

```

T

31F0AF4C

Compute S0

```

Block #1
InputBlock 07101112 13141516 00000000 00000000
OutputBlock C00B851B BC5508C7 DE9B8605 06CA6B84
Text-In 31F0AF4C 00000000 00000000 00000000
Text-Out F1FB2A57 BC5508C7 DE9B8605 06CA6B84

```

Compute S1..Sn

<empty payload>

C is

F1FB2A57

Decrypt-Verify

Compute S0..Sn

```

Block #1
InputBlock 07101112 13141516 00000000 00000000
OutputBlock C00B851B BC5508C7 DE9B8605 06CA6B84
Text-In F1FB2A57 970004C0 06008605 06CA6BC4
Text-Out 31F0AF4C 2B550C07 D89B0000 00000040

```

P
<empty>

T
31F0AF4C

B
4F101112 13141516 00000000 00000000
00400001 02030405 06070809 0A0B0C0D
0E0F1011 12131415 16171819 1A1B1C1D
1E1F2021 22232425 26272829 2A2B2C2D
2E2F3031 32333435 36373839 3A3B3C3D
3E3F0000 00000000 00000000 00000000

Verify the Mac

Block #1
Plaintext
4F101112 13141516 00000000 00000000
InputBlock 4F101112 13141516 00000000 00000000
OutputBlock 9A092A11 7F2BD319 D45C4EF9 9FD0E8A9
Block #2
Plaintext
00400001 02030405 06070809 0A0B0C0D
InputBlock 9A492A10 7D28D71C D25B46F0 95DBE4A4
OutputBlock FACA8BA0 73669FD4 5CF43B42 7E3013F6
Block #3
Plaintext
0E0F1011 12131415 16171819 1A1B1C1D
InputBlock F4C59BB1 61758BC1 4AE3235B 642B0FEB
OutputBlock CEC60BC8 54B4DE20 C7D921EB 4A468269
Block #4
Plaintext
1E1F2021 22232425 26272829 2A2B2C2D
InputBlock D0D92BE9 7697FA05 E1FE09C2 606DAE44
OutputBlock AB7B4C27 CA1ECA3F A3109637 2558D66F
Block #5
Plaintext
2E2F3031 32333435 36373839 3A3B3C3D
InputBlock 85547C16 F82DFE0A 9527AE0E 1F63EA52
OutputBlock 0FFB328B 7D21D483 7E1F1636 2409C26F
Block #6
Plaintext
3E3F0000 00000000 00000000 00000000
InputBlock 31C4328B 7D21D483 7E1F1636 2409C26F
OutputBlock 31F0AF4C E0F62807 70F709E9 8671AD14

Mac
31F0AF4C

Mac'
31F0AF4C

The Mac verifies

P is
<empty>

=====

#####

Block Cipher Modes of Operation

CCM Mode for Authentication and Confidentiality

#####

CCM-AES256

Example #1

Tlen = 32
Nlen = 56
Alen = 64
Plen = 32

Encrypt-Generate

K is
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F
N is
10111213 141516
A is
00010203 04050607
P is
20212223

B
4F101112 13141516 00000000 00000004
00080001 02030405 06070000 00000000
20212223 00000000 00000000 00000000

Compute the Mac

Block #1
Plaintext
4F101112 13141516 00000000 00000004
InputBlock 4F101112 13141516 00000000 00000004
OutputBlock E0E3B7CF 31198BC9 3B59D464 962B4FE1
Block #2

```
Plaintext
00080001 02030405 06070000 00000000
InputBlock   E0EBB7CE 331A8FCC 3D5ED464 962B4FE1
OutputBlock  6303B133 0D864156 A023F693 468A4069
Block #3
Plaintext
20212223 00000000 00000000 00000000
InputBlock   43229310 0D864156 A023F693 468A4069
OutputBlock  F2BAF340 77D1A66B 94DC0EFD FD9ED77D
```

T
F2BAF340

Compute S0

