Advanced Encryption Standard

(AES)

LEARNING OBJECTIVES

After studying this chapter, you should be able to:

- Present an overview of the general structure of Advanced Encryption Standard (AES).
- Understand the four transformations used in AES.
- Explain the AES key expansion algorithm.

OVERVIEW OF AES

AES Was published by the NIST in 2001.

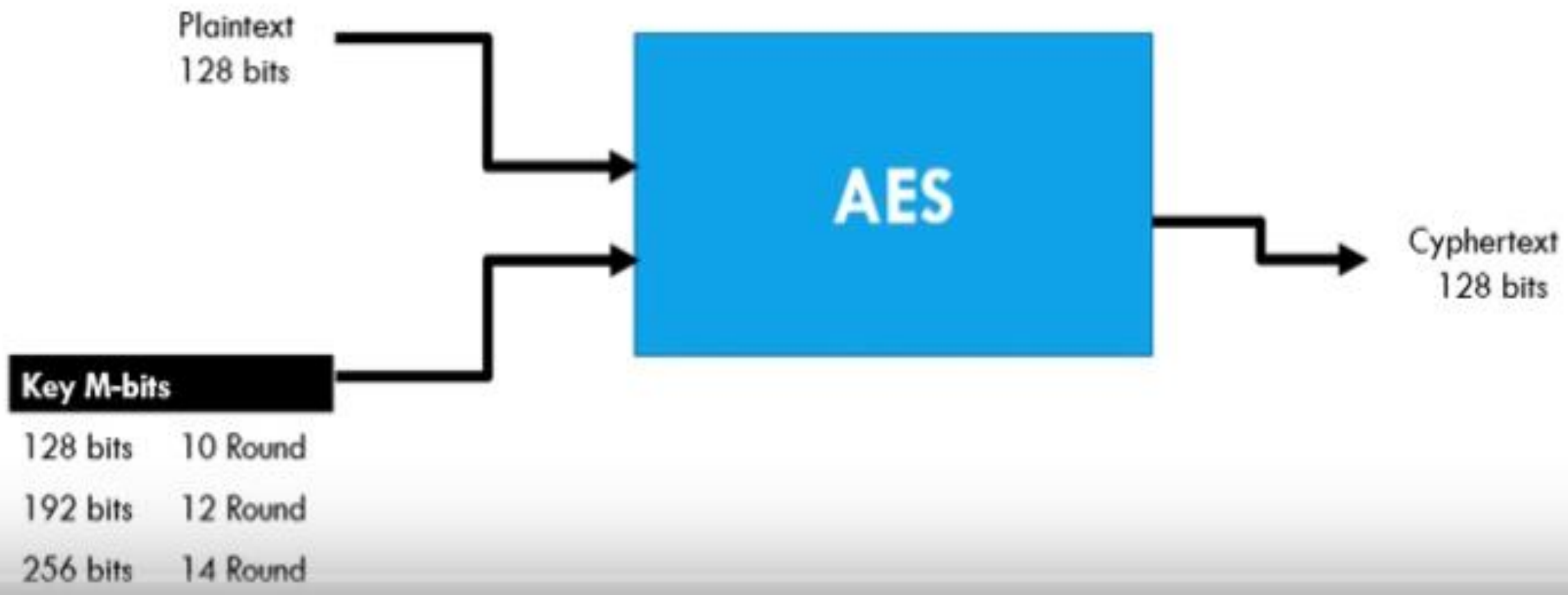
It is a symmetric key encryption algorithm.

It was originally called "Rijndael Cipher" after the name of the developers.

AES is a block cipher encrypt 128-bits (16 bytes) of data at a time.

It treats the 16 bytes as a grid of 4x4. Messages which are longer than 128 bits are broken into blocks of 128 bits. (Each block is encrypted by same steps separately)

AES DESIGN


Plaintext
128 bits
AES
Cyphertext
128 bits
Key M-bits
128 bits 10 Round
192 bits 12 Round
256 bits 14 Round

INPUTS

Message:	32	43	f6	a8	88	5a	30	8d	31	31	98	a2	e0	37	07	34
Key :	2b	7e	15	16	28	ae	d2	a6	ab	f7	15	88	09	cf	4f	3c

