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

  Block Cipher Modes of Operation

      Electronic Codebook (ECB)

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

ECB-AES128 (Encryption)
----------------------------------------------------------------

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

  Block #1
    Plaintext     6BC1BEE2 2E409F96 E93D7E11 7393172A
    InputBlock    6BC1BEE2 2E409F96 E93D7E11 7393172A
    OutputBlock   3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    Ciphertext    E800807C 28FE1200 02000000 60FE1200
  Block #2
    Plaintext     AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    InputBlock    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    OutputBlock   F5D3D585 03B9699D E785895A 96FDBAAF
    Ciphertext    9508917C 0000807C 00000000 29000000
  Block #3
    Plaintext     30C81C46 A35CE411 E5FBC119 1A0A52EF
    InputBlock    30C81C46 A35CE411 E5FBC119 1A0A52EF
    OutputBlock   43B1CD7F 598ECE23 881B00E3 ED030688
    Ciphertext    9C9A917C 0000807C C2FE1200 BCFE1200
  Block #4
    Plaintext     F69F2445 DF4F9B17 AD2B417B E66C3710
    InputBlock    F69F2445 DF4F9B17 AD2B417B E66C3710
    OutputBlock   7B0C785E 27E8AD3F 82232071 04725DD4
    Ciphertext    48033300 C2FE1200 3F9B917C D8C0977C
```

```
Ciphertext is
    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    F5D3D585 03B9699D E785895A 96FDBAAF
    43B1CD7F 598ECE23 881B00E3 ED030688
    7B0C785E 27E8AD3F 82232071 04725DD4

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

ECB-AES128 (Decryption)
----------------------------------------------------------------

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Ciphertext is
    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    F5D3D585 03B9699D E785895A 96FDBAAF
    43B1CD7F 598ECE23 881B00E3 ED030688
    7B0C785E 27E8AD3F 82232071 04725DD4

  Block #1
    Ciphertext    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    InputBlock    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
    OutputBlock   6BC1BEE2 2E409F96 E93D7E11 7393172A
    Plaintext     EB9A917C 70854100 02000000 FFFF0000
  Block #2
    Ciphertext    F5D3D585 03B9699D E785895A 96FDBAAF
    InputBlock    F5D3D585 03B9699D E785895A 96FDBAAF
    OutputBlock   AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    Plaintext     00F0FD7F C01F2500 B4B5B6B7 30363300
  Block #3
    Ciphertext    43B1CD7F 598ECE23 881B00E3 ED030688
    InputBlock    43B1CD7F 598ECE23 881B00E3 ED030688
    OutputBlock   30C81C46 A35CE411 E5FBC119 1A0A52EF
    Plaintext     DC31917C 11000000 6CFF1200 00000004
  Block #4
    Ciphertext    7B0C785E 27E8AD3F 82232071 04725DD4
    InputBlock    7B0C785E 27E8AD3F 82232071 04725DD4
    OutputBlock   F69F2445 DF4F9B17 AD2B417B E66C3710
    Plaintext     04000000 C0FE1200 C0FE1200 00000000

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
```

```
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

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

ECB-AES192 (Encryption)
--------------------------------------------------------------

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

  Block #1
    Plaintext     6BC1BEE2 2E409F96 E93D7E11 7393172A
    InputBlock    6BC1BEE2 2E409F96 E93D7E11 7393172A
    OutputBlock   BD334F1D 6E45F25F F712A214 571FA5CC
    Ciphertext    3AD77BB4 0D7A3660 A89ECAF3 2466EF97
  Block #2
    Plaintext     AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    InputBlock    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    OutputBlock   97410484 6D0AD3AD 7734ECB3 ECEE4EEF
    Ciphertext    F5D3D585 03B9699D E785895A 96FDBAAF
  Block #3
    Plaintext     30C81C46 A35CE411 E5FBC119 1A0A52EF
    InputBlock    30C81C46 A35CE411 E5FBC119 1A0A52EF
    OutputBlock   EF7AFD22 70E2E60A DCE0BA2F ACE6444E
    Ciphertext    43B1CD7F 598ECE23 881B00E3 ED030688
  Block #4
    Plaintext     F69F2445 DF4F9B17 AD2B417B E66C3710
    InputBlock    F69F2445 DF4F9B17 AD2B417B E66C3710
    OutputBlock   9A4B41BA 738D6C72 FB166916 03C18E0E
    Ciphertext    7B0C785E 27E8AD3F 82232071 04725DD4

Ciphertext is
    BD334F1D 6E45F25F F712A214 571FA5CC
    97410484 6D0AD3AD 7734ECB3 ECEE4EEF
    EF7AFD22 70E2E60A DCE0BA2F ACE6444E
    9A4B41BA 738D6C72 FB166916 03C18E0E
```

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

ECB-AES192 (Decryption)
----------------------------------------------------------

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Ciphertext is
    BD334F1D 6E45F25F F712A214 571FA5CC
    97410484 6D0AD3AD 7734ECB3 ECEE4EEF
    EF7AFD22 70E2E60A DCE0BA2F ACE6444E
    9A4B41BA 738D6C72 FB166916 03C18E0E

  Block #1
    Ciphertext    BD334F1D 6E45F25F F712A214 571FA5CC
    InputBlock    BD334F1D 6E45F25F F712A214 571FA5CC
    OutputBlock   6BC1BEE2 2E409F96 E93D7E11 7393172A
    Plaintext     6BC1BEE2 2E409F96 E93D7E11 7393172A
  Block #2
    Ciphertext    97410484 6D0AD3AD 7734ECB3 ECEE4EEF
    InputBlock    97410484 6D0AD3AD 7734ECB3 ECEE4EEF
    OutputBlock   AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    Plaintext     AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
  Block #3
    Ciphertext    EF7AFD22 70E2E60A DCE0BA2F ACE6444E
    InputBlock    EF7AFD22 70E2E60A DCE0BA2F ACE6444E
    OutputBlock   30C81C46 A35CE411 E5FBC119 1A0A52EF
    Plaintext     30C81C46 A35CE411 E5FBC119 1A0A52EF
  Block #4
    Ciphertext    9A4B41BA 738D6C72 FB166916 03C18E0E
    InputBlock    9A4B41BA 738D6C72 FB166916 03C18E0E
    OutputBlock   F69F2445 DF4F9B17 AD2B417B E66C3710
    Plaintext     F69F2445 DF4F9B17 AD2B417B E66C3710

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

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

