

#####

## 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

KeyAddition 40BFABF4 06EE4D30 42CA6B99 7A5C5816

Round = 1

Substitution 090862BF 6F28E304 2C747FEE DA4A6A47  
ShiftRow 09287F47 6F746ABF 2C4A6204 DA08E3EE  
MixColumn 529F16C2 978615CA E01AAE54 BA1A2659  
KeyAddition F265E8D5 1FD2397B C3B9976D 9076505C

Round = 2

Substitution 894D9B03 C0B51221 2E56883C 6038534A  
ShiftRow 89B5884A C0565303 2E389B21 604D123C  
MixColumn 0F31E929 319A3558 AEC95893 39F04D87  
KeyAddition FDF37CDB 4B0C8C1B F7FCD8E9 4AA9BBF8

Round = 3

Substitution 540D10B9 B3FE64AF 68B0611E D6D3EA41  
ShiftRow 54FE6141 B3B0EAB9 68D310AF D60D641E  
MixColumn 9151ABE1 E5541CFD 014A713E DA7E3134  
KeyAddition ACD1EC9C A242E2C3 1F690F7A B704B90F

Round = 4

Substitution	913ECEDE	3A2C982E	C0F976DA	A9F25676
ShiftRow	912C7676	3AF956DE	C0F2CE2E	A93E98DA
MixColumn	4D25CB1E	ECF71646	7658C73B	49BCC9E9
KeyAddition	A2616E5F	44A54D39	C029E200	92B764E9

Round = 5

Substitution	3AEF9FCF	1B06E312	BAA59863	4FA9431E
ShiftRow	3A06981E	1BA543CF	BAA99F12	4FEFE363
MixColumn	F89B35EC	4E40724E	025B00C7	34D7D81B
KeyAddition	2C4AF314	32C3EFC9	C8A9B87B	252ECDA7

Round = 6

Substitution	71D60DFA	232EDFDD	E8D36C21	3F31BD5C
ShiftRow	712E6C5C	23D3BDFA	E8310DDD	3FD6DF21
MixColumn	A0C56369	6FB884E4	4840BFBE	E1D32F0A
KeyAddition	CD4DC013	7EB3BA19	93B939FF	2BD3BCF7

Round = 7

Substitution	BDE3BA7D	F36DF4D4	DC561216	F1666568
ShiftRow	BD6D1268	F356657D	DC66BAD4	F1E3F416
MixColumn	AC394C73	1F8DE8C7	6711B210	253DDB33
KeyAddition	E26DBB7D	40D22134	E3B7FDA2	6B9B077C

Round = 8

Substitution	983CEAFF	09B5FD18	11A9543A	7F14C510
ShiftRow	98B55410	09A9C5FF	1114EA18	7F3CFD3A
MixColumn	AB05B572	C8EB2B92	EC04E2FD	7D21EC34
KeyAddition	41D7C653	7D669140	DD2F179D	02ACC51B

Round = 9

Substitution	830EB4ED	FF338109	C115F05E	7791A6AF
ShiftRow	8333F0AF	FF15A6ED	C191B409	770E815E
MixColumn	1741A118	91C99168	8C36386F	23AD82AA
KeyAddition	BB36C7EB	88334D49	A4E7112E	74F182C4

Substitution	EA05C6E9	C4C3E33B	49948231	92A1131C
ShiftRow	EAC3821C	C49413E9	49A1C63B	9205E331
KeyAddition	3AD77BB4	0D7A3660	A89ECAF3	2466EF97

KeyAddition 85539F41 36AD7E3A 35407A24 4C60C16D

Round = 1

Substitution	97EDDB83	0595F380	9609DA36	29D0783C
ShiftRow	9795DA3C	05097883	96D0DB80	29EDF336
MixColumn	77EFE995	EA1C6263	07DB70B1	BBD06309

KeyAddition D7151782 62484ED2 24784988 91BC150C

Round = 2

Substitution 0E59F013 AA522FB5 36BC3BC4 816559FE  
ShiftRow 0E523BFE AABC5913 3665F0B5 81592FC4  
MixColumn 2F19339C DA319126 86426CBE 1986D17D  
KeyAddition DDDBA66E A0A72865 DF77ECC4 6ADF2702

Round = 3

Substitution C1B9249F E05C344D 9EF5CE1C 029ECC77  
ShiftRow C15CCE77 E0F5CC9F 9E9E244D 02B9341C  
MixColumn C4478324 8CC12C27 F7989F99 FC2BF7B3  
KeyAddition F9C7C459 CBD7D219 E9BBE1DD 91517F88

Round = 4

Substitution 99C61CCB 1F0EB5D4 1EEAF8C1 81D1D2C4  
ShiftRow 990EF8C4 1FEAD2CB 1ED11CD4 81C6B5C1  
MixColumn 07522BD5 02760C94 9C57905C 3C136E72  
KeyAddition E8168E94 AA2457EB 2A26B567 E718C372

Round = 5

Substitution 9B471922 AC365BE9 E5F7D585 94AD2E40  
ShiftRow 9B36D540 ACF72E22 E5AD19E9 94475B85  
MixColumn E2D3DCD5 4D096172 CD665A49 2472F1AA  
KeyAddition 36021A2D 318AFCF5 0794E2F5 358BE416

Round = 6

Substitution 0577A2D8 C77EB0E6 C52298E6 963D6947  
ShiftRow 057E9847 C72269D8 C53DA2E6 9677B0E6  
MixColumn 570D9967 42E044B2 92A4961C F855ABB1  
KeyAddition 3A853A1D 53EB7A4F 495D105D 3255384C

Round = 7

Substitution 809780A4 EDE9DA84 3B4CCA4C 23FC0729  
ShiftRow 80E9CA29 ED4C07A4 3BFC8084 2397DA4C  
MixColumn D8259DEA B6D85834 6DC74B22 722FCFB0  
KeyAddition 96716AE4 E98791C7 E9610490 3C8913FF

Round = 8

Substitution 90A30269 1E1781C6 1EEFF260 EBA77D16  
ShiftRow 9017F216 1EEF7D69 1EA702C6 EBA38160  
MixColumn E6A54262 0235B062 0A8BEC10 D24EF1C4  
KeyAddition 0C773143 B7B80AB0 3BA01970 ADC3D8EB

Round = 9

Substitution FEF5C71A A96C67E7 E2E0D451 952E61E9

ShiftRow FE6CD4E9 A9E0611A E22EC7E7 95F56751  
MixColumn 6EA80168 09CBA555 8D0B6B01 039C5D94  
KeyAddition C2DF679B 10317974 A5DA4240 54C05DFA

Substitution 259E8514 CAC7B692 06572C09 20BA4C2D  
ShiftRow 25C72C2D CA574C14 06BA8592 209EB609  
KeyAddition F5D3D585 03B9699D E785895A 96FDBAAF

KeyAddition 1BB60950 8BF236B7 4E0CD491 13C51DD3

Round = 1

Substitution AF4E0153 3D8905A9 2FFE4881 7DA6A466  
ShiftRow AF894866 3DFEA453 2FA601A9 7D4E0581  
MixColumn EB181CE7 947E65BB 07D26B9F AC6FA1D5  
KeyAddition 4BE2E2F0 1C2A490A 247152A6 8603D7D0

Round = 2

Substitution B398988C 9CE53B67 36A30024 447B0E70  
ShiftRow B3E50070 9CA30E8C 367B9867 44983B24  
MixColumn 3912C6CB 5F5FAC11 1E14CF77 2406C627  
KeyAddition CBD05339 25C91552 47214F0D 575F3058

Round = 3

Substitution 1F70ED12 3FDD5900 A0FD84D7 5BCF046A  
ShiftRow 1FDD846A 3FFD0412 A0CFED00 5B7059D7  
MixColumn AC436FAC 74C0FC9C FC09AED9 A887FB71  
KeyAddition 91C328D1 33D602A2 E22AD09D C5FD734A

Round = 4

Substitution 812E343E C3F6773A 98E5705E A6548FD6  
ShiftRow 81F670D6 C3E58F3E 9854343A A62E775E  
MixColumn BE30F6A9 18A66148 D956EAA7 0C3D8414  
KeyAddition 517453E8 B0F43A37 6F27CF9C D7362914

Round = 5

Substitution D192ED9B E7BF809A A8CC8ADE 0E05A5FA  
ShiftRow D1BF8AFA E7CCA59B A805ED9A 0E9280DE  
MixColumn 13CB74B2 A40BCC76 3314D924 EF74FEA7  
KeyAddition C71AB24A D88851F1 F9E66198 FE8DEB1B

Round = 6

Substitution C6A237D6 61C4D1A1 998EEF46 BB5DE9AF  
ShiftRow C6C4EFAF 618EE9D6 995D37A1 BBA2D146  
MixColumn 80D02D3F 74904773 58DB5283 07CA6A29  
KeyAddition ED588E45 659B798E 8322D4C2 CDCAF9D4

Round = 7

Substitution	556A196E	4D14B619	EC934825	BD749948
ShiftRow	55144848	4D93996E	EC741919	BD6AB625
MixColumn	96ED0933	C3AE4501	5F368170	4C8DCF4A
KeyAddition	D8B9FE3D	9CF18CF2	DB90CEC2	022B1305

Round = 8

Substitution	6156BB27	DEA16489	B9608B25	77F17D6B
ShiftRow	61A18B6B	DE607D27	B9F1BB89	77566425
MixColumn	DAD5705F	5DBE2D2A	531FA593	555286E1
KeyAddition	3007037E	E83397F8	623450F3	2ADFAFCE

Round = 9

Substitution	04C57BF3	9BC38841	AA18530D	E59E798B
ShiftRow	04C3538B	9B1879F3	AA9E7B41	E5C5880D
MixColumn	8EE7E791	8FD37F2A	CC410182	00FA3C63
KeyAddition	22908162	9629A30B	E49028C3	57A63C0D

Substitution	93600CAA	90A50A2B	6960342E	5B24EBD7
ShiftRow	93A534D7	9060EBAA	69240C2B	5B600A2E
KeyAddition	43B1CD7F	598ECE23	881B00E3	ED030688

KeyAddition	DDE13153	F7E149B1	06DC54F3	EFA3782C
-------------	----------	----------	----------	----------

Round = 1

Substitution	C1F8C7ED	68F83BC8	6F86200D	DF0ABC71
ShiftRow	C1F82071	6886BCED	6F0AC7C8	DFF83B0D
MixColumn	DB3BEA62	104DA143	CFE1B3F7	807446A3
KeyAddition	7BC11475	98198DF2	EC428ACE	AA1830A6

Round = 2

Substitution	2178FA9D	46D45D89	CE2C7E8B	ACAD0424
ShiftRow	21D47E24	462C049D	CEADFA89	AC785D8B
MixColumn	7F346581	618FDEC3	18130C17	1D30E8C7
KeyAddition	8DF6F073	1B196780	41268C6D	6E691EB8

Round = 3

Substitution	5D428C8F	AFD485CD	83F7643C	9FF9726C
ShiftRow	5DD4646C	AFF7728F	83F98CCD	9F42853C
MixColumn	D52EF58F	BA43366A	4C28356A	5AB38805
KeyAddition	E8AEB2F2	FD55C854	520B4B2E	37C9003E

Round = 4

Substitution	9BE43789	54FCE820	002BB331	9ADD63B2
ShiftRow	9BFCB3B2	542B6389	00DD3720	9AE4E831
MixColumn	3304D786	3F2E39BD	6BD8D3AA	C15BE6DB

KeyAddition DC4072C7 977C62C2 DDA9F691 1A504BDB

Round = 5

Substitution 860940C6 8810AA25 C1D34281 A253B3B9  
ShiftRow 861042B9 88D3B3C6 C1534025 A209AA81  
MixColumn DCD9C2AA 103D7774 09827D01 6FD47C47  
KeyAddition 08080452 6CBEEAF3 C370C5BD 7E2D69FB

Round = 6

Substitution 3030F200 50AE870D 2E51A67A F3D8F90F  
ShiftRow 30AEA60F 5051F900 2ED8F20D F330877A  
MixColumn 2089D846 AAE2E858 D0851E42 507B584D  
KeyAddition 4D017B3C BBE9D6A5 0B7C9803 9A7BCBB0

