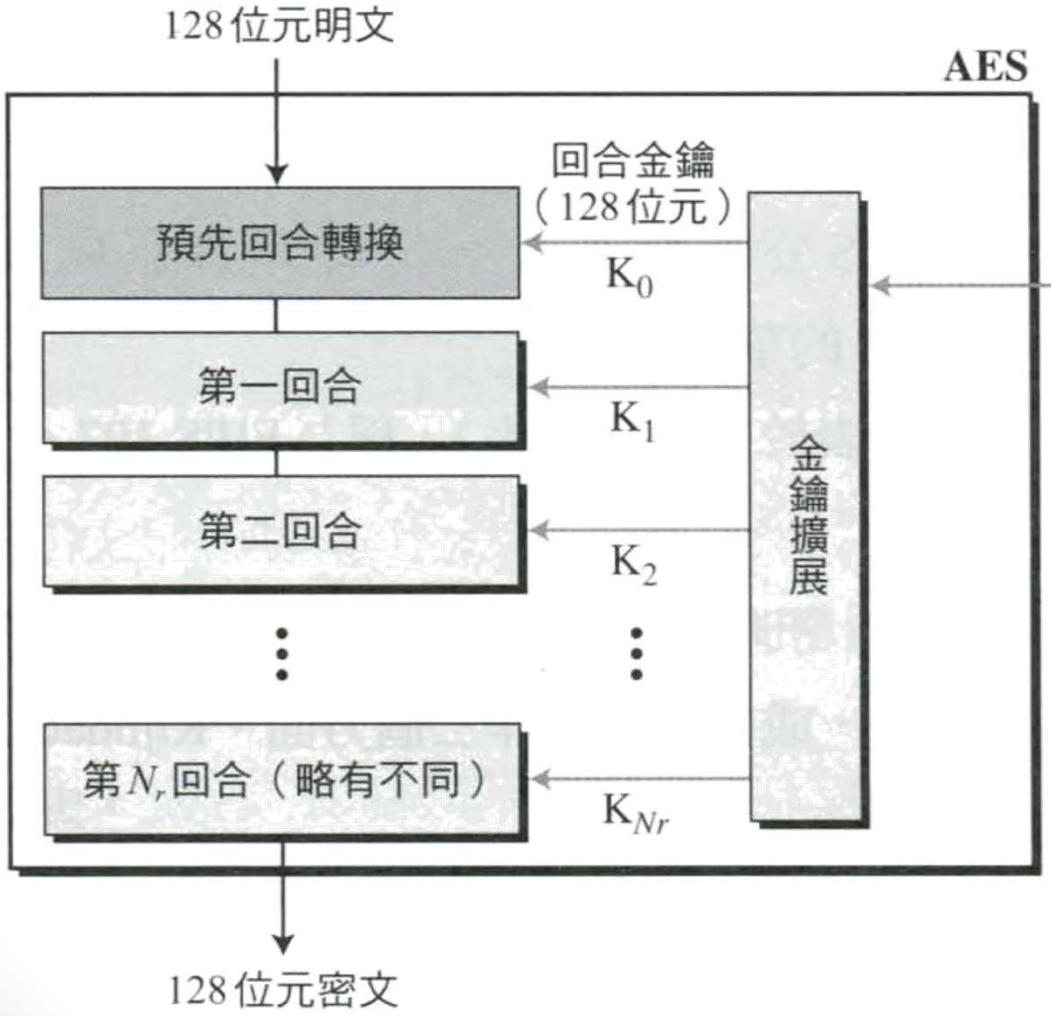
第三章
對稱式金鑰密碼系統–進階加密標準

簡介

- 進階加密系統(Advanced Encryption Standard, AES)是美國國家標準技術局於2001年12月所發布的對稱式區塊加密法。
- NIST從1997年開始尋找取代DES的標準加密法，並命名為進階加密標準。
- 區塊大小為128位元，金鑰長度有128、192和256位元三種長度。
- 運算回合數可為十、十二和十四個回合。

簡介

- AES加密演算的設計概念



Nr	金鑰長度
10	128
12	192
14	256

回合數與加密金鑰長度的關係

簡介

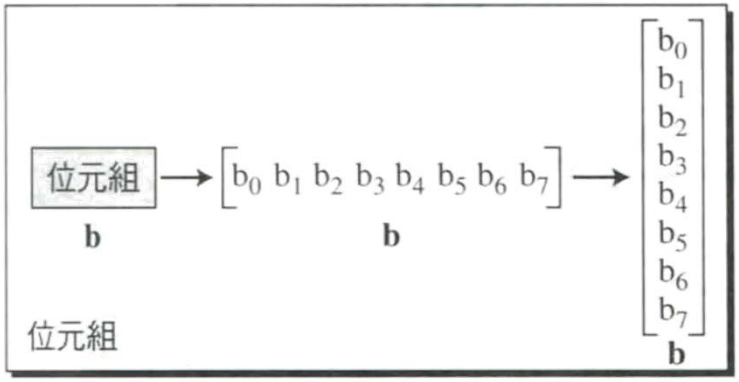
- N_r指的是回合數，根據圖中所示一共有三種AES版本，AES-128、AES-192以及AES-256。
- 然而，每個回合中利用金鑰擴展演算法所產生的回合金鑰長度都是128位元，和明文或密文區塊長度都一樣。
- 利用金鑰擴展演算法所產生之回合金鑰的個數永遠都比回合數多一。

