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

  Block Cipher Modes of Operation

      GCM Mode for Authentication and Confidentiality

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

GCM-AES128
-------------------------------------------------------------

Example #1

Taglen = 128
AADlen = 0
PTlen = 0
-------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    <empty>
P is
    <empty>

H is
    B83B5337 08BF535D 0AA6E529 80D53B78
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    9BB22CE7 D9F372C1 EE2B2872 2B25F206
   E is
    42831EC2 21777424 4B7221B7 84D0D49C
-----------------------
CT is
    <empty>
S is
    00000000 00000000 00000000 00000000
Cipher(K, J0) is
    3247184B 3C4F69A4 4DBCD228 87BBB418

C is
    <empty>
Tag is
    3247184B 3C4F69A4 4DBCD228 87BBB418

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

Decrypt-Verify

-----------------------
 GCM_Ctr
  Block #1:
```

```
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    9BB22CE7 D9F372C1 EE2B2872 2B25F206
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
-----------------------

The Mac verifies

P is
    <empty>

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

Example #2

Taglen = 128
AADlen = 0
PTlen = 512
------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    <empty>
P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39 1AAFD255

H is
    B83B5337 08BF535D 0AA6E529 80D53B78
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    9BB22CE7 D9F372C1 EE2B2872 2B25F206
   E is
    42831EC2 21777424 4B7221B7 84D0D49C
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    650D887C 3936533A 1B8D4E1E A39D2B5C
   E is
    E3AA212F 2C02A4E0 35C17E23 29ACA12E
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    3DE91827 C10E9A4F 5240647E E5221F20
   E is
```

```
    21D514B2 5466931C 7D8F6A5A AC84AA05
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    AAC9E6CC C0074AC0 873B9BA8 5D908BD0
   E is
    1BA30B39 6A0AAC97 3D58E091 473F5985
-----------------------
CT is
    42831EC2 21777424 4B7221B7 84D0D49C
    E3AA212F 2C02A4E0 35C17E23 29ACA12E
    21D514B2 5466931C 7D8F6A5A AC84AA05
    1BA30B39 6A0AAC97 3D58E091 473F5985
S is
    7F1B32B8 1B820D02 614F8895 AC1D4EAC
Cipher(K, J0) is
    3247184B 3C4F69A4 4DBCD228 87BBB418

C is
    42831EC2 21777424 4B7221B7 84D0D49C
    E3AA212F 2C02A4E0 35C17E23 29ACA12E
    21D514B2 5466931C 7D8F6A5A AC84AA05
    1BA30B39 6A0AAC97 3D58E091 473F5985
Tag is
    4D5C2AF3 27CD64A6 2CF35ABD 2BA6FAB4

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

Decrypt-Verify

-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    9BB22CE7 D9F372C1 EE2B2872 2B25F206
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    650D887C 3936533A 1B8D4E1E A39D2B5C
   E is
    86A7A953 1534F7DA 2E4C303D 8A318A72
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    3DE91827 C10E9A4F 5240647E E5221F20
   E is
    1C3C0C95 95680953 2FCF0E24 49A6B525
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    AAC9E6CC C0074AC0 873B9BA8 5D908BD0
   E is
    B16AEDF5 AA0DE657 BA637B39 1AAFD255
-----------------------
```

```
The Mac verifies

P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39 1AAFD255

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

Example #3

Taglen = 128
AADlen = 512
PTlen = 0
------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    F5D3D585 03B9699D E785895A 96FDBAAF
    43B1CD7F 598ECE23 881B00E3 ED030688
    7B0C785E 27E8AD3F 82232071 04725DD4
P is
    <empty>

H is
    B83B5337 08BF535D 0AA6E529 80D53B78
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    9BB22CE7 D9F372C1 EE2B2872 2B25F206
   E is
    42831EC2 21777424 4B7221B7 84D0D49C
-----------------------
CT is
    <empty>
S is
    6DD6CF3A 1FA0371D D4C5C1AC 1C3675F1
Cipher(K, J0) is
    3247184B 3C4F69A4 4DBCD228 87BBB418

C is
    <empty>
Tag is
    5F91D771 23EF5EB9 99791384 9B8DC1E9

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

Decrypt-Verify
```

```
-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    9BB22CE7 D9F372C1 EE2B2872 2B25F206
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
-----------------------