Round = 7

Substitution E37C21EB EA1EF606 2B10467B B8211FE7  
ShiftRow E31E46E7 EA101FEB 2B212106 B87CF67B  
MixColumn 5EF243B3 0B00E2E7 120C4271 623ABEAF  
KeyAddition 10A6B4BD 545F2B14 96AA0DC3 2C9C62E0

Round = 8

Substitution CA248D7A 20CFF1FA 90ACD72E 71DEAAE1  
ShiftRow CACFD7E1 20ACAA7A 90DE8DFA 7124F12E  
MixColumn F3CC8884 7FFC4D92 35415A17 511FDE1A  
KeyAddition 191EFBA5 CA71F740 046AAF77 2E92F735

Round = 9

Substitution D4720F06 74A36809 F20279F5 314F6896  
ShiftRow D4A37996 74026806 F24F0F09 317268F5  
MixColumn A294248A 80CEACFA 2874B85F 699897B8  
KeyAddition 0EE34279 993470DB 00A5911E 3EC497D6

Substitution AB112CB6 EE1851B9 63068172 B21C88F6  
ShiftRow AB1881F6 EE0688B6 631C2CB9 B2115172  
KeyAddition 7B0C785E 27E8AD3F 82232071 04725DD4

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

KeyAddition EAC3821C C49413E9 49A1C63B 9205E331

Substitution BB3311C4 88E782EB A4F1C749 74364D2E

ShiftRow BB36C7EB 88334D49 A4E7112E 74F182C4

Round = 9

KeyAddition 1741A118 91C99168 8C36386F 23AD82AA

InvMixColumn 8333F0AF FF15A6ED C191B409 770E815E

Substitution 4166171B 7D2FC553 DDACC640 02D7919D

ShiftRow 41D7C653 7D669140 DD2F179D 02ACC51B

Round = 8

KeyAddition AB05B572 C8EB2B92 EC04E2FD 7D21EC34

InvMixColumn 98B55410 09A9C5FF 1114EA18 7F3CFD3A

Substitution E2D2FD7C 40B7077D E39BBB34 6B6D21A2

ShiftRow E26DBB7D 40D22134 E3B7FDA2 6B9B077C

Round = 7

KeyAddition AC394C73 1F8DE8C7 6711B210 253DDB33

InvMixColumn BD6D1268 F356657D DC66BAD4 F1E3F416

Substitution CDB339F7 7EB9BC13 93D3C019 2B4DBAFF

ShiftRow CD4DC013 7EB3BA19 93B939FF 2BD3BCF7

Round = 6

KeyAddition A0C56369 6FB884E4 4840BFBE E1D32F0A

InvMixColumn 712E6C5C 23D3BDFA E8310DDD 3FD6DF21

Substitution 2CC3B8A7 32A9CD14 C82EF3C9 254AEF7B

ShiftRow 2C4AF314 32C3EFC9 C8A9B87B 252ECDA7

Round = 5

KeyAddition F89B35EC 4E40724E 025B00C7 34D7D81B

InvMixColumn 3A06981E 1BA543CF BAA99F12 4FEFE363

Substitution A2A5E2E9 4429645F C0B76E39 92614D00

ShiftRow A2616E5F 44A54D39 C029E200 92B764E9

Round = 4

KeyAddition 4D25CB1E ECF71646 7658C73B 49BCC9E9

InvMixColumn 912C7676 3AF956DE C0F2CE2E A93E98DA

Substitution AC420F0F A269B99C 1F04ECC3 B7D1E27A

ShiftRow ACD1EC9C A242E2C3 1F690F7A B704B90F

Round = 3

KeyAddition 9151ABE1 E5541CFD 014A713E DA7E3134

InvMixColumn	54FE6141	B3B0EAB9	68D310AF	D60D641E
Substitution	FD0CD8F8	4BFCBBDB	F7A97C1B	4AF38CE9
ShiftRow	FDF37CDB	4B0C8C1B	F7FCD8E9	4AA9BBF8
Round = 2				
KeyAddition	0F31E929	319A3558	AEC95893	39F04D87
InvMixColumn	89B5884A	C0565303	2E389B21	604D123C
Substitution	F2D2975C	1FB950D5	C376E87B	9065396D
ShiftRow	F265E8D5	1FD2397B	C3B9976D	9076505C
Round = 1				
KeyAddition	529F16C2	978615CA	E01AAE54	BA1A2659
InvMixColumn	09287F47	6F746ABF	2C4A6204	DA08E3EE
Substitution	40EE6B16	06CA58F4	425CAB30	7ABF4D99
ShiftRow	40BFABF4	06EE4D30	42CA6B99	7A5C5816
KeyAddition	6BC1BEE2	2E409F96	E93D7E11	7393172A
KeyAddition	25C72C2D	CA574C14	06BA8592	209EB609
Substitution	C23142FA	10DA5D9B	A5C06774	54DF7940
ShiftRow	C2DF679B	10317974	A5DA4240	54C05DFA
Round = 9				
KeyAddition	6EA80168	09CBA555	8D0B6B01	039C5D94
InvMixColumn	FE6CD4E9	A9E0611A	E22EC7E7	95F56751
Substitution	0CB819EB	B7A0D843	3BC331B0	AD770A70
ShiftRow	0C773143	B7B80AB0	3BA01970	ADC3D8EB
Round = 8				
KeyAddition	E6A54262	0235B062	0A8BEC10	D24EF1C4
InvMixColumn	9017F216	1EEF7D69	1EA702C6	EBA38160
Substitution	968704FF	E96113E4	E9896AC7	3C719190
ShiftRow	96716AE4	E98791C7	E9610490	3C8913FF
Round = 7				
KeyAddition	D8259DEA	B6D85834	6DC74B22	722FCFB0
InvMixColumn	80E9CA29	ED4C07A4	3BFC8084	2397DA4C
Substitution	3AEB104C	535D381D	49553A4F	32857A5D
ShiftRow	3A853A1D	53EB7A4F	495D105D	3255384C
Round = 6				
KeyAddition	570D9967	42E044B2	92A4961C	F855ABB1
InvMixColumn	057E9847	C72269D8	C53DA2E6	9677B0E6
Substitution	368AE216	3194E42D	078B1AF5	3502FCF5
ShiftRow	36021A2D	318AFCF5	0794E2F5	358BE416
Round = 5				
KeyAddition	E2D3DCD5	4D096172	CD665A49	2472F1AA
InvMixColumn	9B36D540	ACF72E22	E5AD19E9	94475B85
Substitution	E824B572	AA26C394	2A188EEB	E7165767
ShiftRow	E8168E94	AA2457EB	2A26B567	E718C372
Round = 4				
KeyAddition	07522BD5	02760C94	9C57905C	3C136E72
InvMixColumn	990EF8C4	1FEAD2CB	1ED11CD4	81C6B5C1



Substitution	F9D7E188	CBBB7F59	E951C419	91C7D2DD
ShiftRow	F9C7C459	CBD7D219	E9BBE1DD	91517F88
Round = 3				
KeyAddition	C4478324	8CC12C27	F7989F99	FC2BF7B3
InvMixColumn	C15CCE77	E0F5CC9F	9E9E244D	02B9341C
Substitution	DDA7EC02	A077276E	DFDFA665	6ADB28C4
ShiftRow	DDDBA66E	A0A72865	DF77ECC4	6ADF2702
Round = 2				
KeyAddition	2F19339C	DA319126	86426CBE	1986D17D
InvMixColumn	0E523BFE	AABC5913	3665F0B5	81592FC4
Substitution	D748490C	62781582	24BC17D2	91154E88
ShiftRow	D7151782	62484ED2	24784988	91BC150C
Round = 1				
KeyAddition	77EFE995	EA1C6263	07DB70B1	BBD06309
InvMixColumn	9795DA3C	05097883	96D0DB80	29EDF336
Substitution	85AD7A6D	3640C141	35609F3A	4C537E24
ShiftRow	85539F41	36AD7E3A	35407A24	4C60C16D
KeyAddition	AE2D8A57	1E03AC9C	9EB76FAC	45AF8E51
KeyAddition	93A534D7	9060EBAA	69240C2B	5B600A2E
Substitution	2229280D	96903C62	E4A6810B	5790A3C3
ShiftRow	22908162	9629A30B	E49028C3	57A63C0D
Round = 9				
KeyAddition	8EE7E791	8FD37F2A	CC410182	00FA3C63
InvMixColumn	04C3538B	9B1879F3	AA9E7B41	E5C5880D
Substitution	303350CE	E834AF7E	62DF03F8	2A0797F3
ShiftRow	3007037E	E83397F8	623450F3	2ADFAFCE
Round = 8				
KeyAddition	DAD5705F	5DBE2D2A	531FA593	555286E1
InvMixColumn	61A18B6B	DE607D27	B9F1BB89	77566425
Substitution	D8F1CE05	9C90133D	DB2BFEF2	02B98CC2
ShiftRow	D8B9FE3D	9CF18CF2	DB90CEC2	022B1305
Round = 7				
KeyAddition	96ED0933	C3AE4501	5F368170	4C8DCF4A
InvMixColumn	55144848	4D93996E	EC741919	BD6AB625
Substitution	ED9BD4D4	6522F945	83CA8E8E	CD5879C2
ShiftRow	ED588E45	659B798E	8322D4C2	CDCAF9D4
Round = 6				
KeyAddition	80D02D3F	74904773	58DB5283	07CA6A29
InvMixColumn	C6C4EFAF	618EE9D6	995D37A1	BBA2D146
Substitution	C788611B	D8E6EB4A	F98DB2F1	FE1A5198
ShiftRow	C71AB24A	D88851F1	F9E66198	FE8DEB1B
Round = 5				
KeyAddition	13CB74B2	A40BCC76	3314D924	EF74FEA7
InvMixColumn	D1BF8AFA	E7CCA59B	A805ED9A	0E9280DE
Substitution	51F4CF14	B02729E8	6F365337	D7743A9C