回合金鑰個數= N_r+1

簡介

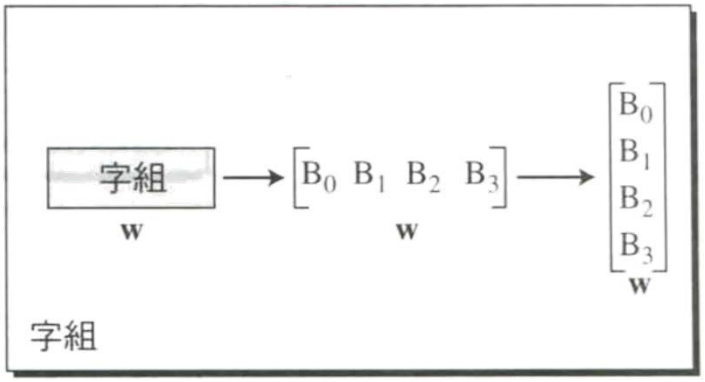
資料單位

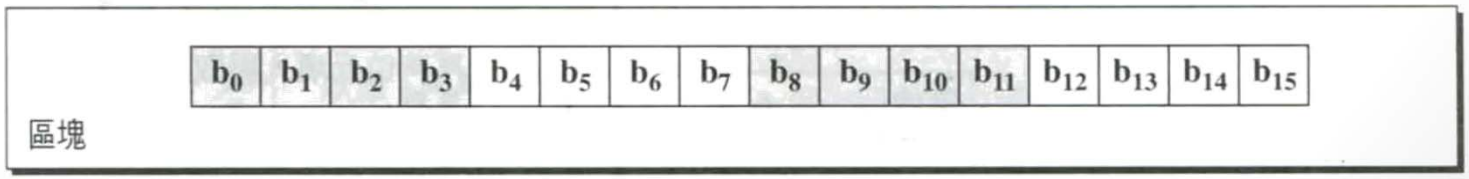
- AES使用五種資料單位分別是位元、位元組、字組、區塊和狀態。
- 位元(bit)：在AES中，位元指二進位，通常會用小寫字母表示一個位元。
- 位元組(byte)：由八位元所組成的單位，是一個1×8的矩陣或是8×1的矩陣，通常用小寫的粗體字母表示一個位元組。



簡介

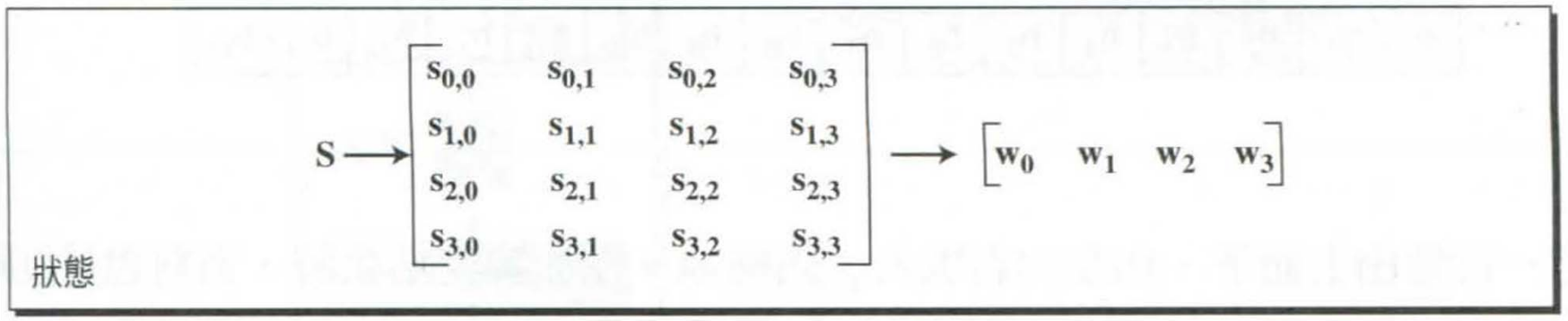
- 字組(word)：長度為32位元，為四個位元組的列矩陣或行矩陣，用小寫粗體字母**w**表示一個字組。
- 區塊(block)：一個區塊有128位元，可用一個長度為16個位元組的列矩陣來表示。





