

Cryptography and Network Security

Sixth Edition by William Stallings



Chapter 5

Advanced Encryption Standard

"It seems very simple."

"It is very simple. But if you don't know what the key is it's virtually indecipherable."

—Talking to Strange Men, Ruth Rendell

Finite Field Arithmetic

- In the Advanced Encryption Standard (AES) all operations are performed on 8-bit bytes
- The arithmetic operations of addition, multiplication, and division are performed over the finite field GF(2⁸)
- A field is a set in which we can do addition, subtraction, multiplication, and division without leaving the set
- Division is defined with the following rule:
 - $a/b = a(b^{-1})$
- An example of a finite field (one with a finite number of elements) is the set Z_p consisting of all the integers {0, 1,, p 1}, where p is a prime number and in which arithmetic is carried out modulo p

Finite Field Arithmetic

If one of the operations used in the algorithm is division, then we need to work in arithmetic defined over a field

• Division requires that each nonzero element have a multiplicative inverse For convenience and for implementation efficiency we would like to work with integers that fit exactly into a given number of bits with no wasted bit patterns

Integers in the range o through
 2ⁿ – 1, which fit into an *n*-bit word

The set of such integers, Z_2^n , using modular arithmetic, is not a field

For example, the integer 2 has no multiplicative inverse in Z₂ⁿ, that is, there is no integer b, such that 2b mod 2ⁿ = 1

A finite field containing 2^n elements is referred to as $GF(2^n)$

• Every polynomial in GF(2ⁿ) can be represented by an n-bit number

AES Encryption Process



Figure 5.1 AES Encryption Process

Key

16

24

32

AES Data Structures



(a) Input, state array, and output



(b) Key and expanded key

Figure 5.2 AES Data Structures

Table 5.1 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 Encryption and Decryption





Detailed Structure

- Processes the entire data block as a single matrix during each round using substitutions and permutation
- The key that is provided as input is expanded into an array of forty-four 32-bit words, w[i]

Four different stages are used:

- Substitute bytes uses an S-box to perform a byte-by-byte substitution of the block
- ShiftRows a simple permutation
- MixColumns a substitution that makes use of arithmetic over GF(2⁸)
- AddRoundKey a simple bitwise XOR of the current block with a portion of the expanded key
- The cipher begins and ends with an AddRoundKey stage
- Can view the cipher as alternating operations of XOR encryption (AddRoundKey) of a block, followed by scrambling of the block (the other three stages), followed by XOR encryption, and so on
- Each stage is easily reversible
- The decryption algorithm makes use of the expanded key in reverse order, however the decryption algorithm is not identical to the encryption algorithm
- State is the same for both encryption and decryption
- Final round of both encryption and decryption consists of only three stages



Figure 5.4 AES Encryption Round

AES Byte Level Operations



(a) Substitute byte transformation



S0,3

s'2.3

 W_i

 \oplus

 $s_{0,1}$

*s*_{1,1}

\$3,1

S0,3

\$2,3

3,2 S3,3

S_{1,2} S_{1,3}

S_{0,2}

\$2,2

S_{0,0}

\$1,0

S_{2,0}

\$3,0

(b) Add round key Transformation

Figure 5.5 AES Byte-Level Operations

Table 5.2

(a) S-box

			3.0		1 states				J	V		4370			1992		
	122	0	1	2	3	4	5	6	7	8	9	Α	В	С	D	E	F
198	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	C0
2	2	B7	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
1	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
33	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
1	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
	Α	EO	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
	С	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
23	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	$\overline{0}$ D	BF	E6	42	68	41	99	$\overline{2D}$	0F	B0	54	BB	16

(Table can be found on page 139 in textbook)

X

Table 5.2

(b) Inverse S-box

		1025	2.944	Sec.2	2244			1913	J	,	43.34	SPA	100	2222		20.24	4501
	1592	0	1	2	3	4	5	6	7	8	9	Α	В	С	D	E	F
200	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	CB
	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	B6	92
	5	6C	70	48	50	FD	ED	B9	DA	5E	15	46	57	A7	8D	9D	84
	6	90	D8	AB	00	8C	BC	D3	0A	F7	E4	58	05	B8	B3	45	06
r	7	D0	2C	1E	8F	CA	3F	0F	02	C1	AF	BD	03	01	13	8A	6B
A	8	3A	91	11	41	4F	67	DC	EA	97	F2	CF	CE	F0	B4	E6	73
	9	96	AC	74	22	E7	AD	35	85	E2	F9	37	E8	1C	75	DF	6E
	А	47	F1	1A	71	1D	29	C5	89	6F	B7	62	0E	AA	18	BE	1B
	В	FC	56	3E	4B	C6	D2	79	20	9A	DB	C0	FE	78	CD	5A	F4
	С	1F	DD	A8	33	88	07	C7	31	B1	12	10	59	27	80	EC	5F
	D	60	51	7F	A9	19	B5	4A	0D	2D	E5	7A	9F	93	C9	9C	EF
13	E	A0	EO	3B	4D	AE	2A	F5	B0	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

