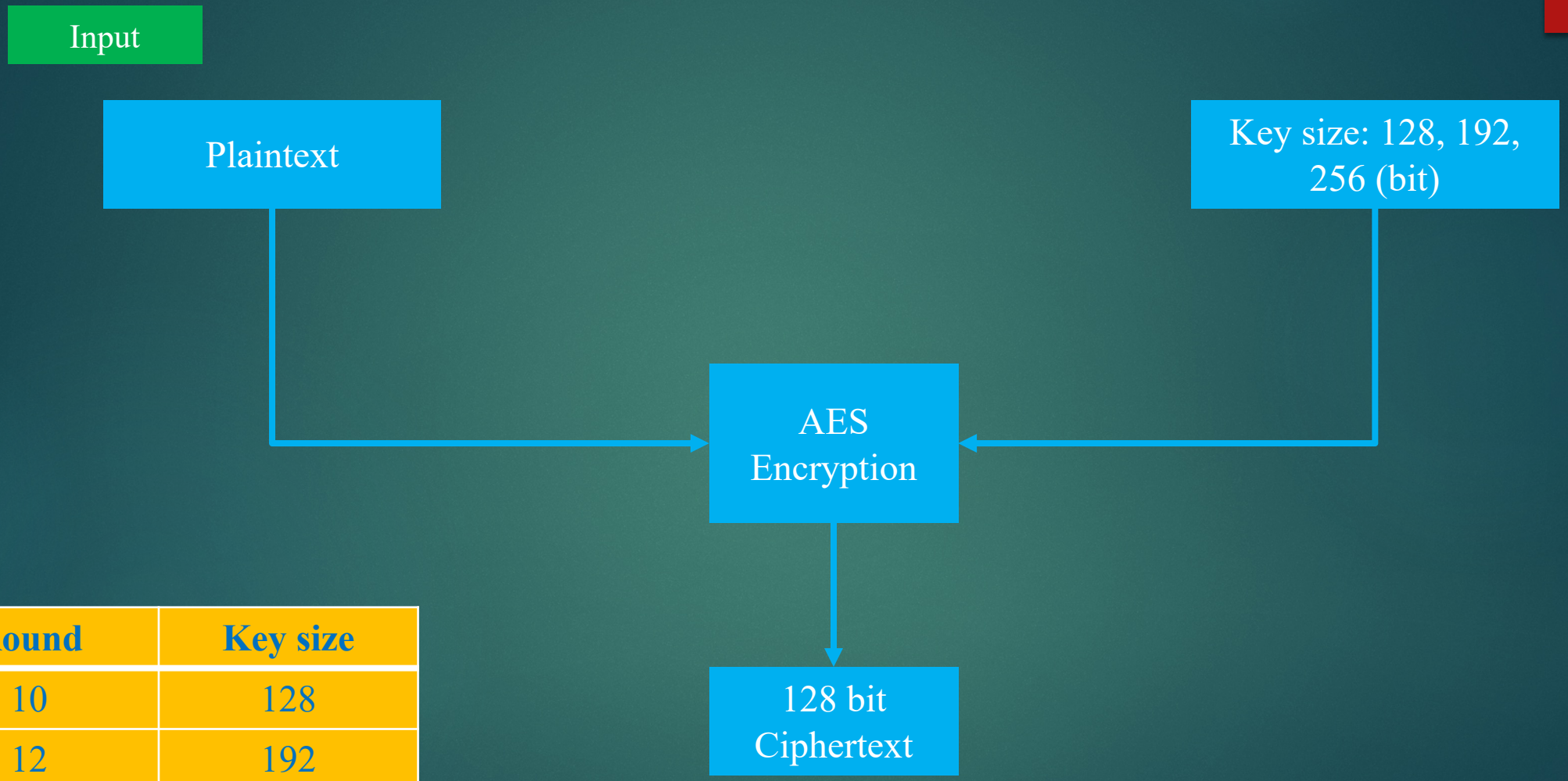
TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI TP. HỒ CHÍ MINH