ShiftRow 517453E8 B0F43A37 6F27CF9C D7362914

Round = 4

KeyAddition BE30F6A9 18A66148 D956EAA7 0C3D8414

InvMixColumn 81F670D6 C3E58F3E 9854343A A62E775E

Substitution 91D6D04A 332A73D1 E2FD28A2 C5C3029D

ShiftRow 91C328D1 33D602A2 E22AD09D C5FD734A

Round = 3

KeyAddition AC436FAC 74C0FC9C FC09AED9 A887FB71

InvMixColumn 1FDD846A 3FFD0412 A0CFED00 5B7059D7

Substitution CBC94F58 25213039 475F5352 57D0150D

ShiftRow CBD05339 25C91552 47214F0D 575F3058

Round = 2

KeyAddition 3912C6CB 5F5FAC11 1E14CF77 2406C627

InvMixColumn B3E50070 9CA30E8C 367B9867 44983B24

Substitution 4B2A52D0 1C71D7F0 2403E20A 86E249A6

ShiftRow 4BE2E2F0 1C2A490A 247152A6 8603D7D0

Round = 1

KeyAddition EB181CE7 947E65BB 07D26B9F AC6FA1D5

InvMixColumn AF894866 3DFEA453 2FA601A9 7D4E0581

Substitution 1BF2D4D3 8B0C1D50 4EC509B7 13B63691

ShiftRow 1BB60950 8BF236B7 4E0CD491 13C51DD3

KeyAddition 30C81C46 A35CE411 E5FBC119 1A0A52EF

KeyAddition AB1881F6 EE0688B6 631C2CB9 B2115172

Substitution 0E3491D6 99A59779 00C442DB 3EE3701E

ShiftRow 0EE34279 993470DB 00A5911E 3EC497D6

Round = 9

KeyAddition A294248A 80CEACFA 2874B85F 699897B8

InvMixColumn D4A37996 74026806 F24F0F09 317268F5

Substitution 1971AF35 CA6AF7A5 0492FB40 2E1EF777

ShiftRow 191EFBA5 CA71F740 046AAF77 2E92F735

Round = 8

KeyAddition F3CC8884 7FFC4D92 35415A17 511FDE1A

InvMixColumn CACFD7E1 20ACAA7A 90DE8DFA 7124F12E

Substitution 105F0DE0 54AA62BD 969CB414 2CA62BC3

ShiftRow 10A6B4BD 545F2B14 96AA0DC3 2C9C62E0

Round = 7

KeyAddition 5EF243B3 0B00E2E7 120C4271 623ABEAF

InvMixColumn E31E46E7 EA101FEB 2B212106 B87CF67B

Substitution 4DE998B0 BB7CCB3C 0B7B7BA5 9A01D603

ShiftRow 4D017B3C BBE9D6A5 0B7C9803 9A7BCBB0

Round = 6

KeyAddition 2089D846 AAE2E858 D0851E42 507B584D

InvMixColumn 30AEA60F 5051F900 2ED8F20D F330877A

Substitution 08BEC5FB 6C706952 C32D04F3 7E08EABD

ShiftRow 08080452 6CBEEAF3 C370C5BD 7E2D69FB

```

Round = 5
  KeyAddition   DCD9C2AA 103D7774 09827D01 6FD47C47
  InvMixColumn  861042B9 88D3B3C6 C1534025 A209AA81
  Substitution  DC7CF6DB 97A94BC7 DD5072C2 1A406291
  ShiftRow     DC4072C7 977C62C2 DDA9F691 1A504BDB
Round = 4
  KeyAddition   3304D786 3F2E39BD 6BD8D3AA C15BE6DB
  InvMixColumn  9BFCB3B2 542B6389 00DD3720 9AE4E831
  Substitution  E8554B3E FD0B00F2 52C9B254 37AEC82E
  ShiftRow     E8AEB2F2 FD55C854 520B4B2E 37C9003E
Round = 3
  KeyAddition   D52EF58F BA43366A 4C28356A 5AB38805
  InvMixColumn  5DD4646C AFF7728F 83F98CCD 9F42853C
  Substitution  8D198CB8 1B261E73 4169F080 6EF6676D
  ShiftRow     8DF6F073 1B196780 41268C6D 6E691EB8
Round = 2
  KeyAddition   7F346581 618FDEC3 18130C17 1D30E8C7
  InvMixColumn  21D47E24 462C049D CEADFA89 AC785D8B
  Substitution  7B198AA6 98423075 EC1814F2 AAC18DCE
  ShiftRow     7BC11475 98198DF2 EC428ACE AA1830A6
Round = 1
  KeyAddition   DB3BEA62 104DA143 CFE1B3F7 807446A3
  InvMixColumn  C1F82071 6886BCED 6F0AC7C8 DFF83B0D
  Substitution  DDE1542C F7DC7853 06A331B1 EFE149F3
  ShiftRow     DDE13153 F7E149B1 06DC54F3 EFA3782C
KeyAddition    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

### Electronic Codebook (ECB)

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

KeyAddition E5B20E15 F44EFBC4 212D8D3A F3036ECF

Round = 1

Substitution	D937AB59	BF2F0F1C	FDD85D80	0D7B9F8A
ShiftRow	D92F5D8A	bfd89f59	FD7BAB1C	0D370F80
MixColumn	0FEAC90D	D0F7A92F	DBF1EFF4	CCF2BF34
KeyAddition	6D1223DF	82DBC254	25FD7E03	E8F04A91

Round = 2

Substitution	3CC9269E	13B92520	3F54F37B	9B8CD681
ShiftRow	3CB9F381	1354D69E	3F8C2620	9BC9257B
MixColumn	DADAE017	92444990	F7769FAB	330695AC
KeyAddition	36C8E699	FEC636FB	F90C0A12	6F506B6E

Round = 3

Substitution	05E88EEE	BBB4050F	99FE67C9	A8537F9F
ShiftRow	05B4679F	BBFE7FEE	99538E0F	A8E805C9

MixColumn	3540C5F9	E5339290	5DB9DC73	A4A50A87
KeyAddition	78F77144	8C86D388	D81E9BE5	4D80327A

Round = 4

Substitution	BC68A31B	644466C4	617214D9	E3CD23DA
ShiftRow	BC4414DA	6472231B	61CDA3C4	E36866D9
MixColumn	61D2A520	66FE7DCB	E9DAA65E	DA403799
KeyAddition	868D0864	DDF72E4D	A1805609	FBAF86D6

Round = 5

Substitution	445D3043	C16831E3	32CDB101	0F7944F6
ShiftRow	4468B1F6	C1CD4443	327930E3	0F5D3101
MixColumn	77AA54E2	D2CF4157	3C7315C2	C9E7337F
KeyAddition	D3E2A23B	9FA28F73	964176A2	D8DC0399

Round = 6

Substitution	66983AE2	DB3A738F	9083383A	61867BEE
ShiftRow	663A38EE	DB837BE2	90863A8F	6198733A
MixColumn	54B4056F	AAA99351	1F46E812	38E5513C
KeyAddition	F6EA7BBA	29185CCB	38BFD151	5271A65B

Round = 7

Substitution	428721F4	A5AD4A1F	07083ED1	00A32439
ShiftRow	42AD3E39	A50824F4	07A3211F	00874AD1
MixColumn	6F78D827	992DE22B	CE26C7B5	091A7B74
KeyAddition	AFDE4C20	48B046CA	2231415E	66BC3205

Round = 8

Substitution	791D29B7	52E75A74	93C78358	3365236B
ShiftRow	79E7836B	52C723B7	93652974	331D5A58
MixColumn	28593E39	62151167	CF56380A	43BF72A2
KeyAddition	60064E0B	40DE9632	2D3B2B58	704FC511

Round = 9

Substitution	D06F2F2B	091D9023	D8E2F16A	5184A682
ShiftRow	D01DF182	09E2A62B	D8842F23	516F906A
MixColumn	EF60A998	A20CC109	3099679E	E94EBBD8
KeyAddition	AFDE42B0	8D146350	57DEB5F5	ACC2EEE6

Round = 10

Substitution	791D2CE7	5DFAFB53	5B1DD5E6	9125288E
ShiftRow	79FAD58E	5D1D28E7	5B252C53	911DFBE6
MixColumn	BC7CBBA3	52F82207	A636D342	035B5099
KeyAddition	1B9DFDCF	C6E9D3D8	2429A648	AE5C87CA

Round = 11

Substitution AF5E548A B41E6661 36A52452 E44A1774  
ShiftRow AF1E2474 B4A5178A 364A5461 E45E6652  
MixColumn 378B6538 1A56BA7A 873F7786 05A080AB  
KeyAddition FDCB6000 959AEA7C AF1261EC B99C671E

Substitution 541FD063 2AB88710 79C9EFCE 56DE8572  
ShiftRow 54B8EF72 2AC98563 79DED010 561F87CE  
KeyAddition BD334F1D 6E45F25F F712A214 571FA5CC

KeyAddition 205E3AA0 C40DC8CE 56A79C87 C53FF7B4

Round = 1

Substitution B75880E0 1CD7E88B B15CDE17 A675688D  
ShiftRow B7D7DE8D 1C5C68E0 B175808B A658E817  
MixColumn 44F64BCA 54FCABCB ED4B5930 40220C6F  
KeyAddition 260EA118 06D0C0B0 1347C8C7 6420F9CA

Round = 2

Substitution F7AB32AD 6F70BAE7 7DA0E8C6 43B79974  
ShiftRow F770E874 6FA099AD 7DB732E7 43ABBAC6  
MixColumn F940D072 11290AC9 EDB99CD7 1C1DD643  
KeyAddition 1552D6FC 7DAB75A2 E3C3096E 404B2881

Round = 3

Substitution 5900F6B0 FF629D3A 112E019F 09B3340C  
ShiftRow 5962010C FF2E34B0 11B3F63A 09009D9F  
MixColumn 19922D90 134F727B 20571B02 102A92A3  
KeyAddition 5425992D 7AFA3363 A5F05C94 F90FAA5E

Round = 4

Substitution 203FEED8 DA2DC3FB 068C4A22 9976AC58  
ShiftRow 202D4A58 DA8CACD8 0676EEFB 993FC322  
MixColumn 25FC71B7 54EE66FE 8338A17F 899B5D08  
KeyAddition C2A3DCF3 EFE73578 CB625128 A874EC47

Round = 5

Substitution 250A860D DF9496BC 1FAAD134 C292CEA0  
ShiftRow 2594D1A0 DFAACE0D 1F9286BC C20A9634  
MixColumn 9CDEF371 83D4E504 A90D4556 2343A3A9  
KeyAddition 389605A8 CEB92B20 033F2636 3278934F

Round = 6

Substitution 07906BC2 8B56F1B7 7B75F705 23BCDC84  
ShiftRow 0756F784 8B75DCC2 7BBC6BB7 2390F105  
MixColumn 872D33BB 8CDC00B0 F512D32F 1915450E  
KeyAddition 25734D6E 0F6DCF2A D2EBEA6C 7381B269

Round = 7

Substitution	3F8FE39F	763C8AE5	B5E98750	8F0C37F9
ShiftRow	3F3C87F9	76E9379F	B50CE3E5	8F8F8A50
MixColumn	442C0613	64794B61	637650FA	555FFF2F
KeyAddition	848A9214	B5E4EF80	8F61D611	3AF9B65E

Round = 8

Substitution	5F7E4FFA	D569DFCD	73EFF682	80994E58
ShiftRow	5F69F658	D5EF4EFA	73994FCD	807EDF82
MixColumn	ABD429CE	2F38B32A	D44638C2	C484C625
KeyAddition	E38B59FC	0DF3347F	362B2B90	F7747196

Round = 9

Substitution	113DCBB0	D70D18D2	05F1F160	6892A390
ShiftRow	110DF190	D7F1A3B0	0592CBD2	683D1860
MixColumn	54934EF4	AE60B04B	BEAE77E9	EF5AC55D
KeyAddition	142DA5DC	81781212	D9E9A582	AAD69063

Round = 10

Substitution	FAD80686	0CBCC9C9	351E0613	ACF660FB
ShiftRow	FABC06FB	0C1E6086	35F606C9	ACD8C913
MixColumn	CD685C42	DC16437D	A4018F26	EA54C8D8
KeyAddition	6A891A2E	4807B2A2	261EFA2C	47531F8B

Round = 11

Substitution	02A7A231	52C5373A	F7722D71	A0EDC03D
ShiftRow	02C52D3D	5272C031	F7EDA23A	A0A73771
MixColumn	40D9DA94	C3DCE826	41F10B39	EFDDFA89
KeyAddition	8A99DFAC	4C10B820	69DC1D53	53E11D3C

Substitution	7EEE9E91	29CA6CB7	F986A4ED	EDF8A4EB
ShiftRow	7ECAA4EB	2986A491	F9F89EB7	EDEE6CED
KeyAddition	97410484	6D0AD3AD	7734ECB3	ECEE4EEF

KeyAddition BEBBACB1 79528043 2DEB3232 9A9A2B0A

Round = 1

Substitution	AEEA91C8	B600CD1A	D8E92323	B8B8F167
ShiftRow	AE002367	B6E9F1C8	D8B8911A	B8EACD23
MixColumn	03AC4104	6EBFE552	F301776E	A018B6B2
KeyAddition	6154ABD6	3C938E29	0D0DE699	841A4317

Round = 2

Substitution	EF2062F6	EBDC19A5	D7D78EEE	5FA21AF0
ShiftRow	EFDC8EF0	EBD71AF6	D7A262A5	5F2019EE

MixColumn	C4353F83	4386091C	8F8B45F3	29DA641F
KeyAddition	2827390D	2F047677	81F1D04A	758C9ADD

Round = 3

Substitution	34CC12D7	15F238F5	0CA170D6	9D64B8C1
ShiftRow	34F270C1	15A1B8D7	0C6412F5	9DCC38D6
MixColumn	D49A7E47	BD48BD93	53074893	808040FF
KeyAddition	992DCAFA	D4FDFC8B	D6A00F05	69A57802

Round = 4

Substitution	EED8742D	4854B03D	F6E0766B	F906BC77
ShiftRow	EE547677	48E0BC2D	F606743D	F9D8B06B
MixColumn	3AABCFE5	3A61BCDE	B45B5F09	41F2E7AE
KeyAddition	DDF462A1	8168EF58	FC01AF5E	601D56E1

Round = 5

Substitution	C1BFAA32	0C45DF6A	B07C7958	D0A4B1F8
ShiftRow	C14579F8	0C7CB132	B0A4AA6A	D0BFDF58
MixColumn	D738658F	1F0E5FBD	4C6CE511	E69722BB
KeyAddition	73709356	52639199	E65E8671	F7AC125D

Round = 6

Substitution	8F51DCB1	00FB81EE	8E5844A3	6891C94C
ShiftRow	8FFB444C	0058C9B1	8E91DCEE	685181A3
MixColumn	1BE228AD	904119E8	9D269503	01F1DE35
KeyAddition	B9BC5678	13F0D672	BADFAC40	6B652952

Round = 7

Substitution	5665B1BC	7D8CF640	F49E9109	7F4DA500
ShiftRow	568C9100	7D9EA5BC	F44DB140	7F65F609
MixColumn	B2FDE3E7	5A126DDF	D5E6007B	AEBDF600
KeyAddition	725B77E0	8B8FC93E	39F18690	C11BBF71

Round = 8

Substitution	4039F5E1	3D73DDB2	12A14460	78AF08A3
ShiftRow	407344A3	3DA108E1	12AFF5B2	7839DD60
MixColumn	F2C945AA	6B9DB437	89E18113	061640AC
KeyAddition	BA963598	49563362	6B8C9241	35E6F71F

Round = 9

Substitution	F4909646	3BB1C3AA	7F644F83	968E68C0
ShiftRow	F4B14FC0	3B646846	7F8E96AA	9690C383
MixColumn	B49C8062	F40D45CD	4B7323D6	DC7005EF
KeyAddition	F4226B4A	DB15E794	2C34F1BD	99FC50D1

Round = 10



Substitution BF937FD6 B9599422 7118A17A EEB0533E  
ShiftRow BF59A13E B91853D6 71B07F22 EE93947A  
MixColumn 11CBFD5E C4AA662C 74A95918 870EC0DA  
KeyAddition B62ABB32 50BB97F3 F6B62C12 2A091789

Round = 11

Substitution 4EE5EA23 53EA880D 424E71C9 E501F0A7  
ShiftRow 4EEA71A7 534EF023 4201EA0D E5E588C9  
MixColumn 6FB5B41C A7E7830D 60689B37 A47E4BD0  
KeyAddition A5F5B124 282BD30B 48458D5D 1842AC65

Substitution 06E6C836 34F1662B 526E5D4C AD2C914D  
ShiftRow 06F15D4D 346E9136 522CC82B ADE6664C  
KeyAddition EF7AFD22 70E2E60A DCE0BA2F ACE6444E

KeyAddition 78EC94B2 0541FF45 653BB250 66FC4EF5

Round = 1

Substitution BCCE2237 6B83166E 4DE23753 33B02FE6  
ShiftRow BC8337E6 6BE22F37 4DB0226E 33CE1653  
MixColumn 2C1E60BC F3F28E1E 1D3E0B99 6ADD242B  
KeyAddition 4EE68A6E A1DEE565 E3329A6E 4EDFD18E

Round = 2

Substitution 2F8E7E9F 321DD94D 1123B89F 2F9E3E19  
ShiftRow 2F1DB819 32233E9F 119E7E4D 2F8ED99F  
MixColumn D8DF72E6 A0A9D76E A8F9A449 91C7B203  
KeyAddition 34CD7468 CC2BA805 A68331F0 CD914CC1

