```
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 F69F2445 DF4F9B17 AD2B417B E66C3710 Plaintext InputBlock F69F2445 DF4F9B17 AD2B417B E66C3710 OutputBlock 7B0C785E 27E8AD3F 82232071 04725DD4 Ciphertext 48033300 C2FE1200 3F9B917C D8C0977C

Ciphertext is

3AD77BB4 ØD7A366Ø A89ECAF3 2466EF97 F5D3D585 Ø3B9699D E785895A 96FDBAAF 43B1CD7F 598ECE23 881BØØE3 EDØ3Ø688 7BØC785E 27E8AD3F 82232Ø71 Ø4725DD4

ECB-AES128 (Decryption)

Key is

2B7E1516 28AED2A6 ABF71588 09CF4F3C

Ciphertext is

3AD77BB4 ØD7A366Ø A89ECAF3 2466EF97 F5D3D585 Ø3B9699D E785895A 96FDBAAF 43B1CD7F 598ECE23 881BØØE3 EDØ3Ø688 7BØC785E 27E8AD3F 82232Ø71 Ø4725DD4

Block #1

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

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 6BC1BEE2 2E409F96 E93D7E11 7393172A Plaintext 6BC1BEE2 2E409F96 E93D7E11 7393172A InputBlock OutputBlock BD334F1D 6E45F25F F712A214 571FA5CC 3AD77BB4 0D7A3660 A89ECAF3 2466EF97 Ciphertext Block #2 Plaintext AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51 InputBlock AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51 97410484 6D0AD3AD 7734ECB3 ECEE4EEF OutputBlock Ciphertext F5D3D585 03B9699D E785895A 96FDBAAF Block #3 Plaintext 30C81C46 A35CE411 E5FBC119 1A0A52EF 30C81C46 A35CE411 E5FBC119 1A0A52EF InputBlock EF7AFD22 70E2E60A DCE0BA2F ACE6444E OutputBlock 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

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 F3EED1BD B5D2A03C 064B5A7E 3DB181F8 OutputBlock BD334F1D 6E45F25F F712A214 571FA5CC Ciphertext Block #2 AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51 Plaintext AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51 InputBlock 591CCB10 D410ED26 DC5BA74A 31362870 OutputBlock 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

Ciphertext is

OutputBlock

Ciphertext

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

23304B7A 39F9F3FF 067D8D8F 9E24ECC7

9A4B41BA 738D6C72 FB166916 03C18E0E

ECB-AES256 (Decryption)

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

Cimbon on and	ESEED4DD	DEDOMAGO	OCADEA7E	20040450
Ciphertext	F3EED1BD	R2DZA03C	064B5A7E	2DRT8TL8
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