```
Block #1
InputBlock   07101112 13141516 00000000 00000000
OutputBlock  6746FB60 9785DCD1 6A4A5203 5D2E067B
Text-In      F2BAF340 00000000 00000000 00000000
Text-Out     95FC0820 9785DCD1 6A4A5203 5D2E067B
```

Compute S1..Sn

```
Block #1
InputBlock   07101112 13141516 00000000 00000001
OutputBlock  AA908A57 D2A01903 6B8CBF2B DBA03908
Text-In      20212223 24010000 00010000 0028F9FF
Text-Out     8AB1A874 F6A11903 6B8DBF2B DB88C0F7
```

C is
8AB1A874 95FC0820

Decrypt-Verify

Compute S0..Sn

```
Block #1
InputBlock   07101112 13141516 00000000 00000000
OutputBlock  6746FB60 9785DCD1 6A4A5203 5D2E067B
Text-In      95FC0820 030000C0 02008605 06CA6BC4
Text-Out     F2BAF340 9485DC11 684AD406 5BE46DBF
Block #2
InputBlock   07101112 13141516 00000000 00000001
OutputBlock  AA908A57 D2A01903 6B8CBF2B DBA03908
Text-In      8AB1A874 F6A11903 6B8DBF2B DB880200
Text-Out     20212223 24010000 00010000 00283B08
```

P
20212223

T

F2BAF340

B

4F101112 13141516 00000000 00000004
00080001 02030405 06070000 00000000
20212223 00000000 00000000 00000000

Verify the Mac

Block #1

Plaintext

4F101112 13141516 00000000 00000004

InputBlock 4F101112 13141516 00000000 00000004

OutputBlock E0E3B7CF 31198BC9 3B59D464 962B4FE1

Block #2

Plaintext

00080001 02030405 06070000 00000000

InputBlock E0EBB7CE 331A8FCC 3D5ED464 962B4FE1

OutputBlock 6303B133 0D864156 A023F693 468A4069

Block #3

Plaintext

20212223 00000000 00000000 00000000

InputBlock 43229310 0D864156 A023F693 468A4069

OutputBlock F2BAF340 77D1A66B 94DC0EFD FD9ED77D

Mac

F2BAF340

Mac'

F2BAF340

The Mac verifies

P is

20212223

=====

Example #2

Tlen = 48

Nlen = 64

Alen = 128

Plen = 128

Encrypt-Generate

K is

40414243 44454647 48494A4B 4C4D4E4F

50515253 54555657 58595A5B 5C5D5E5F

N is

10111213 14151617
A is
00010203 04050607 08090A0B 0C0D0E0F
P is
20212223 24252627 28292A2B 2C2D2E2F

B
56101112 13141516 17000000 00000010
00100001 02030405 06070809 0A0B0C0D
0E0F0000 00000000 00000000 00000000
20212223 24252627 28292A2B 2C2D2E2F

Compute the Mac

Block #1
Plaintext
56101112 13141516 17000000 00000010
InputBlock 56101112 13141516 17000000 00000010
OutputBlock 067CB8E5 D59D8225 A9C1ECE9 ACF1469C
Block #2
Plaintext
00100001 02030405 06070809 0A0B0C0D
InputBlock 066CB8E4 D79E8620 AFC6E4E0 A6FA4A91
OutputBlock B7B77DB8 7195ADBC D529D9D9 8E0EC0A8
Block #3
Plaintext
0E0F0000 00000000 00000000 00000000
InputBlock B9B87DB8 7195ADBC D529D9D9 8E0EC0A8
OutputBlock 38539AC0 F34ADDEF 19A699BB F7DCCF68
