

#####

## 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	87CECFC7	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	BEB9EAEE	077952AD	6E65D9EC
ShiftRow	3CB952EC	BE79D9DB	076567EE	6EE3EAAD
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 0BF55F2 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	42EFEFA9	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
```

\*\*\*\*\*