

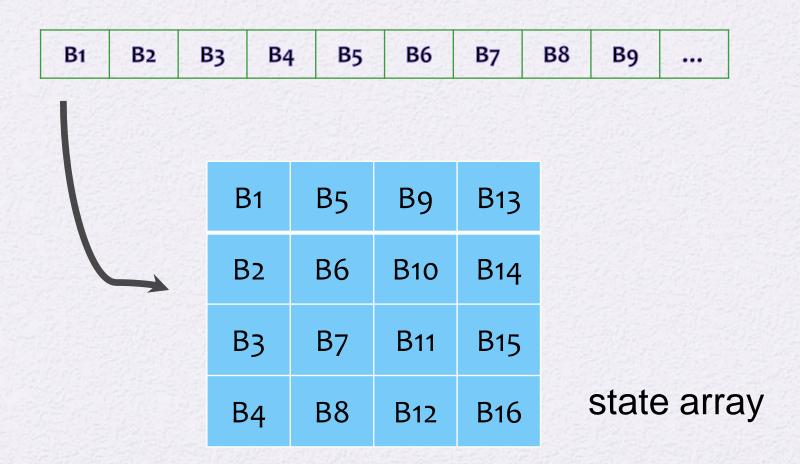
Chapter 6

Advanced Encryption Standard

AES Parameters

Key Size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext Block Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of Rounds	10	12	14
Round Key Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded Key Size (words/bytes)	44/176	52/208	60/240

AES Data Structure



AES arithmetic: Finite Field

- Byte operation: $GF(2^8)/x^8+x^4+x^3+x+1$
- Column/word (4 bytes) operation:
 GF(2^{8x4})/x⁸+x⁴+x³+x+1, 01_Hy⁴+01_H
 - $2Ay^3 + B5y^2 + 7Fy + 3E$

3E 7F

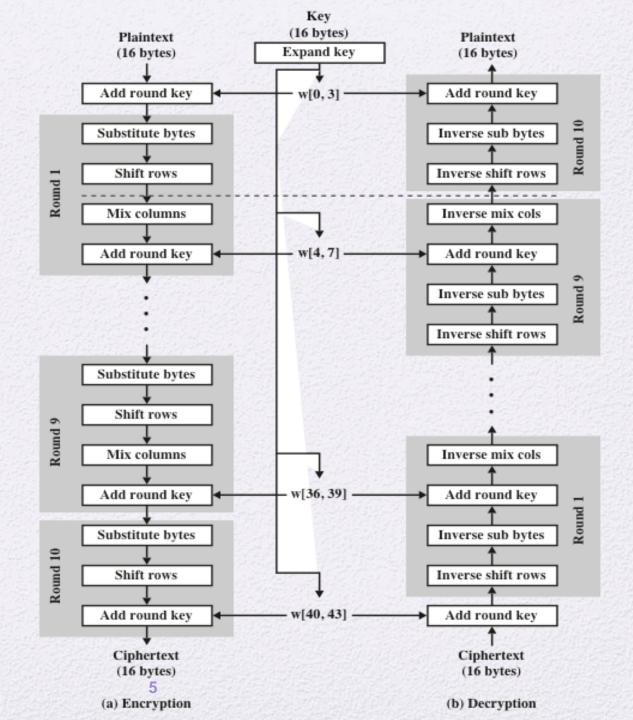
B5 Word

2A

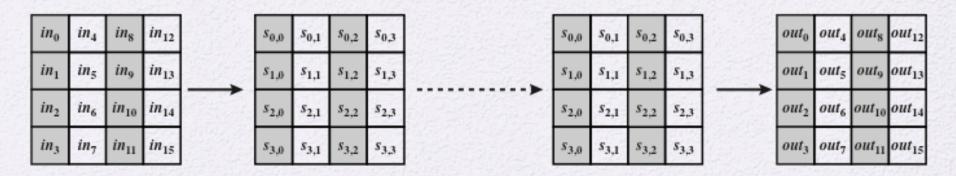
Enc/Dec:

- Key: 16 bytes
- Plaintext: 16 bytes
- Round: 10
- Subkeys: 11

A substitution and permutation network



Data flow



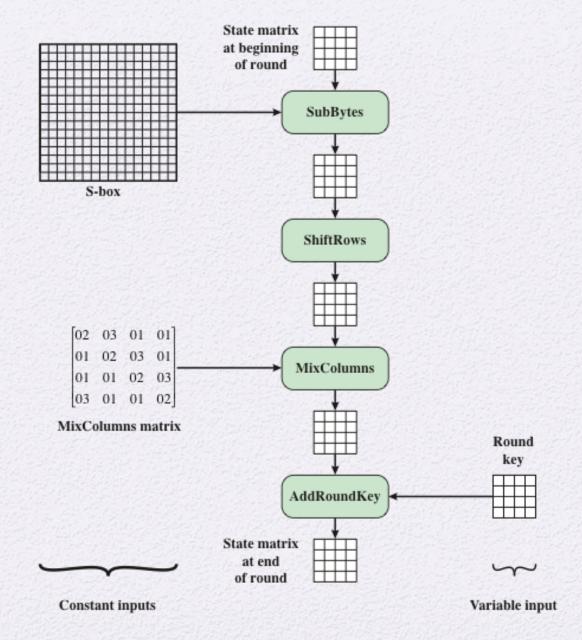
(a) Input, state array, and output



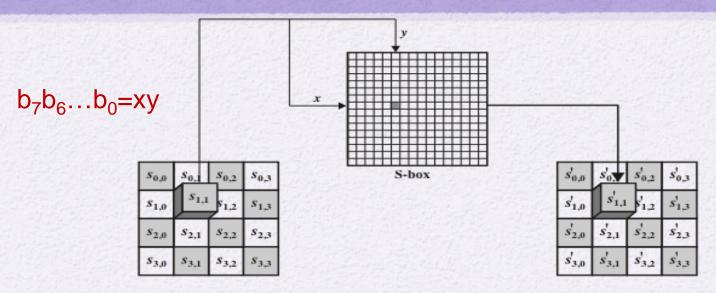
Four functions

- SubBytes use an S-box to perform a byteby-byte substitution
- ShiftRows simple row permutation
- MixColumns a substitution that mixes the bytes in a column
- AddRoundKey simple bitwise XOR of the current state with the subkey

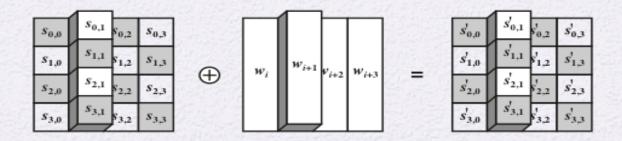
Single round



SubByte and AddRoundKey



(a) Substitute byte transformation



(b) Add round key Transformation

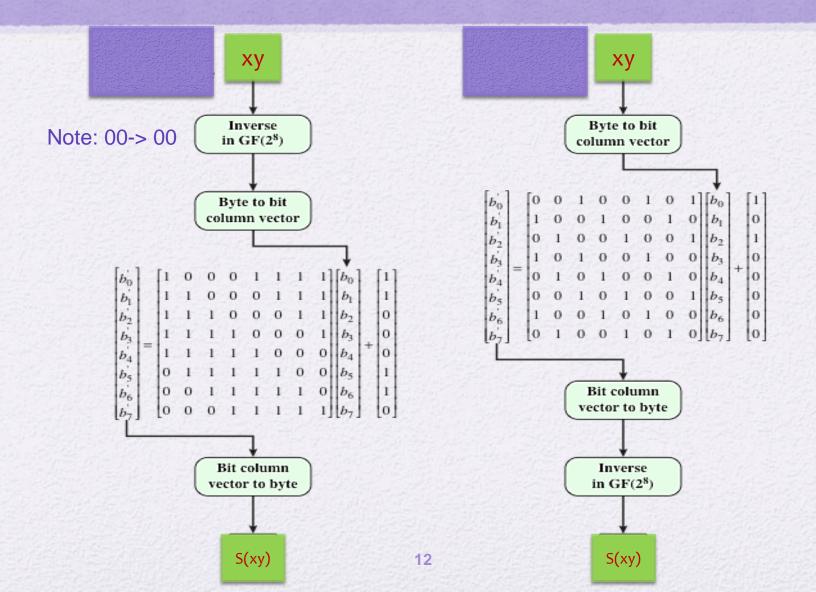
S-box: 8 bits→8bits

									J	,							
		0	1	2	3	4	5	6	7	8	9	A	В	C	D	Е	F
	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C 0
	2	В7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	В3	29	E3	2F	84
300	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
x	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	В	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
1	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	Е	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Inverse S-box