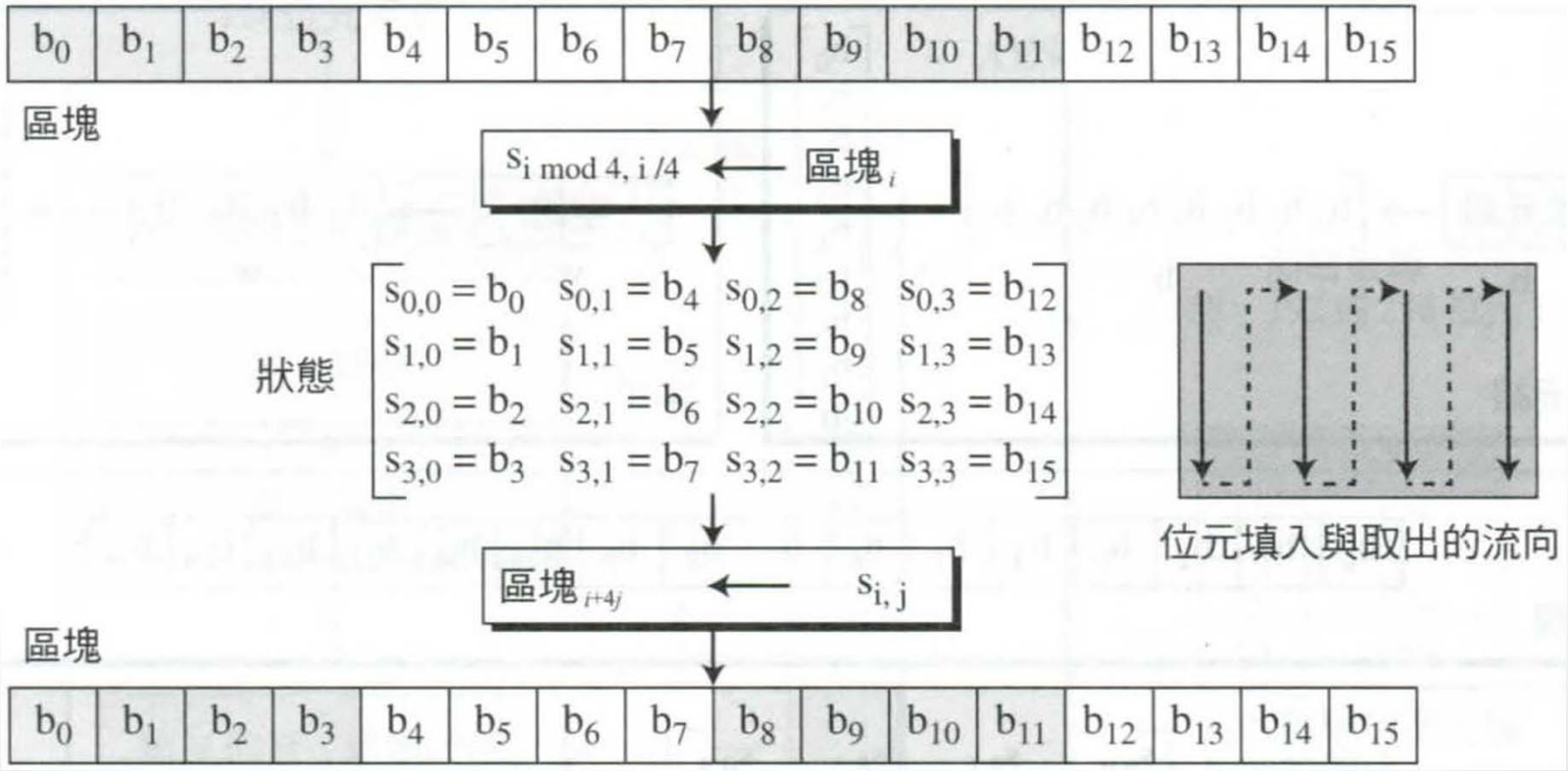
簡介

- 狀態(state)：AES執行可分為許多回合，每回合又分為很多個階段。
- 在AES加密法的開頭與結尾，每個單位的資料稱為資料區塊(data block)，每個階段的開頭與結尾，此單位被稱為狀態。
- 通常使用大寫的粗體S來代表狀態，和區塊一樣用16個位元組且為當作一個4×4個位元組所構成的矩陣。



簡介

- $s_{r,c}$來代表矩陣的元素(其中r代表矩陣列數，c代表矩陣行數，且$0 \le r \le 3, 0 \le c \le 3$)。
- 開始加密時是一行一行地由上而下、由左向右填入。



簡介

- 範例 3.1 我們來看看如何使用一個4 × 4的陣列來表示英文字母。假設文字區塊內容是「AES uses a matrix」。
- 1. 首先必須再填入兩個無意義的字母來湊滿16個。

AESUSESAMATRIXZZ

- 2. 用00到25的數字取代這些字母(十進制)。

00 04 18 20 18 04 18 00 12 00 19 17 08 23 25 25

- 3. 將十進制改為十六進制。

00 04 12 14 12 04 12 00 0C 00 13 11 08 17 19 19

簡介

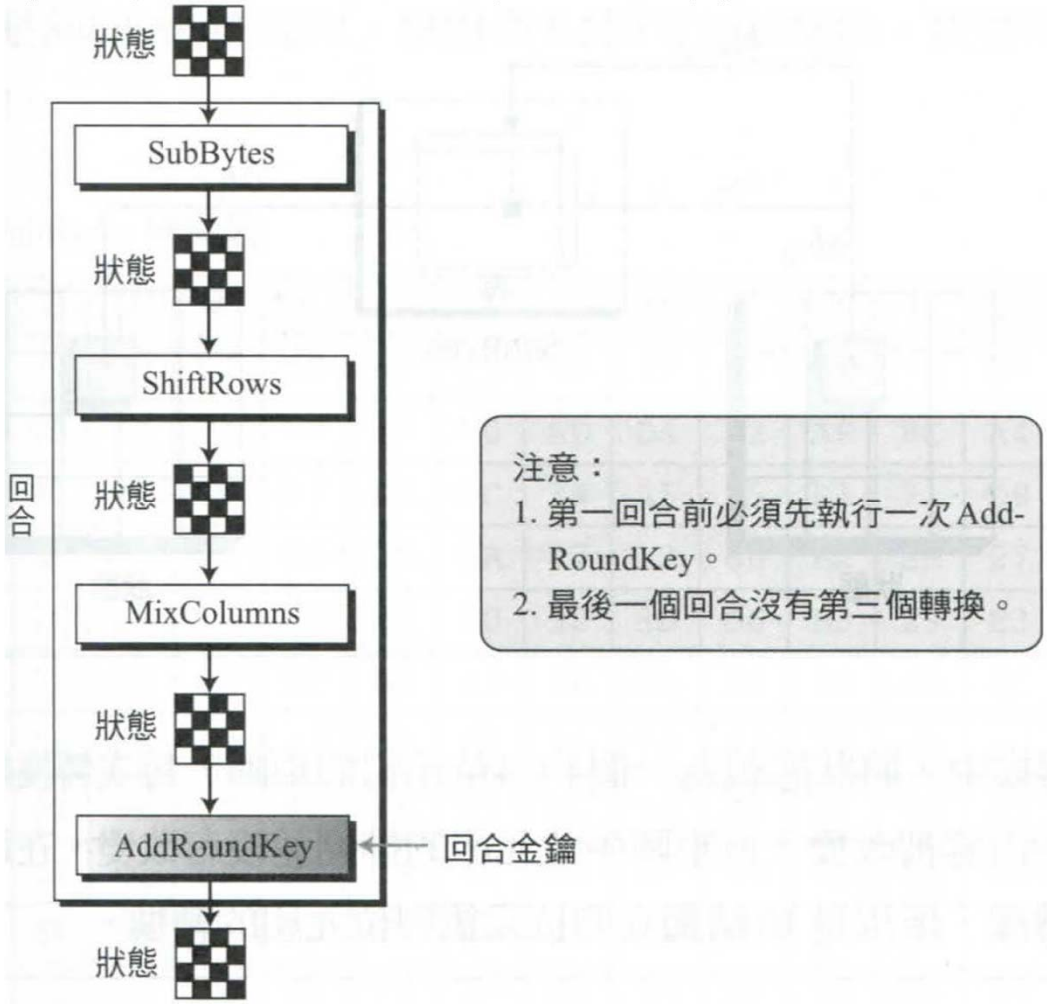
- 4. 最後，將這些十六進制的數字由上到下由左到右的順序填入狀態陣列。

文字	A	E	S	U	S	E	S	A	M	A	T	R	I	X	Z	Z
十六進位	00	04	12	14	12	04	12	00	0C	00	13	11	08	23	19	19