Block #4
Plaintext
20212223 24252627 28292A2B 2C2D2E2F
InputBlock 1872B8E3 D76FFBC8 318FB390 DBF1E147
OutputBlock 3DD67149 DBD1CF3B F003B424 3B2C074C

T
3DD67149 DBD1

Compute S0

Block #1
InputBlock 06101112 13141516 17000000 00000000
OutputBlock A96E5781 5F4F7C7B 8860376F DF23150A
Text-In 3DD67149 DBD10000 00000000 00000000
Text-Out 94B826C8 849E7C7B 8860376F DF23150A

Compute S1..Sn

Block #1
InputBlock 06101112 13141516 17000000 00000001
OutputBlock 8F36A7DF 2B7B81F7 E793A959 6A656AB8
Text-In 20212223 24252627 28292A2B 2C2D2E2F
Text-Out AF1785FC 0F5EA7D0 CFBA8372 46484497

C is
AF1785FC 0F5EA7D0 CFBA8372 46484497
94B826C8 849E

Decrypt-Verify

Compute S0..Sn

Block #1
InputBlock 06101112 13141516 17000000 00000000
OutputBlock A96E5781 5F4F7C7B 8860376F DF23150A
Text-In 94B826C8 849E00C0 0D00D406 5BE46DBF
Text-Out 3DD67149 DBD17CBB 8560E369 84C778B5
Block #2
InputBlock 06101112 13141516 17000000 00000001
OutputBlock 8F36A7DF 2B7B81F7 E793A959 6A656AB8
Text-In AF1785FC 0F5EA7D0 CFBA8372 46484497
Text-Out 20212223 24252627 28292A2B 2C2D2E2F

P
20212223 24252627 28292A2B 2C2D2E2F

T
3DD67149 DBD1

B
56101112 13141516 17000000 00000010
00100001 02030405 06070809 0A0B0C0D
0E0F0000 00000000 00000000 00000000
20212223 24252627 28292A2B 2C2D2E2F

Verify the Mac

Block #1
Plaintext
56101112 13141516 17000000 00000010
InputBlock 56101112 13141516 17000000 00000010
OutputBlock 067CB8E5 D59D8225 A9C1ECE9 ACF1469C
Block #2
Plaintext
00100001 02030405 06070809 0A0B0C0D
InputBlock 066CB8E4 D79E8620 AFC6E4E0 A6FA4A91
OutputBlock B7B77DB8 7195ADBC D529D9D9 8E0EC0A8
Block #3
Plaintext
0E0F0000 00000000 00000000 00000000
InputBlock B9B87DB8 7195ADBC D529D9D9 8E0EC0A8
OutputBlock 38539AC0 F34ADDEF 19A699BB F7DCCF68

Block #4
Plaintext
20212223 24252627 28292A2B 2C2D2E2F
InputBlock 1872B8E3 D76FFBC8 318FB390 DBF1E147
OutputBlock 3DD67149 DBD1CF3B F003B424 3B2C074C

Mac
3DD67149 DBD1

Mac'
3DD67149 DBD1

The Mac verifies

P is
20212223 24252627 28292A2B 2C2D2E2F

=====
Example #3

Tlen = 64
Nlen = 96
Alen = 160
Plen = 192

Encrypt-Generate

K is
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F
N is
10111213 14151617 18191A1B
A is
00010203 04050607 08090A0B 0C0D0E0F
10111213
P is
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637

B
5A101112 13141516 1718191A 1B000018
00140001 02030405 06070809 0A0B0C0D
0E0F1011 12130000 00000000 00000000
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 00000000 00000000

Compute the Mac

Block #1
Plaintext

