Computer Security

Lecture 6

Advanced Encryption Standard

Dr. Mohamed Loey

Lecturer, Faculty of Computers and Information

Benha University

Egypt

Table of Contents

Advanced Encryption Standard

AES Key Expansion

AES Encryption

AES Decryption

DES vs AES

Advantages of AES

Table of Contents

Advanced Encryption Standard

AES Key Expansion

AES Encryption

AES Decryption

DES vs AES

Advantages of AES

Advanced Encryption Standard

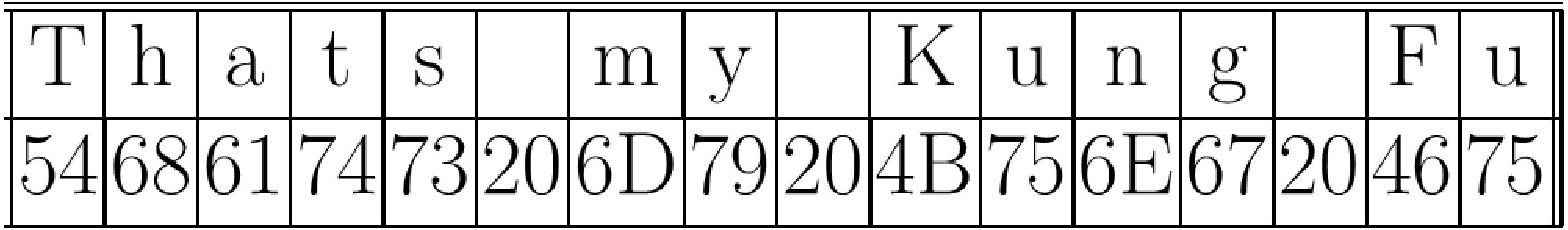
- ❑ The Advanced Encryption Standard (AES) was published by the National Institute of Standards and Technology (NIST) in 2001.
- ❑ AES is a symmetric block cipher that is intended to replace DES as the approved standard for a wide range of applications.
- ❑ Input(128 bit key and message)

Table of Contents

- Advanced Encryption Standard
- AES Key Expansion
- AES Encryption
- AES Decryption
- DES vs AES
- Advantages of AES

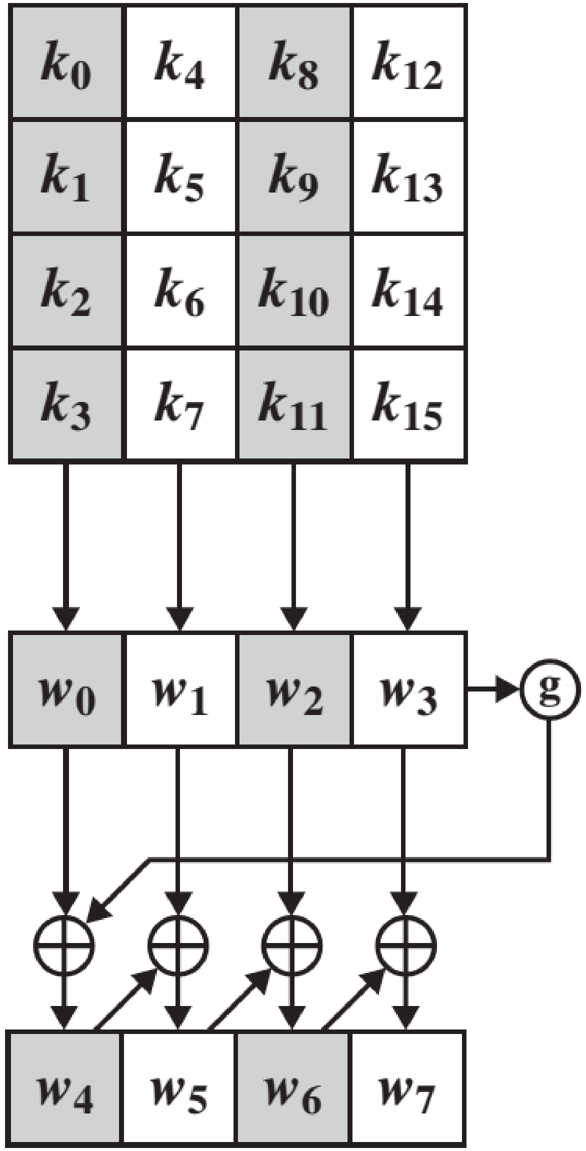
AES Key Expansion

- ❑ Key = Thats my Kung Fu (16 ASCII characters, 1byte each)
- ❑ Key in Hex(128bits):54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75 (32 Hex characters)



T	h	a	t	s		m	y		K	u	n	g		F	u
54	68	61	74	73	20	6D	79	20	4B	75	6E	67	20	46	75

AES Key Expansion

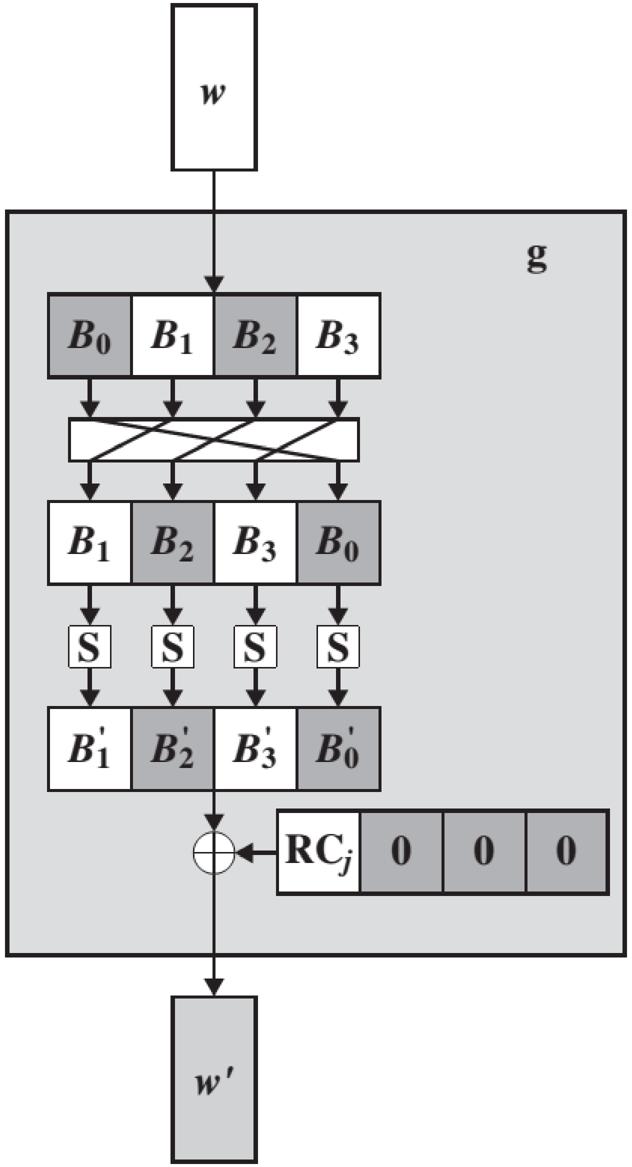

k_0 k_4 k_8 k_{12}
k_1 k_5 k_9 k_{13}
k_2 k_6 k_{10} k_{14}
k_3 k_7 k_{11} k_{15}
w_0 w_1 w_2 w_3
g
w_4 w_5 w_6 w_7

AES Key Expansion

- w[0]= (54,68,61,74)
- w[1]= (73,20,6D,79)
- w[2]= (20,4B,75,6E)
- w[3]= (67,20,46,75)
- g(w[3])

AES Key Expansion

- Function g



AES Key Expansion

- □ w[3]= (67,20,46,75)

- □ g(w[3])

1) Circular byte left shift of w[3]:(20,46,75,67)

2) Byte Substitution (S-Box):(B7,5A,9D,85)

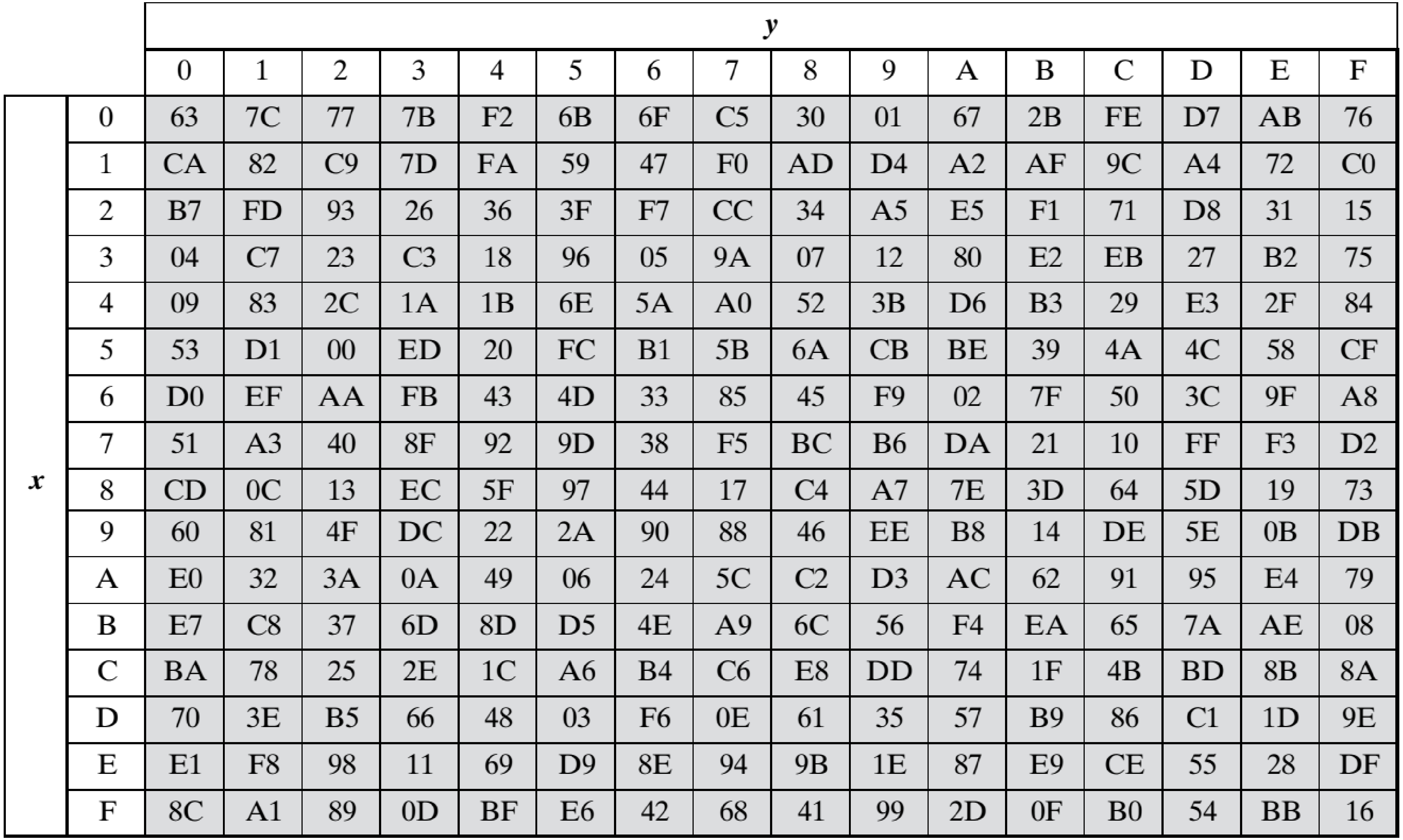
3) Adding round constant (01,00,00,00)

- ✓ The round constant is a word in which the three rightmost bytes are always 0.

