Homework #6

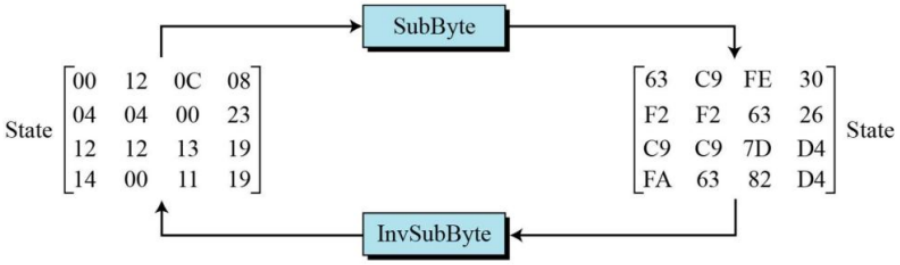
I. Lý thuyết

1. Mô tả phép biến đổi **SubBytes**. Cho ví dụ.

SubBytes được sử dụng tại trang mã hóa. Để thay thế một byte, chúng ta hiểu byte đó là hai chữ số thập lục phân. Thực hiện phép thay thế các byte của mảng trạng thái bằng cách sử dụng một bảng thế S-Box. Phép biến đổi sử dụng trường GF(28) AES cũng xác định phép biến đổi đại số bằng cách sử dụng trường GF(28) với các đa thức tối giản (x8 + x4 + x3+ x + 1)

Hình 7.7 cho thấy cách một trạng thái được chuyển đổi bằng cách sử dụng phép biến đổi SubBytes. Hình này cũng cho thấy phép biến đổi InvSubBytes tạo ra phép biến đổi ban đầu. Lưu ý rằng nếu hai byte có cùng giá trị thì phép biến đổi của chúng cũng giống nhau.

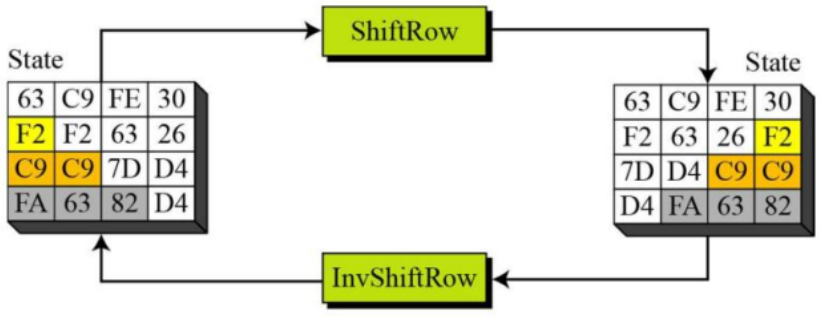
Hình 7.7 Chuyển đổi SubByte cho Ví dụ 7.2



2. Mô tả phép biến đổi **ShiftRows**. Cho ví dụ.

Một phép biến đổi khác được tìm thấy trong một vòng là phép dịch chuyển, phép này hoán vị các byte. Trong quá trình mã hóa, phép biến đổi được gọi là ShiftRows. Áp dụng lên mảng trạng thái bằng cách dịch vòng 3 hàng cuối của mảng trạng thái với số lần dịch (hay số byte bị dịch) khác nhau.

Hình 7.10 cho thấy cách chuyển đổi một trạng thái bằng cách sử dụng phép biến đổi ShiftRows. Hình cũng cho thấy phép biến đổi InvShiftRows tạo ra trạng thái ban đầu.



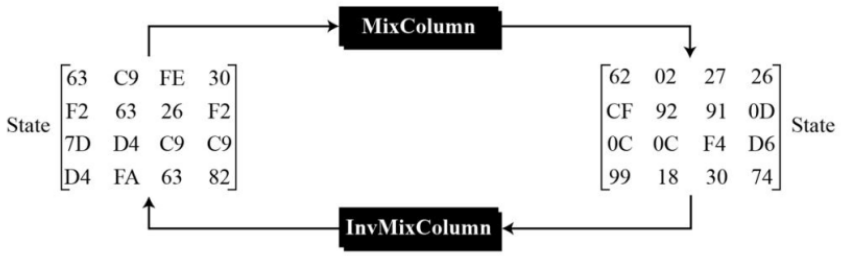
3. Mô tả phép biến đổi **MixColumns**. Cho ví dụ.

