BÀI GIẢNG AN TOÀN & BẢO MẬT THÔNG TIN
CHƯƠNG 4-MÃ KHỐI HIỆN ĐẠI

TS. NGUYỄN ĐÌNH DƯƠNG
BỘ MÔN KHMT - KHOA CÔNG NGHỆ THÔNG TIN

Email: duongnd@utc.edu.vn

Ngày 03/07/2022

Nội dung

Nội dung

1. Chuẩn mã hoá nâng cao AES

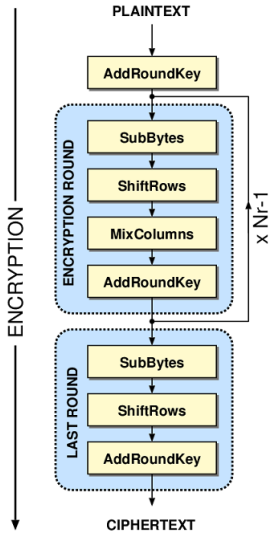
1. 1. Giới thiệu

Chronology of DES Cracking	
Broken for the first time	1997
Broken in 56 hours	1998
Broken in 22 hours and 15 minutes	1999
Capable of broken in 5 minutes	2021

1. Chuẩn mã hoá nâng cao AES

1. 1. Giới thiệu

- AES là hệ mật mã đối xứng sử dụng SPN được NIST đề xuất thay thế cho DES và 3DES (2002)
- Cốt lõi của AES là hệ mã Rijndael (do hai nhà mật mã học người Bỉ là Joan Daemen và Vincent Rijmen đưa ra).
- AES là **hệ mã khối** → size(plaintext) = size(ciphertext)
- AES thao tác trên **byte data** thay vì bit data
- AES cho phép xử lý các khối dữ liệu 128 bit và sử dụng khoá có độ dài 128, 192 hay 256 bit → AES-128, AES-192, AES-256.
- Thuật toán trong AES bao gồm nhiều vòng lặp và sử dụng các khoá khác nhau (sinh ra từ khoá ban đầu):
  - khoá 128 bit → 10 vòng lặp
  - khoá 192 bit → 12 vòng lặp
  - khoá 256 bit → 14 vòng lặp



1. Chuẩn mã hoá nâng cao AES

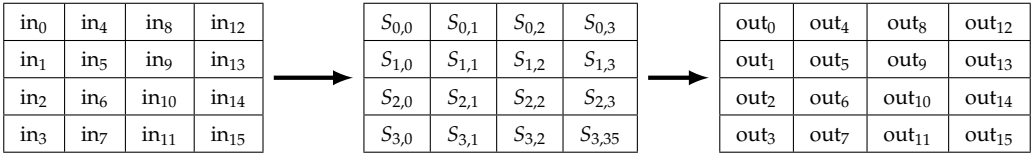
Một số ký hiệu và qui ước

- Input và Output của AES đều là 128 bit và được đánh số từ 0
- Khoá của AES có độ dài 128/192/256 bit
- **Byte**: được xem là một *đơn vị đo cơ bản* trong AES, viết dưới dạng $b_7b_6 \cdots b_1b_0$
  - Input, Output, Key là mảng các byte, ví dụ 128 bit $\rightarrow$ 16 byte hay `Input[n]` với $0 \leq n < 16$
  - 1 Byte $\leftrightarrow$ 1 phần tử trên trường hữu hạn GF (2^8)

$$b_7b_6 \cdots b_1b_0 \leftrightarrow b_7X^7 + b_6X^6 + \cdots + b_1X + b_0$$

  Ví dụ: 01100011 $\leftrightarrow X^6 + X^5 + X + 1$
- Để thuận tiện, các giá trị Byte được biểu diễn trong hệ Hexa, ví dụ `01100011` $\rightarrow$ `63`