The Mac verifies

P is
    <empty>

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

Example #4

Taglen = 128
AADlen = 512
PTlen = 512
------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    F5D3D585 03B9699D E785895A 96FDBAAF
    43B1CD7F 598ECE23 881B00E3 ED030688
    7B0C785E 27E8AD3F 82232071 04725DD4
P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39 1AAFD255

H is
    B83B5337 08BF535D 0AA6E529 80D53B78
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    9BB22CE7 D9F372C1 EE2B2872 2B25F206
   E is
    42831EC2 21777424 4B7221B7 84D0D49C
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    650D887C 3936533A 1B8D4E1E A39D2B5C
   E is
    E3AA212F 2C02A4E0 35C17E23 29ACA12E
```

```
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    3DE91827 C10E9A4F 5240647E E5221F20
   E is
    21D514B2 5466931C 7D8F6A5A AC84AA05
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    AAC9E6CC C0074AC0 873B9BA8 5D908BD0
   E is
    1BA30B39 6A0AAC97 3D58E091 473F5985
-----------------------
CT is
    42831EC2 21777424 4B7221B7 84D0D49C
    E3AA212F 2C02A4E0 35C17E23 29ACA12E
    21D514B2 5466931C 7D8F6A5A AC84AA05
    1BA30B39 6A0AAC97 3D58E091 473F5985
S is
    56873B62 38E0502E 16DB1323 D41EB655
Cipher(K, J0) is
    3247184B 3C4F69A4 4DBCD228 87BBB418

C is
    42831EC2 21777424 4B7221B7 84D0D49C
    E3AA212F 2C02A4E0 35C17E23 29ACA12E
    21D514B2 5466931C 7D8F6A5A AC84AA05
    1BA30B39 6A0AAC97 3D58E091 473F5985
Tag is
    64C02329 04AF398A 5B67C10B 53A5024D

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

Decrypt-Verify

-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    9BB22CE7 D9F372C1 EE2B2872 2B25F206
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    650D887C 3936533A 1B8D4E1E A39D2B5C
   E is
    86A7A953 1534F7DA 2E4C303D 8A318A72
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    3DE91827 C10E9A4F 5240647E E5221F20
   E is
    1C3C0C95 95680953 2FCF0E24 49A6B525
  Block #4:
   CB is
```

```
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    AAC9E6CC C0074AC0 873B9BA8 5D908BD0
   E is
    B16AEDF5 AA0DE657 BA637B39 1AAFD255
----------------------

The Mac verifies

P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39 1AAFD255

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

Example #5

Taglen = 128
AADlen = 160
PTlen = 480
------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    F5D3D585
P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39

H is
    B83B5337 08BF535D 0AA6E529 80D53B78
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    9BB22CE7 D9F372C1 EE2B2872 2B25F206
   E is
    42831EC2 21777424 4B7221B7 84D0D49C
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    650D887C 3936533A 1B8D4E1E A39D2B5C
   E is
    E3AA212F 2C02A4E0 35C17E23 29ACA12E
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
```

```
   CT is
    3DE91827 C10E9A4F 5240647E E5221F20
   E is
    21D514B2 5466931C 7D8F6A5A AC84AA05
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    AAC9E6CC C0074AC0 873B9BA8 5D908BD0
   E is
    1BA30B39 6A0AAC97 3D58E091 473F5985
----------------------
CT is
    42831EC2 21777424 4B7221B7 84D0D49C
    E3AA212F 2C02A4E0 35C17E23 29ACA12E
    21D514B2 5466931C 7D8F6A5A AC84AA05
    1BA30B39 6A0AAC97 3D58E091
S is
    C23B3D63 D2ED9505 6CA34276 9CD13C03
Cipher(K, J0) is
    3247184B 3C4F69A4 4DBCD228 87BBB418

C is
    42831EC2 21777424 4B7221B7 84D0D49C
    E3AA212F 2C02A4E0 35C17E23 29ACA12E
    21D514B2 5466931C 7D8F6A5A AC84AA05
    1BA30B39 6A0AAC97 3D58E091
Tag is
    F07C2528 EEA2FCA1 211F905E 1B6A881B

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

Decrypt-Verify

----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    9BB22CE7 D9F372C1 EE2B2872 2B25F206
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    650D887C 3936533A 1B8D4E1E A39D2B5C
   E is
    86A7A953 1534F7DA 2E4C303D 8A318A72
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    3DE91827 C10E9A4F 5240647E E5221F20
   E is
    1C3C0C95 95680953 2FCF0E24 49A6B525
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    AAC9E6CC C0074AC0 873B9BA8 5D908BD0
```