```
ECB-AES256 (Encryption)
----------------------------------------------------------------

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

  Block #1
    Plaintext     6BC1BEE2 2E409F96 E93D7E11 7393172A
    InputBlock    6BC1BEE2 2E409F96 E93D7E11 7393172A
    OutputBlock   F3EED1BD B5D2A03C 064B5A7E 3DB181F8
    Ciphertext    BD334F1D 6E45F25F F712A214 571FA5CC
  Block #2
    Plaintext     AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    InputBlock    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    OutputBlock   591CCB10 D410ED26 DC5BA74A 31362870
    Ciphertext    97410484 6D0AD3AD 7734ECB3 ECEE4EEF
  Block #3
    Plaintext     30C81C46 A35CE411 E5FBC119 1A0A52EF
    InputBlock    30C81C46 A35CE411 E5FBC119 1A0A52EF
    OutputBlock   B6ED21B9 9CA6F4F9 F153E7B1 BEAFED1D
    Ciphertext    EF7AFD22 70E2E60A DCE0BA2F ACE6444E
  Block #4
    Plaintext     F69F2445 DF4F9B17 AD2B417B E66C3710
    InputBlock    F69F2445 DF4F9B17 AD2B417B E66C3710
    OutputBlock   23304B7A 39F9F3FF 067D8D8F 9E24ECC7
    Ciphertext    9A4B41BA 738D6C72 FB166916 03C18E0E

Ciphertext is
    F3EED1BD B5D2A03C 064B5A7E 3DB181F8
    591CCB10 D410ED26 DC5BA74A 31362870
    B6ED21B9 9CA6F4F9 F153E7B1 BEAFED1D
    23304B7A 39F9F3FF 067D8D8F 9E24ECC7

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

ECB-AES256 (Decryption)
----------------------------------------------------------------

Key is
```

```
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Ciphertext is
    F3EED1BD B5D2A03C 064B5A7E 3DB181F8
    591CCB10 D410ED26 DC5BA74A 31362870
    B6ED21B9 9CA6F4F9 F153E7B1 BEAFED1D
    23304B7A 39F9F3FF 067D8D8F 9E24ECC7

  Block #1
    Ciphertext    F3EED1BD B5D2A03C 064B5A7E 3DB181F8
    InputBlock    F3EED1BD B5D2A03C 064B5A7E 3DB181F8
    OutputBlock   6BC1BEE2 2E409F96 E93D7E11 7393172A
    Plaintext     6BC1BEE2 2E409F96 E93D7E11 7393172A
  Block #2
    Ciphertext    591CCB10 D410ED26 DC5BA74A 31362870
    InputBlock    591CCB10 D410ED26 DC5BA74A 31362870
    OutputBlock   AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    Plaintext     AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
  Block #3
    Ciphertext    B6ED21B9 9CA6F4F9 F153E7B1 BEAFED1D
    InputBlock    B6ED21B9 9CA6F4F9 F153E7B1 BEAFED1D
    OutputBlock   30C81C46 A35CE411 E5FBC119 1A0A52EF
    Plaintext     30C81C46 A35CE411 E5FBC119 1A0A52EF
  Block #4
    Ciphertext    23304B7A 39F9F3FF 067D8D8F 9E24ECC7
    InputBlock    23304B7A 39F9F3FF 067D8D8F 9E24ECC7
    OutputBlock   F69F2445 DF4F9B17 AD2B417B E66C3710
    Plaintext     F69F2445 DF4F9B17 AD2B417B E66C3710

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

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

  Block Cipher Modes of Operation

      Cipher Block Chaining (CBC)

IV is
    00010203 04050607 08090A0B 0C0D0E0F

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

CBC-AES128 (Encryption)
----------------------------------------------------------------

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

  Block #1
    Plaintext     6BC1BEE2 2E409F96 E93D7E11 7393172A
    InputBlock    6BC0BCE1 2A459991 E134741A 7F9E1925
    OutputBlock   7649ABAC 8119B246 CEE98E9B 12E9197D
    Ciphertext    7649ABAC 8119B246 CEE98E9B 12E9197D
  Block #2
    Plaintext     AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    InputBlock    D86421FB 9F1A1EDA 505EE137 5746972C
    OutputBlock   5086CB9B 507219EE 95DB113A 917678B2
    Ciphertext    5086CB9B 507219EE 95DB113A 917678B2
  Block #3
    Plaintext     30C81C46 A35CE411 E5FBC119 1A0A52EF
    InputBlock    604ED7DD F32EFDFF 7020D023 8B7C2A5D
    OutputBlock   73BED6B8 E3C1743B 7116E69E 22229516
    Ciphertext    73BED6B8 E3C1743B 7116E69E 22229516
  Block #4
    Plaintext     F69F2445 DF4F9B17 AD2B417B E66C3710
```