- gives: g(w[3])= (B6,5A,9D,85)

AES Key Expansion

- ❑ S-Box



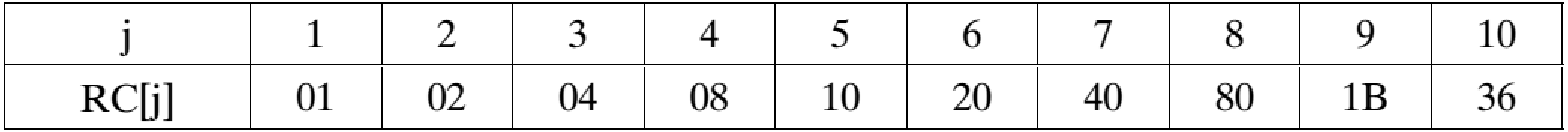
		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	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
	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
	B	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
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	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

(a) S-box

AES Key Expansion

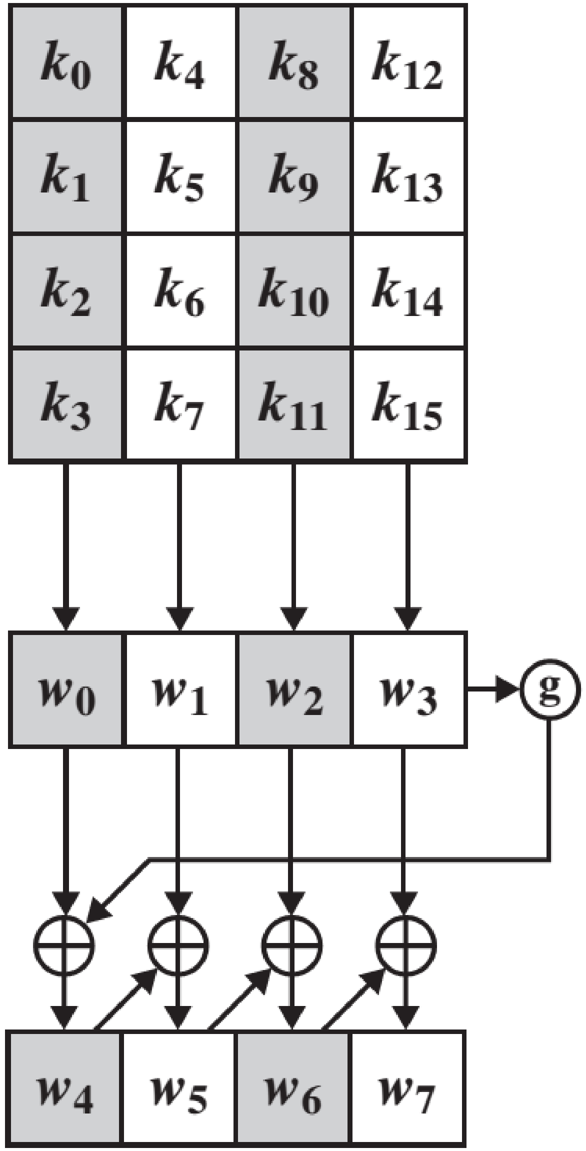
- Round Constant RC[j]

- j= Round iteration



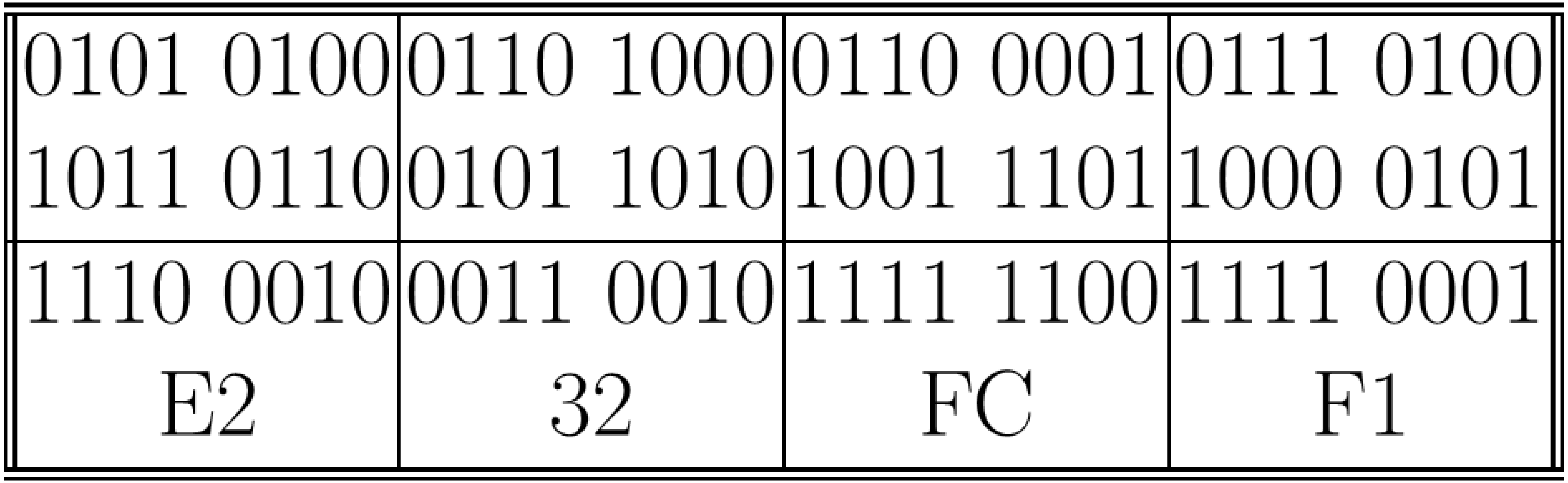
j	1	2	3	4	5	6	7	8	9	10
RC[j]	01	02	04	08	10	20	40	80	1B	36

AES Key Expansion



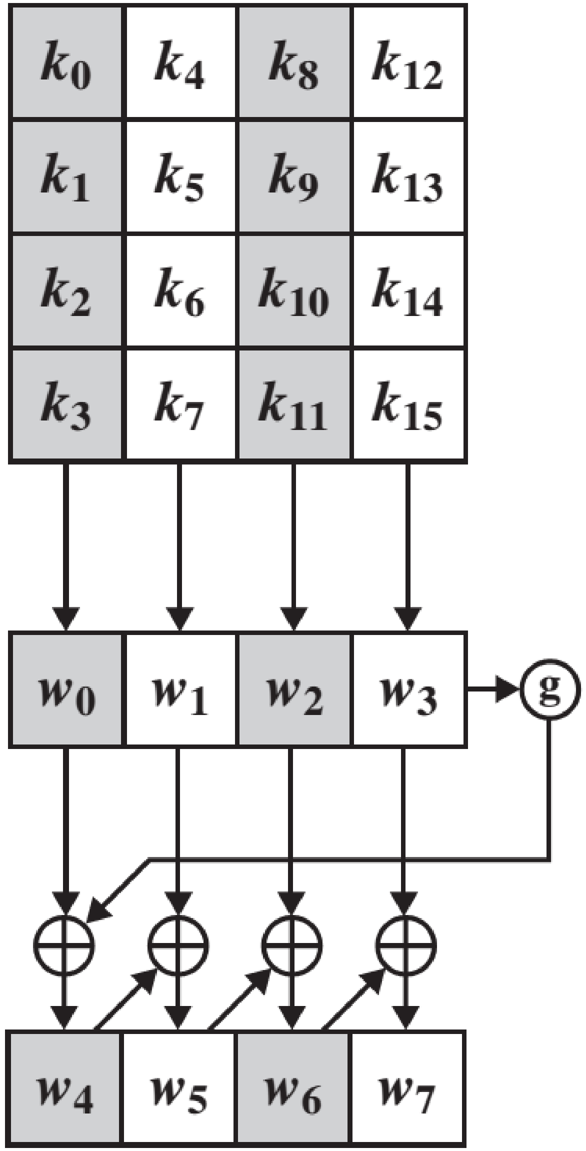
AES Key Expansion

- ❑ w[0]= (54,68,61,74)
- ❑ g(w[3])= (B6,5A,9D,85)
- ❑ w[4]= w[0] $\bigoplus$ g(w[3]) = (E2,32,FC,F1)



0101 0100 1011 0110	0110 1000 0101 1010	0110 0001 1001 1101	0111 0100 1000 0101
1110 0010 E2	0011 0010 32	1111 1100 FC	1111 0001 F1