```

5A101112 13141516 1718191A 1B000018
InputBlock 5A101112 13141516 1718191A 1B000018
OutputBlock D58A04A4 6BEF2857 891838E9 53418E09
Block #2
Plaintext
00140001 02030405 06070809 0A0B0C0D
InputBlock D59E04A5 69EC2C52 8F1F30E0 594AB204
OutputBlock 434DC2F8 D3F4EBE9 E949AABE 0EE56891
Block #3
Plaintext
0E0F1011 12130000 00000000 00000000
InputBlock 4D42D2E9 C1E7EBE9 E949AABE 0EE56891
OutputBlock 8769579F B41C989E 93E0F1DC A682076F
Block #4
Plaintext
20212223 24252627 28292A2B 2C2D2E2F
InputBlock A74875BC 9039BEB9 BBC9DBF7 8AAF2940
OutputBlock AC8556E9 010C8579 0FAB59F6 8827E562
Block #5
Plaintext
30313233 34353637 00000000 00000000
InputBlock 9CB464DA 3539B34E 0FAB59F6 8827E562
OutputBlock 5AE87005 24D79808 E13EB30E BA734755

```

T

```
5AE87005 24D79808
```

Compute S0

```

Block #1
InputBlock 02101112 13141516 1718191A 1B000000
OutputBlock 71A0B873 4BA9EE41 11F51341 C7FE6D3B
Text-In 5AE87005 24D79808 00000000 00000000
Text-Out 2B48C876 6F7E7649 11F51341 C7FE6D3B

```

Compute S1..Sn

```

Block #1
InputBlock 02101112 13141516 1718191A 1B000001
OutputBlock 24D9A18D 97982117 C2DC219D F2628C0E
Text-In 20212223 24252627 28292A2B 2C2D2E2F
Text-Out 04F883AE B3BD0730 EAF50BB6 DE4FA221
Block #2
InputBlock 02101112 13141516 1718191A 1B000002
OutputBlock 1005D6D7 2F3B43D2 4FCF851F 1EFDC8ED
Text-In 30313233 34353637 00E4BCA5 90010000
Text-Out 2034E4E4 1B0E75E5 4F2B39BA 8EFCC8ED

```

C is

```

04F883AE B3BD0730 EAF50BB6 DE4FA221
2034E4E4 1B0E75E5 2B48C876 6F7E7649

```

Decrypt-Verify

Compute S0..Sn

Block #1
InputBlock 02101112 13141516 1718191A 1B000000
OutputBlock 71A0B873 4BA9EE41 11F51341 C7FE6D3B
Text-In 2B48C876 6F7E7649 0C000BB6 DE4FA221
Text-Out 5AE87005 24D79808 1DF518F7 19B1CF1A
Block #2
InputBlock 02101112 13141516 1718191A 1B000001
OutputBlock 24D9A18D 97982117 C2DC219D F2628C0E
Text-In 04F883AE B3BD0730 EAF50BB6 DE4FA221
Text-Out 20212223 24252627 28292A2B 2C2D2E2F
Block #3
InputBlock 02101112 13141516 1718191A 1B000002
OutputBlock 1005D6D7 2F3B43D2 4FCF851F 1EFDC8ED
Text-In 2034E4E4 1B0E75E5 0A002A2B 2C2D2E2F
Text-Out 30313233 34353637 45CFAF34 32D0E6C2

P
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637

T
5AE87005 24D79808

B
5A101112 13141516 1718191A 1B000018
00140001 02030405 06070809 0A0B0C0D
0E0F1011 12130000 00000000 00000000
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 00000000 00000000

Verify the Mac

Block #1
Plaintext
5A101112 13141516 1718191A 1B000018
InputBlock 5A101112 13141516 1718191A 1B000018
OutputBlock D58A04A4 6BEF2857 891838E9 5341BE09
Block #2
Plaintext
00140001 02030405 06070809 0A0B0C0D
InputBlock D59E04A5 69EC2C52 8F1F30E0 594AB204
OutputBlock 434DC2F8 D3F4EBE9 E949AABE 0EE56891
Block #3
Plaintext
0E0F1011 12130000 00000000 00000000
InputBlock 4D42D2E9 C1E7EBE9 E949AABE 0EE56891
OutputBlock 8769579F B41C989E 93E0F1DC A682076F
Block #4
Plaintext
20212223 24252627 28292A2B 2C2D2E2F
InputBlock A74875BC 9039BEB9 BBC9DBF7 8AAF2940

```
OutputBlock AC8556E9 010C8579 0FAB59F6 8827E562
Block #5
Plaintext
30313233 34353637 00000000 00000000
InputBlock 9CB464DA 3539B34E 0FAB59F6 8827E562
OutputBlock 5AE87005 24D79808 E13EB30E BA734755
```