Một số ký hiệu và qui ước

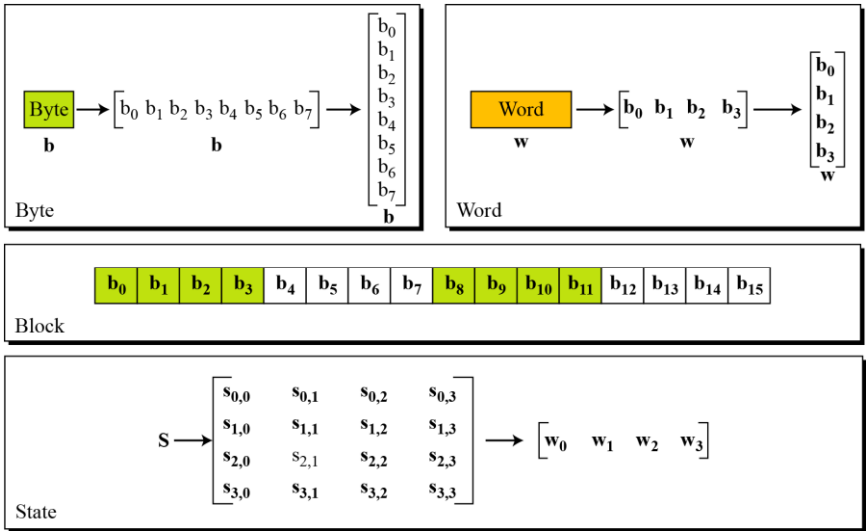


- Mọi thao tác trong AES đều thực hiện trên một mảng 2 chiều các byte $\rightarrow$ **mảng trạng thái *S***:
  - gồm 4 hàng $\times$ 4 cột
  - mỗi byte có chỉ số hàng r, chỉ số cột c ($0 \leq r, c < 4$)
- Mỗi vòng lặp đều có input và output là một mảng trạng thái
- **4 byte = 1 word** $\rightarrow$ 4 cột của mảng trạng thái tạo thành 4 word 32-bit:

$$\begin{cases} w_0 = S_{0,0}S_{1,0}S_{2,0}s_{30} & w_1 = S_{0,1}S_{1,1}S_{2,1}S_{3,1} \\ w_2 = S_{0,2}S_{1,2}S_{2,2}S_{3,2} & w_3 = S_{0,3}S_{1,3}S_{2,3}S_{3,3} \end{cases}$$

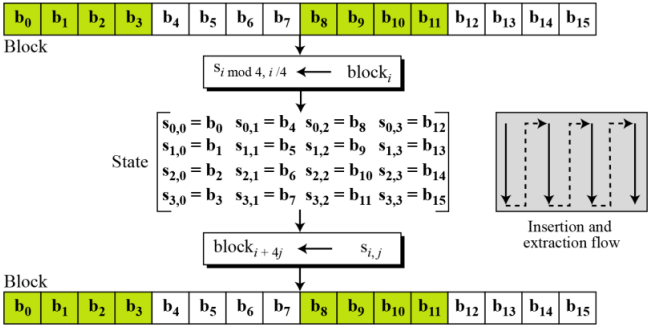
1. Chuẩn mã hoá nâng cao AES

1. 1. Giới thiệu



1. Chuẩn mã hoá nâng cao AES

1. 1. Giới thiệu



Mảng trạng thái:

$$\begin{bmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 23 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 19 \end{bmatrix}$$

Ví dụ 1.1

Plaintext	A	E	S	U	S	E	S	A	M	A	T	R	I	X	Z	Z
Hexadecimal	00	04	12	14	12	04	12	00	0C	00	13	11	23	X	19	19

1. Chuẩn mã hoá nâng cao AES

Một số ký hiệu và qui ước

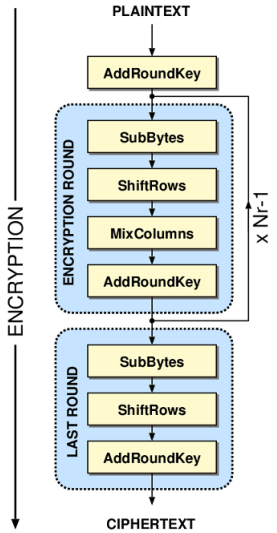
- **Nk** suy ra từ độ dài khoá theo bảng dưới đây

	Độ dài khoá (**Nk**)	Kích thước khối (**Nb**)	Số lần lặp (**Nr**)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Table: Bảng độ dài khoá AES

1. Chuẩn mã hoá nâng cao AES

1. 2. Thuật toán mã hóa



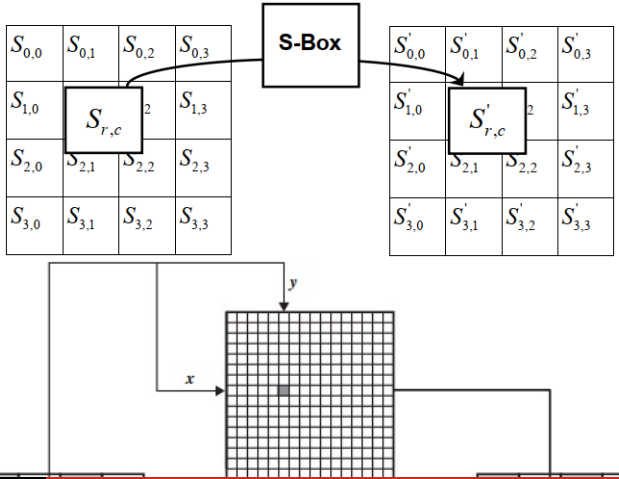
Quá trình mã hoá sử dụng cùng một **hàm lặp** = hợp 4 hàm:

1. **Phép thế byte** → `SubBytes()` - 10 vòng
2. **Dịch hàng** → `ShiftRows()` - 10 vòng
3. **Trộn cột** → `MixColumns()` - 9 vòng
4. **Cộng khoá vòng** → `AddRoundKey()` - 10 vòng