				5.5						y							
		0	1	2	3	4	5	6	7	8	9	Α	В	С	D	Е	F
783	0	52	09	6A	D5	30	36	A5	38	BF	40	A3	9E	81	F3	D7	FB
	1	7C	E3	39	82	9B	2F	FF	87	34	8E	43	44	C4	DE	E9	СВ
	2	54	7B	94	32	A6	C2	23	3D	EE	4C	95	0B	42	FA	C3	4E
	3	08	2E	A1	66	28	D9	24	B2	76	5B	A2	49	6D	8B	D1	25
	4	72	F8	F6	64	86	68	98	16	D4	A4	5C	CC	5D	65	В6	92
5277	5	6C	70	48	50	FD	ED	В9	DA	5E	15	46	57	A7	8D	9D	84
	6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	В8	В3	45	06
x	7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
	8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
100	9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
	A	47	F1	1A	71	1D	29	C5	89	6F	В7	62	0E	AA	18	BE	1B
	В	FC	56	3E	4B	C6	D2	79	20	9A	DB	C 0	FE	78	CD	5A	F4
	C	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
1500	D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
	Е	A0	E0	3B	4D	AE	2A	F5	В0	C8	EB	BB	3C	83	53	99	61
	F	17	2B	04	7E	BA	77	D6	26	E1	69	14	63	55	21	0C	7D

S-box Construction

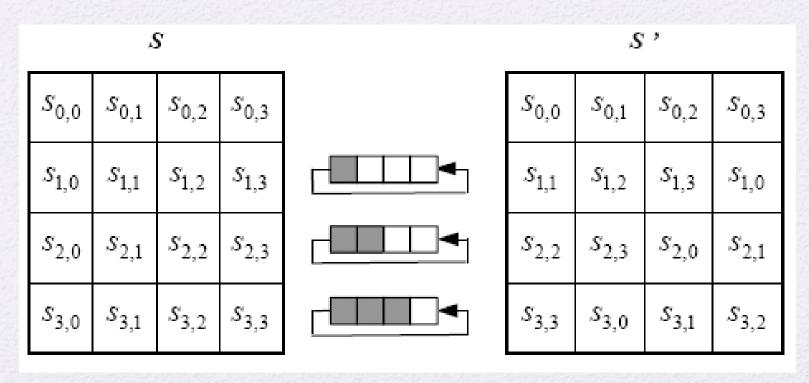


S-Box Rationale

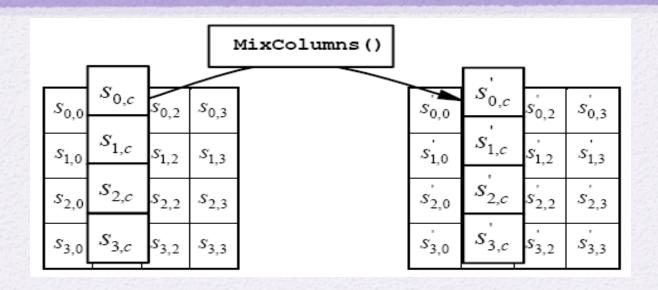
- Design for being resistant to known cryptanalytic attacks, linear and differential analysis
 - A low correlation between input bits and output bits
 - The output bits are not a linear function of the input bits
 - The nonlinearity is due to the use of the multiplicative inverse

ShiftRows

 Eensure that the 4 bytes of one column are spread out to four different columns



MixColumns



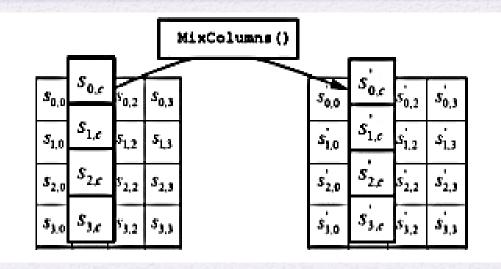
•
$$s'_{3,c}y^3 + s'_{2,c}y^2 + s'_{1,c}y + s'_{0,c}$$

= $(\{(s_{3,c}y^3 + s_{2,c}y^2 + s_{1,c}y + s_{0,c}) \times (\{03\}y^3 + \{01\}y^2 + \{01\}y + \{02\}) \mod \{01\}y^4 + \{$

Coefficient (byte) operation: GF(28)/x8+x4+x3+x+1

MixColumns: Computation

$$\begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$



$$s'_{0,c} = (\{02\} \bullet s_{0,c}) \oplus (\{03\} \bullet s_{1,c}) \oplus s_{2,c} \oplus s_{3,c}$$

$$s'_{1,c} = s_{0,c} \oplus (\{02\} \bullet s_{1,c}) \oplus (\{03\} \bullet s_{2,c}) \oplus s_{3,c}$$

$$s'_{2,c} = s_{0,c} \oplus s_{1,c} \oplus (\{02\} \bullet s_{2,c}) \oplus (\{03\} \bullet s_{3,c})$$

$$s'_{3,c} = (\{03\} \bullet s_{0,c}) \oplus s_{1,c} \oplus s_{2,c} \oplus (\{02\} \bullet s_{3,c})$$

- Two lookup tables:{02}•{x} and {03}•{x}
- 8 table lookups
- 12 xor operations

MixColumns: Speedup

- Temp = $s_{0,c} \oplus s_{1,c} \oplus s_{2,c} \oplus s_{3,c}$
- $s_{o,c}' = \text{temp} \oplus s_{o,c} \oplus \{o2\}*(s_{o,c} \oplus s_{1,c})$
- $s_{1,c}' = \text{temp} \oplus s_{1,c} \oplus \{02\} * (s_{1,c} \oplus s_{2,c})$
- $s_{2,c}' = \text{temp} \oplus s_{2,c} \oplus \{02\} * (s_{2,c} \oplus s_{3,c})$
- $s_{3,c}' = \text{temp} \oplus s_{3,c} \oplus \{02\} * (s_{3,c} \oplus s_{0,c})$
- Computation
 - 1 lookup table: {02}{x}
 - 4 table lookups
 - 12 xor operations

InvMixColumns

• $(s_{3,c}y^3+s_{2,c}y^2+s_{1,c}y+s_{0,c}) \times (\{03\}y^3+\{01\}y^2+\{01\}y+\{02\})^{-1}$ mod $\{01\}y^4+\{01\}$

$$\begin{bmatrix}
S'_{0,c} \\
S'_{1,c} \\
S'_{2,c} \\
S'_{3,c}
\end{bmatrix} = \begin{bmatrix}
0E & 0B & 0D & 09 \\
09 & 0E & 0B & 0D \\
0D & 09 & 0E & 0B \\
0B & 0D & 09 & 0E
\end{bmatrix} \begin{bmatrix}
S_{0,c} \\
S_{1,c} \\
S_{2,c} \\
S_{3,c}
\end{bmatrix}$$