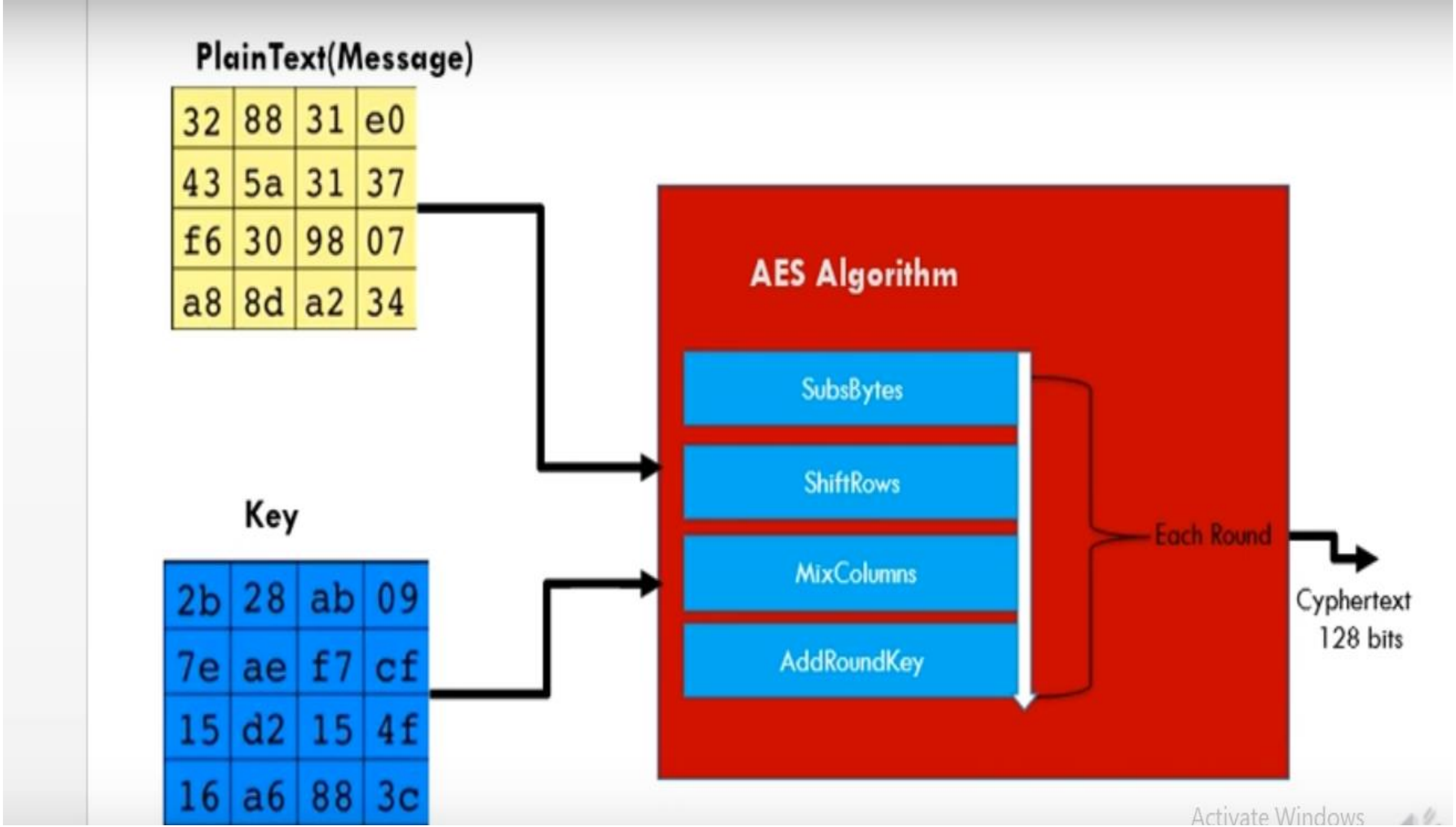
State (Matrix)