```
   E is
    B16AEDF5 AA0DE657 BA637B39 818F4000
----------------------

The Mac verifies

P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39

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

Example #6

Taglen = 96
AADlen = 160
PTlen = 480
------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    F5D3D585
P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39

H is
    B83B5337 08BF535D 0AA6E529 80D53B78
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    9BB22CE7 D9F372C1 EE2B2872 2B25F206
   E is
    42831EC2 21777424 4B7221B7 84D0D49C
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    650D887C 3936533A 1B8D4E1E A39D2B5C
   E is
    E3AA212F 2C02A4E0 35C17E23 29ACA12E
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    3DE91827 C10E9A4F 5240647E E5221F20
   E is
```

```
    21D514B2 5466931C 7D8F6A5A AC84AA05
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    AAC9E6CC C0074AC0 873B9BA8 5D908BD0
   E is
    1BA30B39 6A0AAC97 3D58E091 473F5985
-----------------------
CT is
    42831EC2 21777424 4B7221B7 84D0D49C
    E3AA212F 2C02A4E0 35C17E23 29ACA12E
    21D514B2 5466931C 7D8F6A5A AC84AA05
    1BA30B39 6A0AAC97 3D58E091
S is
    C23B3D63 D2ED9505 6CA34276 9CD13C03
Cipher(K, J0) is
    3247184B 3C4F69A4 4DBCD228 87BBB418

C is
    42831EC2 21777424 4B7221B7 84D0D49C
    E3AA212F 2C02A4E0 35C17E23 29ACA12E
    21D514B2 5466931C 7D8F6A5A AC84AA05
    1BA30B39 6A0AAC97 3D58E091
Tag is
    F07C2528 EEA2FCA1 211F905E

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

Decrypt-Verify

-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    9BB22CE7 D9F372C1 EE2B2872 2B25F206
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    650D887C 3936533A 1B8D4E1E A39D2B5C
   E is
    86A7A953 1534F7DA 2E4C303D 8A318A72
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    3DE91827 C10E9A4F 5240647E E5221F20
   E is
    1C3C0C95 95680953 2FCF0E24 49A6B525
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    AAC9E6CC C0074AC0 873B9BA8 5D908BD0
   E is
    B16AEDF5 AA0DE657 BA637B39 818F4000
-----------------------
```

```
The Mac verifies

P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39

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

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

GCM-AES192
------------------------------------------------------------

Example #1

Taglen = 128
AADlen = 0
PTlen = 0
------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
    FEFFE992 8665731C
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    <empty>
P is
    <empty>

H is
    466923EC 9AE68221 4F2C082B ADB39249
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    E0B1F82E C484EEA4 4E5FF301 28DF01CD
   E is
    3980CA0B 3C00E841 EB06FAC4 872A2757
-----------------------
CT is
    <empty>
S is
    00000000 00000000 00000000 00000000
Cipher(K, J0) is
    C835AA88 AEBBC94F 5A02E179 FDCFC3E4