M

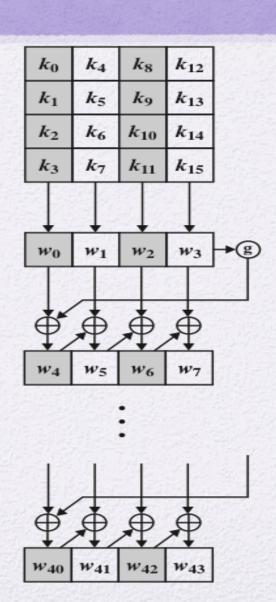
InvMixColumns: Speedup

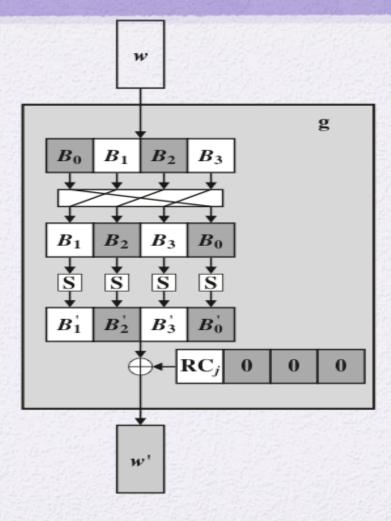
$$\begin{split} & \text{Tmp} = \ 09 * (\ s_{0,j} \oplus s_{1,j} \oplus s_{2,j} \oplus s_{3,j}) \\ & s'_{0,j} = & s_{0,j} \oplus \text{Tmp} \oplus 2 * [2 * (s_{0,j} \oplus s_{2,j})] \oplus 2 * [(s_{0,j} \oplus s_{1,j})] \\ & s'_{1,j} = & s_{1,j} \oplus \text{Tmp} \oplus 2 * [2 * (s_{1,j} \oplus s_{3,j})] \oplus 2 * [(s_{1,j} \oplus s_{2,j})] \\ & s'_{2,j} = & s_{2,j} \oplus \text{Tmp} \oplus 2 * [2 * (s_{0,j} \oplus s_{2,j})] \oplus 2 * [(s_{2,j} \oplus s_{3,j})] \\ & s'_{3,j} = & s_{3,j} \oplus \text{Tmp} \oplus 2 * [2 * (s_{1,j} \oplus s_{3,j})] \oplus 2 * [(s_{3,j} \oplus s_{0,j})] \\ \end{split}$$

MixColumns Rationale

- Coefficients of matrices uses a linear code with maximal distance between codewords.
- Ensure a good mixing among the bytes of each column
- MixColumns combined with ShiftRows ensure that all output bits depend on all input bits after a few rounds (fast avalanche effect)

Key Expansion





(b) Function g

Key Expansion Rationale

- Resistance to known cryptanalytic attacks
- Round constant eliminates the symmetry between round keys in different rounds
- Diffusion of cipher key differences into the round keys
- Enough nonlinearity to prohibit the full determination of round key differences from cipher key differences

Key Expansion Example

Key Words	Auxiliary Function
w0 = 0f 15 71 c9	RotWord(w3) = 7f 67 98 af = x1
w1 = 47 d9 e8 59	SubWord(x1) = d2 85 46 79 = y1
w2 = 0c b7 ad d6	Rcon(1) = 01 00 00 00
w3 = af 7f 67 98	$y1 \oplus Rcon(1) = d3 \ 85 \ 46 \ 79 = z1$
$w4 = w0 \oplus z1 = dc \ 90 \ 37 \ b0$	RotWord(w7) = 81 15 a7 38 = $x2$
$w5 = w4 \oplus w1 = 9b \ 49 \ df \ e9$	SubWord($x4$) = 0c 59 5c 07 = y2
$w6 = w5 \oplus w2 = 97 \text{ fe } 72 \text{ 3f}$	Rcon(2) = 02 00 00 00
$w7 = w6 \oplus w3 = 38 \ 81 \ 15 \ a7$	$y2 \oplus Rcon(2) = 0e 59 5c 07 = z2$
$w8 = w4 \oplus z2 = d2 c9 6b b7$	RotWord(w11)= ff d3 c6 e6 = x3
$w9 = w8 \oplus w5 = 49 \ 80 \ b4 \ 5e$	SubWord(x2)= 16 66 b4 8e = y3
$w10 = w9 \oplus w6 = de 7e c6 61$	Rcon(3) = 04 00 00 00
$w11 = w10 \oplus w7 = e6 \text{ ff d3 c6}$	$y3 \oplus Rcon(3) = 12 66 b4 8e = z3$
$w12 = w8 \oplus z3 = c0 \text{ af df } 39$	RotWord(w15) = ae 7e c0 b1 = x4
$w13 = w12 \oplus w9 = 89 2f 6b 67$	SubWord(x3)= $e4$ f3 ba $c8 = y4$
$w14 = w13 \oplus w10 = 57 51 ad 06$	Rcon(4) = 08 00 00 00
$w15 = w14 \oplus w11 = b1$ ae 7e c0	$y4 \oplus Rcon(4) = ec f3 ba c8 = 4$
$w16 = w12 \oplus z4 = 2c \ 5c \ 65 \ f1$	RotWord(w19) = 8c dd 50 43 = x5
$w17 = w16 \oplus w13 = a5 73 0e 96$	SubWord(x4) = 64 c1 53 1a = y5
$w18 = w17 \oplus w14 = f2 22 a3 90$	Rcon(5) = 10 00 00 00
$w19 = w18 \oplus w15 = 43 \ 8c \ dd \ 50$	y5 ⊕ Rcon(5) = 74 c1 53 1a = z5
$w20 = w16 \oplus z5 = 58 \text{ 9d } 36 \text{ eb}$	RotWord(w23) = $40 \ 46 \ bd \ 4c = x6$
$w21 = w20 \oplus w17 = fd \text{ ee } 38 \text{ 7d}$	SubWord(x5)= 09 5a 7a 29 = y6
$w22 = w21 \oplus w18 = 0f cc 9b ed$	Rcon(6) = 20 00 00 00
$w23 = w22 \oplus w19 = 4c \ 40 \ 46 \ bd$	y6 ⊕ Rcon(6)= 29 5a 7a 29 = z6
$w24 = w20 \oplus z6 = 71 c7 4c c2$	RotWord(w27)= a5 a9 ef cf = $x7$
$w25 = w24 \oplus w21 = 8c \ 29 \ 74 \ bf$	SubWord(x6)= 06 d3 df 8a = y7
$w26 = w25 \oplus w22 = 83 \text{ e5 ef } 52$	Rcon(7)= 40 00 00 00 y7 ⊕ Rcon(7)= 46 d3 df 8a = z7
$w27 = w26 \oplus w23 = cf \ a5 \ a9 \ ef$ $w28 = w24 \oplus z7 = 37 \ 14 \ 93 \ 48$	
	RotWord(w31) = 7d a1 4a f7 = $x8$
$w29 = w28 \oplus w25 = bb \ 3d \ e7 \ f7$	SubWord(x7)= ff 32 d6 68 = y8 Rcon(8)= 80 00 00 00
$w30 = w29 \oplus w26 = 38 d8 08 a5$	$y8 \oplus Rcon(8) = 7f 32 d6 68 = z8$
$w31 = w30 \oplus w27 = f7 \ 7d \ a1 \ 4a$ $w32 = w28 \oplus z8 = 48 \ 26 \ 45 \ 20$	RotWord(w35)= be 0b 38 3c = x9
$w32 = w28 \oplus 28 = 48 \ 26 \ 45 \ 20$ $w33 = w32 \oplus w29 = f3 \ 1b \ a2 \ d7$	SubWord(x8) = ae 2b 07 eb = y9
$w33 = w32 \oplus w29 = 13 \text{ 1b az } \alpha7$ $w34 = w33 \oplus w30 = \text{cb c3 aa } 72$	Rcon(9)= 1B 00 00 00
$w34 - w33 \oplus w30 - cb + c3 + aa + 72$ $w35 = w34 \oplus w32 = 3c + be + 0b + 38$	$y9 \oplus Rcon(9) = b5 \ 2b \ 07 \ eb = z9$
$w36 = w32 \oplus z9 = fd \ 0d \ 42 \ cb$	RotWord(w39)= 6b 41 56 f9 = x10
$w37 = w36 \oplus w33 = 0e 16 e0 1c$	SubWord(x9)= 7f 83 b1 99 = y10
$w38 = w37 \oplus w34 = c5 d5 4a 6e$	Rcon(10) = 36 00 00 00
$w39 = w38 \oplus w35 = f9 \ 6b \ 41 \ 56$	$y10 \oplus Rcon(10) = 49 83 b1 99 = z10$
$w40 = w36 \oplus z10 = b4 \ 8e \ f3 \ 52$. ,
$w41 = w40 \oplus w37 = ba 98 13 4e$	
$w42 = w41 \oplus w38 = 7f_0 4d_0 59_0 20$	
$w43 = w42 \oplus w39 = 86 \ 26 \ 18 \ 76$	