(Table can be found on page 139 in textbook)



Figure 5.6 Construction of S-Box and IS-Box

S-Box Rationale

- The S-box is designed to be resistant to known cryptanalytic attacks
- The Rijndael developers sought a design that has a low correlation between input bits and output bits and the property that the output is not a linear mathematical function of the input
- The nonlinearity is due to the use of the multiplicative inverse

Shift Row Transformation



(a) Shift row transformation

Figure 5.7 AES Row and Column Operations

(Figure can be found on page 144 in textbook)

Shift Row Rationale

- More substantial than it may first appear
- The State, as well as the cipher input and output, is treated as an array of four 4-byte columns
- On encryption, the first 4 bytes of the plaintext are copied to the first column of State, and so on
- The round key is applied to State column by column
 - Thus, a row shift moves an individual byte from one column to another, which is a linear distance of a multiple of 4 bytes
- Transformation ensures that the 4 bytes of one column are spread out to four different columns

MixColumn Transformation



(b) Mix column transformation Figure 5.7 AES Row and Column Operations

(Figure can be found on page 144 in textbook)

Mix Columns Rationale

- Coefficients of a matrix based on a linear code with maximal distance between code words ensures a good mixing among the bytes of each column
- The mix column transformation combined with the shift row transformation ensures that after a few rounds all output bits depend on all input bits

AddRoundKey Transformation

- The 128 bits of State are bitwise XORed with the 128 bits of the round key
- Operation is viewed as a columnwise operation between the 4 bytes of a State column and one word of the round key
 - Can also be viewed as a byte-level operation

Rationale:

Is as simple as possible and affects every bit of State

The complexity of the round key expansion plus the complexity of the other stages of AES ensure security Inputs for Single AES Round



Figure 5.8 Inputs for Single AES Round

AES Key Expansion

- Takes as input a four-word (16 byte) key and produces a linear array of 44 words (176) bytes
 - This is sufficient to provide a four-word round key for the initial AddRoundKey stage and each of the 10 rounds of the cipher
- Key is copied into the first four words of the expanded key
 - The remainder of the expanded key is filled in four words at a time
- Each added word w[i] depends on the immediately preceding word, w[i 1], and the word four positions back, w[i 4]
 - In three out of four cases a simple XOR is used
 - For a word whose position in the *w* array is a multiple of 4, a more complex function is used

AES Key Expansion







(a) Overall algorithm

Figure 5.9 AES Key Expansion

Key Expansion Rationale

- The Rijndael developers designed the expansion key algorithm to be resistant to known cryptanalytic attacks
- Inclusion of a rounddependent round
 constant eliminates the
 symmetry between the
 ways in which round keys
 are generated in different
 rounds

The specific criteria that were used are:

- Knowledge of a part of the cipher key or round key does not enable calculation of many other round-key bits
- An invertible transformation
- Speed on a wide range of processors
- Usage of round constants to eliminate symmetries
- Diffusion of cipher key differences into the round keys
- Enough nonlinearity to prohibit the full determination of round key differences from cipher key differences only
- Simplicity of description