```
    InputBlock    8521F2FD 3C8EEF2C DC3DA7E5 C44EA206
    OutputBlock   3FF1CAA1 681FAC09 120ECA30 7586E1A7
    Ciphertext    3FF1CAA1 681FAC09 120ECA30 7586E1A7

Ciphertext is
    7649ABAC 8119B246 CEE98E9B 12E9197D
    5086CB9B 507219EE 95DB113A 917678B2
    73BED6B8 E3C1743B 7116E69E 22229516
    3FF1CAA1 681FAC09 120ECA30 7586E1A7

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

CBC-AES128 (Decryption)
----------------------------------------------------------------

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Ciphertext is
    7649ABAC 8119B246 CEE98E9B 12E9197D
    5086CB9B 507219EE 95DB113A 917678B2
    73BED6B8 E3C1743B 7116E69E 22229516
    3FF1CAA1 681FAC09 120ECA30 7586E1A7

  Block #1
    Ciphertext    7649ABAC 8119B246 CEE98E9B 12E9197D
    InputBlock    7649ABAC 8119B246 CEE98E9B 12E9197D
    OutputBlock   6BC0BCE1 2A459991 E134741A 7F9E1925
    Plaintext     6BC1BEE2 2E409F96 E93D7E11 7393172A
  Block #2
    Ciphertext    5086CB9B 507219EE 95DB113A 917678B2
    InputBlock    5086CB9B 507219EE 95DB113A 917678B2
    OutputBlock   D86421FB 9F1A1EDA 505EE137 5746972C
    Plaintext     AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
  Block #3
    Ciphertext    73BED6B8 E3C1743B 7116E69E 22229516
    InputBlock    73BED6B8 E3C1743B 7116E69E 22229516
    OutputBlock   604ED7DD F32EFDFF 7020D023 8B7C2A5D
    Plaintext     30C81C46 A35CE411 E5FBC119 1A0A52EF
  Block #4
    Ciphertext    3FF1CAA1 681FAC09 120ECA30 7586E1A7
    InputBlock    3FF1CAA1 681FAC09 120ECA30 7586E1A7
    OutputBlock   8521F2FD 3C8EEF2C DC3DA7E5 C44EA206
    Plaintext     F69F2445 DF4F9B17 AD2B417B E66C3710

Plaintext is
```

```
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

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

CBC-AES192 (Encryption)
--------------------------------------------------------------

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

  Block #1
    Plaintext     6BC1BEE2 2E409F96 E93D7E11 7393172A
    InputBlock    6BC0BCE1 2A459991 E134741A 7F9E1925
    OutputBlock   4F021DB2 43BC633D 7178183A 9FA071E8
    Ciphertext    4F021DB2 43BC633D 7178183A 9FA071E8
  Block #2
    Plaintext     AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    InputBlock    E12F97E5 5DBFCFA1 EFCF7796 DA0FFFB9
    OutputBlock   B4D9ADA9 AD7DEDF4 E5E73876 3F69145A
    Ciphertext    B4D9ADA9 AD7DEDF4 E5E73876 3F69145A
  Block #3
    Plaintext     30C81C46 A35CE411 E5FBC119 1A0A52EF
    InputBlock    8411B1EF 0E2109E5 001CF96F 256346B5
    OutputBlock   571B2420 12FB7AE0 7FA9BAAC 3DF102E0
    Ciphertext    571B2420 12FB7AE0 7FA9BAAC 3DF102E0
  Block #4
    Plaintext     F69F2445 DF4F9B17 AD2B417B E66C3710
    InputBlock    A1840065 CDB4E1F7 D282FBD7 DB9D35F0
    OutputBlock   08B0E279 88598881 D920A9E6 4F5615CD
    Ciphertext    08B0E279 88598881 D920A9E6 4F5615CD

Ciphertext is
    4F021DB2 43BC633D 7178183A 9FA071E8
    B4D9ADA9 AD7DEDF4 E5E73876 3F69145A
```

```
    571B2420 12FB7AE0 7FA9BAAC 3DF102E0
    08B0E279 88598881 D920A9E6 4F5615CD

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

CBC-AES192 (Decryption)
--------------------------------------------------------------

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Ciphertext is
    4F021DB2 43BC633D 7178183A 9FA071E8
    B4D9ADA9 AD7DEDF4 E5E73876 3F69145A
    571B2420 12FB7AE0 7FA9BAAC 3DF102E0
    08B0E279 88598881 D920A9E6 4F5615CD

  Block #1
    Ciphertext    4F021DB2 43BC633D 7178183A 9FA071E8
    InputBlock    4F021DB2 43BC633D 7178183A 9FA071E8
    OutputBlock   6BC0BCE1 2A459991 E134741A 7F9E1925
    Plaintext     6BC1BEE2 2E409F96 E93D7E11 7393172A
  Block #2
    Ciphertext    B4D9ADA9 AD7DEDF4 E5E73876 3F69145A
    InputBlock    B4D9ADA9 AD7DEDF4 E5E73876 3F69145A
    OutputBlock   E12F97E5 5DBFCFA1 EFCF7796 DA0FFFB9
    Plaintext     AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
  Block #3
    Ciphertext    571B2420 12FB7AE0 7FA9BAAC 3DF102E0
    InputBlock    571B2420 12FB7AE0 7FA9BAAC 3DF102E0
    OutputBlock   8411B1EF 0E2109E5 001CF96F 256346B5
    Plaintext     30C81C46 A35CE411 E5FBC119 1A0A52EF
  Block #4
    Ciphertext    08B0E279 88598881 D920A9E6 4F5615CD
    InputBlock    08B0E279 88598881 D920A9E6 4F5615CD
    OutputBlock   A1840065 CDB4E1F7 D282FBD7 DB9D35F0
    Plaintext     F69F2445 DF4F9B17 AD2B417B E66C3710