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

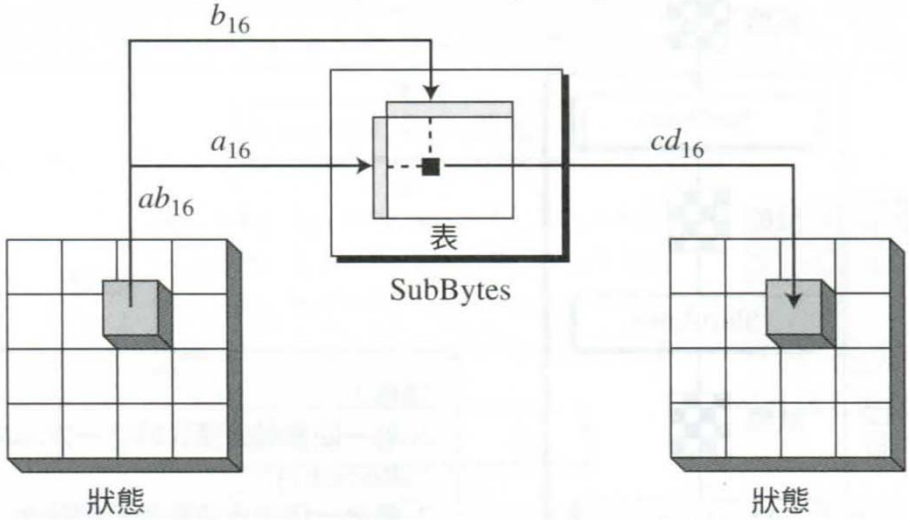
加密每回合的結構

- 每個回合的結構：每個回合有四個可逆的轉換，最後一回合只有三個轉換。



轉換-取代(SubBytes)

- 為了安全起見，AES使用四種類型的轉換，取代、排列、混合以及加入金鑰。
- 取代：AES的取代是以位元組為單位。
- SubBytes：第一種轉換是在加密端使用，將位元組表示成兩個十六進位，左邊為取代表的列，右邊為取代表的行，行列交叉處形成新的兩個十六進制數字，即為新的位元組。



轉換-取代(SubBytes)

- SubBytes 轉換表：

表 7.1　SubBytes 轉換表

	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

轉換-取代(SubBytes)

- 範例 3.2 展示一組狀態如何使用SubBytes進行轉換。

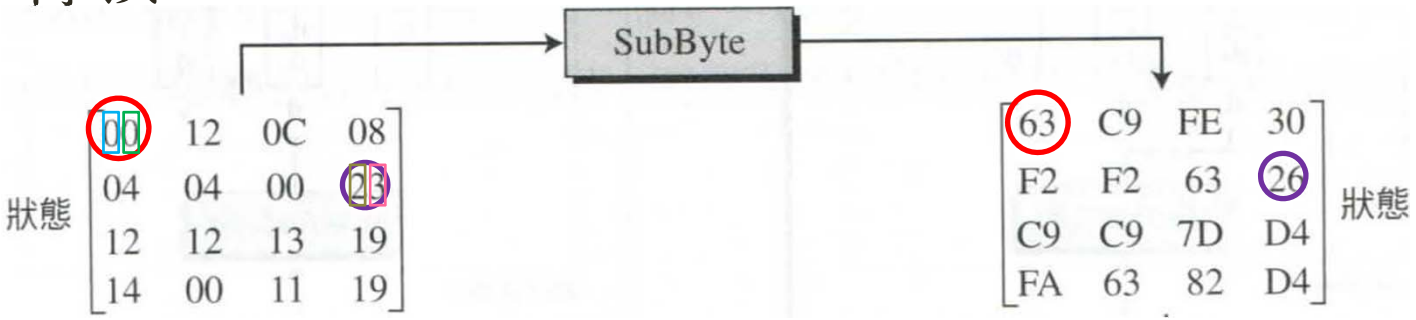


表 7.1 SubBytes 轉換表

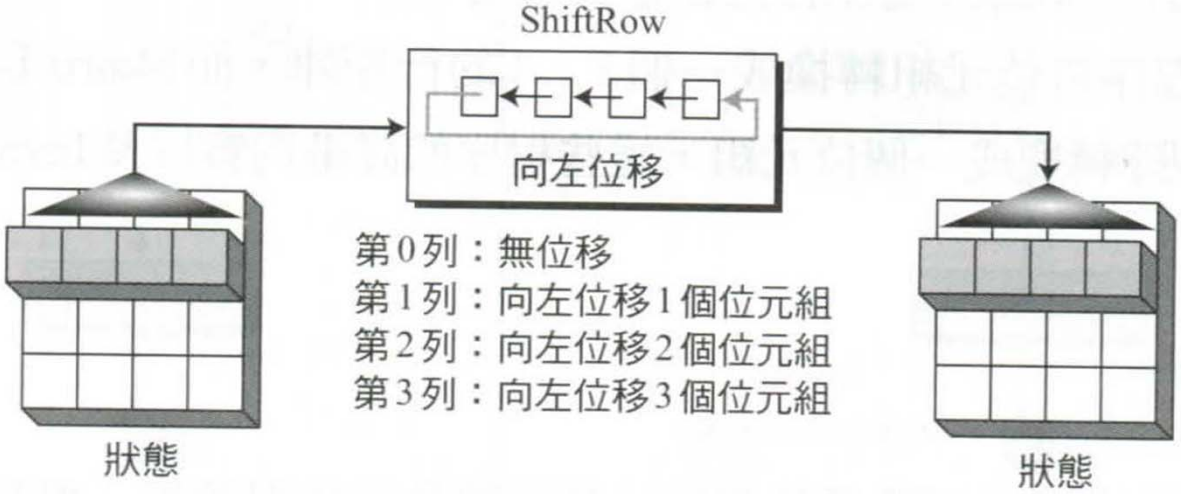
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC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

表 7.2 InvSubBytes 轉換表

	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

轉換-排列(ShiftRows)