C is
    <empty>
Tag is
    C835AA88 AEBBC94F 5A02E179 FDCFC3E4

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

```
Decrypt-Verify

----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    E0B1F82E C484EEA4 4E5FF301 28DF01CD
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
----------------------

The Mac verifies

P is
    <empty>

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

Example #2

Taglen = 128
AADlen = 0
PTlen = 512
------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
    FEFFE992 8665731C
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    <empty>
P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39 1AAFD255

H is
    466923EC 9AE68221 4F2C082B ADB39249
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    E0B1F82E C484EEA4 4E5FF301 28DF01CD
   E is
    3980CA0B 3C00E841 EB06FAC4 872A2757
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    0339B5B9 B3DB2E5E 4CC9A389 86906BEE
   E is
```

```
    859E1CEA A6EFD984 628593B4 0CA1E19C
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    614B3195 542CCC76 83AE933C 81EC8A62
   E is
    7D773D00 C144C525 AC619D18 C84A3F47
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    A988A97E 85EEC28E 76B95C29 B6023003
   E is
    18E2448B 2FE324D9 CCDA2710 ACADE256
-----------------------
CT is
    3980CA0B 3C00E841 EB06FAC4 872A2757
    859E1CEA A6EFD984 628593B4 0CA1E19C
    7D773D00 C144C525 AC619D18 C84A3F47
    18E2448B 2FE324D9 CCDA2710 ACADE256
S is
    51110D40 F6C8FFF0 EB1AE334 45A889F0
Cipher(K, J0) is
    C835AA88 AEBBC94F 5A02E179 FDCFC3E4

C is
    3980CA0B 3C00E841 EB06FAC4 872A2757
    859E1CEA A6EFD984 628593B4 0CA1E19C
    7D773D00 C144C525 AC619D18 C84A3F47
    18E2448B 2FE324D9 CCDA2710 ACADE256
Tag is
    9924A7C8 587336BF B118024D B8674A14

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

Decrypt-Verify

-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    E0B1F82E C484EEA4 4E5FF301 28DF01CD
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    0339B5B9 B3DB2E5E 4CC9A389 86906BEE
   E is
    86A7A953 1534F7DA 2E4C303D 8A318A72
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    614B3195 542CCC76 83AE933C 81EC8A62
   E is
    1C3C0C95 95680953 2FCF0E24 49A6B525
  Block #4:
```

```
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    A988A97E 85EEC28E 76B95C29 B6023003
   E is
    B16AEDF5 AA0DE657 BA637B39 1AAFD255
-----------------------

The Mac verifies

P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39 1AAFD255

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

Example #3

Taglen = 128
AADlen = 512
PTlen = 0
------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
    FEFFE992 8665731C
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    F5D3D585 03B9699D E785895A 96FDBAAF
    43B1CD7F 598ECE23 881B00E3 ED030688
    7B0C785E 27E8AD3F 82232071 04725DD4
P is
    <empty>

H is
    466923EC 9AE68221 4F2C082B ADB39249
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    E0B1F82E C484EEA4 4E5FF301 28DF01CD
   E is
    3980CA0B 3C00E841 EB06FAC4 872A2757
-----------------------
CT is
    <empty>
S is
    CAF9DDB3 67A23DAE 9FEB243A EE706F04
Cipher(K, J0) is
    C835AA88 AEBBC94F 5A02E179 FDCFC3E4

C is
```

```
    <empty>
Tag is
    02CC773B C919F4E1 C5E9C543 13BFACE0

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

Decrypt-Verify

-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    E0B1F82E C484EEA4 4E5FF301 28DF01CD
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
-----------------------

The Mac verifies

P is
    <empty>

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

Example #4

Taglen = 128
AADlen = 512
PTlen = 512
------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
    FEFFE992 8665731C
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    F5D3D585 03B9699D E785895A 96FDBAAF
    43B1CD7F 598ECE23 881B00E3 ED030688
    7B0C785E 27E8AD3F 82232071 04725DD4
P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39 1AAFD255

H is
    466923EC 9AE68221 4F2C082B ADB39249
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    E0B1F82E C484EEA4 4E5FF301 28DF01CD
```

```
   E is
    3980CA0B 3C00E841 EB06FAC4 872A2757
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    0339B5B9 B3DB2E5E 4CC9A389 86906BEE
   E is
    859E1CEA A6EFD984 628593B4 0CA1E19C