Round = 3

Substitution 18BD9245 4BF1C26B 24ECC78C BD812978  
ShiftRow 18F1C778 4BEC2945 2481926B BDBDC28C  
MixColumn 87CBF4EE D5B63A92 29FB27A9 F30D10A0  
KeyAddition CA7C4053 BC037B8A AC5C603F 1A28285D

Round = 4

Substitution 741009ED 657B217E 914AD075 A234344C  
ShiftRow 747BD04C 654A34ED 9134097E A2102175  
MixColumn F9A560AF CD406B10 129C3569 3B946F26  
KeyAddition 1EFACDEB 76493896 5AC6C53E 1A7BDE69

Round = 5

Substitution 722DBDE9 383B0790 BEB4A6B2 A2211DF9  
ShiftRow 723BA6F9 38B41DE9 BE21BD90 A22D07B2  
MixColumn F60C0EE2 43859628 29B0557E 9D434CA8  
KeyAddition 5244F83B 0EE8580C 8382361E 8C787C4E

Round = 6

Substitution	001B41E2	AB9B6AFE	EC130572	64BC102F
ShiftRow	009B052F	AB1310E2	ECBC41FE	641B6A72
MixColumn	9C0DE0C0	8A5FA53A	A3B2CB35	FD9E3D39
KeyAddition	3E539E15	09EE6AA0	844BF276	970ACA5E

Round = 7

Substitution	B2ED0B59	012802E0	5FB38938	88677458
ShiftRow	B2288958	01B37459	5F670BE0	88ED0238
MixColumn	D63A7BDC	E1B9B176	FC6C1556	1D77291C
KeyAddition	169CEADB	30241597	107B93BD	72D1606D

Round = 8

Substitution	47DEDFB9	04365988	CA21DC7A	403ED03C
ShiftRow	4736DC3C	0421D0B9	CA3EDF88	40DE597A
MixColumn	3468965B	02944E94	9A44D2AF	DA76A2B3
KeyAddition	7C37E669	205FC9C1	7829C1FD	E9861500

Round = 9

Substitution	109A8EF9	B7CFDD78	BCA57854	1E445963
ShiftRow	10CF7863	B7A559F9	BC448E78	1E9ADD54
MixColumn	717E8A41	21F4B0D7	59C577E5	0019D9CD
KeyAddition	31C06169	0EEC128E	3E82A58E	45958CF3

Round = 10

Substitution	C7BAEFF9	ABCEC919	B2130619	6E2A640D
ShiftRow	C7CE060D	AB1364F9	B22AEF19	6EBAC919
MixColumn	D7471280	E5D86078	F7D5763A	D95876F3
KeyAddition	70A654EC	71C991A7	75CA0330	745FA1A0

Round = 11

Substitution	512420CE	A3DD815C	9D747B04	92CF32E0
ShiftRow	51DD7BE0	A37432CE	9DCF205C	92248104
MixColumn	459D418E	3DD3FA3F	1724F6EB	D646A300
KeyAddition	8FDD44B6	B21FAA39	3F09E081	6A7A44B5

Substitution	73C11B4E	37C0AC12	7501E10C	02DA1BD5
ShiftRow	73C0E1D5	37011B4E	75DA1B12	02C1AC0C
KeyAddition	9A4B41BA	738D6C72	FB166916	03C18E0E

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

KeyAddition 54B8EF72 2AC98563 79DED010 561F87CE  
Substitution FD9A611E 95126700 AF9C607C B9CBEAEC  
ShiftRow FDCB6000 959AEA7C AF1261EC B99C671E

Round = 11

KeyAddition 378B6538 1A56BA7A 873F7786 05A080AB  
InvMixColumn AF1E2474 B4A5178A 364A5461 E45E6652  
Substitution 1BE9A6CA C62987CF 245CFDD8 AE9DD348  
ShiftRow 1B9DFDCF C6E9D3D8 2429A648 AE5C87CA

Round = 10

KeyAddition BC7CBBA3 52F82207 A636D342 035B5099  
InvMixColumn 79FAD58E 5D1D28E7 5B252C53 911DFBE6  
Substitution AF14B5E6 8DDEEEB0 57C24250 ACDE63F5  
ShiftRow AFDE42B0 8D146350 57DEB5F5 ACC2EEE6

Round = 9

KeyAddition EF60A998 A20CC109 3099679E E94EBBD8  
InvMixColumn D01DF182 09E2A62B D8842F23 516F906A  
Substitution 60DE2B11 403BC50B 2D4F4E32 70069658  
ShiftRow 60064E0B 40DE9632 2D3B2B58 704FC511

Round = 8

KeyAddition 28593E39 62151167 CF56380A 43BF72A2  
InvMixColumn 79E7836B 52C723B7 93652974 331D5A58  
Substitution AFB04105 48313220 22BC4CCA 66DE465E  
ShiftRow AFDE4C20 48B046CA 2231415E 66BC3205

Round = 7

KeyAddition 6F78D827 992DE22B CE26C7B5 091A7B74  
InvMixColumn 42AD3E39 A50824F4 07A3211F 00874AD1  
Substitution F618D15B 29BFA6BA 38717BCB 52EA5C51  
ShiftRow F6EA7BBA 29185CCB 38BFD151 5271A65B

Round = 6

KeyAddition 54B4056F AAA99351 1F46E812 38E5513C  
InvMixColumn 663A38EE DB837BE2 90863A8F 6198733A  
Substitution D3A27699 9F41033B 96DCA273 D8E28FA2  
ShiftRow D3E2A23B 9FA28F73 964176A2 D8DC0399

Round = 5

KeyAddition 77AA54E2 D2CF4157 3C7315C2 C9E7337F  
InvMixColumn 4468B1F6 C1CD4443 327930E3 0F5D3101  
Substitution 86F756D6 DD808664 A1AF084D FB8D2E09  
ShiftRow 868D0864 DDF72E4D A1805609 FBAF86D6

Round = 4

KeyAddition 61D2A520 66FE7DCB E9DAA65E DA403799  
InvMixColumn BC4414DA 6472231B 61CDA3C4 E36866D9  
Substitution 78869B7A 8C1E3244 D8807188 4DF7D3E5  
ShiftRow 78F77144 8C86D388 D81E9BE5 4D80327A

Round = 3

KeyAddition 3540C5F9 E5339290 5DB9DC73 A4A50A87  
InvMixColumn 05B4679F BBFE7FEE 99538E0F A8E805C9  
Substitution 36C60A6E FE0C6B99 F950E6FB 6FC83612  
ShiftRow 36C8E699 FEC636FB F90C0A12 6F506B6E

Round = 2

KeyAddition DADAE017 92444990 F7769FAB 330695AC  
InvMixColumn 3CB9F381 1354D69E 3F8C2620 9BC9257B  
Substitution 6DDB7E91 82FD4ADF 25F02354 E812C203  
ShiftRow 6D1223DF 82DBC254 25FD7E03 E8F04A91

Round = 1

KeyAddition 0FEAC90D D0F7A92F DBF1EFF4 CCF2BF34  
InvMixColumn D92F5D8A BFD89F59 FD7BAB1C 0D370F80  
Substitution E54E8DCF F42D6E15 21030EC4 F3B2FB3A  
ShiftRow E5B20E15 F44EFBC4 212D8D3A F3036ECF

KeyAddition 6BC1BEE2 2E409F96 E93D7E11 7393172A

KeyAddition 7ECAA4EB 2986A491 F9F89EB7 EDEE6CED  
Substitution 8A101D3C 4CDC1DAC 69E1DF20 5399B853  
ShiftRow 8A99DFAC 4C10B820 69DC1D53 53E11D3C

Round = 11

KeyAddition 40D9DA94 C3DCE826 41F10B39 EFDDFA89  
InvMixColumn 02C52D3D 5272C031 F7EDA23A A0A73771  
Substitution 6A07FA8B 481E1F2E 26531AA2 4789B22C  
ShiftRow 6A891A2E 4807B2A2 261EFA2C 47531F8B

Round = 10

KeyAddition CD685C42 DC16437D A4018F26 EA54C8D8  
InvMixColumn FABC06FB 0C1E6086 35F606C9 ACD8C913  
Substitution 1478A563 81E990DC D9D6A512 AA2D1282  
ShiftRow 142DA5DC 81781212 D9E9A582 AAD69063

Round = 9

KeyAddition 54934EF4 AE60B04B BEAE77E9 EF5AC55D

InvMixColumn	110DF190	D7F1A3B0	0592CBD2	683D1860
Substitution	E3F32B96	0D2B71FC	3674597F	F78B3490
ShiftRow	E38B59FC	0DF3347F	362B2B90	F7747196
Round = 8				
KeyAddition	ABD429CE	2F38B32A	D44638C2	C484C625
InvMixColumn	5F69F658	D5EF4EFA	73994FCD	807EDF82
Substitution	84E4D65E	B561B614	8FF99280	3A8AEF11
ShiftRow	848A9214	B5E4EF80	8F61D611	3AF9B65E
Round = 7				
KeyAddition	442C0613	64794B61	637650FA	555FFF2F
InvMixColumn	3F3C87F9	76E9379F	B50CE3E5	8F8F8A50
Substitution	256DEA69	0FEBB26E	D2814D2A	7373CF6C
ShiftRow	25734D6E	0F6DCF2A	D2EBEA6C	7381B269
Round = 6				
KeyAddition	872D33BB	8CDC00B0	F512D32F	1915450E
InvMixColumn	0756F784	8B75DCC2	7BBC6BB7	2390F105
Substitution	38B9264F	CE3F93A8	03780520	32962B36
ShiftRow	389605A8	CEB92B20	033F2636	3278934F
Round = 5				
KeyAddition	9CDEF371	83D4E504	A90D4556	2343A3A9
InvMixColumn	2594D1A0	DFAACE0D	1F9286BC	C20A9634
Substitution	C2E75147	EF62ECF3	CB74DC78	A8A33528
ShiftRow	C2A3DCF3	EFE73578	CB625128	A874EC47
Round = 4				
KeyAddition	25FC71B7	54EE66FE	8338A17F	899B5D08
InvMixColumn	202D4A58	DA8CACD8	0676EEFB	993FC322
Substitution	54FA5C5E	7AF0AA2D	A50F9963	F9253394
ShiftRow	5425992D	7AFA3363	A5F05C94	F90FAA5E
Round = 3				
KeyAddition	19922D90	134F727B	20571B02	102A92A3
InvMixColumn	5962010C	FF2E34B0	11B3F63A	09009D9F
Substitution	15AB0981	7DC328FC	E34BD6A2	4052756E
ShiftRow	1552D6FC	7DAB75A2	E3C3096E	404B2881
Round = 2				
KeyAddition	F940D072	11290AC9	EDB99CD7	1C1DD643
InvMixColumn	F770E874	6FA099AD	7DB732E7	43ABBAC6
Substitution	26D0C8CA	0647F918	1320A1B0	640EC0C7
ShiftRow	260EA118	06D0C0B0	1347C8C7	6420F9CA
Round = 1				
KeyAddition	44F64BCA	54FCABCB	ED4B5930	40220C6F
InvMixColumn	B7D7DE8D	1C5C68E0	B175808B	A658E817
Substitution	200D9CB4	C4A7F7A0	563F3ACE	C55EC887
ShiftRow	205E3AA0	C40DC8CE	56A79C87	C53FF7B4
KeyAddition	AE2D8A57	1E03AC9C	9EB76FAC	45AF8E51
KeyAddition	06F15D4D	346E9136	522CC82B	ADE6664C

Substitution	A52B8D65	2845AC24	4842B10B	18F5D35D
ShiftRow	A5F5B124	282BD30B	48458D5D	1842AC65
Round = 11				
KeyAddition	6FB5B41C	A7E7830D	60689B37	A47E4BD0
InvMixColumn	4EEA71A7	534EF023	4201EA0D	E5E588C9
Substitution	B6BB2C89	50B61732	F609BBF3	2A2A9712
ShiftRow	B62ABB32	50BB97F3	F6B62C12	2A091789
Round = 10				
KeyAddition	11CBFD5E	C4AA662C	74A95918	870EC0DA
InvMixColumn	BF59A13E	B91853D6	71B07F22	EE93947A
Substitution	F415F1D1	DB34504A	2CFC6B94	9922E7BD
ShiftRow	F4226B4A	DB15E794	2C34F1BD	99FC50D1
Round = 9				
KeyAddition	B49C8062	F40D45CD	4B7323D6	DC7005EF
InvMixColumn	F4B14FC0	3B646846	7F8E96AA	9690C383
Substitution	BA56921F	498CF798	6BE63562	35963341
ShiftRow	BA963598	49563362	6B8C9241	35E6F71F
Round = 8				
KeyAddition	F2C945AA	6B9DB437	89E18113	061640AC
InvMixColumn	407344A3	3DA108E1	12AFF5B2	7839DD60
Substitution	728F8671	8BF1BFE0	391B773E	C15BC990
ShiftRow	725B77E0	8B8FC93E	39F18690	C11BBF71
Round = 7				
KeyAddition	B2FDE3E7	5A126DDF	D5E6007B	AEBDF600
InvMixColumn	568C9100	7D9EA5BC	F44DB140	7F65F609
Substitution	B9F0AC52	13DF2978	BA655672	6BBCD640
ShiftRow	B9BC5678	13F0D672	BADFAC40	6B652952
Round = 6				
KeyAddition	1BE228AD	904119E8	9D269503	01F1DE35
InvMixColumn	8FFB444C	0058C9B1	8E91DCEE	685181A3
Substitution	7363865D	525E1256	E6AC9399	F7709171
ShiftRow	73709356	52639199	E65E8671	F7AC125D
Round = 5				
KeyAddition	D738658F	1F0E5FBD	4C6CE511	E69722BB
InvMixColumn	C14579F8	0C7CB132	B0A4AA6A	D0BFDF58
Substitution	DD68AFE1	810156A1	FC1D6258	60F4EF5E
ShiftRow	DDF462A1	8168EF58	FC01AF5E	601D56E1
Round = 4				
KeyAddition	3AABCFE5	3A61BCDE	B45B5F09	41F2E7AE
InvMixColumn	EE547677	48E0BC2D	F606743D	F9D8B06B
Substitution	99FD0F02	D4A078FA	D6A5CA8B	692DFC05
ShiftRow	992DCAFA	D4FDFC8B	D6A00F05	69A57802
Round = 3				
KeyAddition	D49A7E47	BD48BD93	53074893	808040FF
InvMixColumn	34F270C1	15A1B8D7	0C6412F5	9DCC38D6
Substitution	2804D0DD	2FF19A0D	818C3977	7527764A

ShiftRow 2827390D 2F047677 81F1D04A 758C9ADD

Round = 2

KeyAddition C4353F83 4386091C 8F8B45F3 29DA641F

InvMixColumn EFDC8EF0 EBD71AF6 D7A262A5 5F2019EE

Substitution 6193E617 3C0D43D6 0D1AAB29 84548E99

ShiftRow 6154ABD6 3C938E29 0D0DE699 841A4317

Round = 1

KeyAddition 03AC4104 6EBFE552 F301776E A018B6B2

InvMixColumn AE002367 B6E9F1C8 D8B8911A B8EACD23

Substitution BE52320A 79EB2BB1 2D9AAC43 9ABB8032

ShiftRow BEBBACB1 79528043 2DEB3232 9A9A2B0A

KeyAddition 30C81C46 A35CE411 E5FBC119 1A0A52EF

KeyAddition 73C0E1D5 37011B4E 75DA1B12 02C1AC0C

Substitution 8F1FE0B5 B20944B6 3F7A4439 6ADDAA81

ShiftRow 8FDD44B6 B21FAA39 3F09E081 6A7A44B5

Round = 11

KeyAddition 459D418E 3DD3FA3F 1724F6EB D646A300

InvMixColumn 51DD7BE0 A37432CE 9DCF205C 92248104

Substitution 70C903A0 71CAA1EC 755F54A7 74A69130

ShiftRow 70A654EC 71C991A7 75CA0330 745FA1A0

Round = 10

KeyAddition D7471280 E5D86078 F7D5763A D95876F3

InvMixColumn C7CE060D AB1364F9 B22AEF19 6EBAC919

Substitution 31ECA5F3 0E828C69 3E95618E 45C0128E

ShiftRow 31C06169 0EEC128E 3E82A58E 45958CF3

Round = 9

KeyAddition 717E8A41 21F4B0D7 59C577E5 0019D9CD

InvMixColumn 10CF7863 B7A559F9 BC448E78 1E9ADD54

Substitution 7C5FC100 20291569 7886E6C1 E937C9FD

ShiftRow 7C37E669 205FC9C1 7829C1FD E9861500

Round = 8

KeyAddition 3468965B 02944E94 9A44D2AF DA76A2B3

InvMixColumn 4736DC3C 0421D0B9 CA3EDF88 40DE597A

Substitution 1624936D 307B60DB 10D1EF97 729C15BD

ShiftRow 169CEFD8 30241597 107B93BD 72D1606D

Round = 7

KeyAddition D63A7BDC E1B9B176 FC6C1556 1D77291C

InvMixColumn B2288958 01B37459 5F670BE0 88ED0238

Substitution 3EEEF25E 094BCA15 840A9EA0 97536A76

ShiftRow 3E539E15 09EE6AA0 844BF276 970ACA5E

Round = 6

KeyAddition 9C0DE0C0 8A5FA53A A3B2CB35 FD9E3D39

InvMixColumn 009B052F AB1310E2 ECBC41FE 641B6A72

Substitution 52E8364E 0E827C3B 8378F80C 8C44581E

ShiftRow 5244F83B 0EE8580C 8382361E 8C787C4E