AES Key Expansion



AES Key Expansion

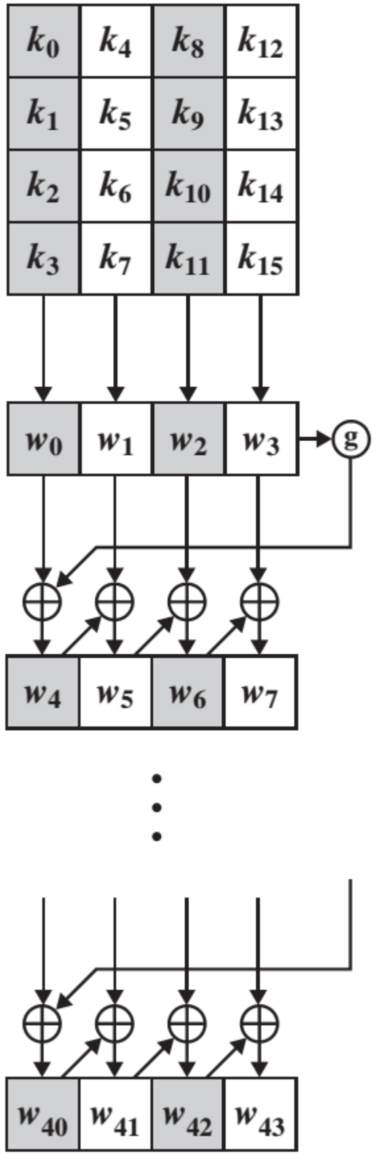
- $w[5]=w[4]\oplus w[1]=$ (91,12,91,88)

- $w[6]=w[5]\oplus w[2]=$ (B1,59,E4,E6)

- $w[7]=w[6]\oplus w[3]=$ (D6,79,A2,93)

- First round key : E232FCF1 91129188 B159E4E6 D679A293

AES Key Expansion


k_0 k_4 k_8 k_{12}
k_1 k_5 k_9 k_{13}
k_2 k_6 k_{10} k_{14}
k_3 k_7 k_{11} k_{15}
w_0 w_1 w_2 w_3
g
w_4 w_5 w_6 w_7
w_{40} w_{41} w_{42} w_{43}

AES Key Expansion

❑ **Round0:5468617473206D79204B756E67204675**

❑ Round1:E232FCF191129188B159E4E6D679A293

❑ Round2:56082007C71AB18F76435569A03AF7FA

❑ Round3:D2600DE7157ABC686339E901C3031EFB

❑ Round4:A11202C9B468BEA1D75157A01452495B

❑ Round5:B1293B3305418592D210D232C6429B69

❑ Round6:BD3DC2B7B87C47156A6C9527AC2E0E4E

❑ Round7:CC96ED1674EAAA031E863F24B2A8316A

❑ Round8:8E51EF21FABB4522E43D7A0656954B6C

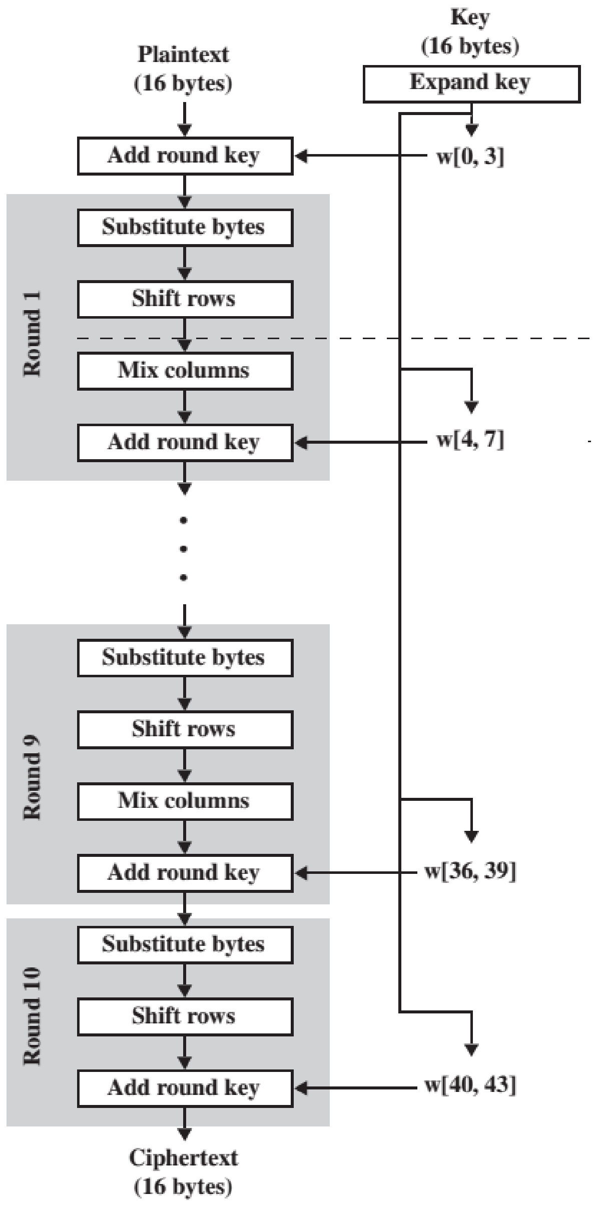
❑ Round9:BFE2BF904559FAB2A16480B4F7F1CBD8

❑ Round10:28FDDEF86DA4244ACCC0A4FE3B316F26

Table of Contents

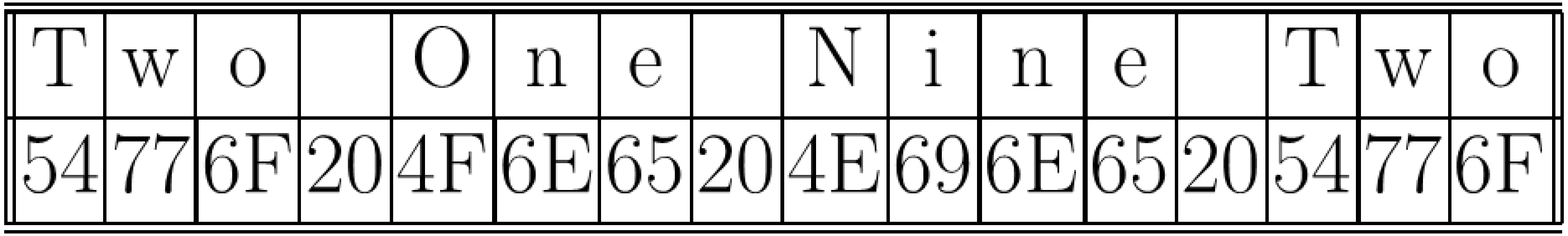
- Advanced Encryption Standard
- AES Key Expansion
- AES Encryption
- AES Decryption
- DES vs AES
- Advantages of AES

AES Encryption



AES Encryption

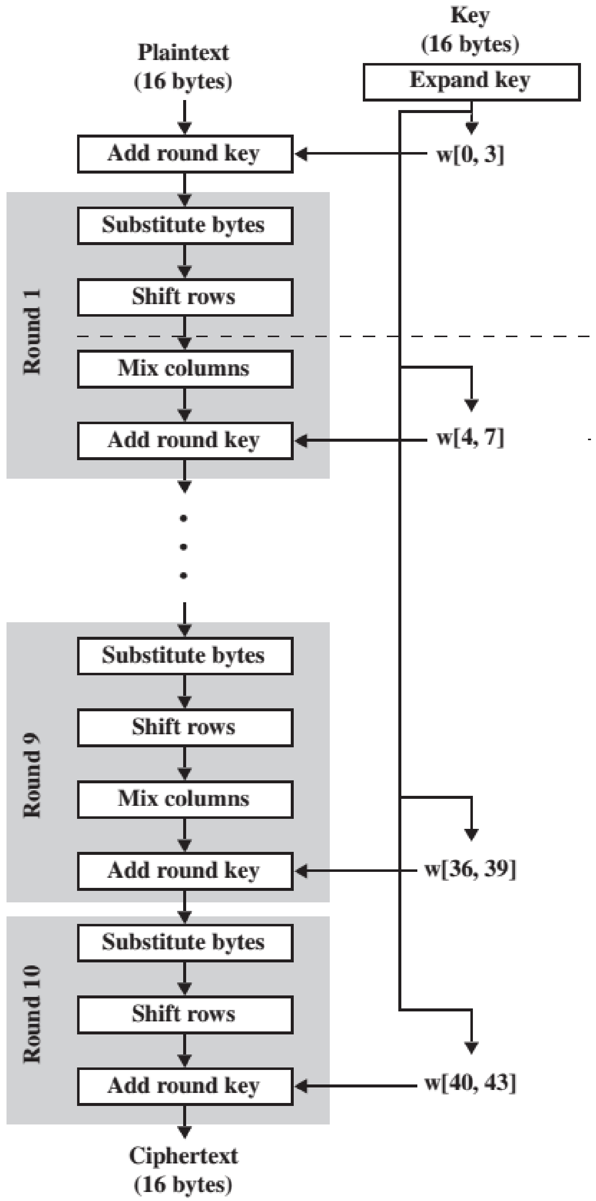
- ❑ Plain text in English : Two One Nine Two (16 ASCII characters)



T	w	o		O	n	e		N	i	n	e		T	w	o
54	77	6F	20	4F	6E	65	20	4E	69	6E	65	20	54	77	6F

- ❑ Plain text in Hex (128bits) : 54 77 6F 20 4F 6E 65 20 4E 69 6E 65 20 54 77 6F