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

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

CBC-AES256 (Encryption)
----------

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

  Block #1
    Plaintext     6BC1BEE2 2E409F96 E93D7E11 7393172A
    InputBlock    6BC0BCE1 2A459991 E134741A 7F9E1925
    OutputBlock   F58C4C04 D6E5F1BA 779EABFB 5F7BFBD6
    Ciphertext    F58C4C04 D6E5F1BA 779EABFB 5F7BFBD6
  Block #2
    Plaintext     AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    InputBlock    5BA1C653 C8E65D26 E929C457 1AD47587
    OutputBlock   9CFC4E96 7EDB808D 679F777B C6702C7D
    Ciphertext    9CFC4E96 7EDB808D 679F777B C6702C7D
  Block #3
    Plaintext     30C81C46 A35CE411 E5FBC119 1A0A52EF
    InputBlock    AC3452D0 DD87649C 8264B662 DC7A7E92
    OutputBlock   39F23369 A9D9BACF A530E263 04231461
    Ciphertext    39F23369 A9D9BACF A530E263 04231461
  Block #4
    Plaintext     F69F2445 DF4F9B17 AD2B417B E66C3710
    InputBlock    CF6D172C 769621D8 081BA318 E24F2371
    OutputBlock   B2EB05E2 C39BE9FC DA6C1907 8C6A9D1B
    Ciphertext    B2EB05E2 C39BE9FC DA6C1907 8C6A9D1B

Ciphertext is
    F58C4C04 D6E5F1BA 779EABFB 5F7BFBD6
    9CFC4E96 7EDB808D 679F777B C6702C7D
    39F23369 A9D9BACF A530E263 04231461
    B2EB05E2 C39BE9FC DA6C1907 8C6A9D1B

==========

CBC-AES256 (Decryption)
```

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

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Ciphertext is
    F58C4C04 D6E5F1BA 779EABFB 5F7BFBD6
    9CFC4E96 7EDB808D 679F777B C6702C7D
    39F23369 A9D9BACF A530E263 04231461
    B2EB05E2 C39BE9FC DA6C1907 8C6A9D1B

  Block #1
    Ciphertext    F58C4C04 D6E5F1BA 779EABFB 5F7BFBD6
    InputBlock    F58C4C04 D6E5F1BA 779EABFB 5F7BFBD6
    OutputBlock   6BC0BCE1 2A459991 E134741A 7F9E1925
    Plaintext     6BC1BEE2 2E409F96 E93D7E11 7393172A
  Block #2
    Ciphertext    9CFC4E96 7EDB808D 679F777B C6702C7D
    InputBlock    9CFC4E96 7EDB808D 679F777B C6702C7D
    OutputBlock   5BA1C653 C8E65D26 E929C457 1AD47587
    Plaintext     AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
  Block #3
    Ciphertext    39F23369 A9D9BACF A530E263 04231461
    InputBlock    39F23369 A9D9BACF A530E263 04231461
    OutputBlock   AC3452D0 DD87649C 8264B662 DC7A7E92
    Plaintext     30C81C46 A35CE411 E5FBC119 1A0A52EF
  Block #4
    Ciphertext    B2EB05E2 C39BE9FC DA6C1907 8C6A9D1B
    InputBlock    B2EB05E2 C39BE9FC DA6C1907 8C6A9D1B
    OutputBlock   CF6D172C 769621D8 081BA318 E24F2371
    Plaintext     F69F2445 DF4F9B17 AD2B417B E66C3710

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

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

  Block Cipher Modes of Operation

      Cipher FeedBack (CFB)

IV is
    00010203 04050607 08090A0B 0C0D0E0F

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

CFB-AES128 (Encryption)

  Segment Length = 128

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

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710


Ciphertext is
    3B3FD92E B72DAD20 333449F8 E83CFB4A
    C8A64537 A0B3A93F CDE3CDAD 9F1CE58B
    26751F67 A3CBB140 B1808CF1 87A4F4DF
    C04B0535 7C5D1C0E EAC4C66F 9FF7F2E6

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

CFB-AES128 (Decryption)

  Segment Length = 128

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

```
Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Ciphertext is
    3B3FD92E B72DAD20 333449F8 E83CFB4A
    C8A64537 A0B3A93F CDE3CDAD 9F1CE58B
    26751F67 A3CBB140 B1808CF1 87A4F4DF
    C04B0535 7C5D1C0E EAC4C66F 9FF7F2E6


Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

CFB-AES128 (Encryption)

  Segment Length = 8

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

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A


Ciphertext is
    3B79424C 9C0DD436 BACE9E0E D4586A4F

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

CFB-AES128 (Decryption)

  Segment Length = 8

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

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C
```

```
Ciphertext is
    3B79424C 9C0DD436 BACE9E0E D4586A4F


Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A

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

CFB-AES128 (Encryption)

  Segment Length = 1

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

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Plaintext is
    6BC1


Ciphertext is
    69C8

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

CFB-AES128 (Decryption)