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    614B3195 542CCC76 83AE933C 81EC8A62
   E is
    7D773D00 C144C525 AC619D18 C84A3F47
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    A988A97E 85EEC28E 76B95C29 B6023003
   E is
    18E2448B 2FE324D9 CCDA2710 ACADE256
-----------------------
CT is
    3980CA0B 3C00E841 EB06FAC4 872A2757
    859E1CEA A6EFD984 628593B4 0CA1E19C
    7D773D00 C144C525 AC619D18 C84A3F47
    18E2448B 2FE324D9 CCDA2710 ACADE256
S is
    F3A4F93C 498A4310 61BC4D69 72454D3F
Cipher(K, J0) is
    C835AA88 AEBBC94F 5A02E179 FDCFC3E4

C is
    3980CA0B 3C00E841 EB06FAC4 872A2757
    859E1CEA A6EFD984 628593B4 0CA1E19C
    7D773D00 C144C525 AC619D18 C84A3F47
    18E2448B 2FE324D9 CCDA2710 ACADE256
Tag is
    3B9153B4 E7318A5F 3BBEAC10 8F8A8EDB

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

Decrypt-Verify

-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    E0B1F82E C484EEA4 4E5FF301 28DF01CD
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    0339B5B9 B3DB2E5E 4CC9A389 86906BEE
   E is
    86A7A953 1534F7DA 2E4C303D 8A318A72
```

```
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    614B3195 542CCC76 83AE933C 81EC8A62
   E is
    1C3C0C95 95680953 2FCF0E24 49A6B525
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    A988A97E 85EEC28E 76B95C29 B6023003
   E is
    B16AEDF5 AA0DE657 BA637B39 1AAFD255
-----------------------

The Mac verifies

P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39 1AAFD255

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

Example #5

Taglen = 128
AADlen = 160
PTlen = 480
------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
    FEFFE992 8665731C
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    F5D3D585
P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39

H is
    466923EC 9AE68221 4F2C082B ADB39249
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    E0B1F82E C484EEA4 4E5FF301 28DF01CD
   E is
    3980CA0B 3C00E841 EB06FAC4 872A2757
```

```
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    0339B5B9 B3DB2E5E 4CC9A389 86906BEE
   E is
    859E1CEA A6EFD984 628593B4 0CA1E19C
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    614B3195 542CCC76 83AE933C 81EC8A62
   E is
    7D773D00 C144C525 AC619D18 C84A3F47
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    A988A97E 85EEC28E 76B95C29 B6023003
   E is
    18E2448B 2FE324D9 CCDA2710 ACADE256
-----------------------
CT is
    3980CA0B 3C00E841 EB06FAC4 872A2757
    859E1CEA A6EFD984 628593B4 0CA1E19C
    7D773D00 C144C525 AC619D18 C84A3F47
    18E2448B 2FE324D9 CCDA2710
S is
    5BDF824E F759A0DF 70824DAB F5283F64
Cipher(K, J0) is
    C835AA88 AEBBC94F 5A02E179 FDCFC3E4

C is
    3980CA0B 3C00E841 EB06FAC4 872A2757
    859E1CEA A6EFD984 628593B4 0CA1E19C
    7D773D00 C144C525 AC619D18 C84A3F47
    18E2448B 2FE324D9 CCDA2710
Tag is
    93EA28C6 59E26990 2A80ACD2 08E7FC80

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

Decrypt-Verify

-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    E0B1F82E C484EEA4 4E5FF301 28DF01CD
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    0339B5B9 B3DB2E5E 4CC9A389 86906BEE
   E is
    86A7A953 1534F7DA 2E4C303D 8A318A72
  Block #3:
   CB is
```

```
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    614B3195 542CCC76 83AE933C 81EC8A62
   E is
    1C3C0C95 95680953 2FCF0E24 49A6B525
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    A988A97E 85EEC28E 76B95C29 B6023003
   E is
    B16AEDF5 AA0DE657 BA637B39 818F4000
-----------------------

The Mac verifies

P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39

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

Example #6

Taglen = 96
AADlen = 160
PTlen = 480
------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
    FEFFE992 8665731C
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    F5D3D585
P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39

H is
    466923EC 9AE68221 4F2C082B ADB39249
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    E0B1F82E C484EEA4 4E5FF301 28DF01CD
   E is
    3980CA0B 3C00E841 EB06FAC4 872A2757
  Block #2:
   CB is
```

```
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    0339B5B9 B3DB2E5E 4CC9A389 86906BEE
   E is
    859E1CEA A6EFD984 628593B4 0CA1E19C