BẢO MẬT HỆ THỐNG THÔNG TIN
INFORMATION SYSTEM SECURITY

MÃ HÓA ĐỐI XỨNG AES 128 bit

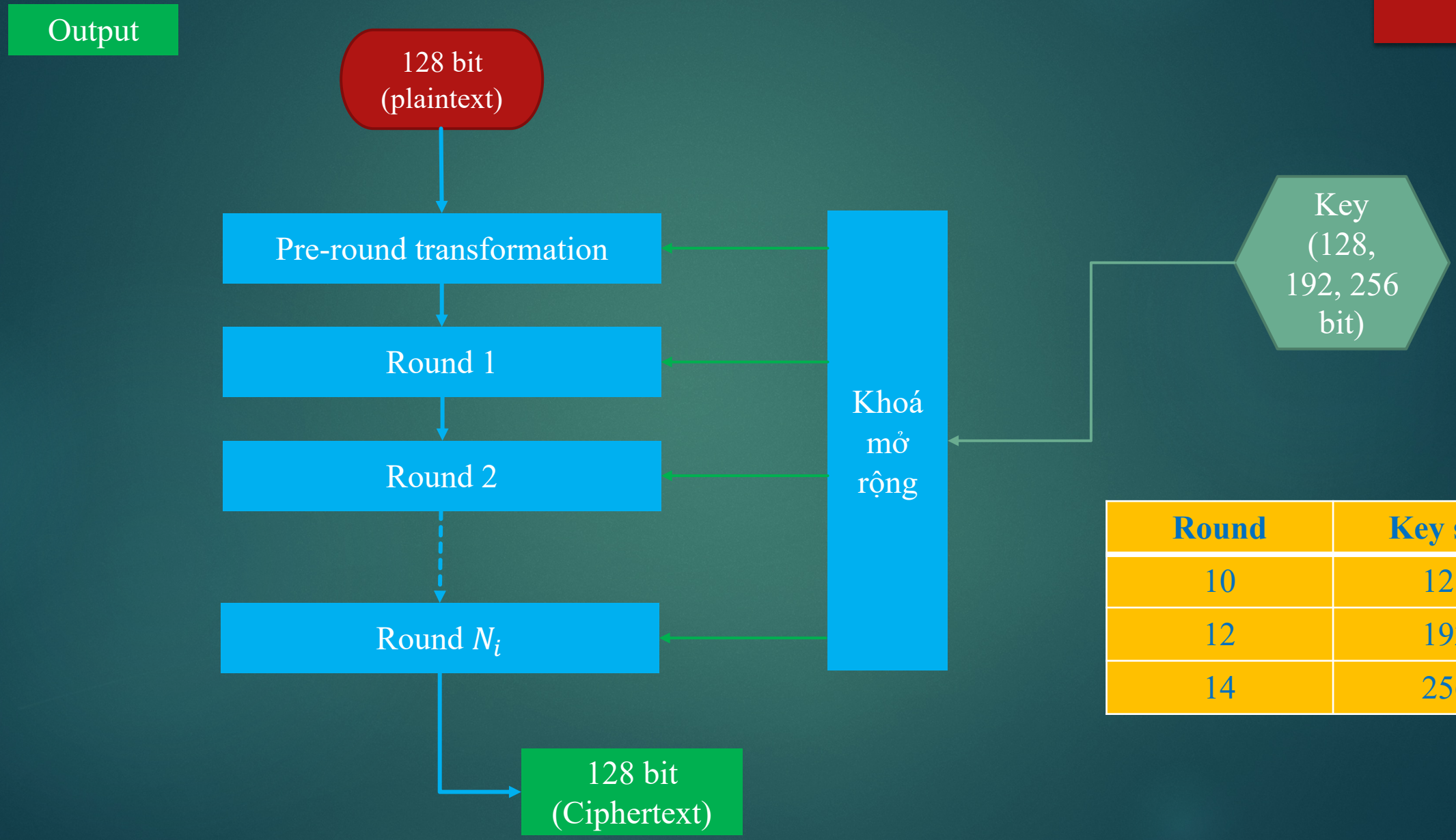
Giảng viên: TS. Trần Thế Vinh

ADVANCED ENCRYPTION STANDARD - AES



Round	Key size
10	128
12	192
14	256

ADVANCED ENCRYPTION STANDARD - AES



Round	Key size
10	128
12	192
14	256

ADVANCED ENCRYPTION STANDARD - AES

Mã hoá AES có hai bước:
1 – Sinh khoá (Key generation)
2 – Vòng (Rounds)

1. Sinh khoá:

- ROTWORD của cột cuối
- Sub byte của ROTWORD
- XOR với RCON và cột đầu tiên của khoá và subbyte
- Kết quả cột đầu tiên của khoá vòng 1 (Round 1)

2. Rounds

Round đầu tiên	Round chính	Round cuối
XOR với khoá Round 0	• Sub byte • Shift Rows (Chuyển hàng) • Mix Columns (Trộn cột) • Add Round Key (Thêm khoá Round)	• Sub byte • Shift Rows (Chuyển hàng) • Add Last Round Key

ADVANCED ENCRYPTION STANDARD - AES

1. SINH KHOÁ

128 bit – Key: VIETNAMUKRAINE12 (8*16=128 bits)