Chúng ta cần một phép biến đổi xen kẽ để thay đổi các bit bên trong một byte, dựa trên các bit bên trong các byte lân cận. Chúng ta cần trộn các byte để cung cấp khả năng khuếch tán ở cấp độ bit. biến đổi MixColumns hoạt động ở cấp độ cột; nó chuyển đổi từng cột của trạng thái thành một cột mới. Làm việc trên các cột của mảng trạng thái. Các cột được coi như đa thức trong trường GF(28) và nhân với 1 đa thức a(x) với: A(x) = 3x^3 + x^2 + x + 2

InvMixColumns Phép biến đổi InvMixColumns về cơ bản giống như phép biến đổi MixColumns.

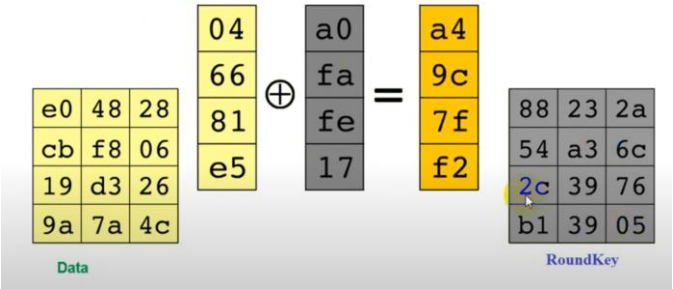
Hình 7.14 cho thấy cách chuyển đổi một trạng thái bằng cách sử dụng phép biến đổi MixColumns. Hình này cũng cho thấy phép biến đổi InvMixColumns tạo ra phép biến đổi ban đầu.

Hình 7.14 Phép biến đổi MixColumns trong Ví dụ 7.5



4. Mô tả phép biến đổi **AddRoundKey**. Cho ví dụ.

AddRoundKey tiến hành mỗi lần một cột. AddRoundKey thêm một từ khóa tròn vào mỗi ma trận cột trạng thái; phép toán trong AddRoundKey là phép cộng ma trận. Một khoá vòng (Round Key) sẽ được cộng vào mảng trạng thái bằng một thao tác XOR bit.



II. Bài tập:

Cho bản rõ (Plaintext) *P*= “DAIHOCTRAVINH”, *P* thuộc bảng mã ASCII và khóa *k* ={01010101010101010101010101010101}

1. Biểu diễn nội dung bản rõ *P* theo ma trận trạng thái 4×4.

ầu tiên, chuyển đổi chuỗi ASCII sang mã hex:

"D" = 44, "A" = 41, "I" = 49, "H" = 48, "O" = 4F, "C" = 43, "T" = 54, "R" = 52

"A" = 41, "V" = 56, "I" = 49, "N" = 4E, "H" = 48

Bản rõ có 13 ký tự, nên cần thêm 3 ký tự để đủ 16 ký tự. Thêm các ký tự đệm, chẳng hạn như 00 (mã hex của NUL). Chuỗi thành kết quả là:

P="DAIHOCTRAVINH"+3 x 00

Chuyển thành mã hex:

44 41 49 48 4F 43 54 52 41 56 49 4E 48 00 00 00

Sau đó chuyển sang ma trận trạng thái 4x4 (theo cột):

44 4F 4148

41 43 56 00

49 54 49 00

48 52 4E 00

2. Biểu diễn bảng giá trị SubBytes.

	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	CB	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

Ma trận trạng thái ban đầu:

$$\begin{bmatrix} 44 & 4F & 41 & 48 \\ 41 & 43 & 56 & 00 \\ 49 & 54 & 49 & 00 \\ 48 & 52 & 4E & 00 \end{bmatrix}$$

Ma trận sau SubBytes:

$$\begin{bmatrix} 1B & 84 & 83 & 52 \\ 83 & 1A & B1 & 63 \\ 3B & 20 & 3B & 63 \\ 52 & 00 & 2F & 63 \end{bmatrix}$$

3. Biểu diễn bảng giá trị ShiftRows.

ShiftRows là bước dịch hàng trong ma trận trạng thái:

- Hàng 0: không dịch
- Hàng 1: dịch vòng trái 1 byte
- Hàng 2: dịch vòng trái 2 byte
- Hàng 3: dịch vòng trái 3 byte

