

#####

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