V	I	E	T	N	A	M	U	K	R	A	I	N	E	1	2

V	Trong hệ 16 là	56	Trong hệ nhị phân là	01010110

8 bit

56	49	45	54	4E	41	4D	55	4B	52	41	49	4E	45	31	32

56	49	45	54

4 byte này trở thành cột đầu tiên của khoá trạng thái

56
49
45
54

56	4E	4B	4E
49	41	52	45
45	4D	41	31
54	55	49	32

Key state

128 bit khoá trạng thái sẽ tạo ra 10 khoá con trong 10 Rounds

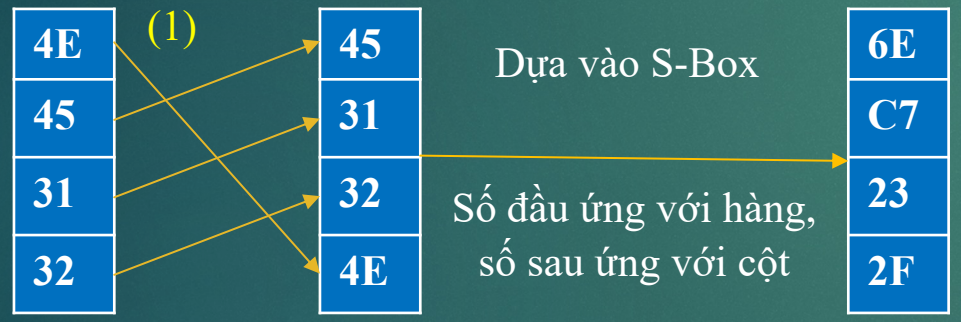
ADVANCED ENCRYPTION STANDARD - AES

Tạo Sub-key

56	4E	4B	4E
49	41	52	45
45	40	41	31
54	55	49	32

Khoá trạng thái K_0

Lấy cột cuối của khoá và thực hiện ROT WORD



ROT WORD

S-box

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

ADVANCED ENCRYPTION STANDARD - AES

RCON là bảng được xác định trước để sinh khoá trong AES

Round	1	2	3	4	5	6	7	8	9	10
RCON	01	02	04	08	10	20	40	80	18	36
	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00

56	4E	4B	4E
49	41	52	45
45	40	41	31
54	55	49	32

Key 1

56		6E		01	=	39	77	3C	72
49		C7		00		8E	CF	9D	D8
45		23		00		66	2B	6A	5B
54		2F		00		7B	2E	67	55
Cột đầu tiên		Sau khi Sub-byte cột		RCON 1		1	2	3	4

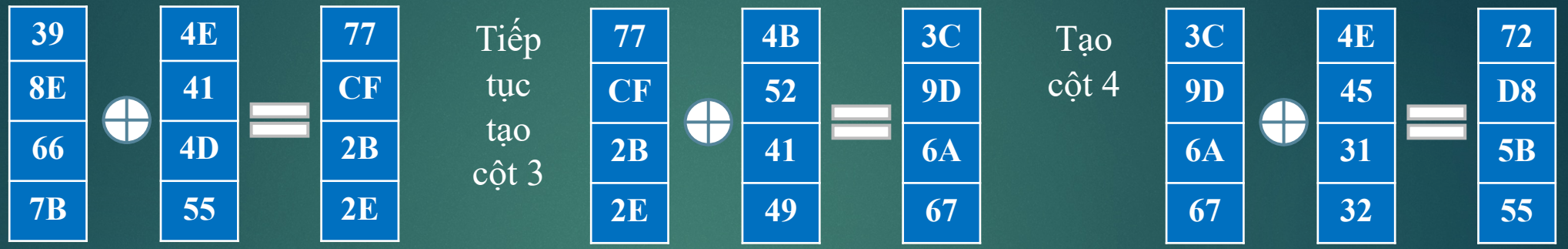
56	01010110
6E	01101110
01	00000001

Key trạng thái trở thành Key 0
Key 1 được tạo ra như trên và tương tự với $K_2 \rightarrow K_{10}$.
K_1 tạo ra K_2
K_2 tạo ra K_3
… K_9 tạo ra K_{10}

39	00111001

ADVANCED ENCRYPTION STANDARD - AES

Tiếp đến: Cột thứ 1 thu được tiếp tục XOR với cột thứ 2 của khoá trạng thái:



2 3 4

56	4E	4B	4E
49	41	52	45
45	4D	41	31
54	55	49	32

K_0

39	77	3C	72
8E	CF	9D	D8
66	2B	6A	5B
7B	2E	67	55

K_1

ADVANCED ENCRYPTION STANDARD - AES

Thiết lập K_2 từ K_1

Lấy cột cuối của K_1 và thực hiện ROTWORD, sub-byte

D8
5B
55
72

Tương tự thiết lập K_1 từ S-Box ta có

61
39
FC
40

Sau khi tính sub-byte cột cuối

39
8E
66
7B

Cột đầu tiên K_1

⊕

61
39
FC
40

Sau khi Sub-byte cột

⊕

02
00
00
00

RCON 2

=

5A
B7
9A
3B

1

S-box

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

39	77	3C	72
8E	CF	9D	D8
66	2B	6A	5B
7B	2E	67	55
K_1			

5A	2D	11	63
B7	78	E5	3D
9A	B1	DB	80
3B	15	72	27
K_2			

ADVANCED ENCRYPTION STANDARD - AES

Thiết lập K_2 từ K_1

Lấy cột của K_1 và thực hiện sub-byte (không thực hiện ROTWORD)