  Segment Length = 1

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

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Ciphertext is
    69C8


Plaintext is
    6A59

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

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

```
CFB-AES192 (Encryption)

  Segment Length = 128

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

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710


Ciphertext is
    CDC80D6F DDF18CAB 34C25909 C99A4174
    67CE7F7F 81173621 961A2B70 171D3D7A
    2E1E8A1D D59B88B1 C8E60FED 1EFAC4C9
    C05F9F9C A9834FA0 42AE8FBA 584B09FF

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

CFB-AES192 (Decryption)

  Segment Length = 128

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

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Ciphertext is
    CDC80D6F DDF18CAB 34C25909 C99A4174
    67CE7F7F 81173621 961A2B70 171D3D7A
    2E1E8A1D D59B88B1 C8E60FED 1EFAC4C9
    C05F9F9C A9834FA0 42AE8FBA 584B09FF


Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
```

```
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

CFB-AES192 (Encryption)

  Segment Length = 8

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

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A


Ciphertext is
    CDA2521E F0A905CA 44CD057C BF0D47A0

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

CFB-AES192 (Decryption)

  Segment Length = 8

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

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Ciphertext is
    CDA2521E F0A905CA 44CD057C BF0D47A0


Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A

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

CFB-AES192 (Encryption)

  Segment Length = 1
```

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

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Plaintext is
    6BC1


Ciphertext is
    9776

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

CFB-AES192 (Decryption)

  Segment Length = 1

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

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Ciphertext is
    9776


Plaintext is
    6EE0

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

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

CFB-AES256 (Encryption)

  Segment Length = 128

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

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4
```

```
Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710


Ciphertext is
    DC7E84BF DA79164B 7ECD8486 985D3860
    39FFED14 3B28B1C8 32113C63 31E5407B
    DF101324 15E54B92 A13ED0A8 267AE2F9
    75A38574 1AB9CEF8 2031623D 55B1E471

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

CFB-AES256 (Decryption)

  Segment Length = 128

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

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Ciphertext is
    DC7E84BF DA79164B 7ECD8486 985D3860
    39FFED14 3B28B1C8 32113C63 31E5407B
    DF101324 15E54B92 A13ED0A8 267AE2F9
    75A38574 1AB9CEF8 2031623D 55B1E471


Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

CFB-AES256 (Encryption)