1. Chuẩn mã hoá nâng cao AES

Hàm `SubBytes()`

- Thực hiện phép thay thế các byte của mảng ***s*** nhờ S-Box
- S-Box là một ma trận 16×16 chứa tất cả 256 hoán vị của 8 bit



1. Chuẩn mã hoá nâng cao AES

1. 2. Thuật toán mã hóa

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

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

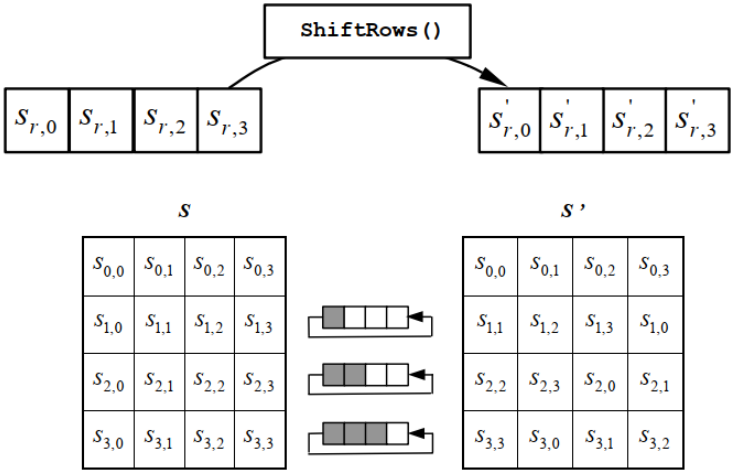
1. Chuẩn mã hoá nâng cao AES

Hàm InvSubBytes()

x \ y	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
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
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
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	b7	62	0e	aa	18	be	1b
b	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c	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
e	a0	e0	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

1. Chuẩn mã hoá nâng cao AES

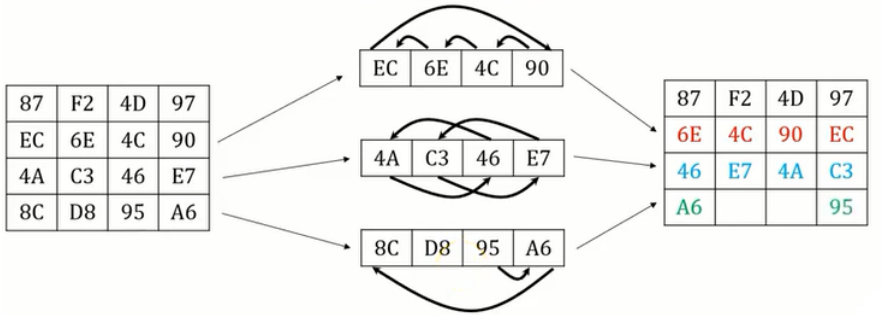
Hàm `ShiftRows()`



- **hàng đầu tiên** ($r = 0$) của S giữ nguyên
- **3 hàng cuối** ($1 \leq r \leq 3$) của S được dịch vòng trái với số byte khác nhau.

1. Chuẩn mã hoá nâng cao AES

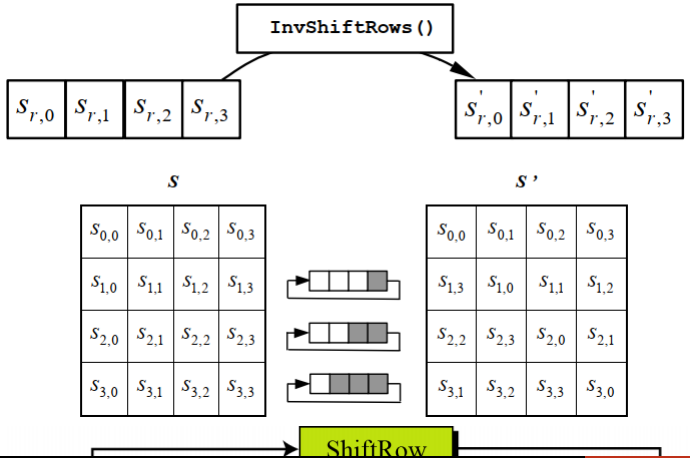
1. 2. Thuật toán mã hóa



- hàng đầu → giữ nguyên
- hàng 2 → dịch vòng trái 1 byte
- hàng 3 → dịch vòng trái 2 byte
- hàng 4 → dịch vòng trái 3 byte

1. Chuẩn mã hoá nâng cao AES

Hàm `InvShiftRows()`



- **hàng đầu tiên** ($r = 0$) của S giữ nguyên
- **3 hàng cuối** ($1 \leq r \leq 3$) của S được dịch vòng phải với số byte khác nhau