5A	⊕	77	=	2D	Tiếp tục tạo cột 3	2D	⊕	3C	=	11	Tạo cột 4	11	⊕	72	=	63
B7		CF		78		78		9D		E5		E5		D8		3D
9A		2B		B1		B1		6A		DB		DB		5B		80
3B		2E		15		15		67		72		72		55		27
				2						3						4

39	77	3C	72
8E	CF	9D	D8
66	2B	6A	5B
7B	2E	67	55
K_1			

5A	2D	11	63
B7	78	E5	3D
9A	B1	DB	80
3B	15	72	27
K_2			

Từ K_3 đến K_{10} tương tự như K_1 tạo ra K_2

ADVANCED ENCRYPTION STANDARD - AES

Ta thu được tập hợp khóa con được sinh ra từ khóa trạng thái:

56	4E	4B	4E
49	41	52	45
45	4D	41	31
54	55	49	32

K_0

39	77	3C	72
8E	CF	9D	D8
66	2B	6A	5B
7B	2E	67	55

K_1

5A	2D	11	63
B7	78	E5	3D
9A	B1	DB	80
3B	15	72	27

K_2

79	54	45	26
7A	02	E7	DA
56	E7	3C	BC
C0	D5	A7	80

K_3

26	72	37	11
1F	1D	FA	20
9B	7C	40	FC
37	E2	45	C5

K_4

81	F3	C4	D5
AF	B2	48	68
3D	41	01	FD
B5	57	12	D7

K_5

E4	17	D3	06
FB	49	01	69
33	72	73	8E
B6	E1	F3	24

K_6

5D	4A	99	9F
E2	AB	AA	C3
05	77	04	8A
D9	38	CB	EF

K_7

F3	B9	20	BF
9C	37	9D	5E
DA	AD	A9	23
02	3A	F1	1E

K_8

B0	09	29	96
BA	8D	10	4E
A8	05	AC	8F
0A	30	C1	DF

K_9

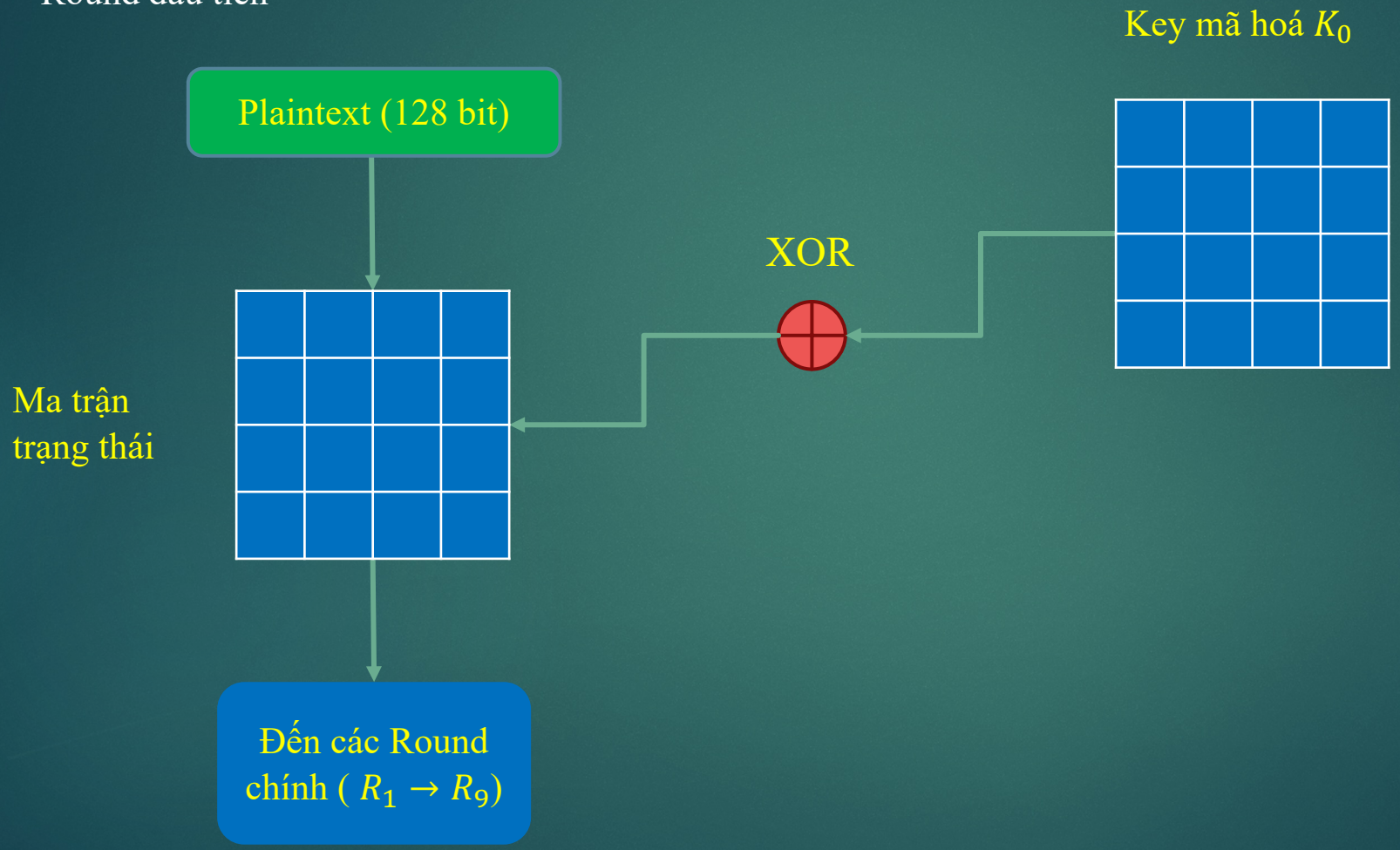
A9	A0	89	1F
C9	44	54	1A
36	33	9F	10
9A	AA	6B	B4