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    614B3195 542CCC76 83AE933C 81EC8A62
   E is
    7D773D00 C144C525 AC619D18 C84A3F47
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    A988A97E 85EEC28E 76B95C29 B6023003
   E is
    18E2448B 2FE324D9 CCDA2710 ACADE256
-----------------------
CT is
    3980CA0B 3C00E841 EB06FAC4 872A2757
    859E1CEA A6EFD984 628593B4 0CA1E19C
    7D773D00 C144C525 AC619D18 C84A3F47
    18E2448B 2FE324D9 CCDA2710
S is
    5BDF824E F759A0DF 70824DAB F5283F64
Cipher(K, J0) is
    C835AA88 AEBBC94F 5A02E179 FDCFC3E4

C is
    3980CA0B 3C00E841 EB06FAC4 872A2757
    859E1CEA A6EFD984 628593B4 0CA1E19C
    7D773D00 C144C525 AC619D18 C84A3F47
    18E2448B 2FE324D9 CCDA2710
Tag is
    93EA28C6 59E26990 2A80ACD2

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

Decrypt-Verify

-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    E0B1F82E C484EEA4 4E5FF301 28DF01CD
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    0339B5B9 B3DB2E5E 4CC9A389 86906BEE
   E is
    86A7A953 1534F7DA 2E4C303D 8A318A72
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
```

```
    614B3195 542CCC76 83AE933C 81EC8A62
   E is
    1C3C0C95 95680953 2FCF0E24 49A6B525
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    A988A97E 85EEC28E 76B95C29 B6023003
   E is
    B16AEDF5 AA0DE657 BA637B39 818F4000
-----------------------

The Mac verifies

P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39

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

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

GCM-AES256
------------------------------------------------------------

Example #1

Taglen = 128
AADlen = 0
PTlen = 0
------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
    FEFFE992 8665731C 6D6A8F94 67308308
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    <empty>
P is
    <empty>

H is
    ACBEF205 79B4B8EB CE889BAC 8732DAD7
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    8B1CF3D5 61D27BE2 51263E66 857164E7
   E is
    522DC1F0 99567D07 F47F37A3 2A84427D
-----------------------
CT is
    <empty>
```

```
S is
    00000000 00000000 00000000 00000000
Cipher(K, J0) is
    FD2CAA16 A5832E76 AA132C14 53EEDA7E

C is
    <empty>
Tag is
    FD2CAA16 A5832E76 AA132C14 53EEDA7E

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

Decrypt-Verify

-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    8B1CF3D5 61D27BE2 51263E66 857164E7
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
-----------------------

The Mac verifies

P is
    <empty>

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

Example #2

Taglen = 128
AADlen = 0
PTlen = 512
-----------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
    FEFFE992 8665731C 6D6A8F94 67308308
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    <empty>
P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39 1AAFD255

H is
    ACBEF205 79B4B8EB CE889BAC 8732DAD7
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
-----------------------
 GCM_Ctr
  Block #1:
   CB is
```

```
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    8B1CF3D5 61D27BE2 51263E66 857164E7
   E is
    522DC1F0 99567D07 F47F37A3 2A84427D
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    E29D258F AAD13713 5BD49280 AF645BD8
   E is
    643A8CDC BFE5C0C9 7598A2BD 2555D1AA
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    908C82DD CC65B26E 887F8534 1F243D1D
   E is
    8CB08E48 590DBB3D A7B08B10 56828838
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    749CF396 39B79C5D 06AA8D5B 932FC7F8
   E is
    C5F61E63 93BA7A0A BCC9F662 898015AD
-----------------------
CT is
    522DC1F0 99567D07 F47F37A3 2A84427D
    643A8CDC BFE5C0C9 7598A2BD 2555D1AA
    8CB08E48 590DBB3D A7B08B10 56828838
    C5F61E63 93BA7A0A BCC9F662 898015AD
S is
    4DB870D3 7CB75FCB 46097C36 230D1612
Cipher(K, J0) is
    FD2CAA16 A5832E76 AA132C14 53EEDA7E

C is
    522DC1F0 99567D07 F47F37A3 2A84427D
    643A8CDC BFE5C0C9 7598A2BD 2555D1AA
    8CB08E48 590DBB3D A7B08B10 56828838
    C5F61E63 93BA7A0A BCC9F662 898015AD
Tag is
    B094DAC5 D93471BD EC1A5022 70E3CC6C

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

Decrypt-Verify

-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    8B1CF3D5 61D27BE2 51263E66 857164E7
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
```