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
$w^2 = 0c b^7 ad d^6$	$Rcon(1) = 01 \ 00 \ 00 \ 00$
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 ⊕ w1 = 9b 49 df e9	SubWord(x4) = 0c 59 5c 07 = y2
w6 = w5 ⊕ w2 = 97 fe 72 3f	$Rcon(2) = 02 \ 00 \ 00 \ 00$
w7 = w6 ⊕ 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 🕀 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 ⊕ w7 = e6 ff d3 c6	$y3 \oplus Rcon(3) = 12 \ 66 \ b4 \ 8e = z3$
w12 = w8 \oplus z3 = c0 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 ⊕ 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	$Rcon(5) = 10 \ 00 \ 00 \ 00$
$w19 = w18 \oplus w15 = 43 8c dd 50$	$y5 \oplus Rcon(5) = 74 c1 53 1a = z5$
w20 = w16 \oplus z5 = 58 9d 36 eb	$RotWord(w23) = 40 \ 46 \ bd \ 4c = x6$
$w21 = w20 \oplus w17 = fd ee 38 7d$	SubWord(x5) = 09 5a 7a 29 = y6
$w22 = w21 \oplus w18 = 0f cc 9b ed$	$Rcon(6) = 20 \ 00 \ 00 \ 00$
$w23 = w22 \oplus w19 = 4c \ 40 \ 46 \ bd$	$y6 \oplus Rcon(6) = 29 5a 7a 29 = z6$
w24 = w20 ⊕ 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
$w26 = w25 \oplus w22 = 83 e5 ef 52$	$Rcon(7) = 40 \ 00 \ 00 \ 00$
$w27 = w26 \oplus w23 = cf a5 a9 ef$	y/ + Rcon(/)= 46 d3 dI 8a = 2/
$w28 = w24 \oplus z7 = 37 14 93 48$	RotWord(w31) = 7d a1 4a f7 = x8
$w29 = w28 \oplus w25 = bb 3d e7 f7$	SubWord($x7$) = ff 32 d6 68 = y8
$w30 = w29 \oplus w26 = 38 d8 08 a5$	Rcon(8) = 80 00 00 00
$w31 = w30 \oplus w27 = f7 7d a1 4a$	y8 (+) RCon(8) = /1 32 d6 68 = 28
$w32 = w28 \oplus z8 = 48 26 45 20$	RotWord($w35$) = be 0b 38 3c = x9
$w_{33} = w_{32} \oplus w_{29} = f_3 \ 1b \ a_2 \ d_7$	Subword(x8) = ae $2b = 07$ eb = $y9$
$w_{34} = w_{33} \oplus w_{30} = cb c_{3} aa /2$	$x_{0} \oplus B_{con}(9) = 15 00 00 00$
$w_{35} = w_{34} \oplus w_{32} = 3c$ be 0b 38	$y^{3} \oplus \text{Reon}(y) = D^{3} 2D^{3} 07^{2} \text{eb} = 23^{3}$
$w_{36} = w_{32} \oplus z_{9} = id \ 0d \ 42 \ Cb$	Rotword(w39) = 60 41 56 19 = X10
$w_{37} = w_{30} \oplus w_{33} = 00 10 00 10$	$B_{con}(10) = 36,00,00,00$
$w_{30} = w_{37} \oplus w_{34} = C5 \ d5 \ 4a \ be$ $w_{30} = w_{30} \oplus w_{35} = f_0 \ cb \ 41 \ 5c$	$x_{10} \oplus B_{con}(10) = 49.83 \text{ b1 } 99 = 710$
$w_{33} - w_{30} - w_{30} - 19 00 41 30$	y to () (con(10) - 49 65 b1 99 - 210
$w_{40} - w_{50} \oplus 210 = D4 \ 80 \ 13 \ 52$ $w_{41} = w_{40} \oplus w_{37} = b_{20} \oplus 12 \ 4c$	
$w_{11} - w_{10} - w_{11} - w$	
$w_{42} - w_{41} \oplus w_{30} - 71 40 59 20$ $w_{43} = w_{42} \oplus w_{30} = 96 26 10 76$	
w45 - w42 () w59 - 80 20 18 /0	

Table 5.3

AES Example Key Expansion

(Table is located on page 151 in textbook)

Table 5.4

AES Example

(Table is located on page 153 in textbook)