K_{10}

ADVANCED ENCRYPTION STANDARD - AES

QUÁ TRÌNH MÃ HOÁ – ENCRYPTION PROCESS

Round đầu tiên

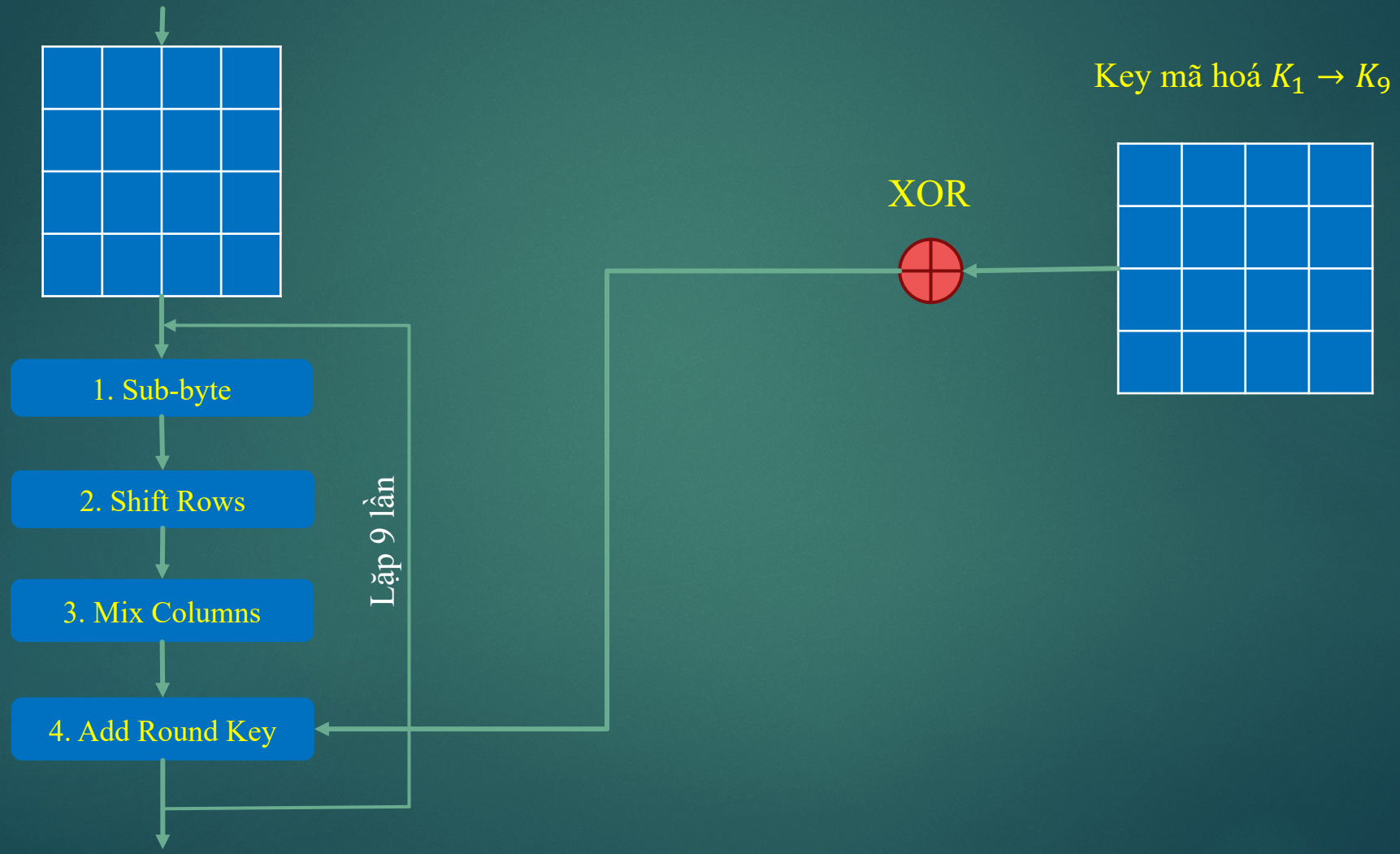


ADVANCED ENCRYPTION STANDARD - AES

QUÁ TRÌNH MÃ HOÁ – ENCRYPTION PROCESS

Round chính từ $R_1 \rightarrow R_9$

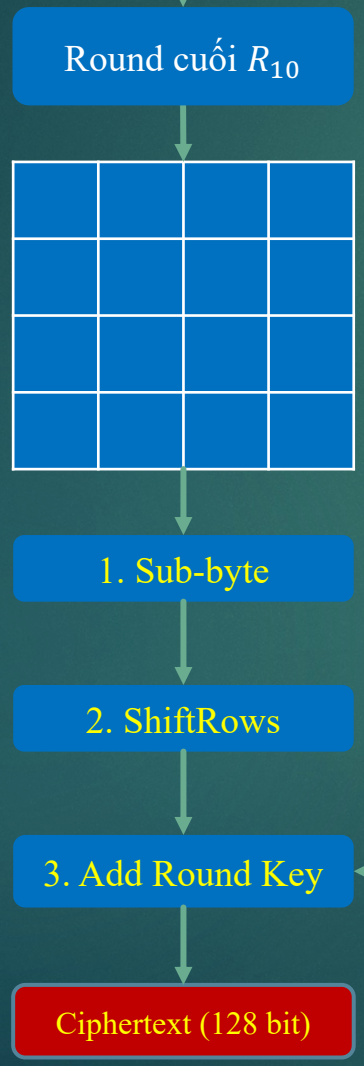
Ma trận trạng thái từ Round đầu tiên

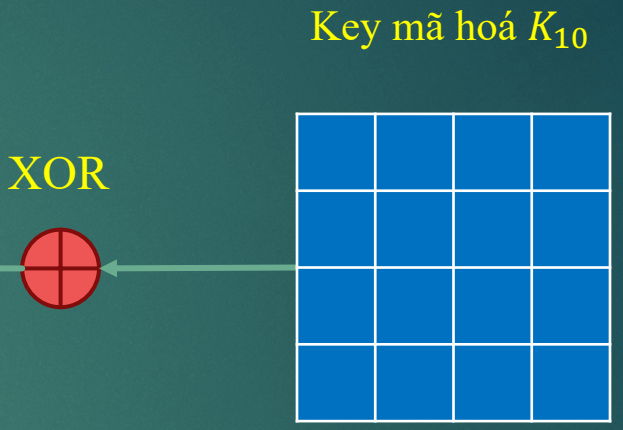