AES Encryption



AES Encryption

- Add Round key, Round 0

- M = 54 77 6F 20 4F 6E 65 20 4E 69 6E 65 20 54 77 6F

- R_0 = 54 68 61 74 73 20 6D 79 20 4B 75 6E 67 20 46 75

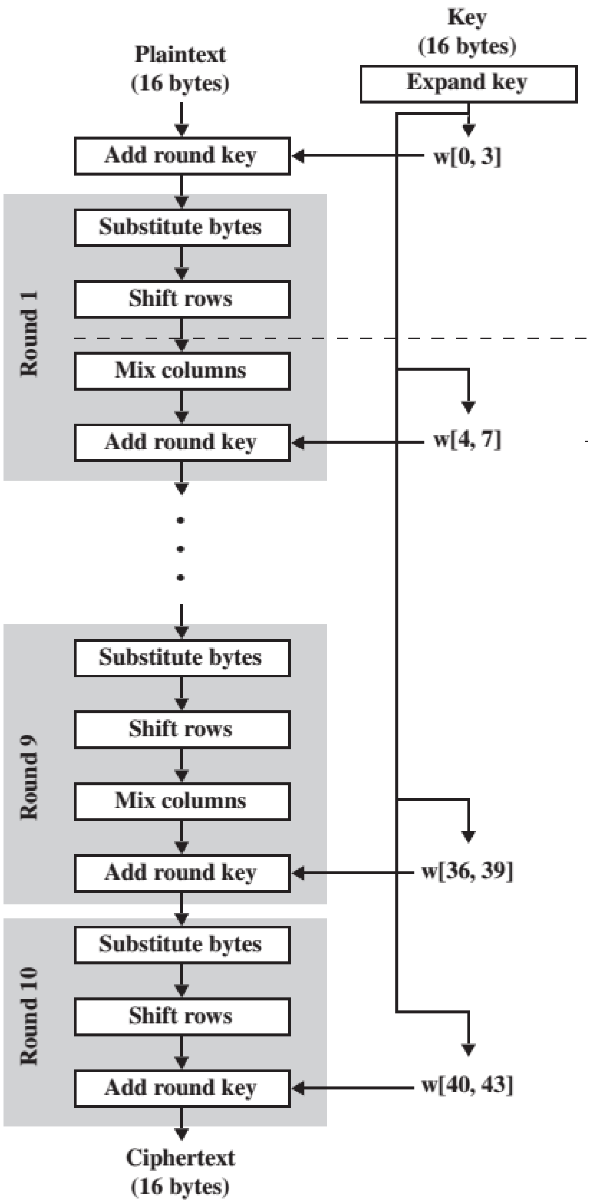
- XOR the corresponding entries, e.g., 69 $\oplus$ 4B = 22

$$\begin{array}{r} 0110\ 1001 \\ 0100\ 1011 \\ \hline 0010\ 0010 \end{array}$$

AES Encryption

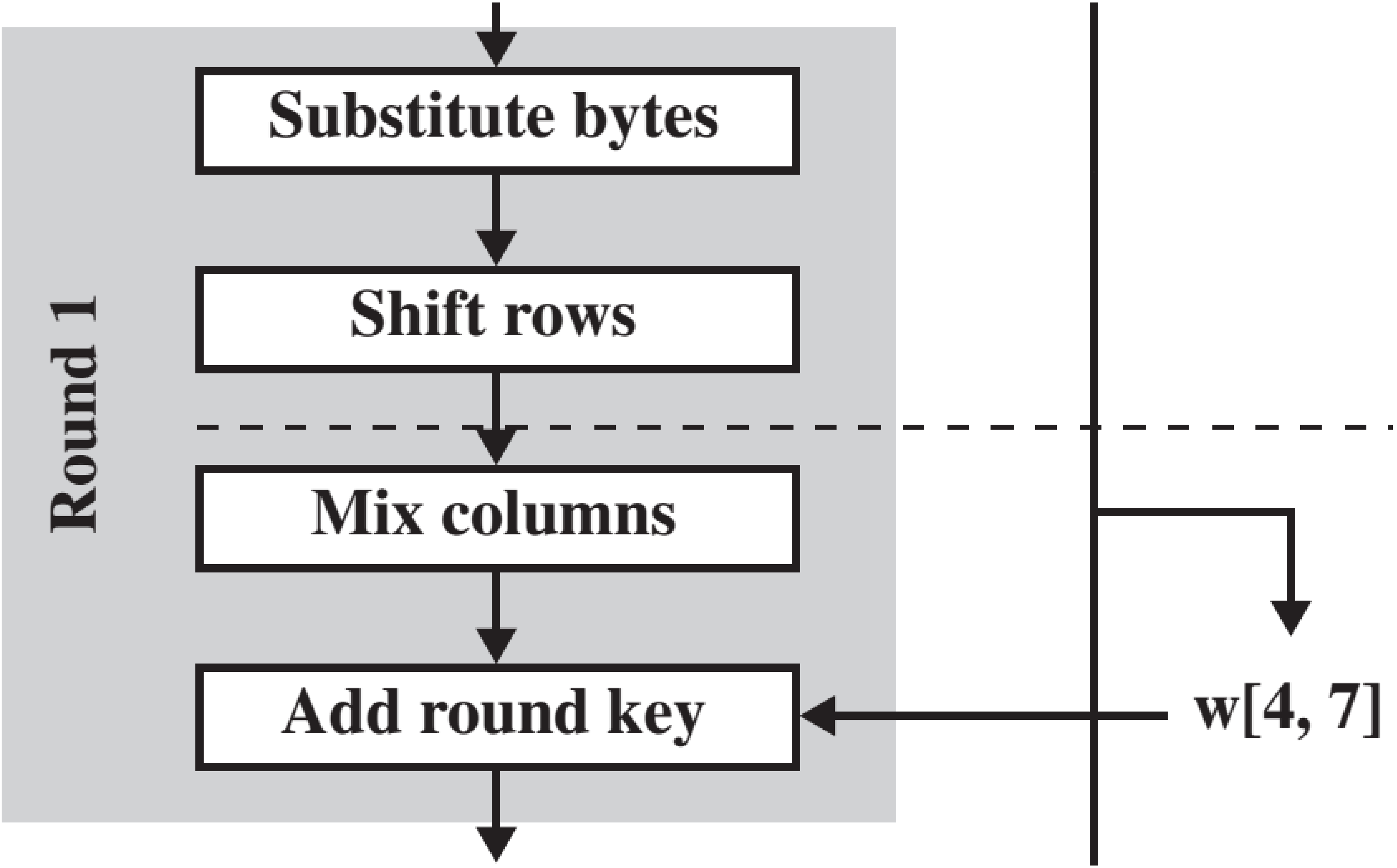
$$\begin{pmatrix} 54 & 4F & 4E & 20 \\ 77 & 6E & 69 & 54 \\ 6F & 65 & 6E & 77 \\ 20 & 20 & 65 & 6F \end{pmatrix} \oplus \begin{pmatrix} 54 & 73 & 20 & 67 \\ 68 & 20 & 4B & 20 \\ 61 & 6D & 75 & 46 \\ 74 & 79 & 6E & 75 \end{pmatrix} = \begin{pmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{pmatrix}$$

AES Encryption



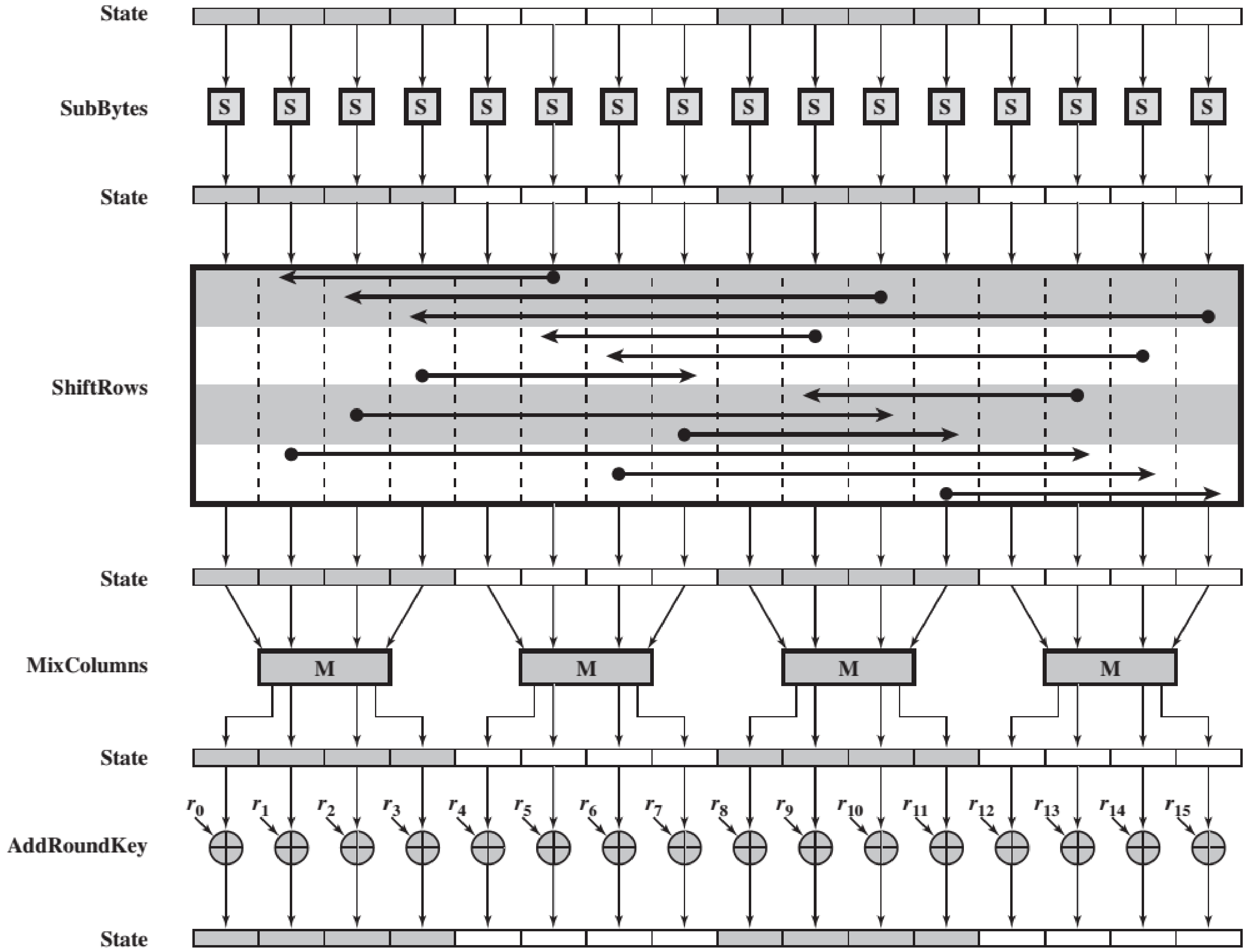
AES Encryption

- Round1:



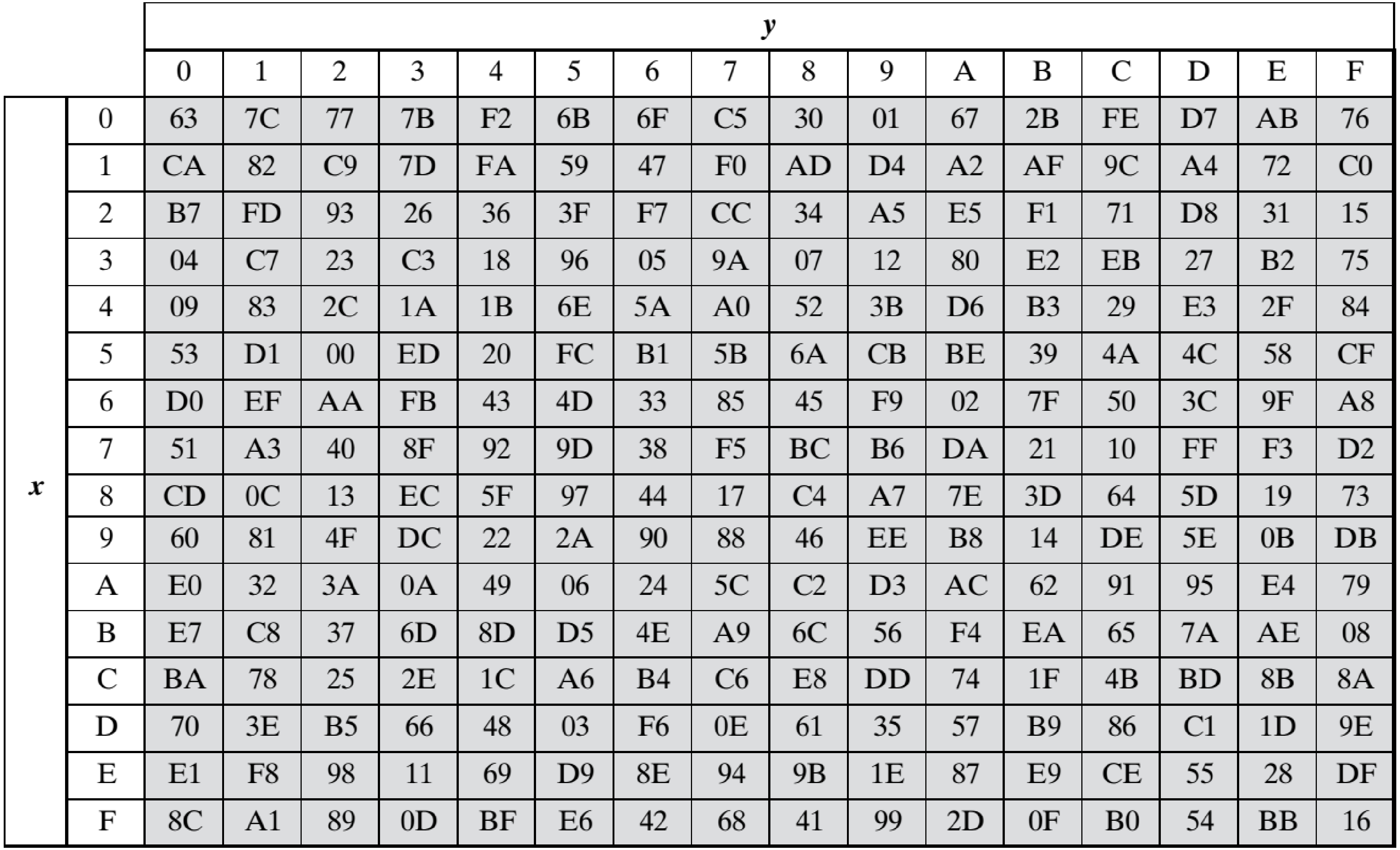
AES Encryption

- AES Encryption Round


State
SubBytes
S
State
ShiftRows
State
MixColumns
M
State
AddRoundKey
r_0 r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8 r_9 r_{10} r_{11} r_{12} r_{13} r_{14} r_{15}
State

AES Encryption

- ❑ S-Box
- ❑ Byte 6E is substituted by entry of S-Box in row 6 and column E ,i.e. by 9F

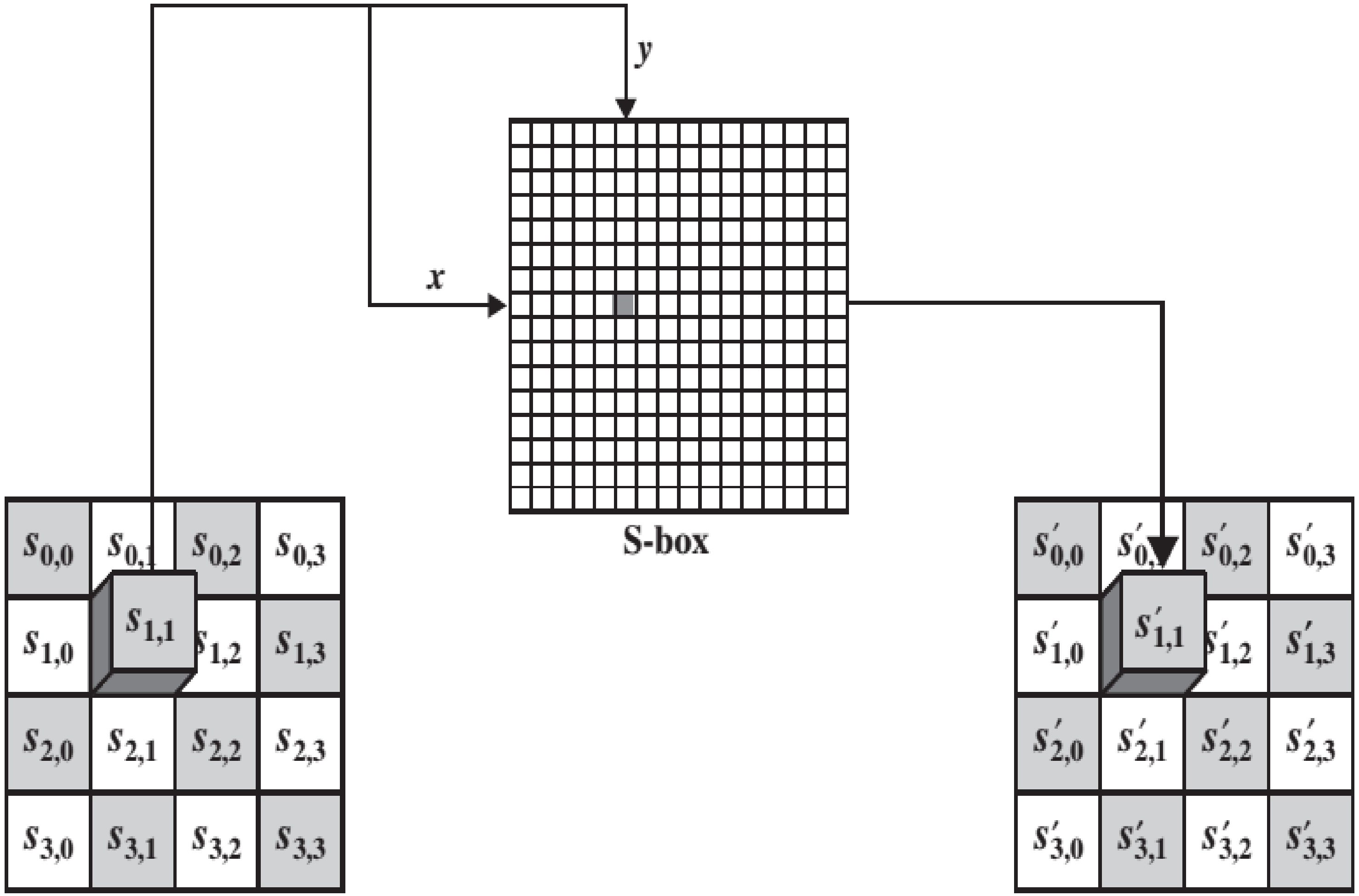


		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
	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
	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
	B	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
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	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

(a) S-box

AES Encryption

- ❑ Substitution transformation


y
x
S-box
$s_{0,0}$ $s_{0,1}$ $s_{0,2}$ $s_{0,3}$
$s_{1,0}$ $s_{1,1}$ $s_{1,2}$ $s_{1,3}$
$s_{2,0}$ $s_{2,1}$ $s_{2,2}$ $s_{2,3}$
$s_{3,0}$ $s_{3,1}$ $s_{3,2}$ $s_{3,3}$
$s'_{0,0}$ $s'_{0,1}$ $s'_{0,2}$ $s'_{0,3}$
$s'_{1,0}$ $s'_{1,1}$ $s'_{1,2}$ $s'_{1,3}$
$s'_{2,0}$ $s'_{2,1}$ $s'_{2,2}$ $s'_{2,3}$
$s'_{3,0}$ $s'_{3,1}$ $s'_{3,2}$ $s'_{3,3}$

AES Encryption

1) Round1,Substitution Bytes:

□ Current State Matrix

$$\begin{pmatrix} 00 & 3C & 6E & 47 \\ 1F & 4E & 22 & 74 \\ 0E & 08 & 1B & 31 \\ 54 & 59 & 0B & 1A \end{pmatrix}$$