1. Chuẩn mã hoá nâng cao AES

Hàm `MixColumns()`

- Biến đổi các cột của S bằng cách nhân với một ma trận cho trước.
- Mảng trạng thái = Output của `ShiftRows()`
- Mỗi byte trong cột được biến đổi thành giá trị mới phụ thuộc vào 4 byte của cột đó
- Ví dụ

$$\underbrace{\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}}_{\text{Ma trận cố định}} * \underbrace{\begin{bmatrix} S_{0,0} & S_{0,1} & S_{0,2} & S_{0,3} \\ S_{1,0} & S_{1,1} & S_{1,2} & S_{1,3} \\ S_{2,0} & S_{2,1} & S_{2,2} & S_{2,3} \\ S_{3,0} & S_{3,1} & S_{3,2} & S_{3,3} \end{bmatrix}}_{\text{Mảng trạng thái}} = \underbrace{\begin{bmatrix} S'_{0,0} & S'_{0,1} & S'_{0,2} & S'_{0,3} \\ S'_{1,0} & S'_{1,1} & S'_{1,2} & S'_{1,3} \\ S'_{2,0} & S'_{2,1} & S'_{2,2} & S'_{2,3} \\ S'_{3,0} & S'_{3,1} & S'_{3,2} & S'_{3,3} \end{bmatrix}}_{\text{Mảng trạng thái mới}}$$

$$S'_{0,0} = (02 * S_{0,0}) \oplus (03 * S_{1,0}) \oplus (01 * S_{2,0}) \oplus (01 * S_{3,0})$$
$$S'_{1,0} = (01 * S_{0,0}) \oplus (02 * S_{1,0}) \oplus (03 * S_{2,0}) \oplus (01 * S_{3,0})$$
$$S'_{2,0} = (01 * S_{0,0}) \oplus (01 * S_{1,0}) \oplus (02 * S_{2,0}) \oplus (03 * S_{3,0})$$
$$S'_{3,0} = (03 * S_{0,0}) \oplus (01 * S_{1,0}) \oplus (01 * S_{2,0}) \oplus (02 * S_{3,0})$$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \end{bmatrix} \quad \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \end{bmatrix} \quad \begin{bmatrix} ? & ? & ? & ? \\ ? & ? & ? & ? \end{bmatrix}$$

1. Chuẩn mã hoá nâng cao AES

1. 2. Thuật toán mã hóa

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} * \begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix} = \begin{bmatrix} 47 & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \\ ? & ? & ? & ? \end{bmatrix}$$

$\{02\} * \{87\} \oplus \{03\} * \{6E\} \oplus \{01\} * \{46\} \oplus \{01\} * \{A6\} = ?$

- $02 = 0000\ 0010 = X$
- $87 = 1000\ 0111 = X^7 + X^2 + X + 1$

$$\begin{aligned} \{02\} * \{87\} &= X * (X^7 + X^2 + X + 1) \\ &= X^8 + X^3 + X^2 + X \\ &= X^4 + X^3 + X + 1 + X^3 + X^2 + X \\ &= X^4 + X^2 + 1 \\ &= 0001\ 0101 \end{aligned}$$

- $03 = 0000\ 0011 = X + 1$

- $6E = 0110\ 1110 = X^6 + X^5 + X^3 + X^2 + X$

$$\begin{aligned} \{03\} * \{6E\} &= (X + 1) * (X^6 + X^5 + X^3 + X^2 + X) \\ &= X^7 + X^5 + X^4 + X \\ &= 1011\ 0010 \end{aligned}$$

- $\{01\} * \{46\} = 46 = 0100\ 0110$
- $\{01\} * \{A6\} = 1010\ 0110$
  $\Rightarrow \{02\} * \{87\} \oplus \{03\} * \{6E\} \oplus \{01\} * \{46\} \oplus \{01\} * \{A6\} = 0100\ 0111 = 47$