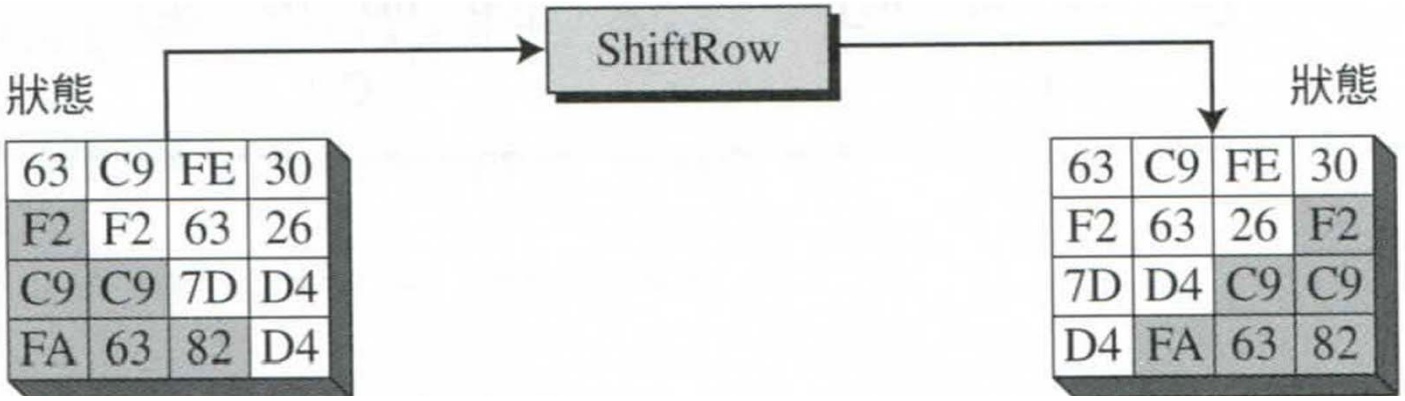
- 排列：另一種轉換式位元組排列的位移，DES位移是以位元為單位，AES位移是以位元組為單位。
- ShiftRows：其位移由右向左，位移的次數取決於狀態矩陣的列數(0、1、2或3)。



- InvShiftRows：在解密時，其位移由左向右，位移的次數取決於狀態矩陣的列數。

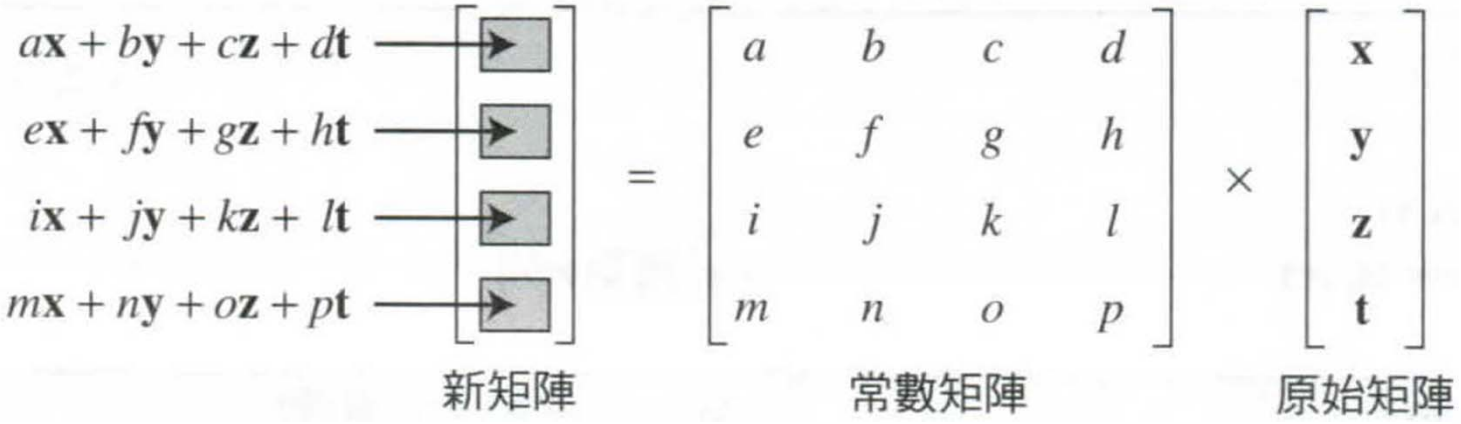
轉換-排列(ShiftRows)

- 範例 3.3 展示一組狀態如何進行ShiftRows轉換。



轉換-混合(MixColumns)

- 混合：改變美個位元組的內容是一次取用四個位元組，加以組合後重新產生四個位元組。
- 新矩陣內的每個元素都是原始矩陣的四個元素乘上常數行矩陣中對應之值的總和。

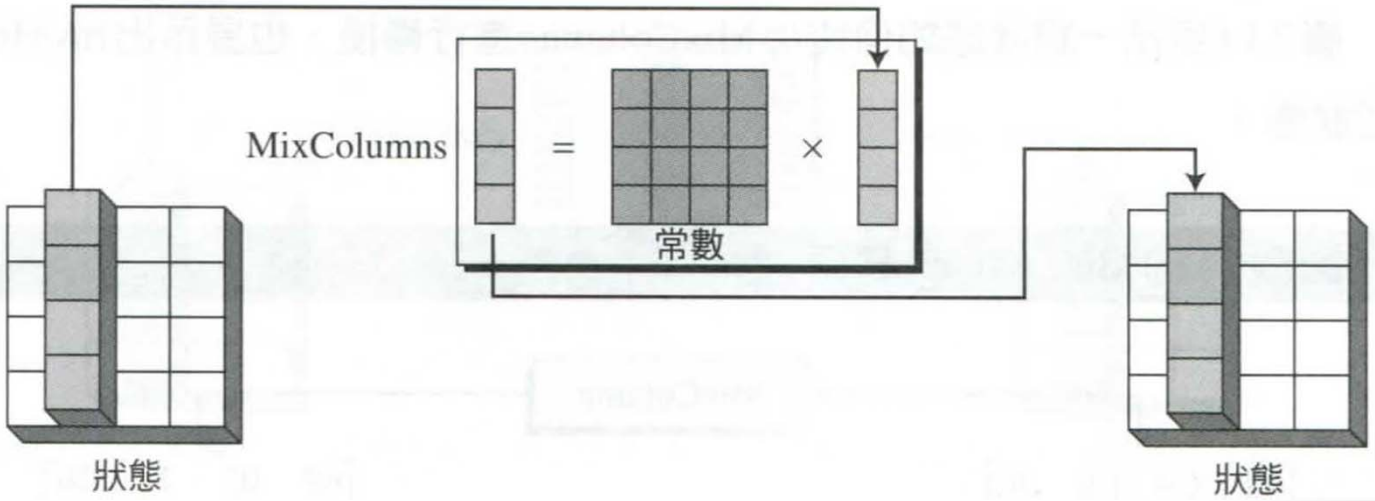


轉換-混合(MixColumns)

- AES定義的混合程序稱為MixColumns。下圖為混合程序裡使用的常數矩陣。

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

- MixColumns：是以行矩陣為單位來執行，他將每個行矩陣轉換成另一組數值。



轉換-混合(MixColumns)