AES Example

Plaintext: 012345678abcdeffedcb a987654321

Key: of1571c947d9e859ocb7 add6af7f6798

Ciphertext: ffob844ao853bf7c6934 ab4364148fb9

SubBytes	Start of round After After Round Key								
01 89 fe 76	Start of round				Kouna Key				
23 ab dc 54	01 00 5 76	SubBytes	ShiftRows	MixColumns	0.5 4.7 0 5				
45 cd ba 32									
67 ef 98 10									
0e ce f2 d9 ab 8b 89 35 b9 94 57 75 dc 9b 97 36 72 6b 2b 05 40 7f f1 05 e4 8e 16 51 90 49 fe 38 37 df 72 32 ae b6 4e 8e c4 e2 fc f0 fc 18 3f 47 20 9a f3 7d df 72 ga b0 e9 3f df 72 0 e4 e4 e2 df 70 f6 ba e3 8e 22 db 12 c5 d6 f5 3b b0 e9 3f e2 de 9b e5 51 16 df 80 e7 c1 6b be e6 e6 e7 e7 e8 e8 e7 e2 e7 e6 </td <td></td> <td></td> <td></td> <td></td> <td></td>									
36 72 6b 2b 05 40 7f f1 40 7f f1 05 e4 8e 16 51 90 49 fe 8 34 25 17 55 18 3f f0 fc f0 fc 18 3f 47 20 9a 3f 37 3f 47 21 3e b6 4e 88 e4 4e 2f c4 e4 4e 2f c5 d6 f5 3b b0 e9 3f a 65 0f c0 4d 4d 76 ba e3 4d 76 ba e3 8e 22 db 12 d2 49 de 6 74 c7 e8 d0 92 c6 9b 70 c6 9b 70 92 b2 f2 dc 92 c9 80 7e f1 70 ff e8 2a 51 16 9b e5 9b e5 51 16 df 80 f7 c1 6b b4 c6 6 75 3f ca 9c 9d 75 74 de de 9d 75 74 2d c5 1e 52 b7 5e 61 c 5c 6b 05 f4 4a 7f 6b bf 4a 7f 6b bf b1 c1 0b cc c0 89 57 t 4b 4a 7f 6b bf 4a 7f 6b bf b1 c1 0b cc c0 89 57 t 4b 4a 34 31 12 8d 18 c7 c9 c7 c9 8d 18 f9 1f 6a c3 df 6b ad 71 48 5c 7d a3 5c 4a ff a3 5c 4a ff 4a 4d 2d 2d 2d 5d 6d		-h 0h 00 25	-l- 0l- 00 2F	1-0 04 F7 7F					
34 25 17 55									
ae b6 4e 88 e4 4e 2f c4 c4 e4 4e 2f c5 d6 f5 3b b0 e9 3f a 65 0f c0 4d 4d 76 ba e3 4d 76 ba e3 8e 22 db 12 2d 9 de e 74 c7 e8 d0 92 c6 9b 70 c6 9b 70 92 b2 f2 dc 92 c9 80 7e f 70 ff e8 2a 51 16 9b e5 9b e5 51 16 df 80 f7 c1 6b b4 c6 c 75 3f ca 9c 9c 75 74 de de 9d 75 74 2d c5 1e 52 b7 5e 61 c 5c 6b 05 f4 4a 7f 6b bf 4a 7f 6b bf b1 c1 0b cc c0 89 57 k 7b 72 a2 6d 21 40 3a 3c 40 3a 3c 21 ba f3 8b 07 af 2f 51 a b4 34 31 12 8d 18 c7 c9 c7 c9 8d 18 f9 1f 6a c3 df 6b ad 7 71 48 5c 7d a3 52 4a ff a3 52 4a ff d4 11 e 19 24 5c 39 67 06 a 26 74 c7 bd f7 92 c6 7a c6 7a c7 a 67 af 79 2 cb ab 62 37 5c 73 22 8 6c 7a 67 92 cb ab 62 37 5c 73 22 8 15 48 b4 0c 4c 41 18 d fe 29 41 8d fe 29 2cb 2a 47 c4 48 58 f3 d3 66 57 a 79 2 cb ab 62 37 67 3c 73 22 8 26 74 c7 bd f5 92 5d 67 a c6 7a 6 78 77 9 2 cb ab 62 34									
65 0f c0 4d 4d 76 ba e3 4d 76 ba e3 8e 22 db 12 d2 49 de e6 74 c7 e8 d0 92 c6 9b 70 c6 9b 70 92 b2 f2 dc 92 c9 80 7e f6 70 ff e8 2a 51 16 9b e5 9b e5 51 16 df 80 f7 c1 6b b4 c6 c6 75 3f ca 9c 9d 75 74 de de 9d 75 74 2d c5 1e 52 b7 5e 61 c6 6b 05 f4 4a 7f 6b bf 4a 7f 6b bf b1 c1 0b cc c0 89 57 k7 b7 2a 2 6d 21 40 3a 3c 40 3a 3c 21 ba f3 8b 07 af 2f 51 a b4 34 31 12 8d 18 c7 c9 c7 c9 8d 18 f9 1f 6a c3 df 6b ad 79 ap b7 f9 4 b8 14 d2 22 22 b8 14 d2 1d 19 24 5c 39 67 06 c7 14 48 5c 7d a3 52 4a ff a3 52 4a ff d4 11 fe 0f 2c a5 f2 4c 7d c7 bd f7 92 c6 7a c6 7a f7 92 cb ab 62 37 65 0e a3 c24 7e 22 9c 36 f3 93 de de 36 f3 93 19 b7 07 ec f1 96 90 5 d8 40 0c 4c 41 8d fe 29 41 8d fe 29 2a 47 c4 48 58 fd 0f 46 67 37 24 ff 85 9a 36 16 9a 36 16 85 83 e8 18 ba 3d ee cc 4a ea 5 c1 ea e4 06 78 87 78 87 e4 06 84 18 27 23 a6 38 8b 20 6d 27 e5 6f 4d 6f 4a 72 6f 48 2d 6f 48 2d 72 le d0 20 40 c7 29 e5 6d 28 20 e6 7a c7 6f 36 64 d5 7a 57 6d 36 6f 39 3 de de 36 f3 93 le d0 6d 6d 7a 5f 6d 6d 6d 7a 5f 6d 7a 6d 7a									
74 c7 e8 d0 92 c6 9b 70 c6 9b 70 92 b2 f2 dc 92 c9 80 7e f7 70 ff e8 2a 51 16 9b e5 9b e5 51 16 df 80 f7 c1 6b b4 c6 c 5c 6b 05 f4 4a 7f 6b bf 4a 7f 6b bf b1 c1 0b cc c0 89 57 k 4a 31 12 8d 18 c7 c9 c7 c9 8d 18 f9 1f 6a c3 df 6b ad 6b 4a 7f 6b bf b1 c1 0b cc c0 89 57 k 4a 31 12 8d 18 c7 c9 c7 c9 8d 18 f9 1f 6a c3 df 6b ad 6b 4a 7f 6b bf b1 c1 0b cc c0 89 57 k 4a 7f 9b e5 7f 94 b8 14 d2 22 22 b8 14 d2 1d 19 24 5c 39 67 06 6b 15 dc da a9 59 86 57 d3 86 57 d3 59 3b 44 06 73 5c 73 22 8 d6 7f 92 c6 7a c6 7a f7 92 cb ab 62 37 65 0a 32 47 e2 29 c 36 f3 93 de de 36 f3 93 19 b7 07 ec f1 96 90 5 d8 8b 00 ca 7 a 78 97 ed ab 2d									
70									
75 3f ca 9c 9d 75 74 de de 9d 75 74 2d c5 le 52 b7 5e 61 c5 c6 b0 5f 4 4a 7f 6b bf b1 c1 0b cc c0 89 57 k1 k2 c3 c4 d3 a3 c2 c4 d3 a5 c4 d3 a3 c2 c5 a5 c5 d3 d5 d5 d5 d5 d5 d5 d									
5c 6b 05 f4 4a 7f 6b bf 4a 7f 6b bf bf bl c1 0b cc c0 89 57 ba f3 8b 07 af 2f 51 ag ba f3 8b 07 af 2f 51 ag 6f 6f 6g 6f 6g 6f 6g 6f 6g 6f 6g 6g<									