```

Round = 5
  KeyAddition   F60C0EE2 43859628 29B0557E 9D434CA8
  InvMixColumn  723BA6F9 38B41DE9 BE21BD90 A22D07B2
  Substitution  1E49C569 76C6DEEB 5A7BCD96 1AFA383E
  ShiftRow      1EFACDEB 76493896 5AC6C53E 1A7BDE69
Round = 4
  KeyAddition   F9A560AF CD406B10 129C3569 3B946F26
  InvMixColumn  747BD04C 654A34ED 9134097E A2102175
  Substitution  CA03605D BC5C2853 AC28408A 1A7C7B3F
  ShiftRow      CA7C4053 BC037B8A AC5C603F 1A28285D
Round = 3
  KeyAddition   87CBF4EE D5B63A92 29FB27A9 F30D10A0
  InvMixColumn  18F1C778 4BEC2945 2481926B BDBDC28C
  Substitution  342B31C1 CC834C68 A6917405 CDCDA8F0
  ShiftRow      34CD7468 CC2BA805 A68331F0 CD914CC1
Round = 2
  KeyAddition   D8DF72E6 A0A9D76E A8F9A449 91C7B203
  InvMixColumn  2F1DB819 32233E9F 119E7E4D 2F8ED99F
  Substitution  4EDE9A8E A132D16E E3DF8A65 4EE6E56E
  ShiftRow      4EE68A6E A1DEE565 E3329A6E 4EDFD18E
Round = 1
  KeyAddition   2C1E60BC F3F28E1E 1D3E0B99 6ADD242B
  InvMixColumn  BC8337E6 6BE22F37 4DB0226E 33CE1653
  Substitution  7841B2F5 053B4EB2 65FC9445 66ECFF50
  ShiftRow      78EC94B2 0541FF45 653BB250 66FC4EF5
KeyAddition    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

Electronic Codebook (ECB)

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

KeyAddition 0BFC55F2 3B8AEE28 C24ED0E1 F6EE60AB

Round = 1

Substitution 2BB0FC89 E27E2834 252F70F8 4228D062  
ShiftRow 2B7E7062 E22FD089 2528FC34 42B028F8  
MixColumn C62513B7 F75EF6CB FA5EB2D3 9FB9B1B5  
KeyAddition D9103FB0 CC3FFE1C D7C6A270 96AD6E41

Round = 2

Substitution 35CA75E7 4B75BB9C 0EB43A51 90959F83  
ShiftRow 35753A83 4BB49FE7 0E95759C 90CABB51  
MixColumn 4C12AA0D 2965E823 513CCED1 9498C478  
KeyAddition D7B1FE1C A70CCD8C F426458E B4FF38A6

Round = 3

Substitution 0EC8BB9C 5CFEBD64 BFF76E19 8D160724  
ShiftRow 0EFE6E24 5CF7079C BF16BB64 8DC8BD19

MixColumn	4F7F40CA	213C1A37	802168BF	E6C30FCB
KeyAddition	E7CFDCD0	B2ED8EFA	3E68ECD1	519E5451

Round = 4

Substitution	948A8670	3755192D	B245CE3E	D10B20D1
ShiftRow	9455CED1	37452070	B20B862D	D18A193E
MixColumn	D3A62E85	F1ADA2DC	C918D91A	1BCB2B87
KeyAddition	063CC23D	AA5E6BCB	37F19B52	C5459511