Start of round	After	After	After	Round Key		
Start of round	SubBytes	ShiftRows	MivColumns	Round Rey		
01 00 50 76	Subbytes	SIIITIKOWS	wirxCorumnis	05 47 00 05		
01 89 10 70				15 d0 b7 7f		
25 ab dc 54						
45 cd ba 32				/1 e8 ad 6/		
67 ef 98 10				<u>c9 59 d6 98</u>		
0e ce f2 d9	ab 8b 89 35	ab 8b 89 35	b9 94 57 75	dc 9b 97 38		
36 72 6b 2b	05 40 7f fl	40 7f fl 05	e4 8e 16 51	90 49 fe 81		
34 25 17 55	18 3f f0 fc	f0 fc 18 3f	47 20 9a 3f	37 df 72 15		
ae b6 4e 88	e4 4e 2f c4	c4 e4 4e 2f	c5 d6 f5 3b	b0 e9 3f a7		
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 ff		
70 ff e8 2a	51 16 9b e5	9b e5 51 16	df 80 f7 c1	6b b4 c6 d3		
75 3f ca 9c	9d 75 74 de	de 9d 75 74	2d c5 1e 52	b7 5e 61 c6		
5c 6b 05 f4	4a 7f 6b bf	4a 7f 6b bf	bl cl Ob cc	c0 89 57 b1		
7b 72 a2 6d	21 40 3a 3c	40 3a 3c 21	ba f3 8b 07	af 2f 51 ae		
b4 34 31 12	8d 18 c7 c9	c7 c9 8d 18	f9 1f 6a c3	df 6b ad 7e		
9a 9b 7f 94	b8 14 d2 22	22 b8 14 d2	1d 19 24 5c	39 67 06 c0		
71 48 5c 7d	a3 52 4a ff	a3 52 4a ff	d4 11 fe 0f	2c a5 f2 43		
15 dc da a9	59 86 57 d3	86 57 d3 59	3b 44 06 73	5c 73 22 8c		
26 74 c7 bd	f7 92 c6 7a	c6 7a f7 92	cb ab 62 37	65 0e a3 dd		
24 7e 22 9c	36 f3 93 de	de 36 f3 93	19 b7 07 ec	f1 96 90 50		
f8 b4 0c 4c	41 8d fe 29	41 8d fe 29	2a 47 c4 48	58 fd 0f 4c		
67 37 24 ff	85 9a 36 16	9a 36 16 85	83 e8 18 ba	9d ee cc 40		
a = a = 5 = c = 1 = a	05 54 50 10	78 87 e^{1} 06	84 18 27 23	36 38 9b 46		
$e^{8} 21 97 bc$	9b fd 88 65	65 9b fd 88	eh 10 27 23	eb 7d ed bd		
72 ha ch 04	$10 f_{1} f_{2}$	40 f 4 1 f f 2	$\frac{20}{7b}$ $\frac{10}{05}$ $\frac{42}{12}$ $\frac{43}{12}$	71 80 83 of		
12 Da CD 04	72 6F 18 2d	6f 18 2d 72	10 d0 20 40	71 00 05 01		
$h^2 = 20 h^2 = 65$	72 01 40 20 27 b7 65 4d	65 1d 27 h7	$10 \ 10 \ 20 \ 40$	10729 es as		
00 6d e7 4e	63 30 9/ 2f	2f 63 30 91	94 03 10 52 94 c4 43 fb	qc fq $er af$		
00 00 e7 4e	67 07 79 07	21 03 30 94	94 C4 45 ID	27 bb 20 f7		
0a 89 CI 85	0/ a/ /8 9/	0/ a/ /8 9/	ec 1a co 80			
d9 19 C5 e5	55 99 ab d9	99 a6 d9 35	0C 50 55 C7	14 30 08 70		
a8 I/I/ID	b1 08 08 01	68 UI 61 68	3D d/ 00 er	93 e7 08 al		
56 /D 11 14	DI 21 82 IA	1a b1 21 82	b/ 22 /2 e0	48 17 a5 4a		
db al 18 77	b9 32 41 15	by 32 41 15	bl 1a 44 17	48 13 CD 3C		
18 6d 8b ba	ad 3c 3d 14	3C 3d 14 ad	3d ZI ec b6	26 1D C3 De		
a8 30 08 4e	C2 04 30 21	30 21 C2 04	0a 6b 21 42	45 a2 aa 0b		
ri d5 d/ aa	16 03 0e ac	ac 16 03 0e	91 68 13 bl	20 a/ /2 38		
19 e9 8f 2b	99 le 73 fl	99 le 73 fl	31 30 3a c2	fd 0e c5 f9		
1b 34 2f 08	af 18 15 30	18 15 30 af	ac 71 8c c4	0d 16 d5 6b		
41 C9 85 49	84 dd 97 3b	97 3b 84 dd	46 65 48 eb	42 e0 4a 41		
bf bf 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 86		
al 67 59 af	32 85 cb 79	85 cb 79 32	b1 cb 27 5a	8e 98 4d 26		
04 85 02 aa	f2 97 77 ac	77 ac f2 97	fb f2 f2 af	f3 13 59 18		
al 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						
84 bf ab 8f						
4a 7c 43 b9						

121.24	1.14	
la	nle	55
Iai		ノ・ノ

Avalanche Effect in AES: Change in Plaintext

(Table is located on page 154 in textbook)

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

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

Table 5.6

Avalanche Effect in AES: Change in Key

(Table is located on page 155 in textbook)

Equivalent Inverse Cipher

- AES decryption cipher is not identical to the encryption cipher
 - The sequence of transformations differs although the form of the key schedules is the same
 - Has the disadvantage that two separate software or firmware modules are needed for applications that require both encryption and decryption

Two separate changes are needed to bring the decryption structure in line with the encryption structure

The first two stages of the decryption round need to be interchanged

The second two stages of the decryption round need to be interchanged

Interchanging InvShiftRows and InvSubBytes

- InvShiftRows affects the sequence of bytes in State but does not alter byte contents and does not depend on byte contents to perform its transformation
- InvSubBytes affects the contents of bytes in State but does not alter byte sequence and does not depend on byte sequence to perform its transformation

Thus, these two operations commute and can be interchanged

Interchanging AddRoundKey and InvMixColumns

The transformations AddRoundKey and InvMixColumns do not alter the sequence of bytes in State

If we view the key as a sequence of words, then both AddRoundKey and InvMixColumns operate on State one column at a time

These two operations are linear with respect to the column input Equivalent Inverse Cipher



Figure 5.10 Equivalent Inverse Cipher

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
- Can precompute 4 tables of 256-words
- Then each column in each round can be computed using 4 table lookups + 4 XORs
- At a cost of 4Kb to store tables
- Designers believe this very 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