  Segment Length = 8

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

```
Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A


Ciphertext is
    DC1F1A85 20A64DB5 5FCC8AC5 54844E88

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

CFB-AES256 (Decryption)

  Segment Length = 8

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

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Ciphertext is
    DC1F1A85 20A64DB5 5FCC8AC5 54844E88


Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A

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

CFB-AES256 (Encryption)

  Segment Length = 1

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

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Plaintext is
    6BC1
```

```
Ciphertext is
    93D0

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

CFB-AES256 (Decryption)

  Segment Length = 1

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

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Ciphertext is
    93D0


Plaintext is
    69F4

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

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

  Block Cipher Modes of Operation

      Output FeedBack (OFB)

IV is
    00010203 04050607 08090A0B 0C0D0E0F

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

OFB-AES128 (Encryption)
----------------------------------------------------------------

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

  Block #1
    InputBlock    00010203 04050607 08090A0B 0C0D0E0F
    OutputBlock   50FE67CC 996D32B6 DA0937E9 9BAFEC60
    Text-In       6BC1BEE2 2E409F96 E93D7E11 7393172A
    Text-Out      3B3FD92E B72DAD20 333449F8 E83CFB4A
  Block #2
    InputBlock    50FE67CC 996D32B6 DA0937E9 9BAFEC60
    OutputBlock   D9A4DADA 0892239F 6B8B3D76 80E15674
    Text-In       AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    Text-Out      7789508D 16918F03 F53C52DA C54ED825
  Block #3
    InputBlock    D9A4DADA 0892239F 6B8B3D76 80E15674
    OutputBlock   A7881958 3F0308E7 A6BF36B1 386ABF23
    Text-In       30C81C46 A35CE411 E5FBC119 1A0A52EF
    Text-Out      9740051E 9C5FECF6 4344F7A8 2260EDCC
  Block #4
    InputBlock    A7881958 3F0308E7 A6BF36B1 386ABF23
```

```
    OutputBlock   C6D3416D 29165C6F CB8E51A2 27BA994E
    Text-In       F69F2445 DF4F9B17 AD2B417B E66C3710
    Text-Out      304C6528 F659C778 66A510D9 C1D6AE5E

Ciphertext is
    3B3FD92E B72DAD20 333449F8 E83CFB4A
    7789508D 16918F03 F53C52DA C54ED825
    9740051E 9C5FECF6 4344F7A8 2260EDCC
    304C6528 F659C778 66A510D9 C1D6AE5E

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

OFB-AES128 (Decryption)
----------------------------------------------------------------

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Ciphertext is
    3B3FD92E B72DAD20 333449F8 E83CFB4A
    7789508D 16918F03 F53C52DA C54ED825
    9740051E 9C5FECF6 4344F7A8 2260EDCC
    304C6528 F659C778 66A510D9 C1D6AE5E

  Block #1
    InputBlock    00010203 04050607 08090A0B 0C0D0E0F
    OutputBlock   50FE67CC 996D32B6 DA0937E9 9BAFEC60
    Text-In       3B3FD92E B72DAD20 333449F8 E83CFB4A
    Text-Out      6BC1BEE2 2E409F96 E93D7E11 7393172A
  Block #2
    InputBlock    50FE67CC 996D32B6 DA0937E9 9BAFEC60
    OutputBlock   D9A4DADA 0892239F 6B8B3D76 80E15674
    Text-In       7789508D 16918F03 F53C52DA C54ED825
    Text-Out      AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
  Block #3
    InputBlock    D9A4DADA 0892239F 6B8B3D76 80E15674
    OutputBlock   A7881958 3F0308E7 A6BF36B1 386ABF23
    Text-In       9740051E 9C5FECF6 4344F7A8 2260EDCC
    Text-Out      30C81C46 A35CE411 E5FBC119 1A0A52EF
  Block #4
    InputBlock    A7881958 3F0308E7 A6BF36B1 386ABF23
    OutputBlock   C6D3416D 29165C6F CB8E51A2 27BA994E
    Text-In       304C6528 F659C778 66A510D9 C1D6AE5E
    Text-Out      F69F2445 DF4F9B17 AD2B417B E66C3710

Plaintext is
```

```
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

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

OFB-AES192 (Encryption)
--------------------------------------------------------------

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

  Block #1
    InputBlock    00010203 04050607 08090A0B 0C0D0E0F
    OutputBlock   A609B38D F3B1133D DDFF2718 BA09565E
    Text-In       6BC1BEE2 2E409F96 E93D7E11 7393172A
    Text-Out      CDC80D6F DDF18CAB 34C25909 C99A4174
  Block #2
    InputBlock    A609B38D F3B1133D DDFF2718 BA09565E
    OutputBlock   52EF01DA 52602FE0 975F78AC 84BF8A50
    Text-In       AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    Text-Out      FCC28B8D 4C63837C 09E81700 C1100401
  Block #3
    InputBlock    52EF01DA 52602FE0 975F78AC 84BF8A50
    OutputBlock   BD5286AC 63AABD7E B067AC54 B553F71D
    Text-In       30C81C46 A35CE411 E5FBC119 1A0A52EF
    Text-Out      8D9A9AEA C0F6596F 559C6D4D AF59A5F2
  Block #4
    InputBlock    BD5286AC 63AABD7E B067AC54 B553F71D
    OutputBlock   9B00044D 8885F729 31871330 3FC0FE3A
    Text-In       F69F2445 DF4F9B17 AD2B417B E66C3710
    Text-Out      6D9F2008 57CA6C3E 9CAC524B D9ACC92A

Ciphertext is
    CDC80D6F DDF18CAB 34C25909 C99A4174
    FCC28B8D 4C63837C 09E81700 C1100401
```

```
    8D9A9AEA C0F6596F 559C6D4D AF59A5F2
    6D9F2008 57CA6C3E 9CAC524B D9ACC92A

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

OFB-AES192 (Decryption)
------------------------------------------------------------

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Ciphertext is
    CDC80D6F DDF18CAB 34C25909 C99A4174
    FCC28B8D 4C63837C 09E81700 C1100401
    8D9A9AEA C0F6596F 559C6D4D AF59A5F2
    6D9F2008 57CA6C3E 9CAC524B D9ACC92A

  Block #1
    InputBlock    00010203 04050607 08090A0B 0C0D0E0F
    OutputBlock   A609B38D F3B1133D DDFF2718 BA09565E
    Text-In       CDC80D6F DDF18CAB 34C25909 C99A4174
    Text-Out      6BC1BEE2 2E409F96 E93D7E11 7393172A
  Block #2
    InputBlock    A609B38D F3B1133D DDFF2718 BA09565E
    OutputBlock   52EF01DA 52602FE0 975F78AC 84BF8A50
    Text-In       FCC28B8D 4C63837C 09E81700 C1100401
    Text-Out      AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
  Block #3
    InputBlock    52EF01DA 52602FE0 975F78AC 84BF8A50
    OutputBlock   BD5286AC 63AABD7E B067AC54 B553F71D
    Text-In       8D9A9AEA C0F6596F 559C6D4D AF59A5F2
    Text-Out      30C81C46 A35CE411 E5FBC119 1A0A52EF
  Block #4
    InputBlock    BD5286AC 63AABD7E B067AC54 B553F71D
    OutputBlock   9B00044D 8885F729 31871330 3FC0FE3A
    Text-In       6D9F2008 57CA6C3E 9CAC524B D9ACC92A
    Text-Out      F69F2445 DF4F9B17 AD2B417B E66C3710

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

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

OFB-AES256 (Encryption)
----------

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

  Block #1
    InputBlock    00010203 04050607 08090A0B 0C0D0E0F
    OutputBlock   B7BF3A5D F43989DD 97F0FA97 EBCE2F4A
    Text-In       6BC1BEE2 2E409F96 E93D7E11 7393172A
    Text-Out      DC7E84BF DA79164B 7ECD8486 985D3860
  Block #2
    InputBlock    B7BF3A5D F43989DD 97F0FA97 EBCE2F4A
    OutputBlock   E1C65630 5ED1A7A6 56380574 6FE03EDC
    Text-In       AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    Text-Out      4FEBDC67 40D20B3A C88F6AD8 2A4FB08D
  Block #3
    InputBlock    E1C65630 5ED1A7A6 56380574 6FE03EDC
    OutputBlock   41635BE6 25B48AFC 1666DD42 A09D96E7
    Text-In       30C81C46 A35CE411 E5FBC119 1A0A52EF
    Text-Out      71AB47A0 86E86EED F39D1C5B BA97C408
  Block #4
    InputBlock    41635BE6 25B48AFC 1666DD42 A09D96E7
    OutputBlock   F7B93058 B8BCE0FF FEA41BF0 012CD394
    Text-In       F69F2445 DF4F9B17 AD2B417B E66C3710
    Text-Out      0126141D 67F37BE8 538F5A8B E740E484

Ciphertext is
    DC7E84BF DA79164B 7ECD8486 985D3860
    4FEBDC67 40D20B3A C88F6AD8 2A4FB08D
    71AB47A0 86E86EED F39D1C5B BA97C408
    0126141D 67F37BE8 538F5A8B E740E484

==========

OFB-AES256 (Decryption)
```