ADVANCED ENCRYPTION STANDARD - AES

QUÁ TRÌNH MÃ HOÁ – ENCRYPTION PROCESS

Round cuối R_{10}





Vòng cuối không thực hiện bước Mix Columns.

ADVANCED ENCRYPTION STANDARD - AES

Tin nhắn cần mã hoá

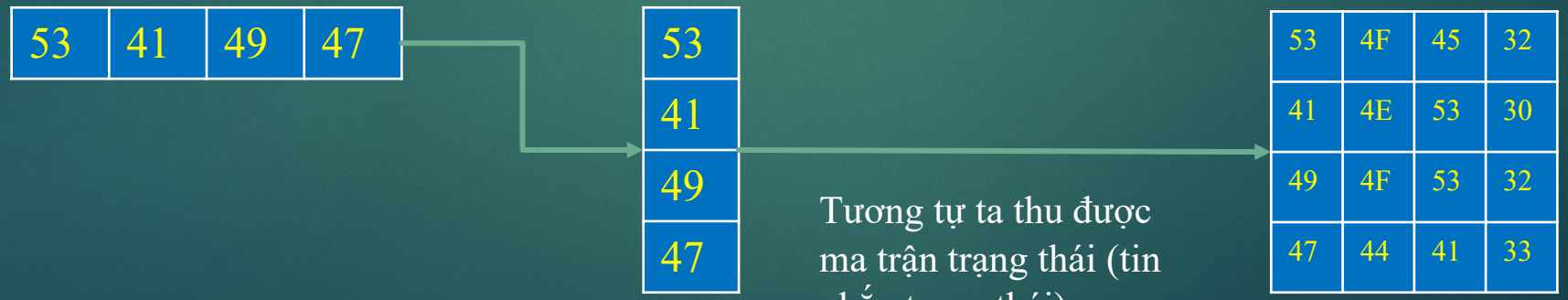
SAIGONODESSA2023 (128 bit)

S	A	I	G	O	N	O	D	E	S	S	A	2	0	2	3

Tương tự như khoá chuyển sang hệ 16

Ta thu được:

53	41	49	47	4F	4E	4F	44	45	53	53	41	32	30	32	33

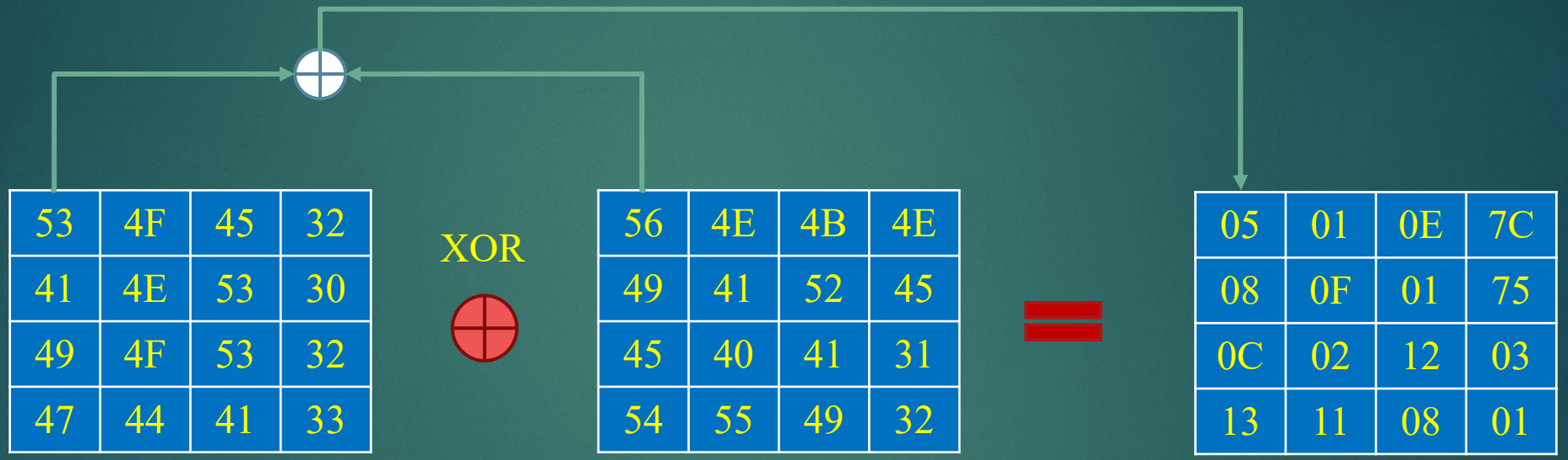


ADVANCED ENCRYPTION STANDARD - AES

Ta có 4 bước trong 1 Round:

1. Add Round Key
2. Sub byte
3. Shift Rows
4. Mix Columns

1.



53	4F	45	32
41	4E	53	30
49	4F	53	32
47	44	41	33

XOR

56	4E	4B	4E
49	41	52	45
45	40	41	31
54	55	49	32

=

05	01	0E	7C
08	0F	01	75
0C	02	12	03
13	11	08	01

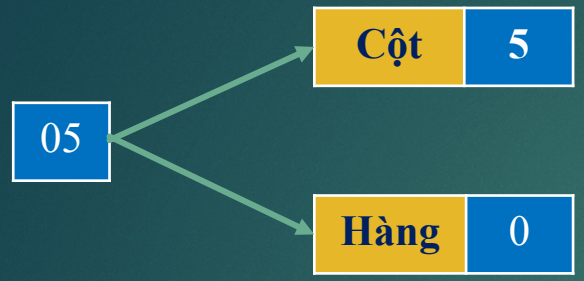
Tin nhắn trạng thái

K_0

Kết quả trạng thái

ADVANCED ENCRYPTION STANDARD - AES

2. Sub bytes



Sử dụng S-Box

05	01	0E	7C
08	0F	01	75
0C	02	12	03
13	11	08	01

Ma trận Trạng thái

S-Box thu được

6B	7C	AB	10
30	76	7C	9D
FE	77	C9	7B
7D	82	30	7C

Sau khi Sub byte ta thu được

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
10	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
20	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
30	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
40	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
50	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
60	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
70	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
80	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
90	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a0	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b0	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c0	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d0	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e0	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f0	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