```
-----
Mac
5AE87005 24D79808
```

```
Mac'
5AE87005 24D79808
```

```
-----
The Mac verifies
```

```
P is
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637
```

```
=====
Example #4
```

```
Tlen = 32
Nlen = 56
Alen = 0
Plen = 512
-----
```

```
Encrypt-Generate
```

```
K is
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F
N is
10111213 141516
A is
<empty>
P is
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F
```

```
-----
B
0F101112 13141516 00000000 00000040
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F
-----
```

```
Compute the Mac
```

```

Block #1
  Plaintext
  0F101112 13141516 00000000 00000040
  InputBlock  0F101112 13141516 00000000 00000040
  OutputBlock 054408C9 5B192F76 3C5CC14A 1CEF6D3C
Block #2
  Plaintext
  20212223 24252627 28292A2B 2C2D2E2F
  InputBlock  25652AEA 7F3C0951 1475EB61 30C24313
  OutputBlock 2AD6BC89 29D3DCC4 8CD22EB9 C72B6382
Block #3
  Plaintext
  30313233 34353637 38393A3B 3C3D3E3F
  InputBlock  1AE78EBA 1DE6EAF3 B4EB1482 FB165DBD
  OutputBlock D5D086CE C0DBCE1B A2D358F5 8925D64F
Block #4
  Plaintext
  40414243 44454647 48494A4B 4C4D4E4F
  InputBlock  9591C48D 849E885C EA9A12BE C5689800
  OutputBlock 1CC4E391 FDF9070C 55AA23D6 1F1E95CE
Block #5
  Plaintext
  50515253 54555657 58595A5B 5C5D5E5F
  InputBlock  4C95B1C2 A9AC515B 0DF3798D 4343CB91
  OutputBlock 58FBF4CE 8C5C6C98 6A92A7FB 0159A4E9

```

T
58FBF4CE

Compute S0

```

Block #1
  InputBlock  07101112 13141516 00000000 00000000
  OutputBlock 6746FB60 9785DCD1 6A4A5203 5D2E067B
  Text-In     58FBF4CE 00000000 00000000 00000000
  Text-Out    3FBD0FAE 9785DCD1 6A4A5203 5D2E067B

```

Compute S1..Sn

```

Block #1
  InputBlock  07101112 13141516 00000000 00000001
  OutputBlock AA908A57 D2A01903 6B8CBF2B DBA03908
  Text-In     20212223 24252627 28292A2B 2C2D2E2F
  Text-Out    8AB1A874 F6853F24 43A59500 F78D1727
Block #2
  InputBlock  07101112 13141516 00000000 00000002
  OutputBlock 1D5C0BEC 92E5D066 3F883D3B FEF3A0D7
  Text-In     30313233 34353637 38393A3B 3C3D3E3F
  Text-Out    2D6D39DF A6D0E651 07B10700 C2CE9EE8
Block #3
  InputBlock  07101112 13141516 00000000 00000003
  OutputBlock 267C7C69 4587A76B 7AA07D3F 0E6E576F
  Text-In     40414243 44454647 48494A4B 4C4D4E4F
  Text-Out    663D3E2A 01C2E12C 32E93774 42231920
Block #4
  InputBlock  07101112 13141516 00000000 00000004
  OutputBlock EE0275DC 1B35FF25 EF50E14D CF7468E5

```

Text-In 50515253 54555657 58595A5B 5C5D5E5F
Text-Out BE53278F 4F60A972 B709BB16 932936BA

C is

8AB1A874 F6853F24 43A59500 F78D1727
2D6D39DF A6D0E651 07B10700 C2CE9EE8
663D3E2A 01C2E12C 32E93774 42231920
BE53278F 4F60A972 B709BB16 932936BA
3FBD0FAE

Decrypt-Verify

Compute S0..Sn

Block #1
InputBlock 07101112 13141516 00000000 00000000
OutputBlock 6746FB60 9785DCD1 6A4A5203 5D2E067B
Text-In 3FBD0FAE 13141516 00000000 00000040
Text-Out 58FBF4CE 8491C9C7 6A4A5203 5D2E063B
Block #2
InputBlock 07101112 13141516 00000000 00000001
OutputBlock AA908A57 D2A01903 6B8CBF2B DBA03908
Text-In 8AB1A874 F6853F24 43A59500 F78D1727
Text-Out 20212223 24252627 28292A2B 2C2D2E2F
Block #3
InputBlock 07101112 13141516 00000000 00000002
OutputBlock 1D5C0BEC 92E5D066 3F883D3B FEF3A0D7
Text-In 2D6D39DF A6D0E651 07B10700 C2CE9EE8
Text-Out 30313233 34353637 38393A3B 3C3D3E3F
Block #4
InputBlock 07101112 13141516 00000000 00000003
OutputBlock 267C7C69 4587A76B 7AA07D3F 0E6E576F
Text-In 663D3E2A 01C2E12C 32E93774 42231920
Text-Out 40414243 44454647 48494A4B 4C4D4E4F
Block #5
InputBlock 07101112 13141516 00000000 00000004
OutputBlock EE0275DC 1B35FF25 EF50E14D CF7468E5
Text-In BE53278F 4F60A972 B709BB16 932936BA
Text-Out 50515253 54555657 58595A5B 5C5D5E5F

P

20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F

T

58FBF4CE

B

0F101112 13141516 00000000 00000040