Message

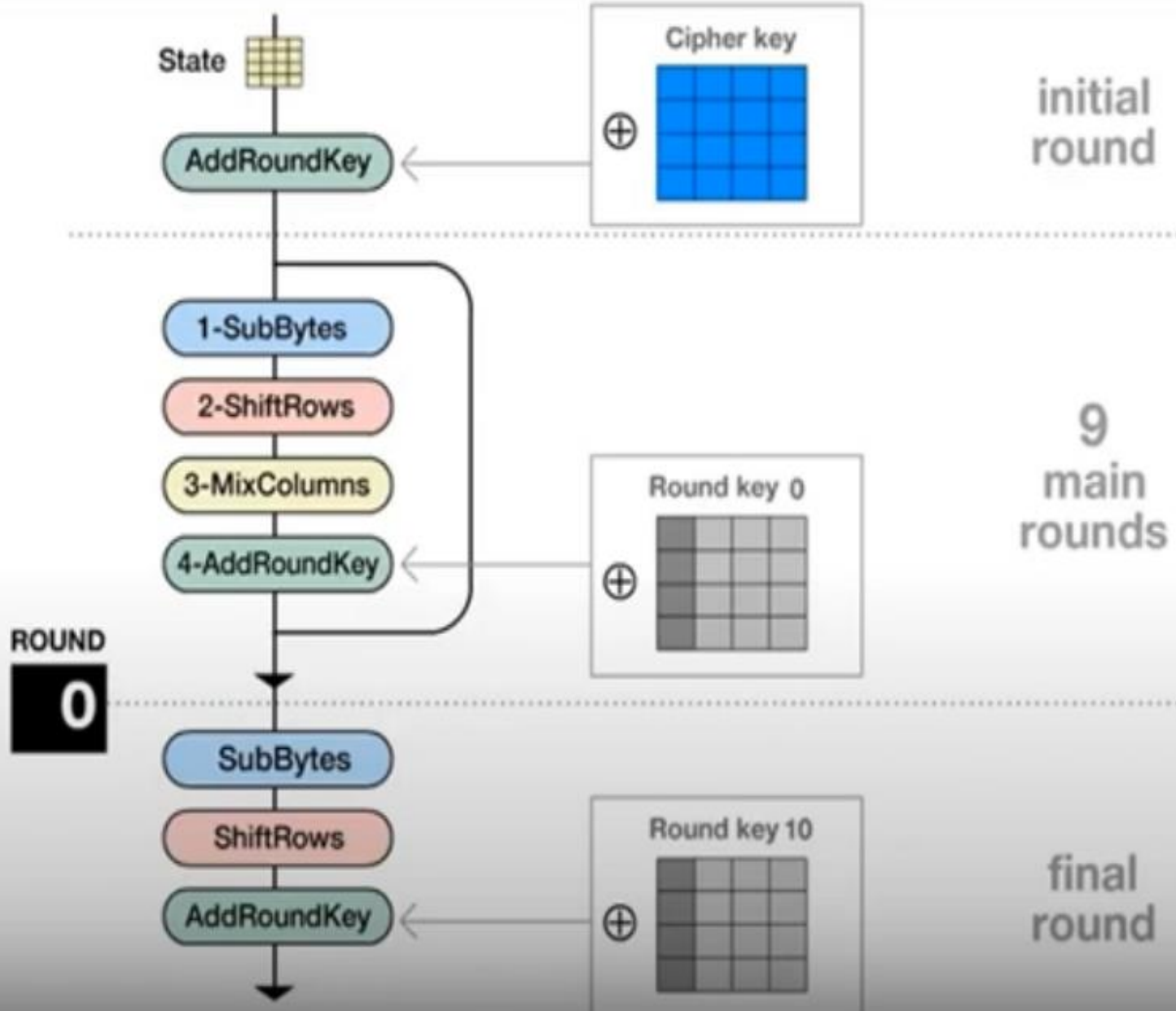
32	88	31	e0
43	5a	31	37
f6	30	98	07
a8	8d	a2	34

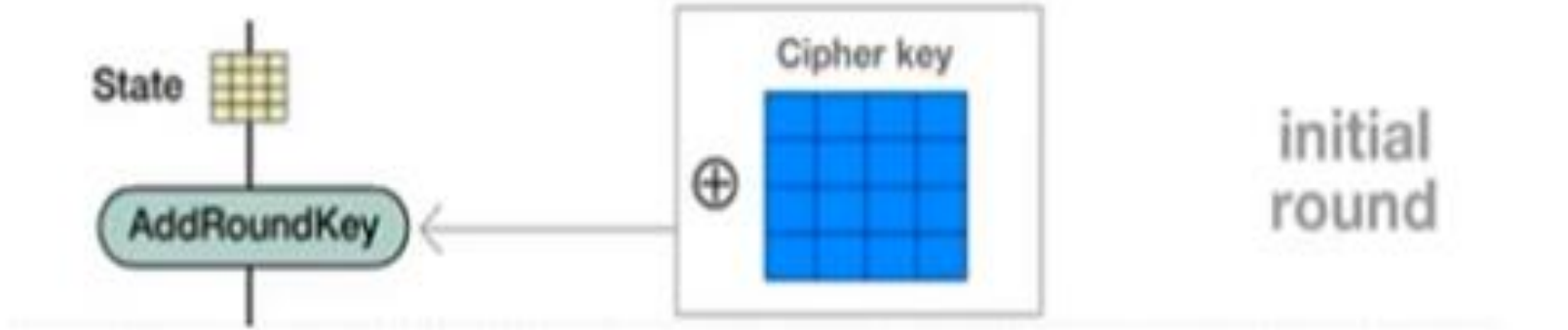
Key

2b	28	ab	09
7e	ae	f7	cf
15	d2	15	4f
16	a6	88	3c



Encryption Process





PlainText(Message)