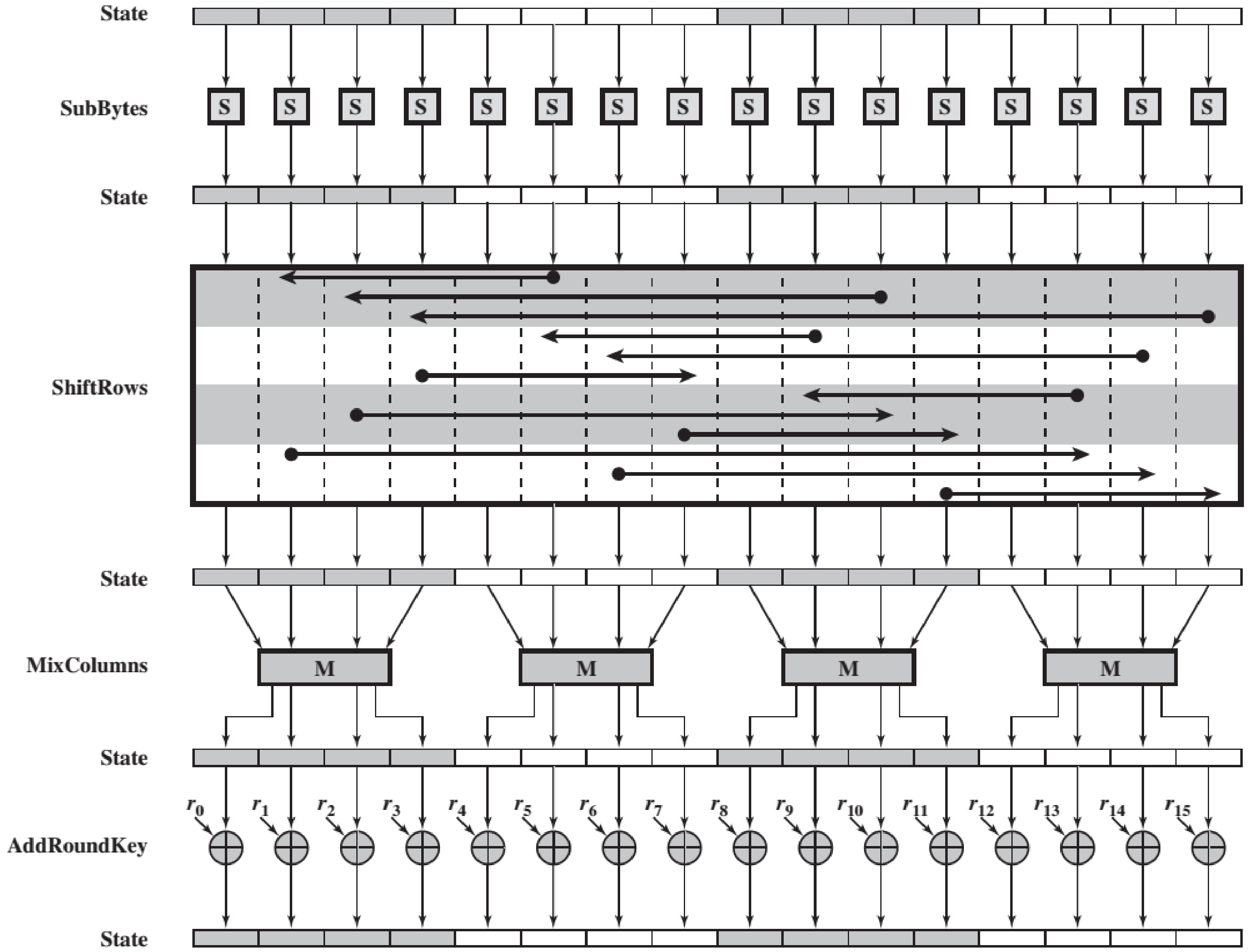
New State Matrix

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{pmatrix}$$

□ This non linear layer is for resistance to differential and linear cryptanalysis attacks

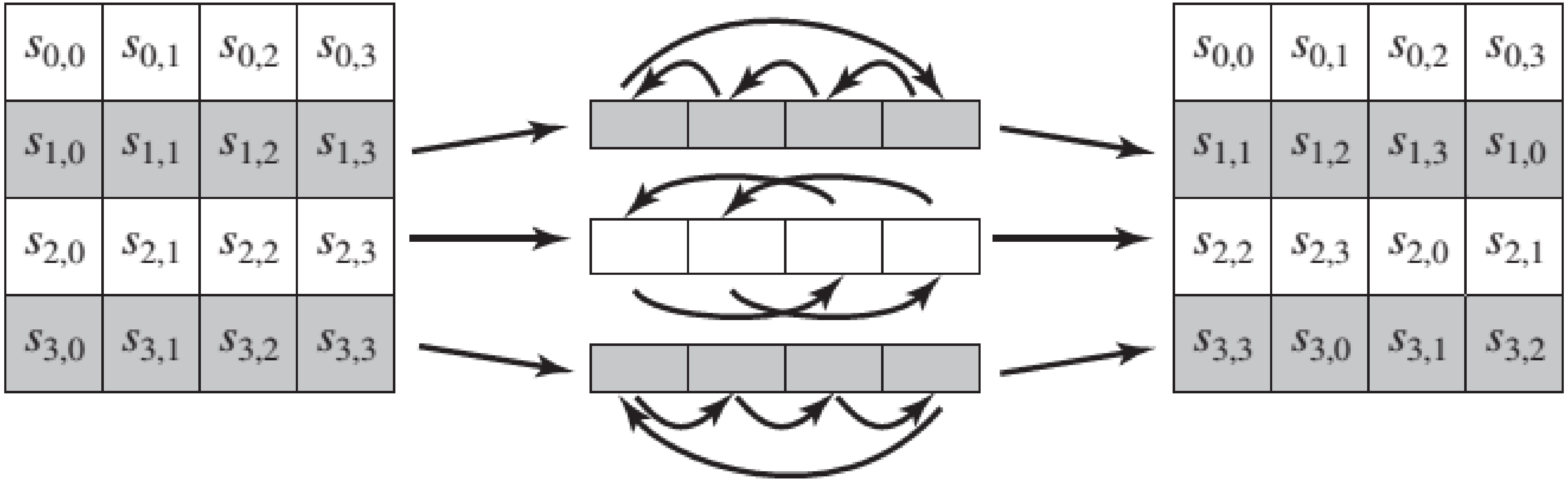
AES Encryption

- ❑ AES Encryption Round


State
SubBytes
S
State
ShiftRows
State
MixColumns
M
State
AddRoundKey
r_0 r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8 r_9 r_{10} r_{11} r_{12} r_{13} r_{14} r_{15}
State

AES Encryption

- Shift row transformation



$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$
$s_{3,0}$	$s_{3,1}$	$s_{3,2}$	$s_{3,3}$

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,1}$	$s_{1,2}$	$s_{1,3}$	$s_{1,0}$
$s_{2,2}$	$s_{2,3}$	$s_{2,0}$	$s_{2,1}$
$s_{3,3}$	$s_{3,0}$	$s_{3,1}$	$s_{3,2}$

AES Encryption

2) Round1,Shift Row:

□ Current State Matrix

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{pmatrix}$$

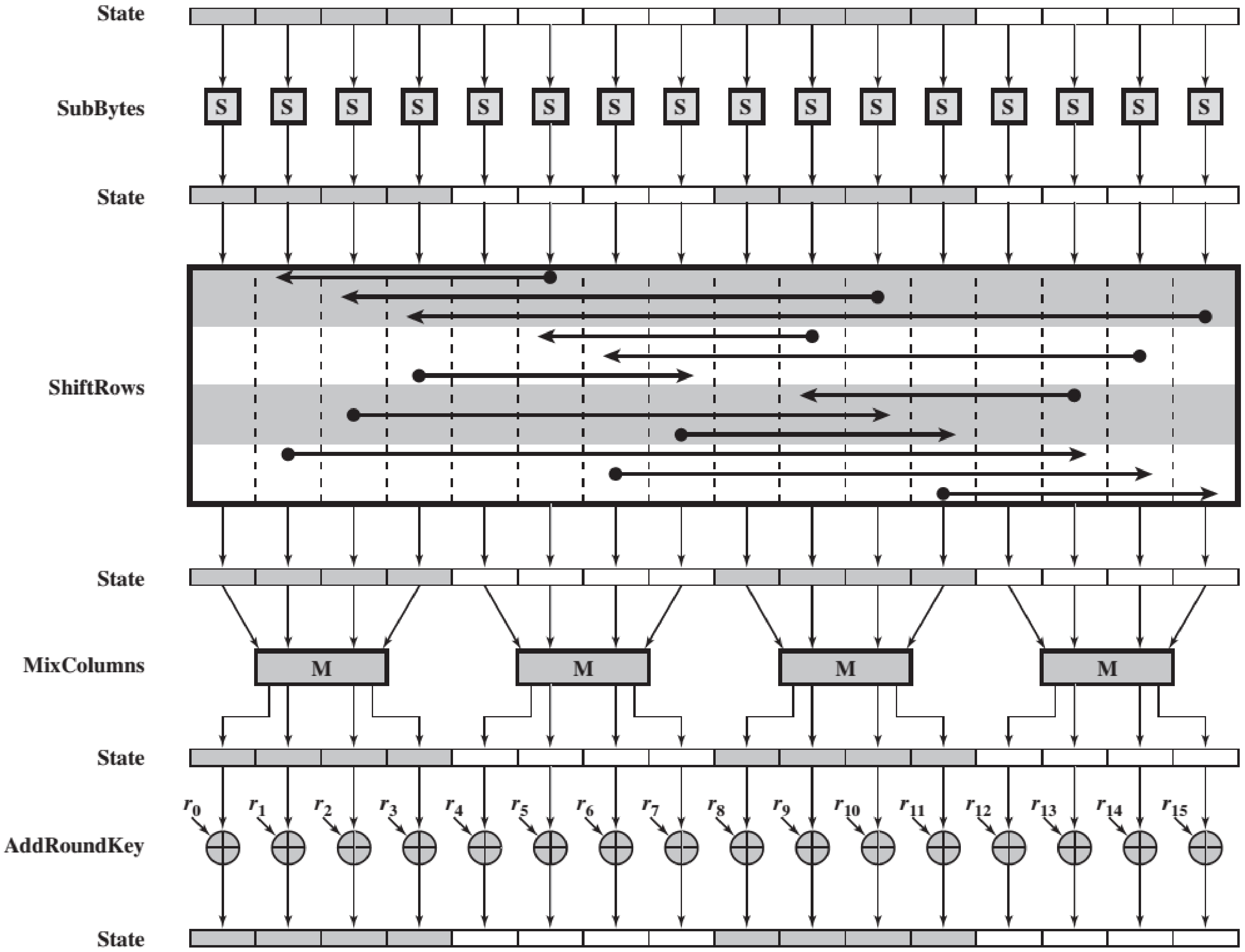
New State Matrix

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix}$$

□ This linear mixing step causes diffusion of the bits over multiple rounds

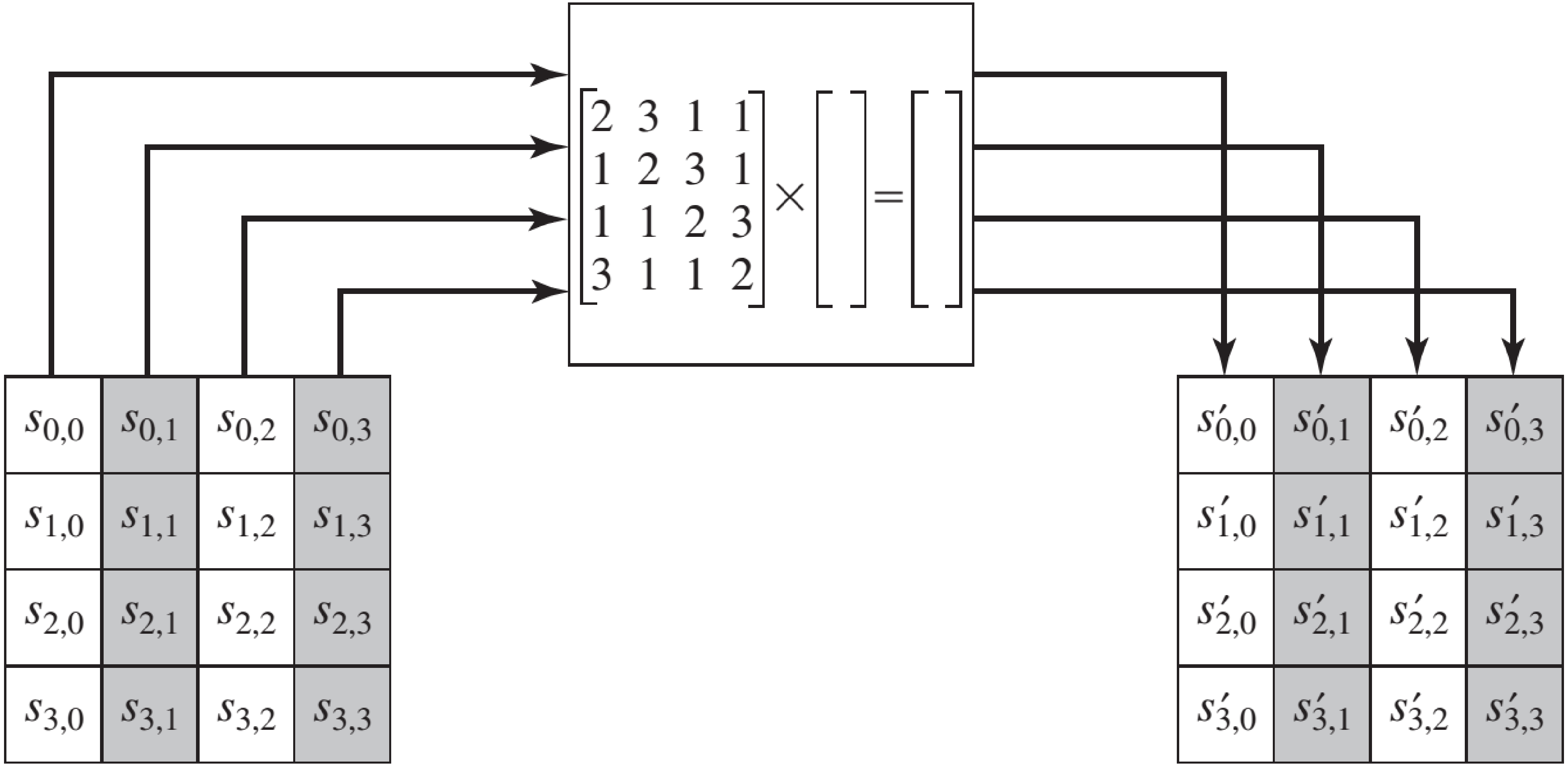
AES Encryption

- ❑ AES Encryption Round



AES Encryption

- Mix column transformation



$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} \; \end{bmatrix} = \begin{bmatrix} \; \end{bmatrix}$$

$$\begin{bmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{bmatrix}$$

$$\begin{bmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{bmatrix}$$

AES Encryption

3) Round1, Mix Column

❑ Current State Matrix New State Matrix

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix} \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} = \begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix}$$

AES Encryption

- Round1, Mix Column

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AF & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{pmatrix} = \begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix}$$

- Entry BA is result of (02• 63)⊕(03•2F)⊕(01•AF) ⊕(01•A2)

- 02•63=00000010•01100011=**11000110 (shift left)**

- 03•2F=(02•2F)⊕2F =

(00000010•00101111)⊕00101111= **01110001**

- 01•AF = AF =**10101111**

- 01•A2 = A2 =**10100010**

$$\begin{array}{cc} & 11000110 \\ & 01110001 \\ \oplus & 10101111 \\ & 10100010 \\ \hline & 10111010 \end{array}$$

AES Encryption

- ❑ Round1, Mix Column

- ❑ 02•63=00000010•01100011=**11000110 (shift left) =**

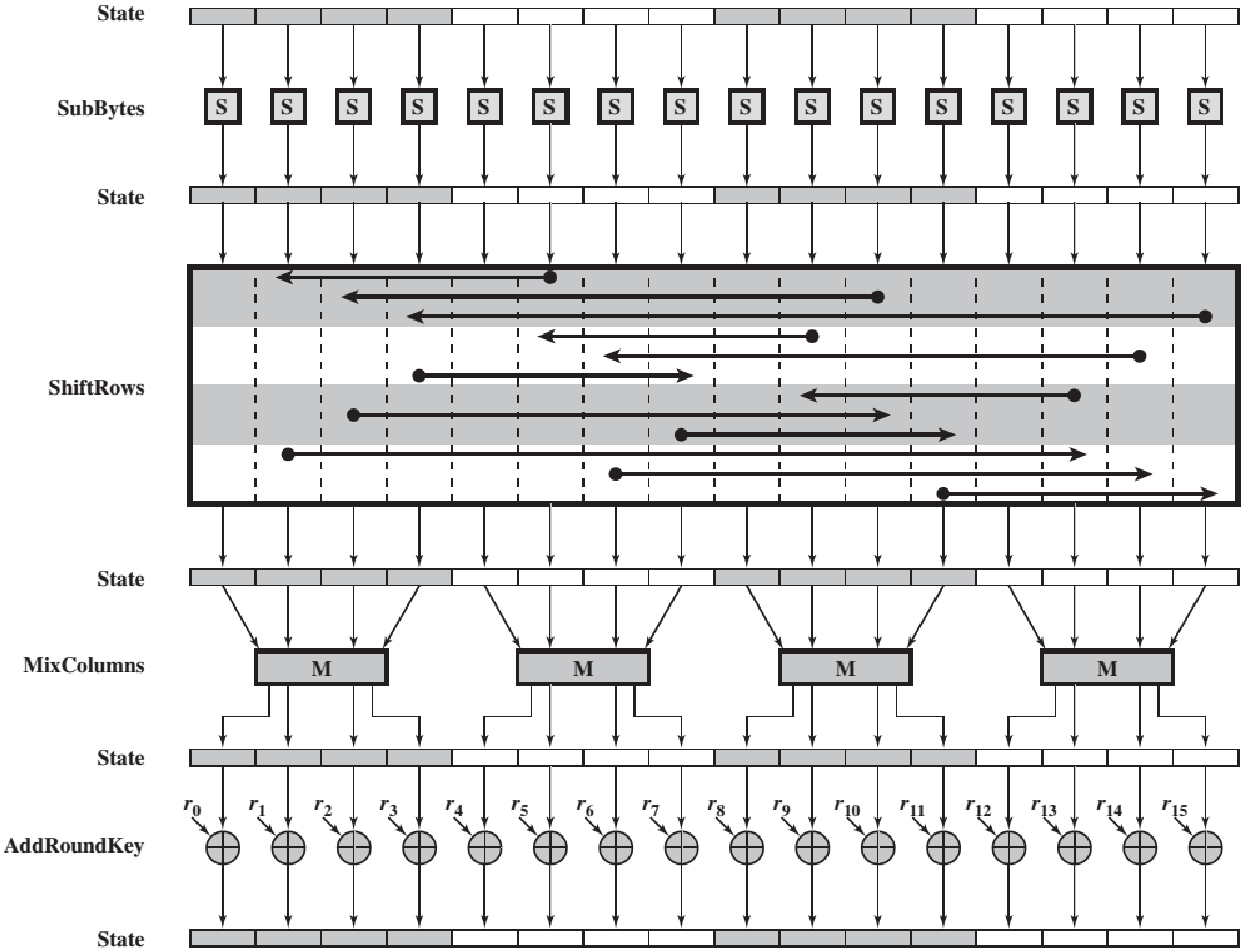
- ❑ 02•F2 = 00000010•11110010 = 01110010 ⊕ 1B=

01110010 ⊕ 0001 1011= 01101001

- ❑ 02 • 87 = 0000 0010•1000 1110 = 00001110 ⊕ 0001 1011 = 0001 0101

AES Encryption

- AES Encryption Round



State
SubBytes
S
State
ShiftRows
State
MixColumns
M
State
AddRoundKey
r_0 r_1 r_2 r_3 r_4 r_5 r_6 r_7 r_8 r_9 r_{10} r_{11} r_{12} r_{13} r_{14} r_{15}
State

AES Encryption

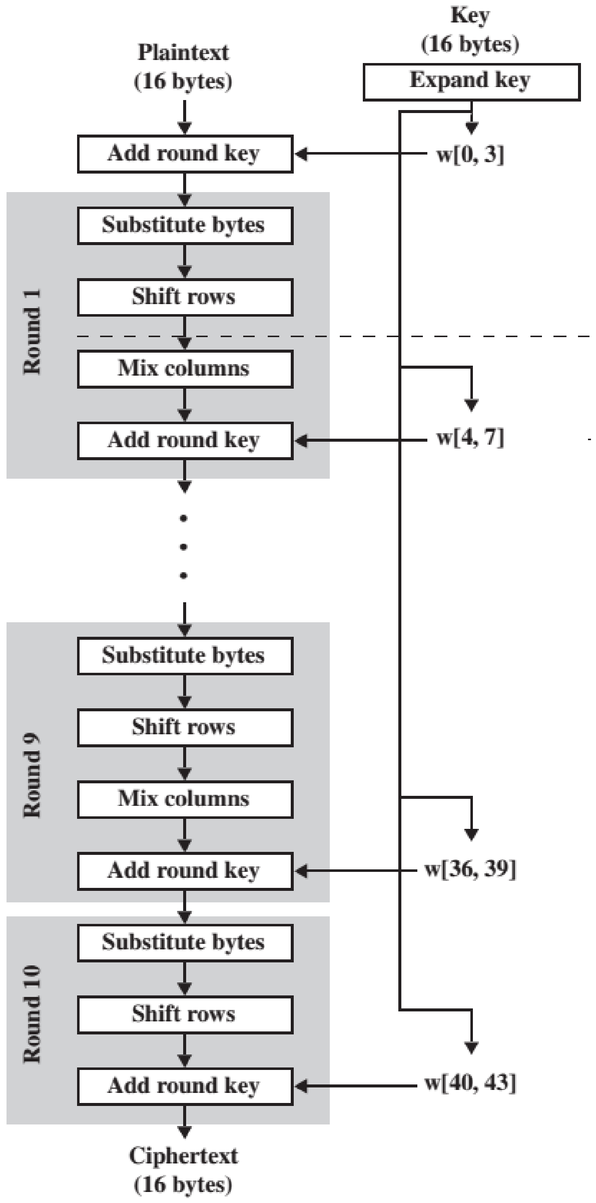
4) Round 1, Add Round key

❑ Round1:E2 32 FC F1 91 12 91 88 B1 59 E4 E6 D6 79 A2 93

❑ Current State Matrix Round1 New State Matrix

$$\begin{pmatrix} BA & 84 & E8 & 1B \\ 75 & A4 & 8D & 40 \\ F4 & 8D & 06 & 7D \\ 7A & 32 & 0E & 5D \end{pmatrix} \oplus \begin{pmatrix} E2 & 91 & B1 & D6 \\ 32 & 12 & 59 & 79 \\ FC & 91 & E4 & A2 \\ F1 & 88 & E6 & 93 \end{pmatrix} = \begin{pmatrix} 58 & 15 & 59 & CD \\ 47 & B6 & D4 & 39 \\ 08 & 1C & E2 & DF \\ 8B & BA & E8 & CE \end{pmatrix}$$