1. Chuẩn mã hoá nâng cao AES

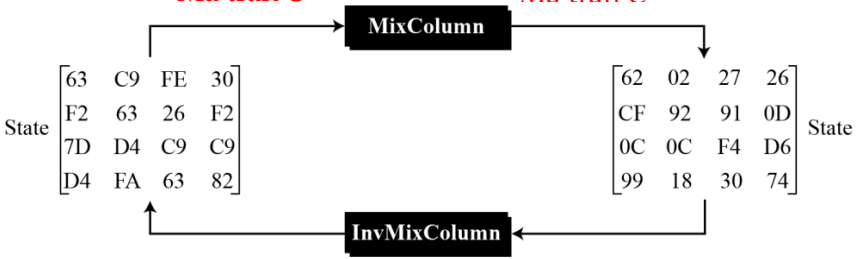
Hàm `MixColumns()`

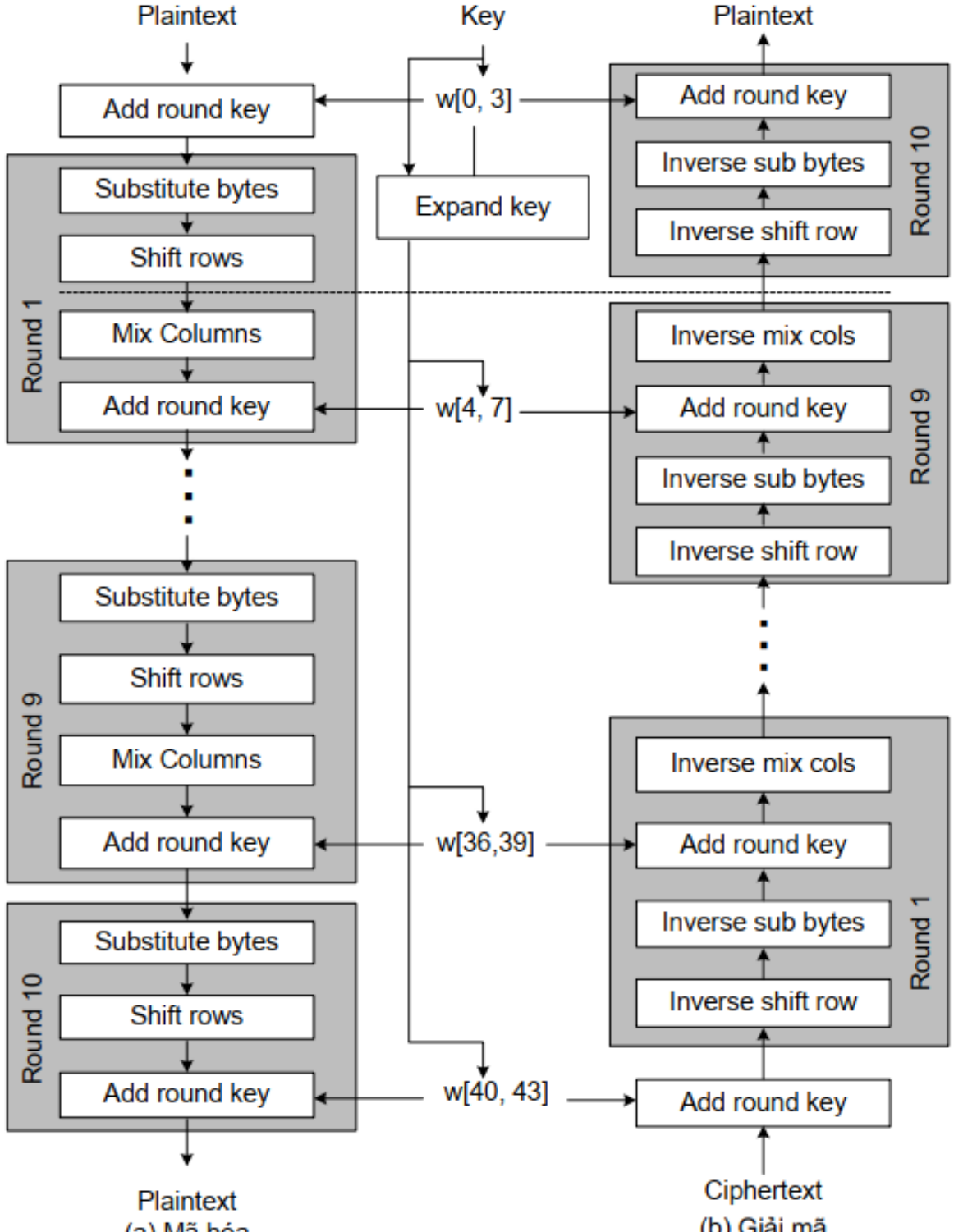
$$\underbrace{\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}}_{\text{Ma trận cố định}} * \underbrace{\begin{bmatrix} 87 & F2 & 4D & 97 \\ 6E & 4C & 90 & EC \\ 46 & E7 & 4A & C3 \\ A6 & 8C & D8 & 95 \end{bmatrix}}_{\text{Mảng trạng thái}} = \underbrace{\begin{bmatrix} 47 & 40 & A3 & 4C \\ 37 & D4 & 70 & 9F \\ 94 & E4 & 3A & 42 \\ ED & A5 & A6 & BC \end{bmatrix}}_{\text{Mảng trạng thái mới}}$$

1. Chuẩn mã hoá nâng cao AES

Hàm `InvMixColumns()`

$$\underbrace{\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}}_{\text{Ma trân } C} \quad \text{inverse} \quad \underbrace{\begin{bmatrix} 0E & 0B & 0D & 09 \\ 09 & 0E & 0B & 0D \\ 0D & 09 & 0E & 0B \\ 0B & 0D & 09 & 0E \end{bmatrix}}_{\text{Ma trân } C^{-1}}$$