32	88	31	e0
43	5a	31	37
f6	30	98	07
a8	8d	a2	34

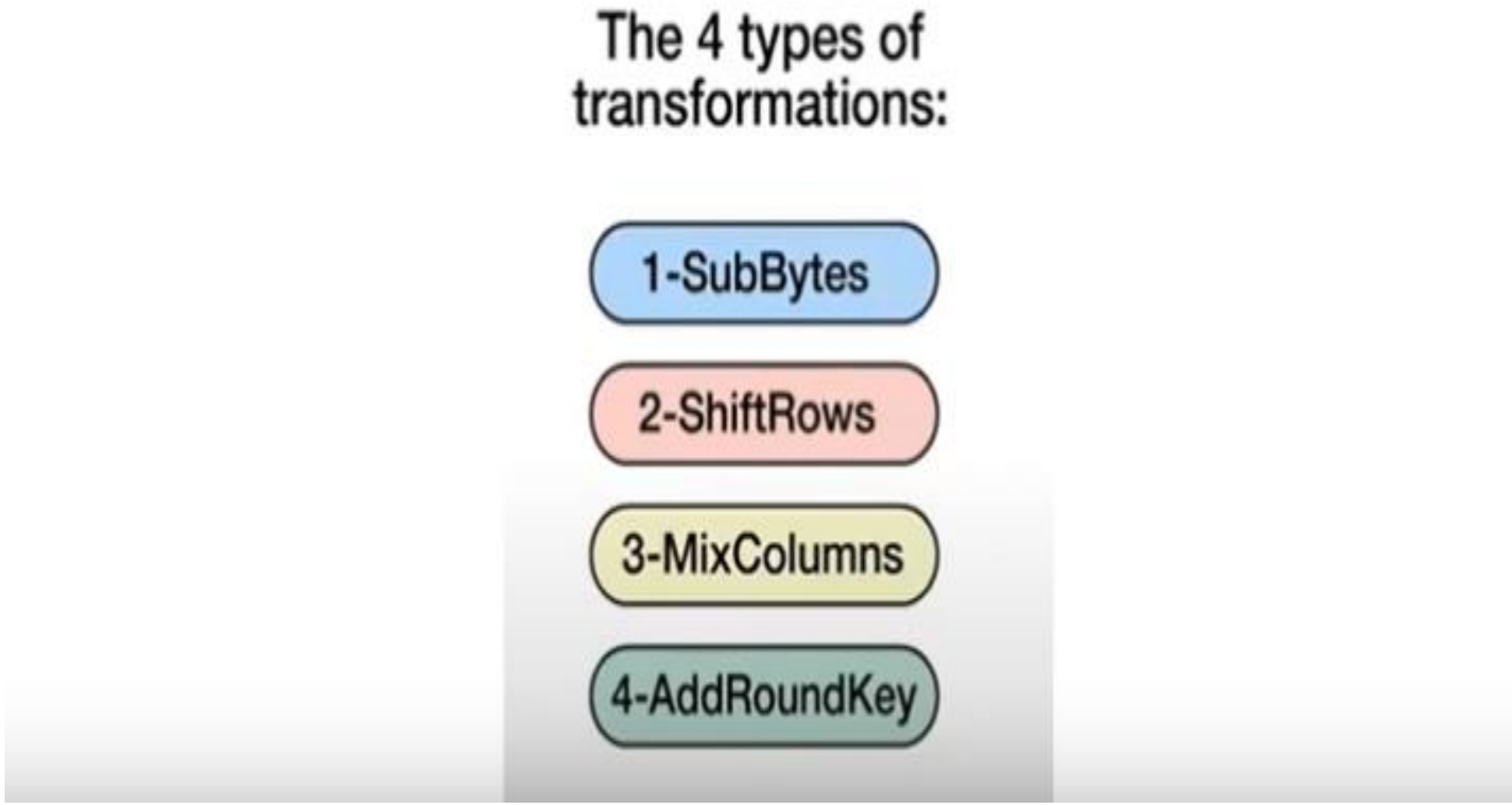
⊕

Key

2b	28	ab	09
7e	ae	f7	cf
15	d2	15	4f
16	a6	88	3c

→

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08


The 4 types of transformations:
1-SubBytes
2-ShiftRows
3-MixColumns
4-AddRoundKey

1- SubsBytes

19	a0	9a	e9
3d	f4	c6	f8
e3	e2	8d	48
be	2b	2a	08

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

(Table can be found

(a) S-box

x \ y	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	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	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