Round = 5

Substitution	6FEB2527	AC587F1F	9AA11400	A66E2A82
ShiftRow	6F581482	ACA12A27	9A6E251F	A6EB7F00
MixColumn	A06182E2	B6AC302A	A7369FC0	0EEAB365
KeyAddition	15C8B068	90D4966D	3F07BDE9	2186CAD6

Round = 6

Substitution	59E8E745	6048903C	75C57A1E	FD4474F6
ShiftRow	59487AF6	60C57445	7544E73C	FDE8901E
MixColumn	E6B1E42E	A528829B	FD3A044	4C830C58
KeyAddition	679D6583	7FF7CA21	D9C5AAB6	B63BB83C

Round = 7

Substitution	855E4DEC	D26874FD	35A6AC4E	4EE26CEB
ShiftRow	8568ACEB	D2A66CEC	35E24DFD	4E5E744E
MixColumn	EE51889D	CEDD8364	E7C05111	44202A64
KeyAddition	76943754	70609AEA	C14C6AB6	4DC06870

Round = 8

Substitution	38229A20	51D0B887	7829024E	E3BA4551
ShiftRow	38D00251	51294520	78BA9A87	E322B84E
MixColumn	48D41F38	BCEC92DF	38257FBD	4D3A7838
KeyAddition	20D46494	0E33A1C9	AECC4659	216BF5B8

Round = 9

Substitution	B7484322	ABC332DD	E44B5ACB	FD7FE66C
ShiftRow	B7C35A6C	AB4BE622	E47F43DD	FD4832CB
MixColumn	1DA87483	542E510F	CC0261AA	C0F097EB
KeyAddition	D5BC9687	2287AA85	9C27A187	993515D2

Round = 10

Substitution	03659017	9317AC97	DECC3217	EE9659B5
ShiftRow	031732B5	93CC5917	DE969097	EE65AC17
MixColumn	B8CEB451	3CECD415	01D5D14A	D3DCF1CE
KeyAddition	66DDDD36	50208E64	FBF0B2DF	45A81FDB

Round = 11

Substitution 33C1C105 53B71943 0F8C379E 6EC2C0B9  
ShiftRow 33B737B9 538CC005 0FC2C143 6EC1199E  
MixColumn 2AA63ABC EC0E4BB3 C18B9194 0342244D  
KeyAddition 7220F0E1 C2217A64 BF81606E 248D578E

Round = 12

Substitution 40B78CF8 25FDDA43 080CD09F 365D5B19  
ShiftRow 40FDD019 250C5BF8 085D8C43 36B7DA9F  
MixColumn 55D32DDF FD288CD3 387E934F EBA99412  
KeyAddition 214F6A74 E5789109 DA0BED00 9FA80448

Round = 13

Substitution FD840292 D9BC8101 572B5563 DBC2F252  
ShiftRow FD8C5552 D92BF292 57C20201 DB848163  
MixColumn 39331D51 B410A096 F0CF923B D833E3B5  
KeyAddition F3C9B7B2 50C53BA2 6A10F8F5 6523FAB8

Substitution 0DDDA937 53A6E23A 02CA41E6 4D262D6C  
ShiftRow 0DA6416C 53CA2D37 0226A93A 4DDDE2E6  
KeyAddition F3EED1BD B5D2A03C 064B5A7E 3DB181F8

KeyAddition CE106147 0BC9DD22 B5C4C15C C0D2F9D0

Round = 1

Substitution 8BCAEFA0 2BDDC193 D51C784A BAB59970  
ShiftRow 8BDD7870 2B1C99A0 D5B5EF93 BACAC14A  
MixColumn 79D236C3 4B03E5A3 091D0B03 A127374A  
KeyAddition 66E71AC4 7062ED74 24851BA0 A833E8BE

Round = 2

Substitution 3394A21C 51AA5592 3697AFE0 C2C39BAE  
ShiftRow 33AAFAE 51979B1C 36C3A292 C29455E0  
MixColumn 82383517 87CECF7 02C40704 8DEEC747  
KeyAddition 199B6106 09A7EA68 A7DE8C5B AD893B99

Round = 3

Substitution D414EF6F 015C8745 5C1D6439 95A7E2EE  
ShiftRow D45C64EE 011DE26F 5CA7EF45 95148739  
MixColumn DD2E6998 A8697222 E066F126 B316DF45  
KeyAddition 759EF582 3BB8E6EF 5E2F7548 044B84DF

Round = 4

Substitution 9D0BE613 E26C8EDF 58159D52 F2B35F9E  
ShiftRow 9D6C9D9E E2155F13 58B3E6DF F20B8E52  
MixColumn 9667696A AC3A7C51 47CB4618 3E3F082C  
KeyAddition 43FD85D2 F7C9B546 B9220450 E0B1B6BA

Round = 5

Substitution	1A5497B5	68DDD55A	5693F253	E1C84EF4
ShiftRow	1ADDF2F4	68934EB5	56C8975A	E154D553
MixColumn	4E423FF2	8532A314	22254511	A37EF11F
KeyAddition	FBEB0D78	A34A0553	BA146738	8C1288AC

Round = 6

Substitution	0FE9D7BC	0AD66BED	F4FA8507	64C9C491
ShiftRow	0FD68591	0AFAC4BC	F4C9D7ED	64E96B07
MixColumn	6BBD607B	790EBC43	89F2A4D8	84175220
KeyAddition	EA91E1D6	A3D1F4F9	ADC4AE2A	7EAFE644

Round = 7

Substitution	8781F8F6	0A3EBF99	951CE4E5	F3798E1B
ShiftRow	873EE41B	0A1C8EF6	9579F899	F381BFE5
MixColumn	A8D7477E	484D107B	DBEDB70C	3FD523E1
KeyAddition	3012F8B7	F6F009F5	FD618CAB	363561F5

Round = 8

Substitution	04C941A9	428C01E6	54EF6462	0596EFE6
ShiftRow	048C64E6	42EFEFA9	549641E6	05C90162
MixColumn	054D7133	E804888F	AE4671FC	29ED6803
KeyAddition	6D4D0A9F	5ADBBB99	38AF4818	45BCE583

Round = 9

Substitution	3CE367DB	BEB9EAE	077952AD	6E65D9EC
ShiftRow	3CB952EC	BE79D9DB	076567EE	6EE3EAD
MixColumn	164F0E6C	EEE718D4	288A85CC	A53BAEFA
KeyAddition	DE5BEC68	984EE35E	78AF45E1	FCFE2CC3

Round = 10

Substitution	1D39CE45	462F1158	BC796EF8	B0BB712E
ShiftRow	1D2F6E2E	46797145	BCBBCE58	B03911F8
MixColumn	0BDF9C3A	33621248	23C0681A	D909B808
KeyAddition	D5CCF55D	5FAE4839	D9E50B8F	4F7D561D

Round = 11

Substitution	034BE64C	CFE45212	35D92B73	84FFB1A4
ShiftRow	03E42BA4	CFD9B14C	35FFE612	844B5273
MixColumn	BE094699	08E2BBBA	84F32B62	EF97FE68
KeyAddition	E68F8CC4	26CD8A6D	FAF9DA98	C8588DAB

Round = 12

Substitution	8E73641C	F7BD7E3C	2D995746	E86A5D62
ShiftRow	8EBD5762	F7995D1C	2D6A643C	E8737E46

MixColumn EE743BA7 0425F0FE BC69CB01 66CAADA2  
KeyAddition 9AE87C0C 1C75ED24 5E1CB54E 12CB3DF8

Round = 13

Substitution B89B10FE 9C9D5536 589CD52F C91F2741  
ShiftRow B89DD541 9C9C27FE 581F1036 C99B552F  
MixColumn 43BC5719 452857E3 B7603D8B 453489D0  
KeyAddition 8946FDFA A1FDCCD7 2DBF5745 F82490DD

Substitution A75A542D 32544B0E D8085B6E 413660C1  
ShiftRow A7545BC1 3208602D D836540E 415A4B6E  
KeyAddition 591CCB10 D410ED26 DC5BA74A 31362870

KeyAddition 50F5F756 B69695AF CE886FE9 9F77256E

Round = 1

Substitution 53E668B1 4E902A79 8BC4A81E DBF53F9F  
ShiftRow 5390A89F 4EC43FB1 8BF56879 DBE62A1E  
MixColumn 3A1432E8 452D3C50 18BB25E9 A86C4B86  
KeyAddition 25211EEF 7E4C3487 3523354A A1789472

Round = 2

Substitution 3FFD72DF F3291817 962696D6 32BC2240  
ShiftRow 3F299640 F32622DF 96BC7217 32FD18D6  
MixColumn D38CE17E 6A06EBAF 8D74F741 B62D9E04  
KeyAddition 482FB56F E46FCE00 286E7C1E 964A62DA

Round = 3

Substitution 5215D5A8 69A88B63 349F1072 90D6AA57  
ShiftRow 52A81057 699FAAA8 34D6D563 90158B72  
MixColumn 007E23E0 6A015AC5 BF84F699 FD4E1ED1  
KeyAddition A8CEBFFA F9D0CE08 01CD72F7 4A13454B

Round = 4

Substitution C28B082D 99708B30 7CBD4068 D67D6EB3  
ShiftRow C27040B3 99BD6E2D 7C7D0830 D68B8B68  
MixColumn FC51FC10 B6678F39 47AE4191 D235E8B1  
KeyAddition 29CB10A8 ED94462E B94703D9 0CBB5627

Round = 5

Substitution A51FCAC2 55225A31 56A07B35 FEEAB1CC  
ShiftRow A5227BCC 55A0B1C2 56EACA31 FE1F5A35  
MixColumn 80A03E2E 2204D171 72ED60B8 A91B0A36  
KeyAddition 35090CA4 047C7736 EADC4291 86777385

Round = 6

Substitution	9601FE49	F210F505	87862C81	44F58F97
ShiftRow	96102C97	F2868F49	87F5FE05	4401F581
MixColumn	BC557CA8	A826AA96	EA6A9A93	FFC32C21
KeyAddition	3D79FD05	72F9E22C	CE5C9061	057B9845

Round = 7

Substitution	27B6546B	40999871	8B4A60EF	6B21466E
ShiftRow	2799606E	404A466B	8B215471	6BB698EF
MixColumn	F0C0CC4C	73753B1A	4B449111	6040DC56
KeyAddition	68057385	CDC82294	6DC8AAB6	69A09E42

Round = 8

Substitution	456B8F97	BDE89322	3CE8AC4E	F9E00B2C
ShiftRow	45E8AC2C	BDE80B97	3CE08F22	F96B934E
MixColumn	294D9AD3	DEFCE10A	EE4FBF6F	89CF7D74
KeyAddition	414DE17F	6C23D21C	78A6868B	E59EF0F4

Round = 9

Substitution	83E3F8D2	5026B59C	BC24443D	D90B8CBF
ShiftRow	832644BF	50248CD2	BC0BF89C	D9E3B53D
MixColumn	8CBCF799	92451AE7	1A25E30F	1FFD0C5C
KeyAddition	44A8159D	E4ECE16D	4A002322	46388E65

Round = 10

Substitution	1BC2595E	69CEF83C	D6632693	5A07194D
ShiftRow	1BCE264D	6963195E	D607593C	5AC2F893
MixColumn	14BB4E5F	30DADA7D	DB0F2747	8245DDE9
KeyAddition	CAA82738	5C16800C	212A44D2	143133FC

Round = 11

Substitution	74C2CC07	4A47CDFE	FDE51BB5	FAC7C3B0
ShiftRow	74471BB0	4AE5C307	FDC7CCFE	FAC2CDB5
MixColumn	8A67CEBB	64C23BF6	81D9A0F0	CA9C7D6B
KeyAddition	D2E104E6	4AED0A21	FFD3510A	ED530EA8

Round = 12

Substitution	B5F8F28E	D65567FD	1666D167	55EDABC2
ShiftRow	B555D1C2	D666AB8E	16EDF2FD	55F86767
MixColumn	9DB504DF	387274AB	0F2718C4	B970CAAE
KeyAddition	E9294374	20226971	ED52668B	CD715AF4