- MixColumns也可以稱為將一行四位元組經過特殊矩陣運算，得到新的四位元組。

$$\begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix}$$

- 特殊矩陣：*xtime*函數

$$s_{0,0}(new) = (\{02\} \cdot s_{0,0}) \oplus (\{03\} \cdot s_{1,0}) \oplus s_{2,0} \oplus s_{3,0}$$

$$s_{1,0}(new) = (\{02\} \cdot s_{1,0}) \oplus (\{03\} \cdot s_{2,0}) \oplus s_{3,0} \oplus s_{0,0}$$

$$s_{2,0}(new) = (\{02\} \cdot s_{2,0}) \oplus (\{03\} \cdot s_{3,0}) \oplus s_{0,0} \oplus s_{1,0}$$

$$s_{3,0}(new) = (\{02\} \cdot s_{3,0}) \oplus (\{03\} \cdot s_{0,0}) \oplus s_{1,0} \oplus s_{2,0}$$

$$\{02\} \cdot s_{i,j} = s_{i,j} \cdot \{02\} = xtime(s_{i,j})$$

$$\{03\} \cdot s_{i,j} = s_{i,j} \cdot \{03\} = s_{i,j} \cdot (\{01\} \oplus \{02\}) = s_{i,j} \oplus xtime(s_{i,j})$$

轉換-混合(MixColumns)

- *xtime*函數：此函數輸入與輸出皆為八位元，計算方式分為兩種狀況：
- 情況一、如果原始輸入值的最左邊有效位元為0，將輸入位元向左移一位元，最右邊為無效位元補0。
- 情況二、如果原始輸入值的最左邊有效位元為1，則將輸入向左移一位元，最右邊為無效位元補0，再與十六進制$\{1B\}_{16}=\{00011011\}_2$進行XOR運算後再輸出。

轉換-混合(MixColumns)

- 例題3.5 $xtime(57)$

$57_{16} = 01010111_{\ 2}$，只須向左移一位元右邊補0(情況一)。

$$xtime(57) = 10101110_2 = \mathrm{AE}_{16}$$

- 例題3.6 $xtime(\mathrm{AE})$

$\mathrm{AE}_{16} = 10101110_2$須向左移一位元右邊補0，形成$01011100_2$。

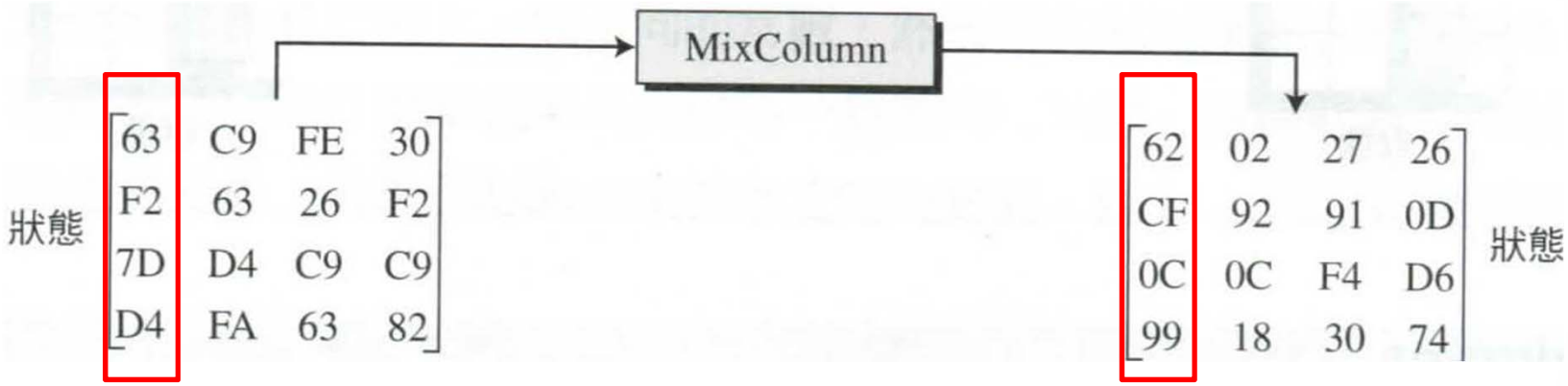
再與十六進制$\{1\mathrm{B}\}_{16}$=$\{00011011\}_2$ 進行XOR運算(情況二)。

$$01011100_2 \oplus 00011011_2 = 01000111_2$$

最後輸出為$xtime(\mathrm{AE}) = 01000111_2 = 47_{16}$

轉換-混合(MixColumns)

- 例題3.7 展示一組狀態如何使用MixColumns進行轉換。



$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} 63 \\ F2 \\ 7D \\ D4 \end{bmatrix} = \begin{bmatrix} s_{0,0} \\ s_{1,0} \\ s_{2,0} \\ s_{3,0} \end{bmatrix} \Rightarrow \begin{cases} s_{0,0}(new) = (\{02\} \cdot 63) \oplus (\{03\} \cdot F2) \oplus 7D \oplus D4 \\ s_{1,0}(new) = (\{02\} \cdot F2) \oplus (\{03\} \cdot 7D) \oplus D4 \oplus 63 \\ s_{2,0}(new) = (\{02\} \cdot 7D) \oplus (\{03\} \cdot D4) \oplus 63 \oplus F2 \\ s_{3,0}(new) = (\{02\} \cdot D4) \oplus (\{03\} \cdot 63) \oplus F2 \oplus 7D \end{cases}$$

轉換-混合(MixColumns)

- 計算 $s_{0,0}(new) = (\{02\} \cdot 63) \oplus (\{03\} \cdot \text{F2}) \oplus 7\text{D} \oplus \text{D4}$

$$\Rightarrow xtime(63) \oplus (\text{F2} \oplus xtime(\text{F2})) \oplus 7\text{D} \oplus \text{D4}$$

- (情況一)$63_{16} = 01100011_2$ $xtime(63) = 11000110_2$
- (情況二)$\text{F2}_{16} = 11110010_2$向左移右捕0