7b 72 a2 6d 21 40 3a 3c 21 ba f3 8b 07 aff 2f 51 ag 9b 7f 94 ba 18 c7 c9 8d 18 f9 1f 6a 3d df 6b ad 6f 6a 7c c9 8d 18 bd 2c ba 6c 3d 6c 7c c6 7c c6 7c 7c 7c 7c ba de 7c c6 7c 7c 7c 7c ba de 7c ba de 7c ba de de 7c ba de de 7c ba de de 7c ba de 7c ba de de 7c de									
b4 34 31 12 8d 18 c7 c9 c7 c9 8d 18 f9 1f 6a c3 df 6b ad 70 c6 c8 70 c6 c8 70 c6 c6 71 c8 c7 c2 c8 c8 c6 c6<									
9a 9b 7f 94 b8 14 d2 22 22 b8 14 d2 1d 19 24 5c 39 67 06 c 71 48 5c 7d a3 52 4a ff a3 52 4a ff d4 11 fe 0f 2c a5 f2 4 15 dc da a9 59 86 57 d3 86 57 d3 59 d4 40 67 73 5c 73 22 8 26 74 c7 bd f7 92 c6 7a c6 7a f7 92 cb ab 62 37 65 0e a3 c 24 7e 22 9c 36 f3 93 de de 36 f3 93 19 b7 07 ec f1 96 90 5 f8 b4 0c 4c 41 8d fe 29 41 8d fe 29 2a 47 c4 48 58 fd 0f 4 67 37 24 ff 85 9a 36 16 9a 36 16 85 83 e8 18 ba 9d ee cc 4 ae a5 c1 ea e4 06 78 87 78 87 e4 06 84 18 27 23 36 38 9b 4 e8 21 97 bc 9b fd 88 65 65 9b fd 88 eb 10 0a f3 eb 7d ed b 72 ba cb 04 40 f4 1f f2 40 f4 1f f2 7b 05 42 4a 71 8c 83 c 1e 06 d4 fa 72 6f 48 2d 6f 48 2d 72 1e d0 20 40 c7 29 e5 a b2 20 bc 65 37 b7 65 4d 65 4d 37 b7 94 83 18 52 4c 74 ef a d9 f9 c5 e5 35 99 a6 d9 99 a6 d9 35 0c 50 53 c7 14 3d 86 7 d8 f7 f7 fb 61 68 68 0f 68 0f 61 68 3b d7 00 ef 93 e7 08 a 68 f7 f7 fb 61 68 68 0f 68 0f 61 68 3b d7 00 ef 93 e7 08 a 68 f7 f7 f8 b 11 14 b1 21 82 fa fa b1 21 82 b7 22 72 e0 48 f7 a5 4 db a1 f8 77 b9 32 41 f5 b9 32 41 f5 b1 1a 44 17 48 f3 cb 3 a8 30 08 4e c2 04 30 2f 30 2f c2 04 0a 6b 2f 42 45 a2 aa 6 ff d5 d7 aa 16 03 0e ac ac 16 03 0e 9f 68 f3 b1 20 d7 72 3 f9 e9 8f 2b 99 1e 73 f1 19 1b 30 af ac 71 8c c4 0d 16 65 6 cc 3e ff 3b 4b b2 16 e2 4b b2 16 e2 4b b2 16 e2 4b 86 8a 36 16 31 35 91 04 85 02 aa f2 97 77 ac 77 ac f2 97 fb f2 f2 af f3 13 59 1 a1 00 5f 34 32 63 cf 18 18 32 63 cf cc 5a 5b cf 52 4e 20 7 ff 08 69 64 0b 53 34 14									
15 dc da a9	9a 9b 7f 94	b8 14 d2 22		1d 19 24 5c	39 67 06 c0				
26 74 c7 bd ff7 92 c6 7a c6 7a ff7 92 cb ab 62 37 65 0e a3 cd 4 7e 22 9c 36 f3 93 de de 36 f3 93 19 b7 07 ec f1 96 90 5 f8 b4 0c 4c 4l 8d fe 29 4l 8d fe 29 2a 47 c4 48 58 fd 0f 4 ae a5 c1 ea e4 06 78 87 78 87 e4 06 84 18 27 23 36 38 9b e8 21 97 bc 9b fd 88 65 65 9b fd 88 eb 10 0a f3 eb 7d ed be 22 0b c 65 37 b7 65 4d 65 4d 37 b7 94 83 18 52 4c 74 ef 60 6d 4fa 72 6f 48 2d 6f 48 2d 72 le d0 20 40 c7 29 e5 ab 22 0b c 65 37 b7 65 4d 65 4d 37 b7 94 83 18 52 4c 74 ef 60 6d 6d 7f 7f 7b 6f 6f 68 6f	71 48 5c 7d	a3 52 4a ff	a3 52 4a ff	d4 11 fe 0f	2c a5 f2 43				
24 7e 22 9c 36 f3 93 de de 36 f3 93 19 b7 07 ec f1 96 90 5 f8 b4 0c 4c 41 8d fe 29 41 8d fe 29 2a 47 c4 48 58 fd 0f 46 67 37 24 ff 85 9a 36 16 9a 36 16 85 83 e8 18 ba 9d ee cc 48 ae a5 c1 ea e4 06 78 87 78 87 e4 06 84 18 27 23 36 38 9b 46 82 21 97 bc 9b fd 88 65 65 9b fd 88 eb 10 0a f3 eb 7d ed 67 72 ba cb 04 40 f4 1f f2 40 f4 1f f2 7b 05 42 4a 71 8c 83 64 1e 06 d4 fa 72 6f 48 2d 6f 48 2d 72 1e d0 20 40 c7 29 e5 68 1b 2 20 bc 65 37 b7 65 4d 65 4d 37 b7 94 83 18 52 4c 74 ef 68 00 6d e7 4e 63 3c 94 2f 2f 63 3c 94 94 c4 43 fb c2 bf 52 e8 00 89 c1 85 67 a7 78 97 67 a7 78 97 ec 1a c0 80 37 bb 38 fd 19 f9 c5 e5 35 99 a6 d9 99 a6 d9 35 0c 50 53 c7 14 3d d8 76 18 6d 8b ba ad 3c 3d f4 3c 3d f4 ad 3d 2f ec b6 26 1b c3 8 88 30 08 4e c2 04 30 2f 30 2f 20 04 06 2f 42 45 a2 ac 6f d5 d7 aa 16 03 0e ac ac 16 03 0e 9f 68 f3 b1 20 d7 72 3 ff 9 e9 8f 2b 99 1e 73 f1 99 1e 73 f1 31 30 3a c2 fd 0e c5 fd 10 48 50 2a aa f2 97 77 ac 77 ac f2 97 fb f2 f2 af f3 13 59 1 14 ff 08 69 64 00 55 34 14	15 dc da a9	59 86 57 d3	86 57 d3 59	3b 44 06 73	5c 73 22 8c				
f8 b4 0c 4c 41 8d fe 29 41 8d fe 29 2a 47 c4 48 58 fd 0f 4 67 37 24 ff 85 9a 36 16 9a 36 16 85 83 e8 18 ba 9d ee cc 4 e8 21 97 bc 9b fd 86 5 65 9b fd 88 eb 10 0a f3 eb 7d ed 7d ea 7d ea 1a eb 7d ea 7d ea 7d ea 7d ea 7d ea	26 74 c7 bd	f7 92 c6 7a	c6 7a f7 92	cb ab 62 37	65 0e a3 dd				
67 37 24 ff 85 9a 36 16 9a 36 16 85 83 e8 18 ba 9d ee cc 4 ae a5 c1 ea e4 06 78 87 78 87 e4 06 84 18 27 23 36 38 9b 4 e8 21 97 bc 9b fd 88 65 65 9b fd 88 eb 10 0a f3 eb 7d ed b 12 ba cb 04 40 f4 1f f2 40 f4 1f f2 7b 05 42 4a 71 8c 83 d 12 eb 20 bc 65 37 b7 65 4d 65 4d 37 b7 94 83 18 52 4c 74 ef a 18 20 6d e7 4e 63 3c 94 2f 2f 63 3c 94 94 c4 43 fb c2 bf 52 eb 10 0a 6d e7 4e 63 3c 94 2f 2f 63 3c 94 94 c4 43 fb c2 bf 52 eb 10 0a 89 c1 85 67 a7 78 97 67 a7 78 97 ec 1a c0 80 37 bb 38 fd 48 f7 f7 fb 61 68 68 0f 68 0f 61 68 3b d7 00 ef 93 e7 08 ab 65 7b 11 14 b1 21 82 fa fa b1 21 82 b7 22 72 e0 48 f7 a5 40 ab 11 14 b1 21 82 fa fa b1 21 82 b7 22 72 e0 48 f7 a5 40 ab 11 14 b1 21 82 fa fa b1 21 82 b7 22 72 e0 48 f7 a5 40 ab 11 14 b1 21 82 fa fa b1 21 82 b7 22 72 e0 48 f7 a5 40 ab 11 14 b1 21 82 fa fa b1 21 82 b7 22 72 e0 48 f7 a5 40 ab 14 15 ab 14 16 03 0e ac ac 16 03 0e 9f 68 f3 b1 20 d7 72 3 ab 15 30 af 42 f0 8 af 18 15 30 af 44 d4 66 54 8 eb 42 e0 4a 44 bf bf 81 89 08 08 0c a7 a7 08 08 0c 6a 1c 31 62 cb 1c 6e 50 cc 3e ff 3b 4b b2 16 e2 4b b2 16 e2 4b 86 8a 36 b4 ba 7f 86 af 18 15 30 af 16 67 59 af 32 85 cb 79 85 cb 79 32 b1 cb 27 5a 8e 98 4d 26 65 34 44 bb 53 34 14	24 7e 22 9c	36 f3 93 de	de 36 f3 93	19 b7 07 ec	f1 96 90 50				