```
    E29D258F AAD13713 5BD49280 AF645BD8
   E is
    86A7A953 1534F7DA 2E4C303D 8A318A72
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    908C82DD CC65B26E 887F8534 1F243D1D
   E is
    1C3C0C95 95680953 2FCF0E24 49A6B525
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    749CF396 39B79C5D 06AA8D5B 932FC7F8
   E is
    B16AEDF5 AA0DE657 BA637B39 1AAFD255
-----------------------

The Mac verifies

P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39 1AAFD255

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

Example #3

Taglen = 128
AADlen = 512
PTlen = 0
------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
    FEFFE992 8665731C 6D6A8F94 67308308
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    F5D3D585 03B9699D E785895A 96FDBAAF
    43B1CD7F 598ECE23 881B00E3 ED030688
    7B0C785E 27E8AD3F 82232071 04725DD4
P is
    <empty>

H is
    ACBEF205 79B4B8EB CE889BAC 8732DAD7
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    8B1CF3D5 61D27BE2 51263E66 857164E7
```

```
   E is
    522DC1F0 99567D07 F47F37A3 2A84427D
-----------------------
CT is
    <empty>
S is
    23181CCA 714DCC8B 14D0E2B4 491F343A
Cipher(K, J0) is
    FD2CAA16 A5832E76 AA132C14 53EEDA7E

C is
    <empty>
Tag is
    DE34B6DC D4CEE2FD BEC3CEA0 1AF1EE44

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

Decrypt-Verify

-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    8B1CF3D5 61D27BE2 51263E66 857164E7
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
-----------------------

The Mac verifies

P is
    <empty>

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

Example #4

Taglen = 128
AADlen = 512
PTlen = 512
-----------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
    FEFFE992 8665731C 6D6A8F94 67308308
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    F5D3D585 03B9699D E785895A 96FDBAAF
    43B1CD7F 598ECE23 881B00E3 ED030688
    7B0C785E 27E8AD3F 82232071 04725DD4
P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39 1AAFD255
```

```
H is
    ACBEF205 79B4B8EB CE889BAC 8732DAD7
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    8B1CF3D5 61D27BE2 51263E66 857164E7
   E is
    522DC1F0 99567D07 F47F37A3 2A84427D
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    E29D258F AAD13713 5BD49280 AF645BD8
   E is
    643A8CDC BFE5C0C9 7598A2BD 2555D1AA
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    908C82DD CC65B26E 887F8534 1F243D1D
   E is
    8CB08E48 590DBB3D A7B08B10 56828838
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    749CF396 39B79C5D 06AA8D5B 932FC7F8
   E is
    C5F61E63 93BA7A0A BCC9F662 898015AD
-----------------------
CT is
    522DC1F0 99567D07 F47F37A3 2A84427D
    643A8CDC BFE5C0C9 7598A2BD 2555D1AA
    8CB08E48 590DBB3D A7B08B10 56828838
    C5F61E63 93BA7A0A BCC9F662 898015AD
S is
    3D41DCE5 BCB3D085 D0D9CE2A 878B741C
Cipher(K, J0) is
    FD2CAA16 A5832E76 AA132C14 53EEDA7E

C is
    522DC1F0 99567D07 F47F37A3 2A84427D
    643A8CDC BFE5C0C9 7598A2BD 2555D1AA
    8CB08E48 590DBB3D A7B08B10 56828838
    C5F61E63 93BA7A0A BCC9F662 898015AD
Tag is
    C06D76F3 1930FEF3 7ACAE23E D465AE62

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

Decrypt-Verify

-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
```

```
   CT is
    8B1CF3D5 61D27BE2 51263E66 857164E7
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    E29D258F AAD13713 5BD49280 AF645BD8
   E is
    86A7A953 1534F7DA 2E4C303D 8A318A72
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    908C82DD CC65B26E 887F8534 1F243D1D
   E is
    1C3C0C95 95680953 2FCF0E24 49A6B525
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    749CF396 39B79C5D 06AA8D5B 932FC7F8
   E is
    B16AEDF5 AA0DE657 BA637B39 1AAFD255
-----------------------

The Mac verifies

P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39 1AAFD255

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

Example #5

Taglen = 128
AADlen = 160
PTlen = 480
------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
    FEFFE992 8665731C 6D6A8F94 67308308
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    F5D3D585
P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39

H is
    ACBEF205 79B4B8EB CE889BAC 8732DAD7
```

```
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    8B1CF3D5 61D27BE2 51263E66 857164E7