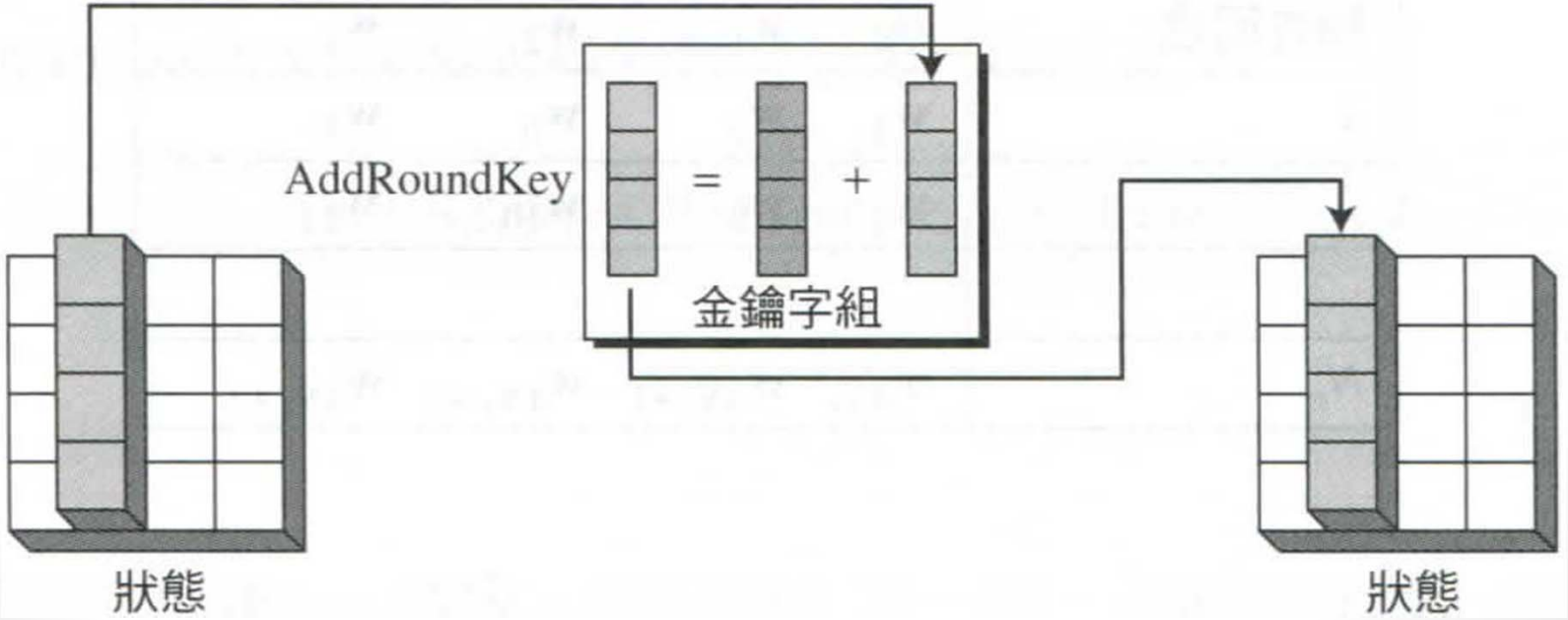
11100100_2與$\{1\text{B}\}_{16} = 00011011_2$XOR運算

$xtime(\text{F2}) = 11100100_2 \oplus 00011011_2 = 11111111_2$

$$\left.\begin{array}{ll} xtime(63): & 11000110 \\ xtime(\text{F2}): & 11111111 \\ \text{F2}: & 11110010 \\ 7\text{D}: & 01111101 \\ \text{D4}: & 11010100 \end{array}\right\} = 01100010_2 = 62_{16}$$

轉換-加入金鑰(AddRoundKey)

- 整個加密過程最重要為加入金鑰，也是Alice與Bob在整個過程中共享的唯一秘密。
- AddRoundKey是將回合金鑰加入狀態矩陣行，是使用矩陣加法。我們可以想像成狀態行與對應的金鑰自組的XOR運算。



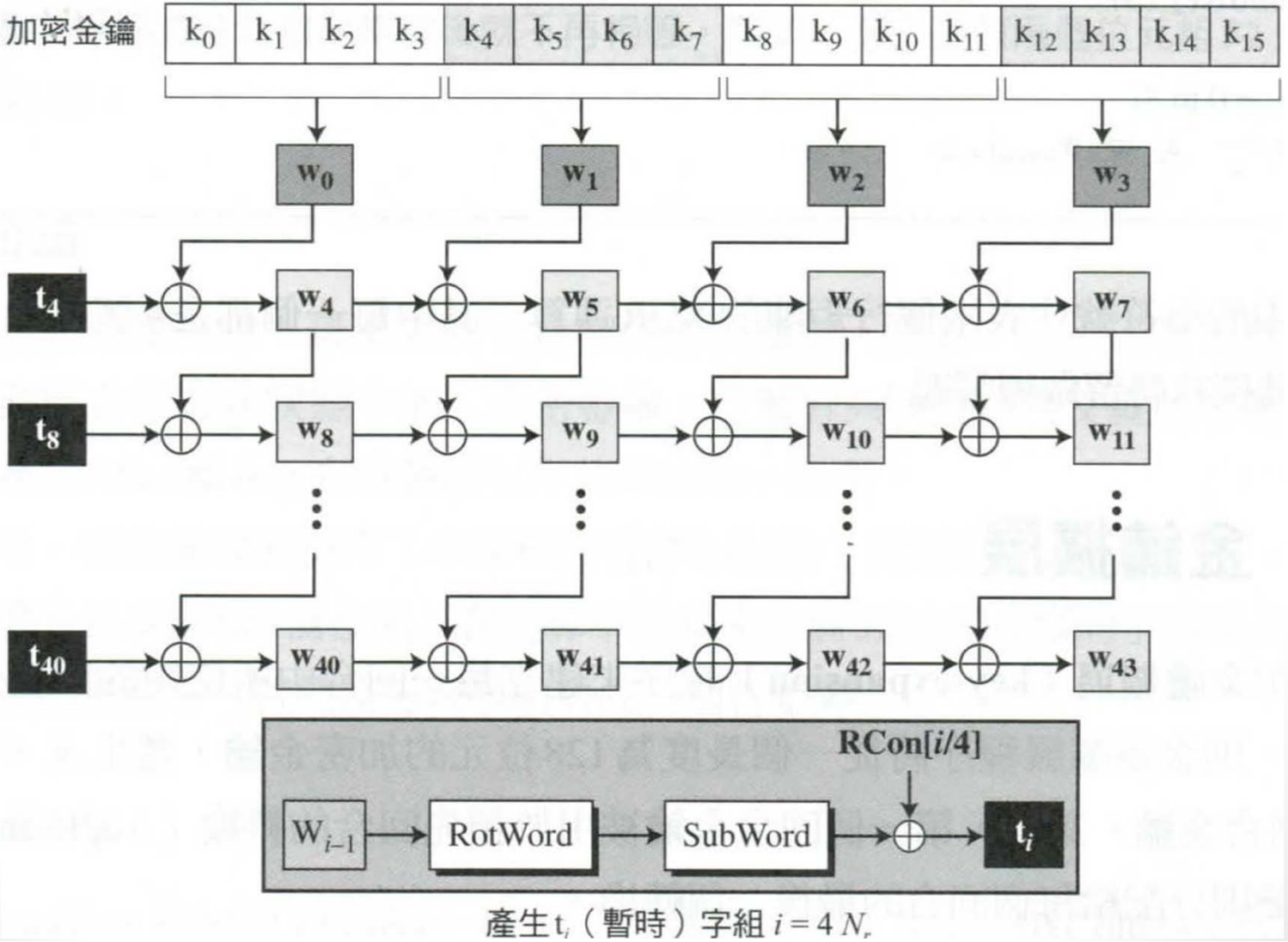
金鑰擴展(Key-expansion)