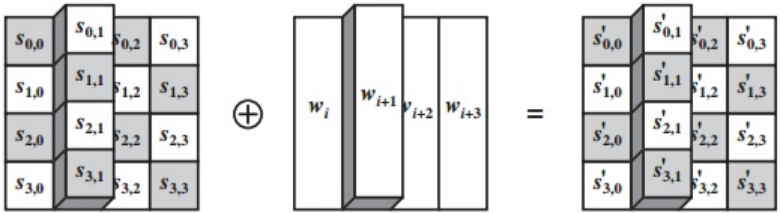




(a) Mã hóa (b) Giải mã

1. Chuẩn mã hoá nâng cao AES

Hàm `AddRoundKey()`



- Một khoá vòng (RoundKey) 128 bit được XOR với mảng trạng thái s

$$\left[S'_{0,c}; S'_{1,c}; S'_{2,c}; S'_{3,c}\right] = \left[S_{0,c}; S_{1,c}; S_{2,c}; S_{3,c}\right] \oplus \left[w_{\text{round}*\text{Nb}+c}\right], \quad 0 \le c \le \text{Nb} = 4$$

- $[w_i]$ là các word khoá, $0 \le \text{round} \le \mathbf{Nr}$ là số lần lặp:
  - Trong bước khởi tạo `AddRoundKey()` thực hiện với round $= 0$
  - Trong thuật toán mã hoá `AddRoundKey()` được thực hiện với $1 \le \text{round} \le \mathbf{Nr}$

1. Chuẩn mã hoá nâng cao AES

Hàm `AddRoundKey()`

$$\begin{bmatrix} 47 & 40 & A3 & 4C \\ 37 & D4 & 70 & 9F \\ 94 & E4 & 3A & 42 \\ ED & A5 & A6 & BC \end{bmatrix} \oplus \begin{bmatrix} AC & 19 & 28 & 57 \\ 77 & FA & D1 & 5C \\ 66 & DC & 29 & 00 \\ F3 & 21 & 41 & 6A \end{bmatrix} = \begin{bmatrix} EB & 59 & 8B & 1B \\ 40 & 2E & A1 & C3 \\ F2 & 38 & 13 & 42 \\ 1E & 84 & E7 & D6 \end{bmatrix}$$

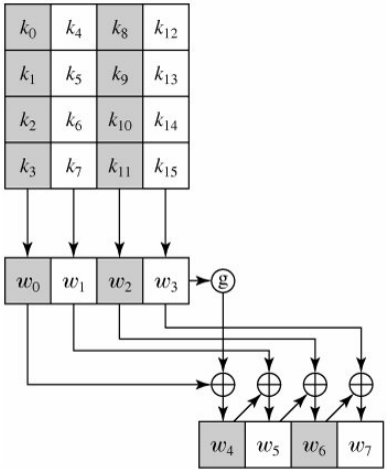
- $47 \oplus AC = 0100\ 0111 \oplus 1010\ 1100 = 1110\ 1011 = \{EB\}$
- $37 \oplus 77 = 0011\ 0111 \oplus 0111\ 0111 = 0100\ 0000 = \{40\}$
- ...

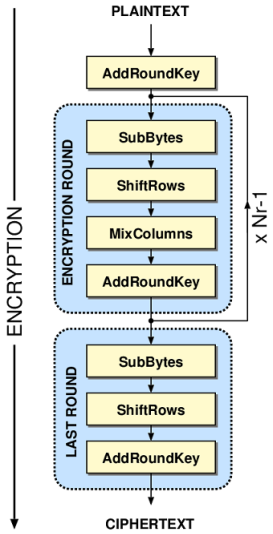
1. Chuẩn mã hoá nâng cao AES

1. 3. Thủ tục sinh khoá (Key Expansion)

- **Input:** Khoá K 128 bit (= 16 bytes = 4 word)
- **Output:** 11 khoá $K_0, \ldots, K_{10}$
- **Mỗi khoá con:** 4 word dạng $w_i\ w_{i+1}\ w_{i+2}\ w_{i+3}$
  $\Rightarrow$ Cần: 44 words w_i,
  $0 \leq 1 \leq 43$

Vòng lặp	Words			
Pre-round	w_0	w_1	w_2	w_3
1	w_4	w_5	w_6	w_7
2	w_8	w_9	w_{10}	w_{11}
...	...			
10	w_{40}	w_{41}	w_{42}	w_{43}

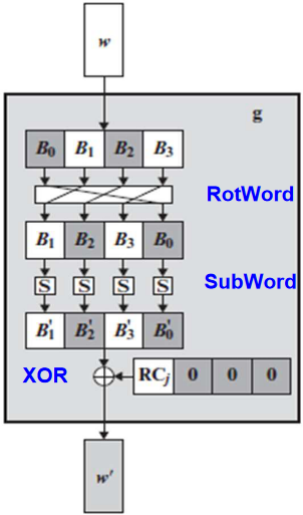




1. Chuẩn mã hoá nâng cao AES

1. 3. Thủ tục sinh khoá (Key Expansion)

- Hàm g là hợp thành của các thao tác sau:
- **Bước 1:** thực hiện dịch vòng trái 1 byte $\rightarrow$ `RotWord(·)`
- **Bước 2:** thực hiện phép thế byte sử dụng S-box $\rightarrow$ `SubWord(·)`
- **Bước 3:** XOR kết quả Bước 2 với $\texttt{Rcon}_j(\cdot)$



