

#####

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

```