ae a5 c1 ea e4 06 78 87 78 87 e4 06 84 18 27 23 36 38 9b 4 e8 21 97 bc 9b fd 88 65 65 9b fd 88 eb 10 0a f3 eb 7d ed b 72 ba cb 04 40 f4 1f f2 40 f4 1f f2 7b 05 42 4a 71 8c 83 c 1e 06 d4 fa 72 6f 48 2d 6f 48 2d 72 1e d0 20 40 c7 29 e5 a 1e d0 20 bc 65 37 b7 65 4d 65 4d 37 b7 94 83 18 52 4c 74 ef a 1e d0 6d e7 4e 63 3c 94 2f 2f 63 3c 94 94 c4 43 fb c2 bf 52 e6 d0 6d e7 4e 63 3c 94 2f 2f 63 3c 94 94 c4 43 fb c2 bf 52 e6 d9 fd 8f 7f 7f fb 61 68 68 0f 68 0f 61 68 3b d7 00 ef 93 e7 08 a 1e db a1 f8 77 b9 32 41 f5 b9 32 41 f5 b1 1a 44 17 48 f3 cb 36 db a1 f8 77 b9 32 41 f5 b9 32 41 f5 b1 1a 44 17 48 f3 cb 36 db a1 f8 77 b9 32 41 f5 b9 32 41 f5 b1 1a 44 17 48 f3 cb 36 db 36 db 36 db 36 db 37 db 38 f4 dd 36 db 37 db 38 f4 db 37 db 38 f4 db 37 db 38 f5 db 48 f5 d7 aa 16 03 0e ac ac 16 03 0e 9f 68 f3 b1 20 d7 72 36 db 4f c9 85 49 84 dd 97 3b 97 3b 84 dd 46 65 48 eb 42 e0 4a 48 db 6f 81 89 08 08 0c a7 a7 08 08 0c 6a 1c 31 62 cb 1c 6e 56 cc 3e ff 3b 4b b2 16 e2 4b b2 16 e2 4b 86 8a 36 b4 ba 7f 8 67 db 64 85 02 aa f2 97 77 ac 77 ac f2 97 fb f2 f2 af f3 13 59 16 ff 08 69 64 0b 53 34 14	f8 b4 0c 4c	41 8d fe 29	41 8d fe 29	2a 47 c4 48	58 fd 0f 4c				
e8 21 97 bc 9b fd 88 65 65 9b fd 88 eb 10 0a f3 eb 7d ed f 7e fa fa ff ff </td <td>67 37 24 ff</td> <td>85 9a 36 16</td> <td>9a 36 16 85</td> <td>83 e8 18 ba</td> <td>9d ee cc 40</td>	67 37 24 ff	85 9a 36 16	9a 36 16 85	83 e8 18 ba	9d ee cc 40				
72 ba cb 04									
1e 06 d4 fa 72 6f 48 2d 6f 48 2d 72 1e d0 20 40 c7 29 e5 a b2 20 bc 65 37 b7 65 4d 65 4d 37 b7 94 83 18 52 4c 74 ef a 00 6d e7 4e 63 3c 94 2f 2f 63 3c 94 94 c4 43 fb c2 bf 52 ec 0a 89 c1 85 67 a7 78 97 ec 1a c0 80 37 bb 38 fd d8 f7 f5 61 68 69 66 68 0f 61 68 35 do 50 53 c7 14 3d 8d 7 36 48 7 7 8 7 18 66 80 66 16 68 3b do<	e8 21 97 bc								
b2 20 bc 65									
00 6d e7 4e 63 3c 94 2f 2f 63 3c 94 94 c4 43 fb c2 bf 52 e 0a 89 c1 85 67 a7 78 97 67 a7 78 97 ec 1a c0 80 37 bb 38 fd d9 f9 c5 e5 35 99 a6 d9 99 a6 d9 35 0c 50 53 c7 14 3d d8 7 d8 f7 f7 fb 61 68 68 0f 68 0f 61 68 3b d7 00 ef 93 e7 08 a 56 7b 11 14 b1 21 82 fa fa b1 21 82 b7 22 72 e0 48 f7 a5 4 db a1 f8 77 b9 32 41 f5 b9 32 41 f5 b1 1a 44 17 48 f3 cb 3 18 6d 8b ba ad 3c 3d f4 3c 3d f4 ad 3d 2f ec b6 26 1b c3 k a8 30 08 4e c2 04 30 2f 30 2f c2 04 0a 6b 2f 42 45 a2 aa 0 ff d5 d7 aa 16 03 0e ac ac 16 03 0e 9f 68 f3 b1 20 d7 72 3 f9 e9 8f 2b 99 1e 73 f1 99 1e 73 f1 31 30 3a c2 fd 0e c5 f 1b 34 2f 08 af 18 15 30 18 15 30 af ac 71 8c c4 0d 16 d5 6 4f c9 85 49 84 dd 97 3b 97 3b 84 dd 46 65 48 eb bf bf 81 89 08 08 0c a7 a7 08 08 0c 6a 1c 31 62 cb 1c 6e 5 a1 67 59 af 32 85 cb 79 85 cb 79 32 b1 cb 27 5a 8e 98 4d 2 ff 08 69 64 0b 53 34 14									
0a 89 c1 85 67 a7 78 97 67 a7 78 97 ec 1a c0 80 37 bb 38 fd fg fg fg c5 e5 35 99 a6 d9 99 a6 d9 35 0c 50 53 c7 14 3d d8 77 fg 61 68 68 0f 61 68 3b d7 00 ef 93 e7 08 a5 56 7b 11 14 b1 21 82 fa b1 21 82 b7 22 72 e0 48 f7 a5 46 db a1 f8 77 b9 32 41 f5 b9 32 41 f5 b1 1a 44 17 48 f3 cb 33 d2f c2 04 0a 6b 2f 4b f3 cb cb 26 1b ca f3 b1 2a da <									
d9 f9 c5 e5 35 99 a6 d9 99 a6 d9 35 0c 50 53 c7 14 3d d8 7 d8 f7 f7 fb 61 68 68 0f 68 0f 61 68 3b d7 00 ef 93 e7 08 e 56 7b 11 14 b1 21 82 fa fa b1 21 82 b7 22 72 e0 48 f7 a5 e db a1 f8 77 b9 32 41 f5 b9 32 41 f5 b1 1a 44 17 48 f3 cb 3a ad 3d f4 ad ad ad 3c 3d f4 ad ad ad ad 3c 3d f4 ad ad ad ad 3c 3d f4 ad									
d8 f7 f7 fb 61 68 68 0f 68 0f 61 68 3b d7 00 ef 93 e7 08 a 56 7b 11 14 b1 21 82 fa fa b1 21 82 b7 22 72 e0 48 f7 a5 4 db a1 f8 77 b9 32 41 f5 b9 32 41 f5 b1 1a 44 17 48 f3 cb 3 18 6d 8b ba ad 3c 3d f4 3c 3d f4 ad 3d 2f ec b6 26 1b c3 b a8 30 08 4e c2 04 30 2f 30 2f c2 04 0a 6b 2f 42 45 a2 aa c ff d5 d7 aa 16 03 0e ac ac 16 03 0e 9f 68 f3 b1 20 d7 72 3 f9 e9 8f 2b 99 1e 73 f1 99 1e 73 f1 31 30 3a c2 fd 0e c5 f 1b 34 2f 08 af 18 15 30 18 15 30 af ac 71 8c c4 0d 16 d5 6 4f c9 85 49 84 dd 97 3b 97 3b 84 dd 46 65 48 eb 42 e0 4a 4 bf bf 81 89 08 08 0c a7 a7 08 08 0c 6a 1c 31 62 cb 1c 6e 5 cc 3e ff 3b 4b b2 16 e2 4b b2 16 e2 4b 86 8a 36 b4 ba 7f 8 a1 67 59 af 32 85 cb 79 85 cb 79 32 b1 cb 27 5a 8e 98 4d 2 a1 00 5f 34 32 63 cf 18 18 32 63 cf cc 5a 5b cf 52 4e 20 7									