1. Chuẩn mã hoá nâng cao AES

1. 3. Thủ tục sinh khoá (Key Expansion)

Hàm `RotWord(·)`

w_0	w_1	w_2	w_3
0F	47	0C	AF
15	D9	B7	7F
71	E8	AD	67
C9	59	D6	98

→

w_3	Dịch vòng trái
AF	7F
7F	67
67	98
98	AF

1. Chuẩn mã hoá nâng cao AES

1. 3. Thủ tục sinh khoá (Key Expansion)

Hàm `SubWord(·)`

AES S-Boxes

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

Thế Bytes	S-box
7F	D2
67	85
98	46
AF	79

1. Chuẩn mã hoá nâng cao AES

1. 3. Thủ tục sinh khoá (Key Expansion)

Hàm $\texttt{Rcon}_j(\cdot)$

Round j	1	2	3	4	5	6	7	8	9	10
Rcon[j]	01	02	04	08	10	20	40	80	1b	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

1. Chuẩn mã hoá nâng cao AES

1. 3. Thủ tục sinh khoá (Key Expansion)

w0	w1	w2	w3
0F	47	0C	AF
15	D9	B7	7F
71	E8	AD	67
C9	59	D6	98

Left Shift (Step-1)	S-box (Step-2)
7F	D2
67	85
98	46
AF	79

Round	1	2	3	4	5	6	7	8	9	10
Rcon[]	01	02	04	08	10	20	40	80	1b	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

w0
0F
15
71
C9

S-box (Step-2)
D2
85
46
79

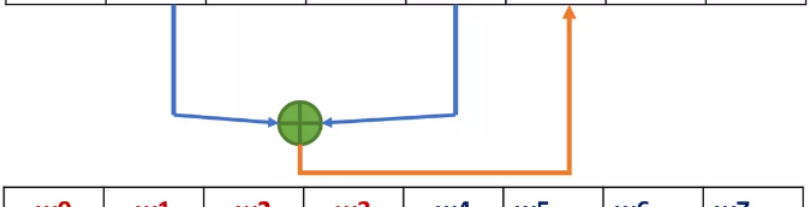
Rcon(Round)
01
00
00
00

W4
DC
90
37
B0

1. Chuẩn mã hoá nâng cao AES

1. 3. Thủ tục sinh khoá (Key Expansion)

w0	w1	w2	w3	w4	w5	w6	w7
0F	47	0C	AF	DC	9B		
15	D9	B7	7F	90	49		
71	E8	AD	67	37	DF		
C9	59	D6	98	B0	E9		



1. Chuẩn mã hoá nâng cao AES

1. 4. Ví dụ minh hoạ

Ví dụ 1.2

Cipher Key = 2b 7e 15 16 28 ae d2 a6 ab f7 15 88 09 cf 4f 3c (với $Nk = 4$)

$\Rightarrow w_0 =$ **2b7e1516** $w_1 =$ **28aed2a6** $w_2 =$ **abf71588** $w_3 =$ **09cf4f3c**

i (dec)	temp	After RotWord()	After SubWord()	Rcon[i/Nk]	After XOR with Rcon	w[i-Nk]	w[i]= temp XOR w[i-Nk]
4	09cf4f3c	cf4f3c09	8a84eb01	01000000	8b84eb01	2b7e1516	a0fafe17
5	a0fafe17					28aed2a6	88542cb1
6	88542cb1					abf71588	23a33939
7	23a33939					09cf4f3c	2a6c7605
8	2a6c7605	6c76052a	50386be5	02000000	52386be5	a0fafe17	f2c295f2
9	f2c295f2					88542cb1	7a96b943
10	7a96b943					23a33939	5935807a
11	5935807a					2a6c7605	7359f67f

1. Chuẩn mã hoá nâng cao AES

1. 4. Ví dụ minh hoạ

i (dec)	temp	After RotWord()	After SubWord()	Rcon[i/Nk]	After XOR with Rcon	w[i-Nk]	w[i]= temp XOR w[i-Nk]
12	7359f67f	59f67f73	cb42d28f	04000000	cf42d28f	f2c295f2	3d80477d
13	3d80477d					7a96b943	4716fe3e
14	4716fe3e					5935807a	1e237e44
15	1e237e44					7359f67f	6d7a883b
16	6d7a883b	7a883b6d	dac4e23c	08000000	d2c4e23c	3d80477d	ef44a541
17	ef44a541					4716fe3e	a8525b7f
18	a8525b7f					1e237e44	b671253b
19	b671253b					6d7a883b	db0bad00
20	db0bad00	0bad00db	2b9563b9	10000000	3b9563b9	ef44a541	d4d1c6f8
21	d4d1c6f8					a8525b7f	7c839d87
22	7c839d87					b671253b	caf2b8bc
23	caf2b8bc					db0bad00	11f915bc