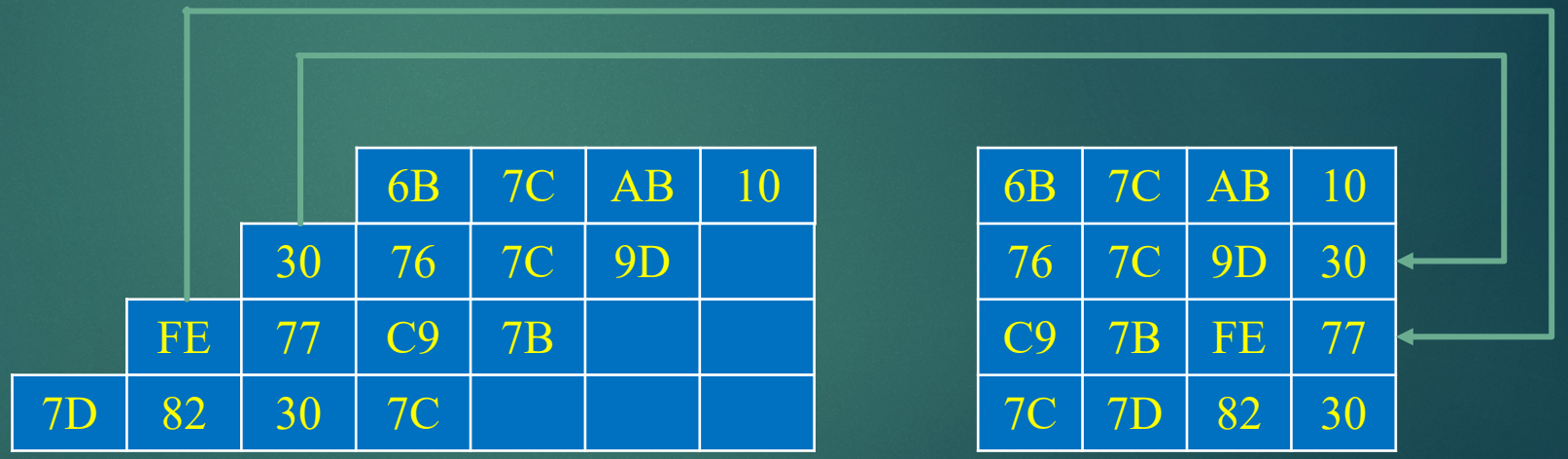
ADVANCED ENCRYPTION STANDARD - AES

3. Shift Rows

6B	7C	AB	10
30	76	7C	9D
FE	77	C9	7B
7D	82	30	7C

Trước khi Shift Rows

0 - Shift
1 - Shift
2 - Shift
3 - Shift



6B	7C	AB	10
76	7C	9D	30
C9	7B	FE	77
7C	7D	82	30

Mỗi hàng đều dịch chuyển vòng trái tương ứng với 0 đến 3 lượt (4 lần)

Sau khi Shift Rows

ADVANCED ENCRYPTION STANDARD - AES

4. Mix Columns

6B	7C	AB	10
76	7C	9D	30
C9	7B	FE	77
7C	7D	82	30

Bốn byte trong từng cột được kết hợp lại theo một phép biến đổi khả nghịch. Mỗi khối 4 byte đầu vào sẽ cho một khối 4 byte ở đầu ra với tính chất mỗi byte ở đầu vào đều ảnh hưởng tới 4 byte đầu ra.

Cùng với bước ShiftRows, Mixcolumns đã tạo ra tính chất khuếch tán cho thuật toán. Mỗi cột được xem như một đa thức trong trường hữu hạn và được nhân với đa thức $f(x) = 3x^3 + x^2 + x + 2 (\text{modulo } x^4 + 1)$

$$\begin{bmatrix} 6B \\ 76 \\ C9 \\ 7C \end{bmatrix} \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \times \begin{bmatrix} 6B \\ 76 \\ C9 \\ 7C \end{bmatrix} = \begin{bmatrix} (2 \cdot 6B) \oplus (3 \cdot 76) \oplus (1 \cdot C9) \oplus (1 \cdot 7C) \\ (1 \cdot 6B) \oplus (2 \cdot 76) \oplus (3 \cdot C9) \oplus (1 \cdot 7C) \\ (1 \cdot 6B) \oplus (1 \cdot 76) \oplus (2 \cdot C9) \oplus (3 \cdot 7C) \\ (3 \cdot 6B) \oplus (1 \cdot 76) \oplus (1 \cdot C9) \oplus (2 \cdot 7C) \end{bmatrix} = \begin{bmatrix} F9 \\ BB \\ 10 \\ FA \end{bmatrix}$$

ADVANCED ENCRYPTION STANDARD - AES

4. Mix Columns

Rijndael sử dụng trường hữu hạn đặc trưng 2 với 256 phần tử, trường này còn có thể được gọi là trường Galois GF(2^8).
Nó sử dụng đa thức rút gọn sau:
GF(2^8) = $x^8 + x^4 + x^3 + x + 1$
$x^8 = x^4 + x^3 + x + 1$

2 · 6B
$10 \cdot 01101011$
$(x^1) \times (x^6 + x^5 + x^3 + x^1 + 1)$
$= x^7 + x^6 + x^4 + x^2 + x \rightarrow 11010110$

3 · 76
$11 \cdot 01110110$
$(x^1 + 1) \times (x^6 + x^5 + x^4 + x^2 + x)$
$= x^7 + x^6 + x^5 + x^3 + x^2 + x^6 + x^5 + x^4 + x^2 + x$
$= x^7 + x^4 + x^3 + x \rightarrow 10011010$

1 · C9
$1 \cdot 11001001$
$(1) \times (x^7 + x^6 + x^3 + 1) \rightarrow 11001001$

$1 \cdot 7C \rightarrow 01111100$

ADVANCED ENCRYPTION STANDARD - AES

4. Mix Columns:

Tương tự ta thu được ma trận Mix Column

F9	**7A**	**8D**	**37**
BB	74	11	D9
10	71	4C	9E
FA	79	9A	17