Round = 13

Substitution	1EA51A92	B793F9A3	5500333D	BDA3BEBF
ShiftRow	1E9333BF	B700BE92	55A31AA3	BDA5F93D
MixColumn	1EC931E7	59FC7D43	ED853C1B	51C1B6FA
KeyAddition	D4339B04	BD29E677	775A56D5	ECD1AFF7

Substitution 48C314F2 7AA58EF5 F5BEB103 CE3E7968  
ShiftRow 48A5B168 7ABE79F2 F53E14F5 CEC38E03  
KeyAddition B6ED21B9 9CA6F4F9 F153E7B1 BEAFED1D

KeyAddition 96A2CF55 CA85EAA9 8658EF8B 63114091

Round = 1

Substitution 903A8AFC 749787D3 446ADF3D FB820981  
ShiftRow 9097DF81 746A09FC 44828AD3 FB3A873D  
MixColumn C75E3AFA A347131C 4C0DA779 192093D1  
KeyAddition D86B16FD 98261BCB 6195B7DA 10344C25

Round = 2

Substitution 617F4754 46F7AF1F EF2AA957 CA18293F  
ShiftRow 61F7A93F 462A2954 EF18471F CA7FAF57  
MixColumn 564B9E83 8F3DC261 B509584B F689093B  
KeyAddition CDE8CA92 0154E7CE 1013D314 D6EEF5E5

Round = 3

Substitution BD9B744F 7C20948B CA7D66FA F628E6D9  
ShiftRow BD2066D9 7C7DE64F CA28748B F69B94FA  
MixColumn BE8E2133 D6F80781 088D8C14 2F864BE1  
KeyAddition 163EBD29 4529934C B6C4087A 98DB107B

Round = 4

Substitution 47B27AA5 6EA5DC29 4E1C30DA 46B9CA21  
ShiftRow 47A53021 6E1CCAA5 4EB97A29 46B2DCDA  
MixColumn 6B67E11E 97B60935 1F807843 479C220B  
KeyAddition BEFD0DA6 CC45C022 E1693A0B 99129C9D

Round = 5

Substitution AE54D724 4B6EBA93 F8F9802B EEC9DE5E  
ShiftRow AE6E805E 4BF9DE24 F8C9D793 EE54BA2B  
MixColumn 2BB739BB 7CFF79B2 EF802A30 AAB8A891  
KeyAddition 9E1E0B31 5A87DFF5 77B10819 85D4D122

Round = 6

Substitution 0B722BC7 BE179EE6 F5C830D4 97483E93  
ShiftRow 0B173093 BEC83EC7 F5482BE6 97729ED4  
MixColumn 8CE6D207 DDB058BA E4FEDAB0 E91EA5FD  
KeyAddition 0DCA53AA 076F1000 C0C8D042 13A61199

Round = 7

Substitution D774EDAC C5A8CA63 BAE8702C 7D2482EE  
ShiftRow D7A870EE C5E882AC BA24ED63 7D74CA2C

MixColumn C8E2B67D 9C3FDD7D 8DBDFADA 80FCF261  
KeyAddition 502709B4 2282C4F3 AB31C17D 891CB075

Round = 8

Substitution 53CC018D 93131C0D 62C778FF A79CE79D  
ShiftRow 5313789D 93C7E78D 629C010D A7CC1CFF  
MixColumn 76600CBF 05B90D8F 774FEB21 F9FF49C7  
KeyAddition 1E607713 B7663E99 E1A6D2C5 95AEC447

Round = 9

Substitution 72D0F57D A933B2EE F824B5A6 2AE41CA0  
ShiftRow 7233B5A0 A9241C7D F8E4F5EE 2AD0B2A6  
MixColumn A470CB4B 44B83222 C7C1C4C5 2BFA744B  
KeyAddition 6C64294F 3211C9A8 97E404E8 723FF672

Round = 10

Substitution 5043A584 2382DDC2 8869F29B 40754240  
ShiftRow 5082F240 23694284 8875A5C2 4043DD9B  
MixColumn 8F02ED00 3BB3595D F354F1CC 03211473  
KeyAddition 51118467 577F032C 09719259 9555FA66

Round = 11

Substitution D1825F85 5BD27B71 01A34FCB 2AFC2D33  
ShiftRow D1D24F33 5BA32D85 01FC5F71 2A827BCB  
MixColumn A88CC893 E0F43672 3372D042 7973180A  
KeyAddition F00A02CE CEDB07A5 4D7821B8 5EBC6BC9

Round = 12

Substitution 8C67778B 8BB9C506 E3BCFD6C 58657FDD  
ShiftRow 8CB9FDDD 8BBC7F8B E3657706 5867C56C  
MixColumn F324A86A 26E24F48 03B66220 B0AE1A92  
KeyAddition 87B8EFC1 3EB25292 E1C31C6F C4AF8AC8

Round = 13

Substitution 176CDF78 B237004F F82E9CA8 1C797EE8  
ShiftRow 17379CE8 B22E7E78 F879DF4F 1C6C00A8  
MixColumn 032E2059 0B14E86D F03FF52B 246C9303  
KeyAddition C9D48ABA EFC17359 6AE09FE5 997C8A0E

Substitution DD487EF4 DF788FCB 02E1DBD9 EE107EAB  
ShiftRow DD78DBAB DFE17EF4 02107ECB EE488FD9  
KeyAddition 23304B7A 39F9F3FF 067D8D8F 9E24ECC7

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

KeyAddition 0DA6416C 53CA2D37 0226A93A 4DDDE2E6  
Substitution F3C5F8B8 5010FAB2 6A23B7A2 65C93BF5  
ShiftRow F3C9B7B2 50C53BA2 6A10F8F5 6523FAB8

Round = 13

KeyAddition 39331D51 B410A096 F0CF923B D833E3B5  
InvMixColumn FD8C5552 D92BF292 57C20201 DB848163  
Substitution 2178ED48 E50B0474 DAA86A09 9F4F9100  
ShiftRow 214F6A74 E5789109 DA0BED00 9FA80448

Round = 12

KeyAddition 55D32DDF FD288CD3 387E934F EBA99412  
InvMixColumn 40FDD019 250C5BF8 085D8C43 36B7DA9F  
Substitution 7221608E C28157E1 BF8DF064 24207A6E  
ShiftRow 7220F0E1 C2217A64 BF81606E 248D578E

Round = 11

KeyAddition 2AA63ABC EC0E4BB3 C18B9194 0342244D  
InvMixColumn 33B737B9 538CC005 0FC2C143 6EC1199E  
Substitution 6620B2DB 50F01F36 FBA8DD64 45DD8EDF  
ShiftRow 66DDDD36 50208E64 FBF0B2DF 45A81FDB

Round = 10

KeyAddition B8CEB451 3CECD415 01D5D14A D3DCF1CE  
InvMixColumn 031732B5 93CC5917 DE969097 EE65AC17  
Substitution D587A1D2 22271587 9C359685 99BCAA87  
ShiftRow D5BC9687 2287AA85 9C27A187 993515D2

Round = 9

KeyAddition 1DA87483 542E510F CC0261AA C0F097EB  
InvMixColumn B7C35A6C AB4BE622 E47F43DD FD4832CB  
Substitution 203346B8 0ECCF594 AE6B64C9 21D4A159

ShiftRow 20D46494 0E33A1C9 AECC4659 216BF5B8

Round = 8

KeyAddition 48D41F38 BCEC92DF 38257FBD 4D3A7838

InvMixColumn 38D00251 51294520 78BA9A87 E322B84E

Substitution 76606A70 704C6854 C1C037EA 4D949AB6

ShiftRow 76943754 70609AEA C14C6AB6 4DC06870

Round = 7

KeyAddition EE51889D CEDD8364 E7C05111 44202A64

InvMixColumn 8568ACEB D2A66CEC 35E24DFD 4E5E744E

Substitution 67F7AA3C 7FC5B883 D93B6521 B69DCAB6

ShiftRow 679D6583 7FF7CA21 D9C5AAB6 B63BB83C

Round = 6

KeyAddition E6B1E42E A528829B FDF3A044 4C830C58

InvMixColumn 59487AF6 60C57445 7544E73C FDE8901E

Substitution 15D4BDD6 9007CA68 3F86B06D 21C896E9

ShiftRow 15C8B068 90D4966D 3F07BDE9 2186CAD6

Round = 5

KeyAddition A06182E2 B6AC302A A7369FC0 0EEAB365

InvMixColumn 6F581482 ACA12A27 9A6E251F A6EB7F00

Substitution 065E9B11 AAF1953D 3745C2CB C53C6B52

ShiftRow 063CC23D AA5E6BCB 37F19B52 C5459511

Round = 4

KeyAddition D3A62E85 F1ADA2DC C918D91A 1BCB2B87

InvMixColumn 9455CED1 37452070 B20B862D D18A193E

Substitution E7EDEC51 B26854D0 3E9EDCFA 51CF8ED1

ShiftRow E7CFDCD0 B2ED8EFA 3E68ECD1 519E5451

Round = 3

KeyAddition 4F7F40CA 213C1A37 802168BF E6C30FCB

InvMixColumn 0EFE6E24 5CF7079C BF16BB64 8DC8BD19

Substitution D70C45A6 A726381C F4FFFE8C B4B1CD8E

ShiftRow D7B1FE1C A70CCD8C F426458E B4FF38A6

Round = 2

KeyAddition 4C12AA0D 2965E823 513CCED1 9498C478

InvMixColumn 35753A83 4BB49FE7 0E95759C 90CABB51

Substitution D93FA241 CCC66EB0 D7AD3F1C 9610FE70

ShiftRow D9103FB0 CC3FFE1C D7C6A270 96AD6E41

Round = 1

KeyAddition C62513B7 F75EF6CB FA5EB2D3 9FB9B1B5

InvMixColumn 2B7E7062 E22FD089 2528FC34 42B028F8

Substitution 0B8AD0AB 3B4E60F2 C2EE5528 F6FCEEE1

ShiftRow 0BFC55F2 3B8AEE28 C24ED0E1 F6EE60AB

KeyAddition 6BC1BEE2 2E409F96 E93D7E11 7393172A

KeyAddition A7545BC1 3208602D D836540E 415A4B6E

Substitution 89FD57DD A1BF90FA 2D24FDD7 F846CC45

ShiftRow 8946FDFA A1FDCCD7 2DBF5745 F82490DD

Round = 13

KeyAddition	43BC5719	452857E3	B7603D8B	453489D0
InvMixColumn	B89DD541	9C9C27FE	581F1036	C99B552F
Substitution	9A75B5F8	1C1C3D0C	5ECB7C24	12E8ED4E
ShiftRow	9AE87C0C	1C75ED24	5E1CB54E	12CB3DF8

Round = 12

KeyAddition	EE743BA7	0425F0FE	BC69CB01	66CAADA2
InvMixColumn	8EBD5762	F7995D1C	2D6A643C	E8737E46
Substitution	E6CDDAAB	26F98DC4	FA588C6D	C88F8A98
ShiftRow	E68F8CC4	26CD8A6D	FAF9DA98	C8588DAB

Round = 11

KeyAddition	BE094699	08E2BBBA	84F32B62	EF97FE68
InvMixColumn	03E42BA4	CFD9B14C	35FFE612	844B5273
Substitution	D5AE0B1D	5FE5565D	D97DF539	4FCC488F
ShiftRow	D5CCF55D	5FAE4839	D9E50B8F	4F7D561D

Round = 10

KeyAddition	0BDF9C3A	33621248	23C0681A	D909B808
InvMixColumn	1D2F6E2E	46797145	BCBBCE58	B03911F8
Substitution	DE4E45C3	98AF2C68	78FEEC5E	FC5BE3E1
ShiftRow	DE5BEC68	984EE35E	78AF45E1	FCFE2CC3

Round = 9

KeyAddition	164F0E6C	EEE718D4	288A85CC	A53BAEFA
InvMixColumn	3CB952EC	BE79D9DB	076567EE	6EE3EAAD
Substitution	6DDB4883	5AAFE59F	38BC0A99	454DBB18
ShiftRow	6D4D0A9F	5ADBBB99	38AF4818	45BCE583

Round = 8

KeyAddition	054D7133	E804888F	AE4671FC	29ED6803
InvMixColumn	048C64E6	42EFEDA9	549641E6	05C90162
Substitution	30F08CF5	F66161B7	FD35F8F5	361209AB
ShiftRow	3012F8B7	F6F009F5	FD618CAB	363561F5