2- ShiftRows

d4	e0	b8	1e
27	bf	b4	41
11	98	5d	52
ae	f1	e5	30

Rotate Over 1 Byte

Rotate Over 2 Byte

Rotate Over 3 Byte

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

3- MixColumns

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

×

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

=

04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

d4	11010100
bf	10111111
5d	01011101
30	00110000
1b	00011011

(d4 . 02) ⊕ (bf . 03) ⊕ (5d) ⊕ (30) = 04

d4	e0	b8	1e
bf	b4	41	27
5d	52	11	98
30	ae	f1	e5

×

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

=

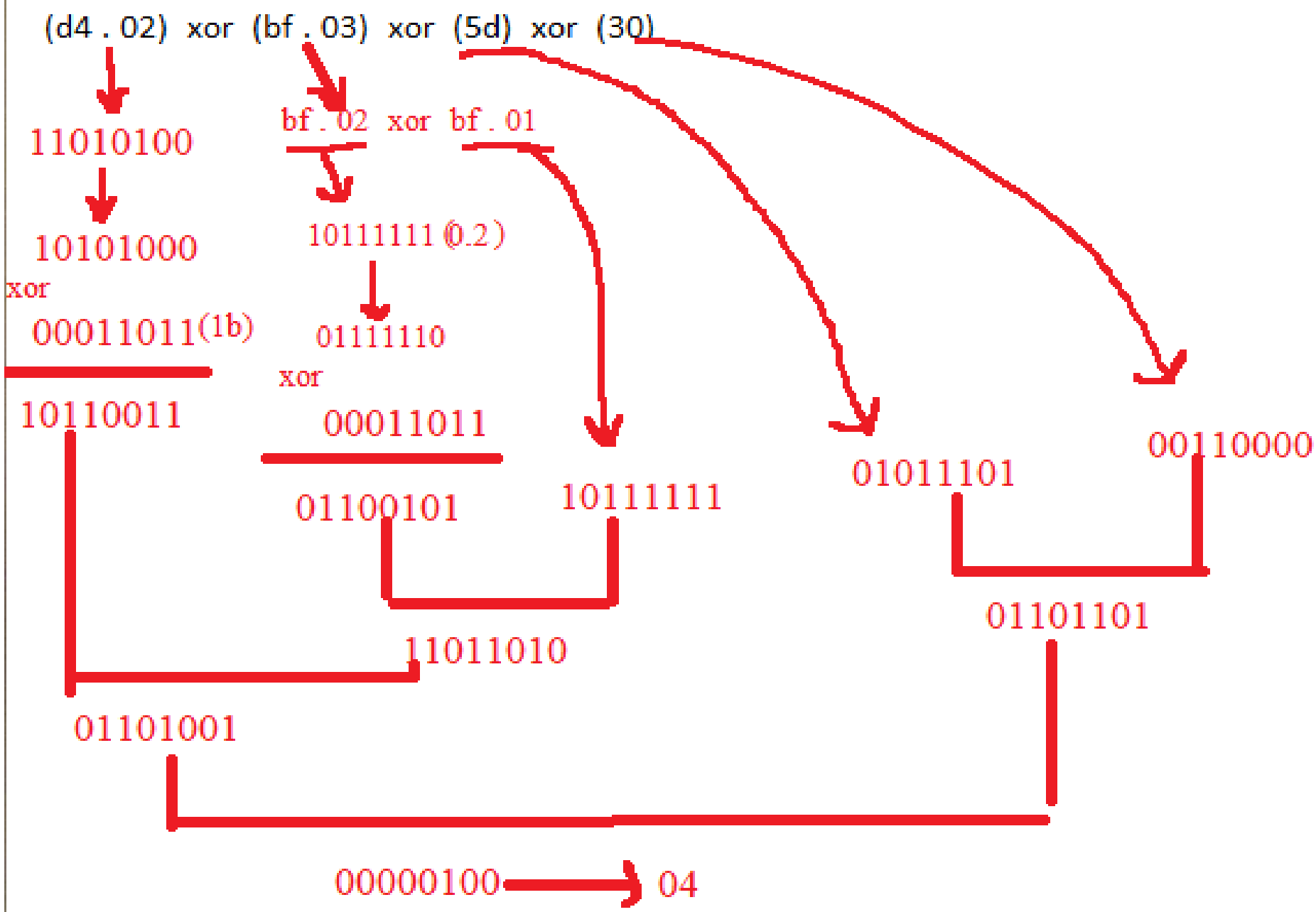
04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

5d . 01 30 . 01

(d4 . 02) ⊕ (bf . 03) ⊕ (5d) ⊕ (30) = 04

d4	11010100
bf	10111111
5d	01011101
30	00110000
1b	00011011

1- When multiply with 01 the value stay the same
2- When multiply with 02 if the number start with 0 we shift this zero left to the last bit.
- When multiply with 02 if the number start with 1 we delete this one and adding zero to the last left bit then we make XOR with 1B.
3- When multiply with 0.3 we split it into 01.02


(d4 . 02) xor (bf . 03) xor (5d) xor (30)
11010100
bf . 02 xor bf . 01
10101000
10111111 (02)
xor
00011011(1b)
01111110
xor
10110011
00011011
01100101
10111111
01011101
00110000
11011010
01101101
01101001
00000100
04