   E is
    522DC1F0 99567D07 F47F37A3 2A84427D
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    E29D258F AAD13713 5BD49280 AF645BD8
   E is
    643A8CDC BFE5C0C9 7598A2BD 2555D1AA
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    908C82DD CC65B26E 887F8534 1F243D1D
   E is
    8CB08E48 590DBB3D A7B08B10 56828838
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    749CF396 39B79C5D 06AA8D5B 932FC7F8
   E is
    C5F61E63 93BA7A0A BCC9F662 898015AD
-----------------------
CT is
    522DC1F0 99567D07 F47F37A3 2A84427D
    643A8CDC BFE5C0C9 7598A2BD 2555D1AA
    8CB08E48 590DBB3D A7B08B10 56828838
    C5F61E63 93BA7A0A BCC9F662
S is
    1DBBB349 E0B1F4FF F5AA3BB1 F6B2B0DE
Cipher(K, J0) is
    FD2CAA16 A5832E76 AA132C14 53EEDA7E

C is
    522DC1F0 99567D07 F47F37A3 2A84427D
    643A8CDC BFE5C0C9 7598A2BD 2555D1AA
    8CB08E48 590DBB3D A7B08B10 56828838
    C5F61E63 93BA7A0A BCC9F662
Tag is
    E097195F 4532DA89 5FB917A5 A55C6AA0

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

Decrypt-Verify

-----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    8B1CF3D5 61D27BE2 51263E66 857164E7
```

```
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    E29D258F AAD13713 5BD49280 AF645BD8
   E is
    86A7A953 1534F7DA 2E4C303D 8A318A72
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    908C82DD CC65B26E 887F8534 1F243D1D
   E is
    1C3C0C95 95680953 2FCF0E24 49A6B525
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    749CF396 39B79C5D 06AA8D5B 932FC7F8
   E is
    B16AEDF5 AA0DE657 BA637B39 818F4000
-----------------------

The Mac verifies

P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39

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

Example #6

Taglen = 96
AADlen = 160
PTlen = 480
------------------------------------------------------------

Encrypt-Generate

K is
    FEFFE992 8665731C 6D6A8F94 67308308
    FEFFE992 8665731C 6D6A8F94 67308308
IV is
    CAFEBABE FACEDBAD DECAF888
A is
    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    F5D3D585
P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39

H is
    ACBEF205 79B4B8EB CE889BAC 8732DAD7
J0 is
    CAFEBABE FACEDBAD DECAF888 00000001
```

```
----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    8B1CF3D5 61D27BE2 51263E66 857164E7
   E is
    522DC1F0 99567D07 F47F37A3 2A84427D
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    E29D258F AAD13713 5BD49280 AF645BD8
   E is
    643A8CDC BFE5C0C9 7598A2BD 2555D1AA
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    908C82DD CC65B26E 887F8534 1F243D1D
   E is
    8CB08E48 590DBB3D A7B08B10 56828838
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    749CF396 39B79C5D 06AA8D5B 932FC7F8
   E is
    C5F61E63 93BA7A0A BCC9F662 898015AD
----------------------
CT is
    522DC1F0 99567D07 F47F37A3 2A84427D
    643A8CDC BFE5C0C9 7598A2BD 2555D1AA
    8CB08E48 590DBB3D A7B08B10 56828838
    C5F61E63 93BA7A0A BCC9F662
S is
    1DBBB349 E0B1F4FF F5AA3BB1 F6B2B0DE
Cipher(K, J0) is
    FD2CAA16 A5832E76 AA132C14 53EEDA7E

C is
    522DC1F0 99567D07 F47F37A3 2A84427D
    643A8CDC BFE5C0C9 7598A2BD 2555D1AA
    8CB08E48 590DBB3D A7B08B10 56828838
    C5F61E63 93BA7A0A BCC9F662
Tag is
    E097195F 4532DA89 5FB917A5

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

Decrypt-Verify

----------------------
 GCM_Ctr
  Block #1:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000002
   CT is
    8B1CF3D5 61D27BE2 51263E66 857164E7
   E is
    D9313225 F88406E5 A55909C5 AFF5269A
```

```
  Block #2:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000003
   CT is
    E29D258F AAD13713 5BD49280 AF645BD8
   E is
    86A7A953 1534F7DA 2E4C303D 8A318A72
  Block #3:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000004
   CT is
    908C82DD CC65B26E 887F8534 1F243D1D
   E is
    1C3C0C95 95680953 2FCF0E24 49A6B525
  Block #4:
   CB is
    CAFEBABE FACEDBAD DECAF888 00000005
   CT is
    749CF396 39B79C5D 06AA8D5B 932FC7F8
   E is
    B16AEDF5 AA0DE657 BA637B39 818F4000
-----------------------

The Mac verifies

P is
    D9313225 F88406E5 A55909C5 AFF5269A
    86A7A953 1534F7DA 2E4C303D 8A318A72
    1C3C0C95 95680953 2FCF0E24 49A6B525
    B16AEDF5 AA0DE657 BA637B39

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

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