Ma trận sau SubBytes:

$$\begin{bmatrix} 1B & 84 & 83 & 52 \\ 83 & 1A & B1 & 63 \\ 3B & 20 & 3B & 63 \\ 52 & 00 & 2F & 63 \end{bmatrix}$$

Ma trận ShiftRows

$$\begin{bmatrix} 1B & 84 & 83 & 52 \\ 1A & B1 & 63 & 83 \\ 3B & 63 & 3B & 20 \\ 63 & 52 & 00 & 2F \end{bmatrix}$$

4. Biểu diễn bảng giá trị MixColumns.

Ma trận cố định trong AES:

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

Ma trận ShiftRows

$$\begin{bmatrix} 1B & 84 & 83 & 52 \\ 1A & B1 & 63 & 83 \\ 3B & 63 & 3B & 20 \\ 63 & 52 & 00 & 2F \end{bmatrix}$$

02 : 0000 0010 = x

1B : 0001 1011 = x^4+x^3+x+1

Phép nhân: x^5+x^4+x^2+x = 110110 => Hex = 36

Tính toán cột đầu tiên

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 1B \\ 1A \\ 2B \\ 63 \end{bmatrix} = \begin{bmatrix} 36 \oplus 4E \oplus 2B \oplus 63 \\ 1B \oplus 34 \oplus 86 \oplus 63 \\ 1B \oplus 1A \oplus 56 \oplus C9 \\ 52 \oplus 1A \oplus 2B \oplus C6 \end{bmatrix} = \begin{bmatrix} 18 \\ 6C \\ B0 \\ D3 \end{bmatrix}$$

Tính toán cột thứ hai

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 84 \\ B1 \\ 63 \\ 52 \end{bmatrix} = \begin{bmatrix} 08 \oplus 33 \oplus 63 \oplus 52 \\ 84 \oplus 62 \oplus C9 \oplus 52 \\ 84 \oplus B1 \oplus C6 \oplus F6 \\ A7 \oplus B1 \oplus 63 \oplus E4 \end{bmatrix} = \begin{bmatrix} 40 \\ EF \\ 55 \\ 0F \end{bmatrix}$$

Tính toán cột thứ ba

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 83 \\ 63 \\ 3B \\ 00 \end{bmatrix} = \begin{bmatrix} 6C \oplus F2 \oplus 3B \oplus 00 \\ 83 \oplus C6 \oplus 9A \oplus 00 \\ 83 \oplus 63 \oplus 76 \oplus B6 \\ 69 \oplus 63 \oplus 3B \oplus F4 \end{bmatrix} = \begin{bmatrix} 87 \\ 59 \\ 1C \\ 64 \end{bmatrix}$$

Tính toán cột thứ tư

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} 52 \\ 83 \\ 20 \\ 2F \end{bmatrix} = \begin{bmatrix} A4 \oplus 99 \oplus 20 \oplus 2F \\ 52 \oplus 66 \oplus 60 \oplus 2F \\ 52 \oplus 83 \oplus 40 \oplus 8D \\ F6 \oplus 83 \oplus 20 \oplus 5E \end{bmatrix} = \begin{bmatrix} 8D \\ 4F \\ 16 \\ A1 \end{bmatrix}$$

Bảng giá trị MixColumns cuối cùng

$$\begin{bmatrix} 18 & 40 & 87 & 8D \\ 6C & EF & 59 & 4F \\ B0 & 55 & 1C & 16 \\ D3 & 0F & 64 & A1 \end{bmatrix}$$

5. Biểu diễn bảng giá trị AddRoundKey

Ma trận khoá:

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

Mixcolumns:

$$\begin{bmatrix} 18 & 40 & 87 & 8D \\ 6C & EF & 59 & 4F \\ B0 & 55 & 1C & 16 \\ D3 & 0F & 64 & A1 \end{bmatrix}$$

Thực hiện phép XOR:

18⊕01 40⊕01 87⊕01 8D⊕01	19 41 86 8C
6C⊕01 EF⊕01 59⊕01 4F⊕01	6D EE 58 4E
B0⊕01 55⊕01 1C⊕01 16⊕01	B1 54 1D 17
D3⊕01 0F⊕01 64⊕01 A1⊕01	D2 0E 65 A0