AES Encryption



AES Encryption

- ❑ Round 2

after Substitute Byte and after Shift Rows:

$$\begin{pmatrix} 6A & 59 & CB & BD \\ A0 & 4E & 48 & 12 \\ 30 & 9C & 98 & 9E \\ 3D & F4 & 9B & 8B \end{pmatrix} \qquad \begin{pmatrix} 6A & 59 & CB & BD \\ 4E & 48 & 12 & A0 \\ 98 & 9E & 30 & 9B \\ 8B & 3D & F4 & 9B \end{pmatrix}$$

after Mixcolumns and after Roundkey:

$$\begin{pmatrix} 15 & C9 & 7F & 9D \\ CE & 4D & 4B & C2 \\ 89 & 71 & BE & 88 \\ 65 & 47 & 97 & CD \end{pmatrix} \qquad \begin{pmatrix} 43 & 0E & 09 & 3D \\ C6 & 57 & 08 & F8 \\ A9 & C0 & EB & 7F \\ 62 & C8 & FE & 37 \end{pmatrix}$$

AES Encryption

- □ Round 9

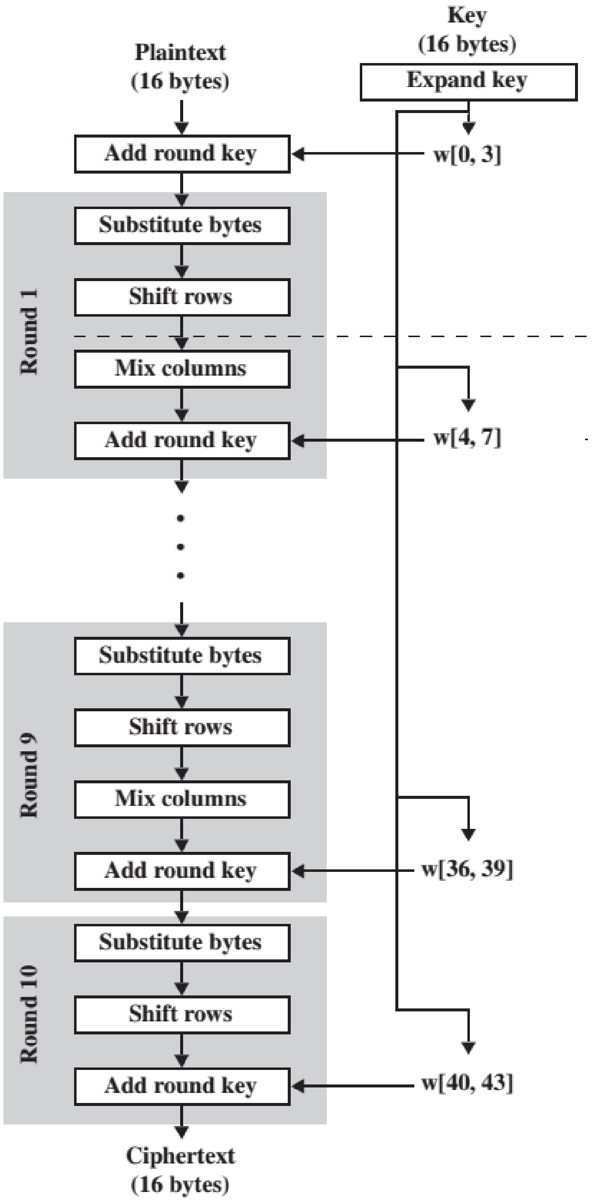
after Substitute Byte and after Shift Rows:

$$\begin{pmatrix} 33 & 51 & 79 & 0A \\ 3F & 8B & 66 & 8F \\ EB & BE & 76 & 7D \\ 92 & C2 & 67 & 20 \end{pmatrix} \qquad \begin{pmatrix} 33 & 51 & 79 & 0A \\ 8B & 66 & 8F & 3F \\ 76 & 7D & EB & BE \\ 20 & 92 & C2 & 67 \end{pmatrix}$$

after Mixcolumns and after Roundkey:

$$\begin{pmatrix} B6 & E7 & 51 & 8C \\ 84 & 88 & 98 & CA \\ 34 & 60 & 66 & FB \\ E8 & D7 & 70 & 51 \end{pmatrix} \qquad \begin{pmatrix} 09 & A2 & F0 & 7B \\ 66 & D1 & FC & 3B \\ 8B & 9A & E6 & 30 \\ 78 & 65 & C4 & 89 \end{pmatrix}$$

AES Encryption



AES Encryption

- ❑ Round 10

after Substitute Byte and after Shift Rows:

$$\begin{pmatrix} 01 & 3A & 8C & 21 \\ 33 & 3E & B0 & E2 \\ 3D & B8 & 8E & 04 \\ BC & 4D & 1C & A7 \end{pmatrix} \qquad \begin{pmatrix} 01 & 3A & 8C & 21 \\ 3E & B0 & E2 & 33 \\ 8E & 04 & 3D & B8 \\ A7 & BC & 4D & 1C \end{pmatrix}$$

after Roundkey (Attention: no Mix columns in last round):

$$\begin{pmatrix} 29 & 57 & 40 & 1A \\ C3 & 14 & 22 & 02 \\ 50 & 20 & 99 & D7 \\ 5F & F6 & B3 & 3A \end{pmatrix}$$

- ❑ ciphertext:29 C3 50 5F 57 14 20 F6 40 22 99 B3 1A 02 D7 3A

Table of Contents

Advanced Encryption Standard

AES Key Expansion

AES Encryption

AES Decryption

DES vs AES

Advantages of AES

AES Decryption

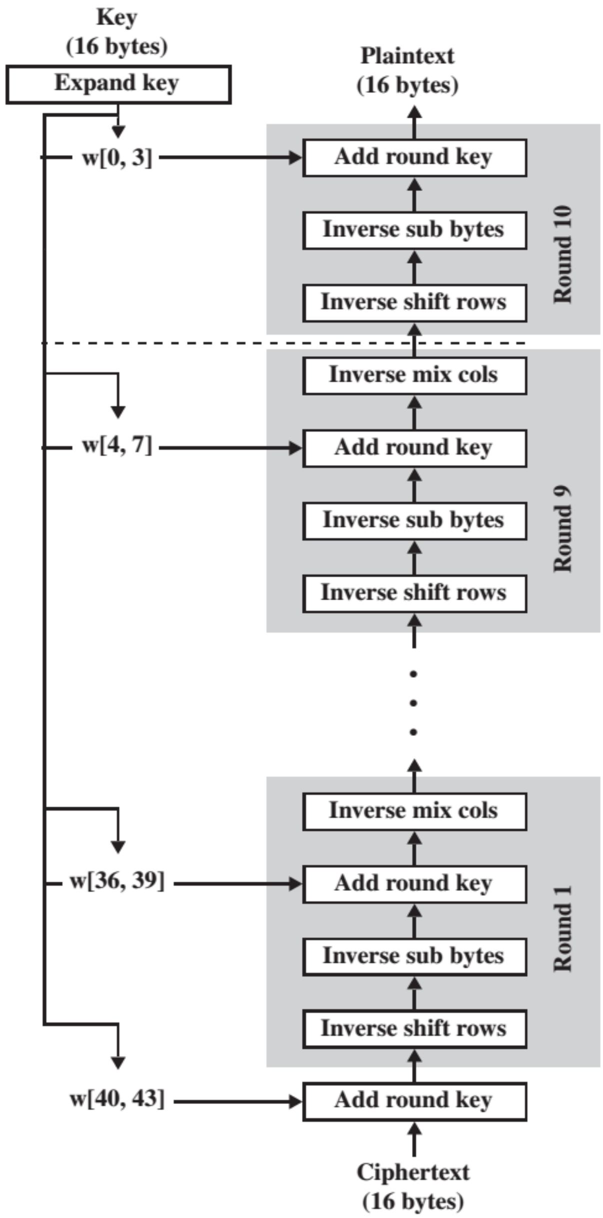


Table of Contents

- Advanced Encryption Standard
- AES Key Expansion
- AES Encryption
- AES Decryption
- DES vs AES
- Advantages of AES

DES vs AES

	DES	AES
Date	1977	2001
Block Size	64	128
Key Size	56	128, 192, 256
Number of Rounds	16	9, 11, 13
Design	open	Open
Encryption primitives	Substitution, Permutation	Substitution, Shift, Mixing
Cryptographic primitives	Confusion, diffusion	Confusion, diffusion

Table of Contents

- Advanced Encryption Standard
- AES Key Expansion
- AES Encryption
- AES Decryption
- DES vs AES
- **Advantages of AES**

Advantages of AES

- ❑ The key is much stronger due to the key length
- ❑ AES runs faster than 3DES on comparable hardware
- ❑ AES is more efficient than DES and 3DES on comparable hardware

THANKS FOR YOUR TIME