

#####

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

```