4- AddRoundKey

04	e0	48	28
66	cb	f8	06
81	19	d3	26
e5	9a	7a	4c

$\oplus$

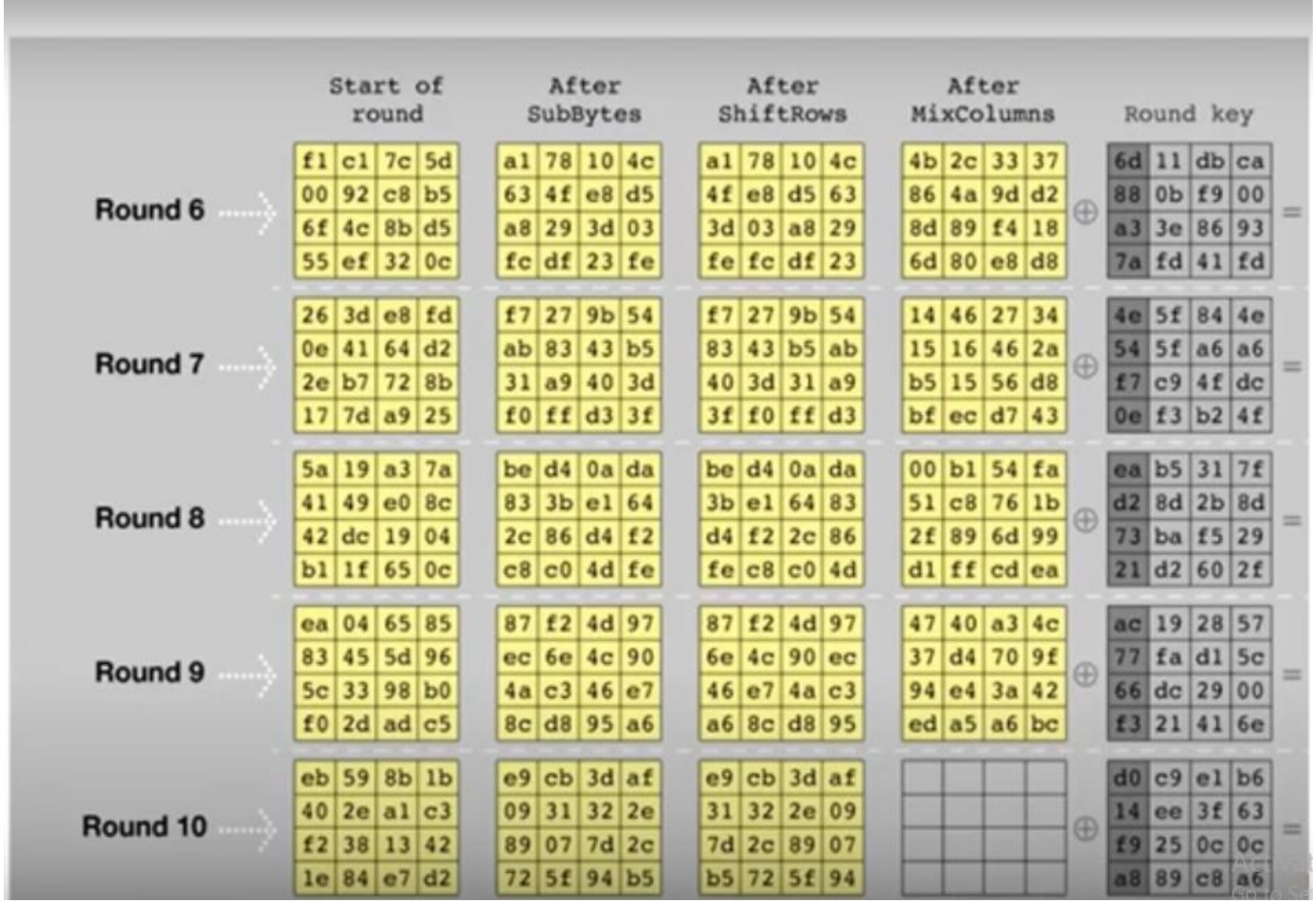
a0	88	23	2a
fa	54	a3	6c
fe	2c	39	76
17	b1	39	05

$=$

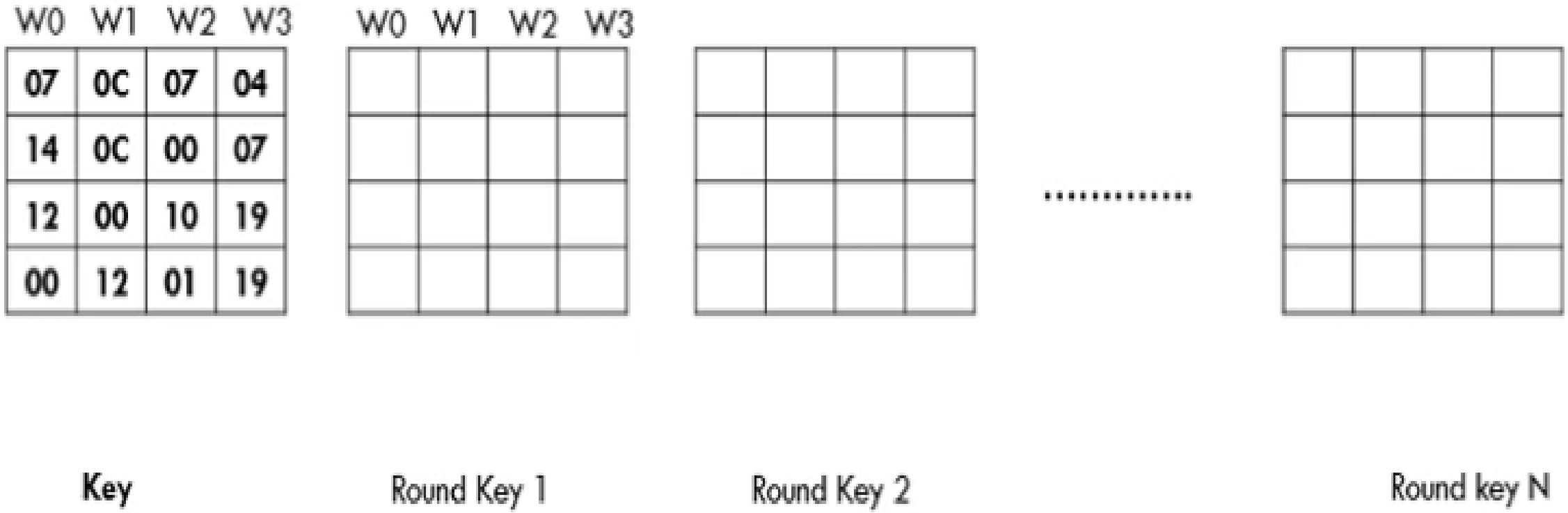
a4	68	6b	02
9c	9f	5b	6a
7f	35	ea	50
f2	2b	43	49