56 7b 11 14 b1 21 82 fa fa b1 21 82 b7 22 72 e0 48 f7 a5 4 db a1 f8 77 b9 32 41 f5 b9 32 41 f5 b1 1a 44 17 48 f3 cb 3 18 6d 8b ba ad 3c 3d f4 3c 3d f4 ad 3d 2f ec b6 26 1b c3 k a8 30 08 4e c2 04 30 2f 30 2f c2 04 0a 6b 2f 42 45 a2 aa 6 ff d5 d7 aa 16 03 0e ac ac 16 03 0e 9f 68 f3 b1 20 d7 72 3 f9 e9 8f 2b 99 1e 73 f1 99 1e 73 f1 31 30 3a c2 fd 0e c5 fd 1b 34 2f 08 af 18 15 30 18 15 30 af ac 71 8c c4 0d 16 d5 6 4f c9 85 49 84 dd 97 3b 97 3b 84 dd 46 65 48 eb 42 e0 4a 48 bf bf 81 89 08 08 0c a7 a7 08 08 0c 6a 1c 31 62 cb 1c 6e 5 cc 3e ff 3b 4b b2 16 e2 4b b2 16 e2 4b 86 8a 36 b4 ba 7f 8 a1 67 59 af 32 85 cb 79 85 cb 79 32 b1 cb 27 5a 8e 98 4d 2 a1 00 5f 34 32 63 cf 18 18 32 63 cf cc 5a 5b cf 52 4e 20 76 ff 08 69 64 0b 53 34 14									
db a1 f8 77 b9 32 41 f5 b9 32 41 f5 b9 32 41 f5 b1 1a 44 17 48 f3 cb 3 18 6d 8b ba ad 3c 3d f4 3c 3d f4 ad 3d 2f ec b6 26 1b c3 ba ad 3d 2f ec b6 26 1b c4 ec b6									
18 6d 8b ba ad 3c 3d f4 3c 3d f4 ad 3d 2f ec b6 26 1b c3 b a8 30 08 4e c2 04 30 2f 30 2f c2 04 0a 6b 2f 42 45 a2 aa 6 ff d5 d7 aa 16 03 0e ac ac 16 03 0e 9f 68 f3 b1 20 d7 72 3 f9 e9 8f 2b 99 1e 73 f1 99 1e 73 f1 31 30 3a c2 fd 0e c5 fd 1b 34 2f 08 af 18 15 30 18 15 30 af ac 71 8c c4 0d 16 d5 6 4f c9 85 49 84 dd 97 3b 97 3b 84 dd 46 65 48 eb 42 e0 4a 44 bf bf 81 89 08 08 0c a7 a7 08 08 0c 6a 1c 31 62 cb 1c 6e 5 at 67 59 af 32 85 cb 79 85 cb 79 32 b1 cb 27 5a 8e 98 4d 2 a1 00 5f 34 32 63 cf 18 18 32 63 cf cc 5a 5b cf 52 4e 20 75 at 68 69 64 0b 53 34 14									
a8 30 08 4e c2 04 30 2f c2 04 0a 6b 2f 42 45 a2 aa 6f d5 d7 aa 16 03 0e ac 16 03 0e 9f 68 f3 b1 20 d7 72 3 f9 e9 8f 2b 99 1e 73 f1 99 1e 73 f1 31 30 3a c2 fd 0e c5 fd 1b 34 2f 08 af 18 15 30 18 15 30 af ac 71 8c c4 0d 16 d5 6 4f c9 85 49 84 dd 97 3b 84 dd 46 65 48 eb 42 e0 4a 4a eb b1 66 54 8e b4 42 e0 4a 4a eb b1 cb 4a b2 eb <td< td=""><td></td><td></td><td></td><td></td><td></td></td<>									
ff d5 d7 aa 16 03 0e ac 16 03 0e 9f 68 f3 b1 20 d7 72 3 f9 e9 8f 2b 99 1e 73 f1 99 1e 73 f1 31 30 3a c2 fd 0e c5 fd 1b 34 2f 08 af 18 15 30 18 15 30 af ac 71 8c c4 0d 16 d5 6 4f c9 85 49 84 dd 97 3b 84 dd 46 65 48 eb 42 e0 4a 46 bf bf 81 89 08 0c a7 a7 08 08 0c 6a 1c 31 62 cb 1c 6e 5 cc 3e ff 3b 4b b2 16 e2 4b 86 8a 36 b4 ba 7f 8e 98 4d 2d a1 67 59 af 32 85 cb <td></td> <td></td> <td></td> <td></td> <td></td>									
f9 e9 8f 2b 99 1e 73 f1 99 1e 73 f1 31 30 3a c2 fd 0e c5 f 1b 34 2f 08 af 18 15 30 af ac 71 8c c4 0d 16 d5 6 4f c9 85 49 84 dd 97 3b 84 dd 46 65 48 eb 42 e0 4a 4 eb 42 e0 4a 4 eb 42 e0 4a 4a eb 4a eb 4a eb 4a eb 4a eb eb 4a eb e									
1b 34 2f 08 4f c9 85 49 af 18 15 30 18 15 30 af ac 71 8c c4 0d 16 d5 64 4f c9 85 49 0d 16 d5 64 4f c9 85 40 0d 16 d5 64 4f c9 85 40 <td< td=""><td></td><td></td><td></td><td></td><td></td></td<>									
4f c9 85 49 bf bf 81 89 84 dd 97 3b 84 dd 87 80 80 80 80 80 80 80 80 80 80 80 80 80									
bf bf 81 89 08 08 0c a7 a7 08 08 0c 6a 1c 31 62 cb 1c 6e 5c 3e ff 3b 4b b2 16 e2 4b b2 16 e2 4b 86 8a 36 b4 ba 7f 8 a1 67 59 af 32 85 cb 79 85 cb 79 32 b1 cb 27 5a 8e 98 4d 2 04 85 02 aa f2 97 77 ac 77 ac f2 97 fb f2 f2 af f3 13 59 1 a1 00 5f 34 32 63 cf 18 18 32 63 cf cc 5a 5b cf 52 4e 20 7 ff 08 69 64 0b 53 34 14									
cc 3e ff 3b 4b b2 16 e2 4b b2 16 e2 4b 86 8a 36 b4 ba 7f 8 a1 67 59 af 32 85 cb 79 85 cb 79 32 b1 cb 27 5a 8e 98 4d 2 04 85 02 aa f2 97 77 ac 77 ac f2 97 fb f2 f2 af f3 13 59 1 a1 00 5f 34 32 63 cf 18 18 32 63 cf cc 5a 5b cf 52 4e 20 7 ff 08 69 64 0b 53 34 14 14									
a1 67 59 af 32 85 cb 79 85 cb 79 32 b1 cb 27 5a 8e 98 4d 2 04 85 02 aa f2 97 77 ac f2 97 fb f2 f2 af f3 13 59 1 a1 00 5f 34 32 63 cf 18 32 63 cf cc 5a 5b cf 52 4e 20 7 ff 08 69 64<	cc 3e ff 3b	4b b2 16 e2	4b b2 16 e2	4b 86 8a 36	b4 ba 7f 86				
04 85 02 aa f2 97 77 ac 77 ac f2 97 fb f2 f2 af f3 13 59 1 a1 00 5f 34 32 63 cf 18 18 32 63 cf cc 5a 5b cf 52 4e 20 7 ff 08 69 64 0b 53 34 14				b1 cb 27 5a	8e 98 4d 26				
a1 00 5f 34 32 63 cf 18 18 32 63 cf cc 5a 5b cf 52 4e 20 7 ff 08 69 64 0b 53 34 14	04 85 02 aa	f2 97 77 ac		fb f2 f2 af	f3 13 59 18				
0b 53 34 14	al 00 5f 34			cc 5a 5b cf	52 4e 20 76				
0b 53 34 14									
	0b 53 34 14								
84 bf ab 8f 24	84 bf ab 8f	24							
4a 7c 43 b9 T	4a 7c 43 b9								