```
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F
```

Verify the Mac

```
Block #1
  Plaintext
  0F101112 13141516 00000000 00000040
  InputBlock  0F101112 13141516 00000000 00000040
  OutputBlock 054408C9 5B192F76 3C5CC14A 1CEF6D3C
Block #2
  Plaintext
  20212223 24252627 28292A2B 2C2D2E2F
  InputBlock  25652AEA 7F3C0951 1475EB61 30C24313
  OutputBlock 2AD6BC89 29D3DCC4 8CD22EB9 C72B6382
Block #3
  Plaintext
  30313233 34353637 38393A3B 3C3D3E3F
  InputBlock  1AE78EBA 1DE6EAF3 B4EB1482 FB165DBD
  OutputBlock D5D086CE C0DBCE1B A2D358F5 8925D64F
Block #4
  Plaintext
  40414243 44454647 48494A4B 4C4D4E4F
  InputBlock  9591C48D 849E885C EA9A12BE C5689800
  OutputBlock 1CC4E391 FDF9070C 55AA23D6 1F1E95CE
Block #5
  Plaintext
  50515253 54555657 58595A5B 5C5D5E5F
  InputBlock  4C95B1C2 A9AC515B 0DF3798D 4343CB91
  OutputBlock 58FBF4CE 8C5C6C98 6A92A7FB 0159A4E9
```

Mac
58FBF4CE

Mac'
58FBF4CE

The Mac verifies

```
P is
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F
40414243 44454647 48494A4B 4C4D4E4F
50515253 54555657 58595A5B 5C5D5E5F
```

=====

Example #5