Round = 7

KeyAddition	A8D7477E	484D107B	DBEDB70C	3FD523E1
InvMixColumn	873EE41B	0A1C8EF6	9579F899	F381BFE5
Substitution	EAD1AE44	A3C4E6D6	ADAFE1F9	7E91F42A
ShiftRow	EA91E1D6	A3D1F4F9	ADC4AE2A	7EAFE644

Round = 6

KeyAddition	6BBD607B	790EBC43	89F2A4D8	84175220
InvMixColumn	0FD68591	0AFAC4BC	F4C9D7ED	64E96B07
Substitution	FB4A67AC	A3148878	BA120D53	8CEB0538
ShiftRow	FBEB0D78	A34A0553	BA146738	8C1288AC

Round = 5

KeyAddition	4E423FF2	8532A314	22254511	A37EF11F
InvMixColumn	1ADDF2F4	68934EB5	56C8975A	E154D553
Substitution	43C904BA	F722B6D2	B9B18546	E0FDB550
ShiftRow	43FD85D2	F7C9B546	B9220450	E0B1B6BA

Round = 4

KeyAddition 9667696A AC3A7C51 47CB4618 3E3F082C  
InvMixColumn 9D6C9D9E E2155F13 58B3E6DF F20B8E52  
Substitution 75B875DF 3B2F8482 5E4BF5EF 049EE648  
ShiftRow 759EF582 3BB8E6EF 5E2F7548 044B84DF

Round = 3

KeyAddition DD2E6998 A8697222 E066F126 B316DF45  
InvMixColumn D45C64EE 011DE26F 5CA7EF45 95148739  
Substitution 19A78C99 09DE3B06 A7896168 AD9BEA5B  
ShiftRow 199B6106 09A7EA68 A7DE8C5B AD893B99

Round = 2

KeyAddition 82383517 87CECF7 02C40704 8DEEC747  
InvMixColumn 33AAFAE 51979B1C 36C3A292 C29455E0  
Substitution 66621BBE 7085E8C4 24331A74 A8E7EDA0  
ShiftRow 66E71AC4 7062ED74 24851BA0 A833E8BE

Round = 1

KeyAddition 79D236C3 4B03E5A3 091D0B03 A127374A  
InvMixColumn 8BDD7870 2B1C99A0 D5B5EF93 BACAC14A  
Substitution CEC9C1D0 0BC4F947 B5D26122 C010DD5C  
ShiftRow CE106147 0BC9DD22 B5C4C15C C0D2F9D0

KeyAddition AE2D8A57 1E03AC9C 9EB76FAC 45AF8E51

KeyAddition 48A5B168 7ABE79F2 F53E14F5 CEC38E03

Substitution D42956F7 BD5AAF04 77D19B77 EC33E6D5

ShiftRow D4339B04 BD29E677 775A56D5 ECD1AFF7

Round = 13

KeyAddition 1EC931E7 59FC7D43 ED853C1B 51C1B6FA  
InvMixColumn 1E9333BF B700BE92 55A31AA3 BDA5F93D  
Substitution E92266F4 20525A74 ED714371 CD29698B  
ShiftRow E9294374 20226971 ED52668B CD715AF4

Round = 12

KeyAddition 9DB504DF 387274AB 0F2718C4 B970CAAE  
InvMixColumn B555D1C2 D666AB8E 16EDF2FD 55F86767  
Substitution D2ED51A8 4AD30EE6 FF530421 EDE10A0A  
ShiftRow D2E104E6 4AED0A21 FFD3510A ED530EA8

Round = 11

KeyAddition 8A67CEBB 64C23BF6 81D9A0F0 CA9C7D6B  
InvMixColumn 74471BB0 4AE5C307 FDC7CCFE FAC2CDB5  
Substitution CA1644FC 5C2A3338 2131270C 14A880D2  
ShiftRow CAA82738 5C16800C 212A44D2 143133FC

Round = 10

KeyAddition 14BB4E5F 30DADA7D DB0F2747 8245DDE9  
InvMixColumn 1BCE264D 6963195E D607593C 5AC2F893  
Substitution 44EC2365 E4008E9D 4A38156D 46A8E122  
ShiftRow 44A8159D E4ECE16D 4A002322 46388E65

Round = 9

KeyAddition 8CBCF799 92451AE7 1A25E30F 1FFD0C5C

InvMixColumn	832644BF	50248CD2	BC0BF89C	D9E3B53D
Substitution	412386F4	6CA6F07F	789EE11C	E54DD28B
ShiftRow	414DE17F	6C23D21C	78A6868B	E59EF0F4
Round = 8				
KeyAddition	294D9AD3	DEFCE10A	EE4FBF6F	89CF7D74
InvMixColumn	45E8AC2C	BDE80B97	3CE08F22	F96B934E
Substitution	68C8AA42	CDC89E85	6DA07394	690522B6
ShiftRow	68057385	CDC82294	6DC8AAB6	69A09E42
Round = 7				
KeyAddition	F0C0CC4C	73753B1A	4B449111	6040DC56
InvMixColumn	2799606E	404A466B	8B215471	6BB698EF
Substitution	3DF99045	725C9805	CE7BFD2C	0579E261
ShiftRow	3D79FD05	72F9E22C	CE5C9061	057B9845
Round = 6				
KeyAddition	BC557CA8	A826AA96	EA6A9A93	FFC32C21
InvMixColumn	96102C97	F2868F49	87F5FE05	4401F581
Substitution	357C4285	04DC73A4	EA770C36	86097791
ShiftRow	35090CA4	047C7736	EADC4291	86777385
Round = 5				
KeyAddition	80A03E2E	2204D171	72ED60B8	A91B0A36
InvMixColumn	A5227BCC	55A0B1C2	56EACA31	FE1F5A35
Substitution	29940327	ED4756A8	B9BB102E	0CCB46D9
ShiftRow	29CB10A8	ED94462E	B94703D9	0CBB5627
Round = 4				
KeyAddition	FC51FC10	B6678F39	47AE4191	D235E8B1
InvMixColumn	C27040B3	99BD6E2D	7C7D0830	D68B8B68
Substitution	A8D0724B	F9CD45FA	0113BF08	4ACECEF7
ShiftRow	A8CEBFFA	F9D0CE08	01CD72F7	4A13454B
Round = 3				
KeyAddition	007E23E0	6A015AC5	BF84F699	FD4E1ED1
InvMixColumn	52A81057	699FAAA8	34D6D563	90158B72
Substitution	486F7CDA	E46E626F	284AB500	962FCE1E
ShiftRow	482FB56F	E46FCE00	286E7C1E	964A62DA
Round = 2				
KeyAddition	D38CE17E	6A06EBAF	8D74F741	B62D9E04
InvMixColumn	3F299640	F32622DF	96BC7217	32FD18D6
Substitution	254C3572	7E2394EF	35781E87	A121344A
ShiftRow	25211EEF	7E4C3487	3523354A	A1789472
Round = 1				
KeyAddition	3A1432E8	452D3C50	18BB25E9	A86C4B86
InvMixColumn	5390A89F	4EC43FB1	8BF56879	DBE62A1E
Substitution	50966F6E	B6882556	CE77F7AF	9FF595E9
ShiftRow	50F5F756	B69695AF	CE886FE9	9F77256E
KeyAddition	30C81C46	A35CE411	E5FBC119	1A0A52EF
KeyAddition	DD78DBAB	DFE17EF4	02107ECB	EE488FD9

Substitution	C9C19F0E	EFE08ABA	6A7C8A59	99D473E5
ShiftRow	C9D48ABA	EFC17359	6AE09FE5	997C8A0E
Round = 13				
KeyAddition	032E2059	0B14E86D	F03FF52B	246C9303
InvMixColumn	17379CE8	B22E7E78	F879DF4F	1C6C00A8
Substitution	87B21CC8	3EC38AC1	E1AFEF92	C4B8526F
ShiftRow	87B8EFC1	3EB25292	E1C31C6F	C4AF8AC8
Round = 12				
KeyAddition	F324A86A	26E24F48	03B66220	B0AE1A92
InvMixColumn	8CB9FDDD	8BBC7F8B	E3657706	5867C56C
Substitution	F0DB21C9	CE786BCE	4DBC02A5	5E0A07B8
ShiftRow	F00A02CE	CEDB07A5	4D7821B8	5EBC6BC9
Round = 11				
KeyAddition	A88CC893	E0F43672	3372D042	7973180A
InvMixColumn	D1D24F33	5BA32D85	01FC5F71	2A827BCB
Substitution	517F9266	5771FA67	0955842C	95110359
ShiftRow	51118467	577F032C	09719259	9555FA66
Round = 10				
KeyAddition	8F02ED00	3BB3595D	F354F1CC	03211473
InvMixColumn	5082F240	23694284	8875A5C2	4043DD9B
Substitution	6C110472	32E4F64F	973F29A8	7264C9E8
ShiftRow	6C64294F	3211C9A8	97E404E8	723FF672
Round = 9				
KeyAddition	A470CB4B	44B83222	C7C1C4C5	2BFA744B
InvMixColumn	7233B5A0	A9241C7D	F8E4F5EE	2AD0B2A6
Substitution	1E66D247	B7A6C413	E1AE7799	95603EC5
ShiftRow	1E607713	B7663E99	E1A6D2C5	95AEC447
Round = 8				
KeyAddition	76600CBF	05B90D8F	774FEB21	F9FF49C7
InvMixColumn	5313789D	93C7E78D	629C010D	A7CC1CFF
Substitution	5082C175	2231B0B4	AB1C09F3	8927C47D
ShiftRow	502709B4	2282C4F3	AB31C17D	891CB075
Round = 7				
KeyAddition	C8E2B67D	9C3FDD7D	8DBDFADA	80FCF261
InvMixColumn	D7A870EE	C5E882AC	BA24ED63	7D74CA2C
Substitution	0D6FD099	07C811AA	C0A65300	13CA1042
ShiftRow	0DCA53AA	076F1000	C0C8D042	13A61199
Round = 6				
KeyAddition	8CE6D207	DDB058BA	E4FEDAB0	E91EA5FD
InvMixColumn	0B173093	BEC83EC7	F5482BE6	97729ED4
Substitution	9E870822	5AB1D131	77D40BF5	851EDF19
ShiftRow	9E1E0B31	5A87DFF5	77B10819	85D4D122
Round = 5				
KeyAddition	2BB739BB	7CFF79B2	EF802A30	AAB8A891
InvMixColumn	AE6E805E	4BF9DE24	F8C9D793	EE54BA2B
Substitution	BE453A9D	CC699CA6	E1120D22	99FDC00B

```
ShiftRow      BEFD0DA6 CC45C022 E1693A0B 99129C9D
Round = 4
KeyAddition   6B67E11E 97B60935 1F807843 479C220B
InvMixColumn  47A53021 6E1CCAA5 4EB97A29 46B2DCDA
Substitution  1629087B 45C41029 B6DBBD4C 983E937A
ShiftRow      163EBD29 4529934C B6C4087A 98DB107B
Round = 3
KeyAddition   BE8E2133 D6F80781 088D8C14 2F864BE1
InvMixColumn  BD2066D9 7C7DE64F CA28748B F69B94FA
Substitution  CD54D3E5 0113F592 10EECACE D6E8E714
ShiftRow      CDE8CA92 0154E7CE 1013D314 D6EEF5E5
Round = 2
KeyAddition   564B9E83 8F3DC261 B509584B F689093B
InvMixColumn  61F7A93F 462A2954 EF18471F CA7FAF57
Substitution  D826B725 98954CFD 613416CB 106B1BDA
ShiftRow      D86B16FD 98261BCB 6195B7DA 10344C25
Round = 1
KeyAddition   C75E3AFA A347131C 4C0DA779 192093D1
InvMixColumn  9097DF81 746A09FC 44828AD3 FB3A873D
Substitution  9685EF91 CA584055 8611CFA9 63A2EA8B
ShiftRow      96A2CF55 CA85EAA9 8658EF8B 63114091
KeyAddition   F69F2445 DF4F9B17 AD2B417B E66C3710
```

Plaintext is

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

\*\*\*\*\*