Avalanche Effect: Change in Plaintext

Plaintext2:

0**0**2345678abcdeffe dcba987654321

Round		Number of Bits that Differ
	0123456789abcdeffedcba9876543210 0023456789abcdeffedcba9876543210	1
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	657470750fc7ff3fc0e8e8ca4dd02a9c c4a9ad090fc7ff3fc0e8e8ca4dd02a9c	20
2	5c7bb49a6b72349b05a2317ff46d1294 fe2ae569f7ee8bb8c1f5a2bb37ef53d5	58
3	7115262448dc747e5cdac7227da9bd9c ec093dfb7c45343d689017507d485e62	59
4	f867aee8b437a5210c24c1974cffeabc 43efdb697244df808e8d9364ee0ae6f5	61
5	721eb200ba06206dcbd4bce704fa654e 7b28a5d5ed643287e006c099bb375302	68
6	0ad9d85689f9f77bc1c5f71185e5fb14 3bc2d8b6798d8ac4fe36a1d891ac181a	64
7	db18a8ffa16d30d5f88b08d777ba4eaa 9fb8b5452023c70280e5c4bb9e555a4b	67
8	f91b4fbfe934c9bf8f2f85812b084989 20264e1126b219aef7feb3f9b2d6de40	65
9	cca104a13e678500ff59025f3bafaa34 b56a0341b2290ba7dfdfbddcd8578205	61
10	ff0b844a0853bf7c6934ab4364148fb9 612b89398d0600cde116227ce72433f0	58

Avalanche Effect: Change in Key

Key2:

0e1571c947d9e859 0cb7add6af7f6798

Round		Number of Bits that Differ
	0123456789abcdeffedcba9876543210 0123456789abcdeffedcba9876543210	0
0	0e3634aece7225b6f26b174ed92b5588 0f3634aece7225b6f26b174ed92b5588	1
1	657470750fc7ff3fc0e8e8ca4dd02a9c c5a9ad090ec7ff3fc1e8e8ca4cd02a9c	22
2	5c7bb49a6b72349b05a2317ff46d1294 90905fa9563356d15f3760f3b8259985	58
3	7115262448dc747e5cdac7227da9bd9c 18aeb7aa794b3b66629448d575c7cebf	67
4	f867aee8b437a5210c24c1974cffeabc f81015f993c978a876ae017cb49e7eec	63
5	721eb200ba06206dcbd4bce704fa654e 5955c91b4e769f3cb4a94768e98d5267	81
6	0ad9d85689f9f77bc1c5f71185e5fb14 dc60a24d137662181e45b8d3726b2920	70
7	db18a8ffa16d30d5f88b08d777ba4eaa fe8343b8f88bef66cab7e977d005a03c	74
8	f91b4fbfe934c9bf8f2f85812b084989 da7dad581d1725c5b72fa0f9d9d1366a	67
9	cca104a13e678500ff59025f3bafaa34 0ccb4c66bbfd912f4b511d72996345e0	59
10	ff0b844a0853bf7c6934ab4364148fb9 fc8923ee501a7d207ab670686839996b	53

Implementation Aspects

- AES can be implemented very efficiently on an 8bit processor
- AddRoundKey is a bytewise XOR operation
- ShiftRows is a simple byte-shifting operation
- SubBytes operates at the byte level and only requires a table of 256 bytes
- MixColumns requires matrix multiplication in the field GF(2⁸), which means that all operations are carried out on bytes

Implementation Aspects

- Can efficiently implement on a 32-bit processor
 - Redefine steps to use 32-bit words
 - Precompute 4 tables of 256-words
 - Each column in each round is computed using 4 table lookups + 4 XORs at a cost of 4K bytes to store tables
- Designers believe that efficient implementation was a key factor in its selection as the AES cipher

Summary

- Finite field arithmetic
- AES structure
 - General structure
 - Detailed structure
- AES key expansion
 - Key expansion algorithm
 - Rationale

- AES transformation functions
 - Substitute bytes
 - ShiftRows
 - MixColumns
 - AddRoundKey
- AES implementation
 - Equivalent inverse cipher
 - Implementation aspects