04	$\oplus$	a0	= a4
66		fa	9c
81		fe	7f
e5		17	f2

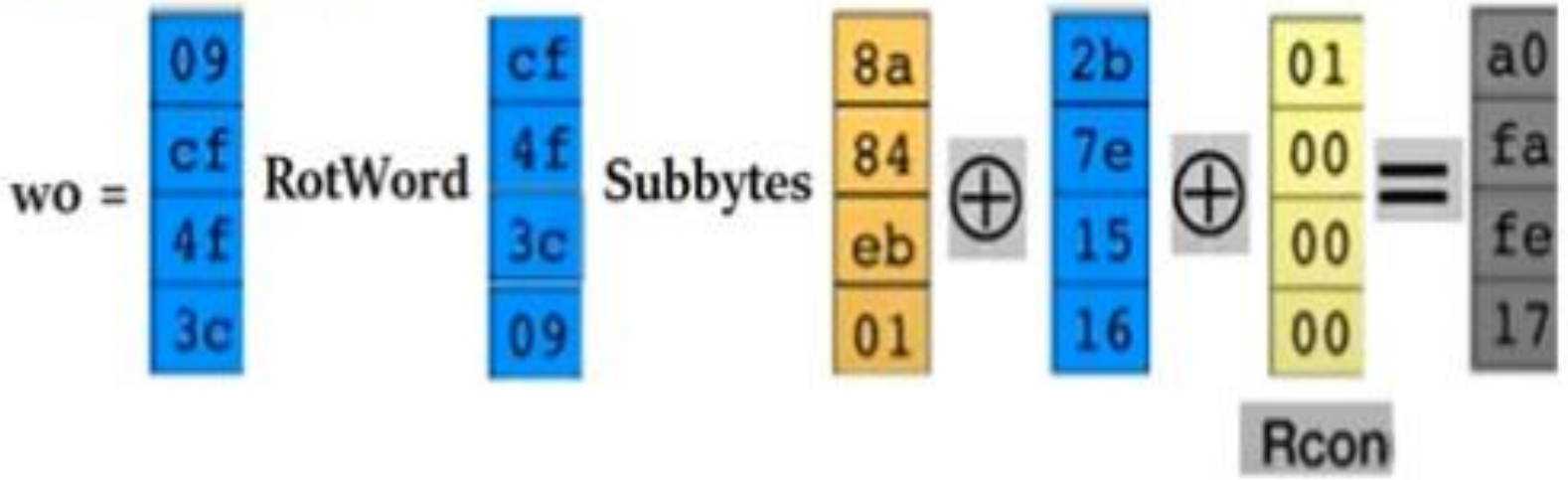

Start of round
After SubBytes
After ShiftRows
After MixColumns
Round key
Input
32 88 31 e0
43 5a 31 37
f6 30 98 07
a8 8d a2 34
2b 28 ab 09
7e ae f7 cf
15 d2 15 4f
16 a6 88 3c
Round 1
19 a0 9a e9
3d f4 c6 f8
e3 e2 8d 48
be 2b 2a 08
d4 e0 b8 1e
27 bf b4 41
11 98 5d 52
ae f1 e5 30
d4 e0 b8 1e
bf b4 41 27
5d 52 11 98
30 ae f1 e5
04 e0 48 28
66 cb f8 06
81 19 d3 26
e5 9a 7a 4c
a0 88 23 2a
fa 54 a3 6c
fe 2c 39 76
17 b1 39 05
Round 2
a4 68 6b 02
9c 9f 5b 6a
7f 35 ea 50
f2 2b 43 49
49 45 7f 77
de db 39 02
d2 96 87 53
89 f1 1a 3b
49 45 7f 77
db 39 02 de
87 53 d2 96
3b 89 f1 1a
58 1b db 1b
4d 4b e7 6b
ca 5a ca b0
f1 ac a8 e5
f2 7a 59 73
c2 96 35 59
95 b9 80 f6
f2 43 7a 7f
Round 3
aa 61 82 68
8f dd d2 32
5f e3 4a 46
03 ef d2 9a
ac ef 13 45
73 c1 b5 23
cf 11 d6 5a
7b df b5 b8
ac ef 13 45
c1 b5 23 73
d6 5a cf 11
b8 7b df b5
75 20 53 bb
ec 0b c0 25
09 63 cf d0
93 33 7c dc
3d 47 1e 6d
80 16 23 7a
47 fe 7e 88
7d 3e 44 3b
Round 4
48 67 4d d6
6c 1d e3 5f
4e 9d b1 58
ee 0d 38 e7
52 85 e3 f6
50 a4 11 cf
2f 5e c8 6a
28 d7 07 94
52 85 e3 f6
a4 11 cf 50
c8 6a 2f 5e
94 28 d7 07
0f 60 6f 5e
d6 31 c0 b3
da 38 10 13
a9 bf 6b 01
ef a8 b6 db
44 52 71 0b
a5 5b 25 ad
41 7f 3b 00
Round 5
e0 c8 d9 85
92 63 b1 b8
7f 63 35 be
e8 c0 50 01
e1 e8 35 97
4f fb c8 6c
d2 fb 96 ae
9b ba 53 7c
e1 e8 35 97
fb c8 6c 4f
96 ae d2 fb
7c 9b ba 53
25 bd b6 4c
d1 11 3a 4c
a9 d1 33 c0
ad 68 8e b0
d4 7c ca 11
d1 83 f2 f9
c6 9d b8 15
f8 87 bc bc