1. Chuẩn mã hoá nâng cao AES

1. 4. Ví dụ minh hoạ

i (dec)	temp	After RotWord()	After SubWord()	Rcon[i/Nk]	After XOR with Rcon	w[i-Nk]	w[i]= temp XOR w[i-Nk]
24	11f915bc	f915bc11	99596582	20000000	b9596582	d4d1c6f8	6d88a37a
25	6d88a37a					7c839d87	110b3efd
26	110b3efd					caf2b8bc	dbf98641
27	dbf98641					11f915bc	ca0093fd
28	ca0093fd	0093fdca	63dc5474	40000000	23dc5474	6d88a37a	4e54f70e
29	4e54f70e					110b3efd	5f5fc9f3
30	5f5fc9f3					dbf98641	84a64fb2
31	84a64fb2					ca0093fd	4ea6dc4f
32	4ea6dc4f	a6dc4f4e	2486842f	80000000	a486842f	4e54f70e	ead27321
33	ead27321					5f5fc9f3	b58dbad2
34	b58dbad2					84a64fb2	312bf560
35	312bf560					4ea6dc4f	7f8d292f

1. Chuẩn mã hoá nâng cao AES

1. 4. Ví dụ minh hoạ

i (dec)	temp	After RotWord()	After SubWord()	Rcon[i/Nk]	After XOR with Rcon	w[i-Nk]	w[i]= temp XOR w[i-Nk]
36	7f8d292f	8d292f7f	5da515d2	1b000000	46a515d2	ead27321	ac7766f3
37	ac7766f3					b58dbad2	19fadc21
38	19fadc21					312bf560	28d12941
39	28d12941					7f8d292f	575c006e
40	575c006e	5c006e57	4a639f5b	36000000	7c639f5b	ac7766f3	d014f9a8
41	d014f9a8					19fadc21	c9ee2589
42	c9ee2589					28d12941	e13f0cc8
43	e13f0cc8					575c006e	b6630ca6

1. Chuẩn mã hoá nâng cao AES

1. 4. Ví dụ minh hoạ

Ví dụ 1.3

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

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

Round Number	Start of Round	After SubBytes	After ShiftRows	After MixColumns	Round Key Value
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 =
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 =

1. Chuẩn mã hoá nâng cao AES

1. 4. Ví dụ minh hoạ

Round Number	Start of Round	After SubBytes	After ShiftRows	After MixColumns		Round Key Value	
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	=
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	=
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	=

1. Chuẩn mã hoá nâng cao AES

1. 4. Ví dụ minh hoạ

Round Number	Start of Round	After SubBytes	After ShiftRows	After MixColumns		Round Key Value	
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	=
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	=

1. Chuẩn mã hoá nâng cao AES

1. 4. Ví dụ minh hoạ

Round Number	Start of Round	After SubBytes	After ShiftRows	After MixColumns		Round Key Value	
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	=
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	=
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	=

1. Chuẩn mã hoá nâng cao AES

1. 4. Ví dụ minh hoạ

Round Number	Start of Round	After SubBytes	After ShiftRows	After MixColumns		Round Key Value	
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	=
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	=
output	39 02 dc 19 25 dc 11 6a 84 09 85 0b 1d fb 97 32						

Luyện tập

Given the plaintext [0001 0203 0405 0607 0809 0A0B 0C0D 0E0F] and the key [0101 0101 0101 0101 0101 0101 0101 0101]

1. Show the original contents of state, displayed as a 4x4 matrix.
2. Show the value of state after initial AddRoundKey.
3. Show the value of State after SubBytes.
4. Show the value of State after ShiftRows.
5. Compute the value of State after MixColumns.

- Uses arithmetic in the finite field $\mathrm{GF}(2^8)$ with irreducible polynomial

$$m(x) = x^8 + x^4 + x^3 + x + 1$$

which is (1 0001 1011) or {11B}

- Example:

$$\begin{aligned}
&\triangleright \{02\} \cdot \{87\} \bmod \{11\ \mathrm{B}\} = (00000010)(10000111) \\
&= x\left(x^7 + x^2 + x + 1\right) \bmod \left(x^8 + x^4 + x^3 + x + 1\right) \\
&= \left(x^8 + x^3 + x^2 + x\right) \bmod \left(x^8 + x^4 + x^3 + x + 1\right) \\
&= x^4 + x^2 + 1 = (0001\ 0101) \\
&\triangleright \{03\} \cdot \{6\mathrm{E}\} = \{11\}\{1101110\} = (x+1)\left(x^6 + x^5 + x^3 + x^2 + x\right) \bmod (\ldots) \\
&= \left(x^7 + x^6 + x^4 + x^3 + x^2 + x^6 + x^5 + x^3 + x^2 + x\right) \bmod \left(x^8 + x^4 + x^3 + x + 1\right) \\
&= x^7 + x^5 + x^4 + x = \{10110010\} \\
&\triangleright 00010101 \oplus 10110010 \oplus 01000110 \oplus 10100110 = 01000111 = 47
\end{aligned}$$

Nội dung

TRAO ĐỔI