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

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Ciphertext is
    DC7E84BF DA79164B 7ECD8486 985D3860
    4FEBDC67 40D20B3A C88F6AD8 2A4FB08D
    71AB47A0 86E86EED F39D1C5B BA97C408
    0126141D 67F37BE8 538F5A8B E740E484

  Block #1
    InputBlock    00010203 04050607 08090A0B 0C0D0E0F
    OutputBlock   B7BF3A5D F43989DD 97F0FA97 EBCE2F4A
    Text-In       DC7E84BF DA79164B 7ECD8486 985D3860
    Text-Out      6BC1BEE2 2E409F96 E93D7E11 7393172A
  Block #2
    InputBlock    B7BF3A5D F43989DD 97F0FA97 EBCE2F4A
    OutputBlock   E1C65630 5ED1A7A6 56380574 6FE03EDC
    Text-In       4FEBDC67 40D20B3A C88F6AD8 2A4FB08D
    Text-Out      AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
  Block #3
    InputBlock    E1C65630 5ED1A7A6 56380574 6FE03EDC
    OutputBlock   41635BE6 25B48AFC 1666DD42 A09D96E7
    Text-In       71AB47A0 86E86EED F39D1C5B BA97C408
    Text-Out      30C81C46 A35CE411 E5FBC119 1A0A52EF
  Block #4
    InputBlock    41635BE6 25B48AFC 1666DD42 A09D96E7
    OutputBlock   F7B93058 B8BCE0FF FEA41BF0 012CD394
    Text-In       0126141D 67F37BE8 538F5A8B E740E484
    Text-Out      F69F2445 DF4F9B17 AD2B417B E66C3710

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

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

  Block Cipher Modes of Operation

      Counter (CTR)

Initial Counter is
    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFEFF

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

CTR-AES128 (Encryption)
----------------------------------------------------------------

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

  Block #1
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFEFF
    OutputBlock   EC8CDF73 98607CB0 F2D21675 EA9EA1E4
    Text-In       6BC1BEE2 2E409F96 E93D7E11 7393172A
    Text-Out      874D6191 B620E326 1BEF6864 990DB6CE
  Block #2
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF00
    OutputBlock   362B7C3C 67735163 18A077D7 FC5073AE
    Text-In       AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    Text-Out      9806F66B 7970FDFF 8617187B B9FFFDFF
  Block #3
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF01
    OutputBlock   6A2CC378 7889374F BEB4C81B 17BA6C44
    Text-In       30C81C46 A35CE411 E5FBC119 1A0A52EF
    Text-Out      5AE4DF3E DBD5D35E 5B4F0902 0DB03EAB
  Block #4
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF02
```

```
    OutputBlock   E89C399F F0F198C6 D40A31DB 156CABFE
    Text-In       F69F2445 DF4F9B17 AD2B417B E66C3710
    Text-Out      1E031DDA 2FBE03D1 792170A0 F3009CEE

Ciphertext is
    874D6191 B620E326 1BEF6864 990DB6CE
    9806F66B 7970FDFF 8617187B B9FFFDFF
    5AE4DF3E DBD5D35E 5B4F0902 0DB03EAB
    1E031DDA 2FBE03D1 792170A0 F3009CEE

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

CTR-AES128 (Decryption)
----------------------------------------------------------------

Key is
    2B7E1516 28AED2A6 ABF71588 09CF4F3C

Ciphertext is
    874D6191 B620E326 1BEF6864 990DB6CE
    9806F66B 7970FDFF 8617187B B9FFFDFF
    5AE4DF3E DBD5D35E 5B4F0902 0DB03EAB
    1E031DDA 2FBE03D1 792170A0 F3009CEE

  Block #1
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFEFF
    OutputBlock   EC8CDF73 98607CB0 F2D21675 EA9EA1E4
    Text-In       874D6191 B620E326 1BEF6864 990DB6CE
    Text-Out      6BC1BEE2 2E409F96 E93D7E11 7393172A
  Block #2
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF00
    OutputBlock   362B7C3C 67735163 18A077D7 FC5073AE
    Text-In       9806F66B 7970FDFF 8617187B B9FFFDFF
    Text-Out      AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
  Block #3
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF01
    OutputBlock   6A2CC378 7889374F BEB4C81B 17BA6C44
    Text-In       5AE4DF3E DBD5D35E 5B4F0902 0DB03EAB
    Text-Out      30C81C46 A35CE411 E5FBC119 1A0A52EF
  Block #4
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF02
    OutputBlock   E89C399F F0F198C6 D40A31DB 156CABFE
    Text-In       1E031DDA 2FBE03D1 792170A0 F3009CEE
    Text-Out      F69F2445 DF4F9B17 AD2B417B E66C3710

Plaintext is
```

```
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

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

CTR-AES192 (Encryption)
--------------------------------------------------------------

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

  Block #1
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFEFF
    OutputBlock   717D2DC6 39128334 A6167A48 8DED7921
    Text-In       6BC1BEE2 2E409F96 E93D7E11 7393172A
    Text-Out      1ABC9324 17521CA2 4F2B0459 FE7E6E0B
  Block #2
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF00
    OutputBlock   A72EB3BB 14A55673 4B7BAD6A B16100C5
    Text-In       AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    Text-Out      090339EC 0AA6FAEF D5CCC2C6 F4CE8E94
  Block #3
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF01
    OutputBlock   2EFEAE2D 72B72261 3446DC7F 4C2AF918
    Text-In       30C81C46 A35CE411 E5FBC119 1A0A52EF
    Text-Out      1E36B26B D1EBC670 D1BD1D66 5620ABF7
  Block #4
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF02
    OutputBlock   B9E783B3 0DD7924F F7BC9B97 BEAA8740
    Text-In       F69F2445 DF4F9B17 AD2B417B E66C3710
    Text-Out      4F78A7F6 D2980958 5A97DAEC 58C6B050