```
Tlen = 32
Nlen = 56
Alen = 512
Plen = 0
```

Encrypt-Generate

K is

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

N is

10111213 141516

A is

00010203 04050607 08090A0B 0C0D0E0F
10111213 14151617 18191A1B 1C1D1E1F
20212223 24252627 28292A2B 2C2D2E2F
30313233 34353637 38393A3B 3C3D3E3F

P is

<empty>

B

4F101112 13141516 00000000 00000000
00400001 02030405 06070809 0A0B0C0D
0E0F1011 12131415 16171819 1A1B1C1D
1E1F2021 22232425 26272829 2A2B2C2D
2E2F3031 32333435 36373839 3A3B3C3D
3E3F0000 00000000 00000000 00000000

Compute the Mac

Block #1

Plaintext

4F101112 13141516 00000000 00000000
InputBlock 4F101112 13141516 00000000 00000000
OutputBlock C06556FD D639F5BF CA0816A2 E748051A

Block #2

Plaintext

00400001 02030405 06070809 0A0B0C0D
InputBlock C02556FC D43AF1BA CC0F1EAB ED430917
OutputBlock E23B799F AC48BF0D 0CEB5302 51CB4D1A

Block #3

Plaintext

0E0F1011 12131415 16171819 1A1B1C1D
InputBlock EC34698E BE5BAB18 1AFC4B1B 4BD05107
OutputBlock 11D1D391 F7E1C1B0 BF900A98 A0C98A83

Block #4

Plaintext

1E1F2021 22232425 26272829 2A2B2C2D
InputBlock 0FCEF3B0 D5C2E595 99B722B1 8AE2A6AE
OutputBlock 811F84F4 3CA03762 6D1B9669 6345AD8B

Block #5

Plaintext

2E2F3031 32333435 36373839 3A3B3C3D
InputBlock AF30B4C5 0E930357 5B2CAE50 597E91B6
OutputBlock 3B1FEBBE 43D2B0F9 7B48475C AE18418B

Block #6

Plaintext

3E3F0000 00000000 00000000 00000000
InputBlock 0520EBBE 43D2B0F9 7B48475C AE18418B

OutputBlock C1897950 4C660131 B4DA0E3E 718626C2

T

C1897950

Compute S0

Block #1

InputBlock	07101112	13141516	00000000	00000000
OutputBlock	6746FB60	9785DCD1	6A4A5203	5D2E067B
Text-In	C1897950	00000000	00000000	00000000
Text-Out	A6CF8230	9785DCD1	6A4A5203	5D2E067B

Compute S1..Sn

<empty payload>

C is

A6CF8230

Decrypt-Verify

Compute S0..Sn

Block #1

InputBlock	07101112	13141516	00000000	00000000
OutputBlock	6746FB60	9785DCD1	6A4A5203	5D2E067B
Text-In	A6CF8230	970004C0	06005203	5D2E063B
Text-Out	C1897950	0085D811	6C4A0000	00000040

P

<empty>

T

C1897950

B

4F101112 13141516 00000000 00000000
00400001 02030405 06070809 0A0B0C0D
0E0F1011 12131415 16171819 1A1B1C1D
1E1F2021 22232425 26272829 2A2B2C2D
2E2F3031 32333435 36373839 3A3B3C3D
3E3F0000 00000000 00000000 00000000

Verify the Mac

```

Block #1
  Plaintext
  4F101112 13141516 00000000 00000000
  InputBlock   4F101112 13141516 00000000 00000000
  OutputBlock  C06556FD D639F5BF CA0816A2 E748051A
Block #2
  Plaintext
  00400001 02030405 06070809 0A0B0C0D
  InputBlock   C02556FC D43AF1BA CC0F1EAB ED430917
  OutputBlock  E23B799F AC48BF0D 0CEB5302 51CB4D1A
Block #3
  Plaintext
  0E0F1011 12131415 16171819 1A1B1C1D
  InputBlock   EC34698E BE5BAB18 1AFC4B1B 4BD05107
  OutputBlock  11D1D391 F7E1C1B0 BF900A98 A0C98A83
Block #4
  Plaintext
  1E1F2021 22232425 26272829 2A2B2C2D
  InputBlock   0FCEF3B0 D5C2E595 99B722B1 8AE2A6AE
  OutputBlock  811F84F4 3CA03762 6D1B9669 6345AD8B
Block #5
  Plaintext
  2E2F3031 32333435 36373839 3A3B3C3D
  InputBlock   AF30B4C5 0E930357 5B2CAE50 597E91B6
  OutputBlock  3B1FEBBE 43D2B0F9 7B48475C AE18418B
Block #6
  Plaintext
  3E3F0000 00000000 00000000 00000000
  InputBlock   0520EBBE 43D2B0F9 7B48475C AE18418B
  OutputBlock  C1897950 4C660131 B4DA0E3E 718626C2

```

```

-----
Mac
  C1897950

```

```

Mac'
  C1897950

```

```

-----

The Mac verifies

```

```

P is
  <empty>

```

```

=====
*****

```