Start of round
After SubBytes
After ShiftRows
After MixColumns
Round key
Round 6
f1 c1 7c 5d
00 92 c8 b5
6f 4c 8b d5
55 ef 32 0c
a1 78 10 4c
63 4f e8 d5
a8 29 3d 03
fc df 23 fe
a1 78 10 4c
4f e8 d5 63
3d 03 a8 29
fe fc df 23
4b 2c 33 37
86 4a 9d d2
8d 89 f4 18
6d 80 e8 d8
6d 11 db ca
88 0b f9 00
a3 3e 86 93
7a fd 41 fd
Round 7
26 3d e8 fd
0e 41 64 d2
2e b7 72 8b
17 7d a9 25
f7 27 9b 54
ab 83 43 b5
31 a9 40 3d
f0 ff d3 3f
f7 27 9b 54
83 43 b5 ab
40 3d 31 a9
3f f0 ff d3
14 46 27 34
15 16 46 2a
b5 15 56 d8
bf ec d7 43
4e 5f 84 4e
54 5f a6 a6
f7 c9 4f dc
0e f3 b2 4f
Round 8
5a 19 a3 7a
41 49 e0 8c
42 dc 19 04
b1 1f 65 0c
be d4 0a da
83 3b e1 64
2c 86 d4 f2
c8 c0 4d fe
be d4 0a da
3b e1 64 83
d4 f2 2c 86
fe c8 c0 4d
00 b1 54 fa
51 c8 76 1b
2f 89 6d 99
d1 ff cd ea
ea b5 31 7f
d2 8d 2b 8d
73 ba f5 29
21 d2 60 2f
Round 9
ea 04 65 85
83 45 5d 96
5c 33 98 b0
f0 2d ad c5
87 f2 4d 97
ec 6e 4c 90
4a c3 46 e7
8c d8 95 a6
87 f2 4d 97
6e 4c 90 ec
46 e7 4a c3
a6 8c d8 95
47 40 a3 4c
37 d4 70 9f
94 e4 3a 42
ed a5 a6 bc
ac 19 28 57
77 fa d1 5c
66 dc 29 00
f3 21 41 6e
Round 10
eb 59 8b 1b
40 2e a1 c3
f2 38 13 42
1e 84 e7 d2
e9 cb 3d af
09 31 32 2e
89 07 7d 2c
72 5f 94 b5
e9 cb 3d af
31 32 2e 09
7d 2c 89 07
b5 72 5f 94
d0 c9 e1 b6
14 ee 3f 63
f9 25 0c 0c
a8 89 c8 a6

AES key expansion algorithm



2b	28	ab	09
7e	ae	f7	cf
15	d2	15	4f
16	a6	88	3c



Rcon Constants (Base 16)			
Round	Constant(Rcon)	Round	Constant(Rcon)
1	01 00 00 00	6	20 00 00 00
2	02 00 00 00	7	40 00 00 00
3	04 00 00 00	8	80 00 00 00
4	08 00 00 00	9	1B 00 00 00
5	10 00 00 00	10	36 00 00 00

W0	W1	W2	W3
A0			
Fa			
Fe			
17			

Round Key 1

W0	W1	W2	W3
2b	28	ab	09
7e	ae	f7	cf
15	d2	15	4f
16	a6	88	3c

W0	W1	W2	W3
A0			
Fa			
Fe			
I7			

$W_1 =$

W1
28
ae
d2
a6

⊕

W0
A0
Fa
Fe
I7

→

88
54
2c
b1

we will repeat those steps at each round

W0	W1	W2	W3
2b	28	ab	09
7e	ae	f7	cf
15	d2	15	4f
16	a6	88	3c

W0	W1	W2	W3
A0	88	23	2a
Fa	54	a3	6C
Fe	2C	39	76
I7	b1	39	05

W2 =

W2
ab
f 7
15
88

⊕

W1
88
54
2c
b1

→

23
a3
39
39

W3 =

W3
09
cf
4f
3c

⊕

W2
23
a3
39
39

→

2a
6c
76
05