Ciphertext is
    1ABC9324 17521CA2 4F2B0459 FE7E6E0B
    090339EC 0AA6FAEF D5CCC2C6 F4CE8E94
```

```
    1E36B26B D1EBC670 D1BD1D66 5620ABF7
    4F78A7F6 D2980958 5A97DAEC 58C6B050

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

CTR-AES192 (Decryption)
------------------------------------------------------------

Key is
    8E73B0F7 DA0E6452 C810F32B 809079E5
    62F8EAD2 522C6B7B

Ciphertext is
    1ABC9324 17521CA2 4F2B0459 FE7E6E0B
    090339EC 0AA6FAEF D5CCC2C6 F4CE8E94
    1E36B26B D1EBC670 D1BD1D66 5620ABF7
    4F78A7F6 D2980958 5A97DAEC 58C6B050

  Block #1
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFEFF
    OutputBlock   717D2DC6 39128334 A6167A48 8DED7921
    Text-In       1ABC9324 17521CA2 4F2B0459 FE7E6E0B
    Text-Out      6BC1BEE2 2E409F96 E93D7E11 7393172A
  Block #2
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF00
    OutputBlock   A72EB3BB 14A55673 4B7BAD6A B16100C5
    Text-In       090339EC 0AA6FAEF D5CCC2C6 F4CE8E94
    Text-Out      AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
  Block #3
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF01
    OutputBlock   2EFEAE2D 72B72261 3446DC7F 4C2AF918
    Text-In       1E36B26B D1EBC670 D1BD1D66 5620ABF7
    Text-Out      30C81C46 A35CE411 E5FBC119 1A0A52EF
  Block #4
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF02
    OutputBlock   B9E783B3 0DD7924F F7BC9B97 BEAA8740
    Text-In       4F78A7F6 D2980958 5A97DAEC 58C6B050
    Text-Out      F69F2445 DF4F9B17 AD2B417B E66C3710

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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

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

CTR-AES256 (Encryption)
----------------------------------------------------------

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

  Block #1
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFEFF
    OutputBlock   0BDF7DF1 59171633 5E9A8B15 C860C502
    Text-In       6BC1BEE2 2E409F96 E93D7E11 7393172A
    Text-Out      601EC313 775789A5 B7A7F504 BBF3D228
  Block #2
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF00
    OutputBlock   5A6E699D 53611906 5433863C 8F657B94
    Text-In       AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    Text-Out      F443E3CA 4D62B59A CA84E990 CACAF5C5
  Block #3
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF01
    OutputBlock   1BC12C9C 01610D5D 0D8BD6A3 378ECA62
    Text-In       30C81C46 A35CE411 E5FBC119 1A0A52EF
    Text-Out      2B0930DA A23DE94C E87017BA 2D84988D
  Block #4
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF02
    OutputBlock   2956E1C8 693536B1 BEE99C73 A31576B6
    Text-In       F69F2445 DF4F9B17 AD2B417B E66C3710
    Text-Out      DFC9C58D B67AADA6 13C2DD08 457941A6

Ciphertext is
    601EC313 775789A5 B7A7F504 BBF3D228
    F443E3CA 4D62B59A CA84E990 CACAF5C5
    2B0930DA A23DE94C E87017BA 2D84988D
    DFC9C58D B67AADA6 13C2DD08 457941A6

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

CTR-AES256 (Decryption)
```

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

Key is
    603DEB10 15CA71BE 2B73AEF0 857D7781
    1F352C07 3B6108D7 2D9810A3 0914DFF4

Ciphertext is
    601EC313 775789A5 B7A7F504 BBF3D228
    F443E3CA 4D62B59A CA84E990 CACAF5C5
    2B0930DA A23DE94C E87017BA 2D84988D
    DFC9C58D B67AADA6 13C2DD08 457941A6

  Block #1
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFEFF
    OutputBlock   0BDF7DF1 59171633 5E9A8B15 C860C502
    Text-In       601EC313 775789A5 B7A7F504 BBF3D228
    Text-Out      6BC1BEE2 2E409F96 E93D7E11 7393172A
  Block #2
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF00
    OutputBlock   5A6E699D 53611906 5433863C 8F657B94
    Text-In       F443E3CA 4D62B59A CA84E990 CACAF5C5
    Text-Out      AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
  Block #3
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF01
    OutputBlock   1BC12C9C 01610D5D 0D8BD6A3 378ECA62
    Text-In       2B0930DA A23DE94C E87017BA 2D84988D
    Text-Out      30C81C46 A35CE411 E5FBC119 1A0A52EF
  Block #4
    InputBlock    F0F1F2F3 F4F5F6F7 F8F9FAFB FCFDFF02
    OutputBlock   2956E1C8 693536B1 BEE99C73 A31576B6
    Text-In       DFC9C58D B67AADA6 13C2DD08 457941A6
    Text-Out      F69F2445 DF4F9B17 AD2B417B E66C3710

Plaintext is
    6BC1BEE2 2E409F96 E93D7E11 7393172A
    AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51
    30C81C46 A35CE411 E5FBC119 1A0A52EF
    F69F2445 DF4F9B17 AD2B417B E66C3710

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