- AES使用金鑰擴展程序來建立每一回合中所使用的回合金鑰。
- 假設回合數為N_r，則金鑰擴展程序將從一個長度為128位元的加密金鑰，產生$N_r + 1$個長度為128位元的回合金鑰。
- 第一回合金鑰被用於預先回合的轉換，剩下的回合金鑰則分配給每個回合的最後一個轉換。
- 金鑰擴展程序產生回合金鑰時，是一個字組一個字組產生的長度為4個位元組。

$$4(N_r + 1)\text{個字組}$$

金鑰擴展(Key-expansion)

- AES的金鑰擴展



金鑰擴展(Key-expansion)

- AES-128的金鑰擴展程序大致如下：
- 1. 前4個字組($\mathbf{w}_0, \mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3$)直接由加密金鑰組成。
- 2. 其他的字組($\mathbf{w}_i$，其中i=4至43)產生程序如下：
- a.當$(i \ mod \ 4) \neq 0$時，$\mathbf{w}_i = \mathbf{w}_{i-1} \oplus \mathbf{w}_{i-4}$。
- b.當$(i \ mod \ 4) = 0$時，$\mathbf{w}_i = \mathbf{t} \oplus \mathbf{w}_{i-4}$。這裡的$\mathbf{t}$是由$\mathbf{w}_{i-1}$經過SubWord和RotWord，在和一個回合常數Rcon做XOR後所得。

$$\mathbf{t} = \text{SubWord}(\text{RotWord}(\mathbf{w}_{i-1})) \oplus \text{Rcon}_{i/4}$$

金鑰擴展(Key-expansion)

- SubWord：將一個字組當作長度為4個位元組的陣列，並將位元組以迴轉的方式向左位移。
- RotWord：使用SubByte轉換表，將字組內的4個位元組用別的位元組加以取代。
- 回合常數：每個回合常數都為4個位元組。

回合	常數（RCon）	回合	常數（RCon）
1	$(\underline{\mathbf{01}}\ 00\ 00\ 00)_{16}$	6	$(\underline{\mathbf{20}}\ 00\ 00\ 00)_{16}$
2	$(\underline{\mathbf{02}}\ 00\ 00\ 00)_{16}$	7	$(\underline{\mathbf{40}}\ 00\ 00\ 00)_{16}$
3	$(\underline{\mathbf{04}}\ 00\ 00\ 00)_{16}$	8	$(\underline{\mathbf{80}}\ 00\ 00\ 00)_{16}$
4	$(\underline{\mathbf{08}}\ 00\ 00\ 00)_{16}$	9	$(\underline{\mathbf{1B}}\ 00\ 00\ 00)_{16}$
5	$(\underline{\mathbf{10}}\ 00\ 00\ 00)_{16}$	10	$(\underline{\mathbf{36}}\ 00\ 00\ 00)_{16}$

金鑰擴展(Key-expansion)

- 例題3.8 顯示使用(24 75 A2 B3 34 75 56 88 31 E2 12 00 13 AA 54 87)16 這個金鑰所產生的回合金鑰。

回合	t值	回合中的第一個字組	回合中的第二個字組	回合中的第二個字組	回合中的第四個字組
—		w_{00} = 2475A2B3	w_{01} = 34755688	w_{02} = 31E21200	w_{03} = 13AA5487
1	AD20177D	w_{04} = 8955B5CE	w_{05} = BD20E346	w_{06} = 8CC2F146	w_{07} = 9F68A5C1
2	470678DB	w_{08} = CE53CD15	w_{09} = 73732E53	w_{10} = FFB1DF15	w_{11} = 60D97AD4
3	31DA48D0	w_{12} = FF8985C5	w_{13} = 8CFAAB96	w_{14} = 734B7483	w_{15} = 2475A2B3
4	47AB5B7D	w_{16} = B822deb8	w_{17} = 34D8752E	w_{18} = 479301AD	w_{19} = 54010FFA
5	6C762D20	w_{20} = D454F398	w_{21} = E08C86B6	w_{22} = A71F871B	w_{23} = F31E88E1
6	52C4F80D	w_{24} = 86900B95	w_{25} = 661C8D23	w_{26} = C1030A38	w_{27} = 321D82D9
7	E4133523	w_{28} = 62833EB6	w_{29} = 049FB395	w_{30} = C59CB9AD	w_{31} = F7813B74
8	8CE29268	w_{32} = EE61ACDE	w_{33} = EAFE1F4B	w_{34} = 2F62A6E6	w_{35} = D8E39D92
9	0A5E4F61	w_{36} = E43FE3BF	w_{37} = 0EC1FCF4	w_{38} = 21A35A12	w_{39} = F940C780
10	3FC6CD99	w_{40} = DBF92E26	w_{41} = D538D2D2	w_{42} = F49B88C0	w_{43} = 0DDB4F40

即使加密金鑰只差一位元

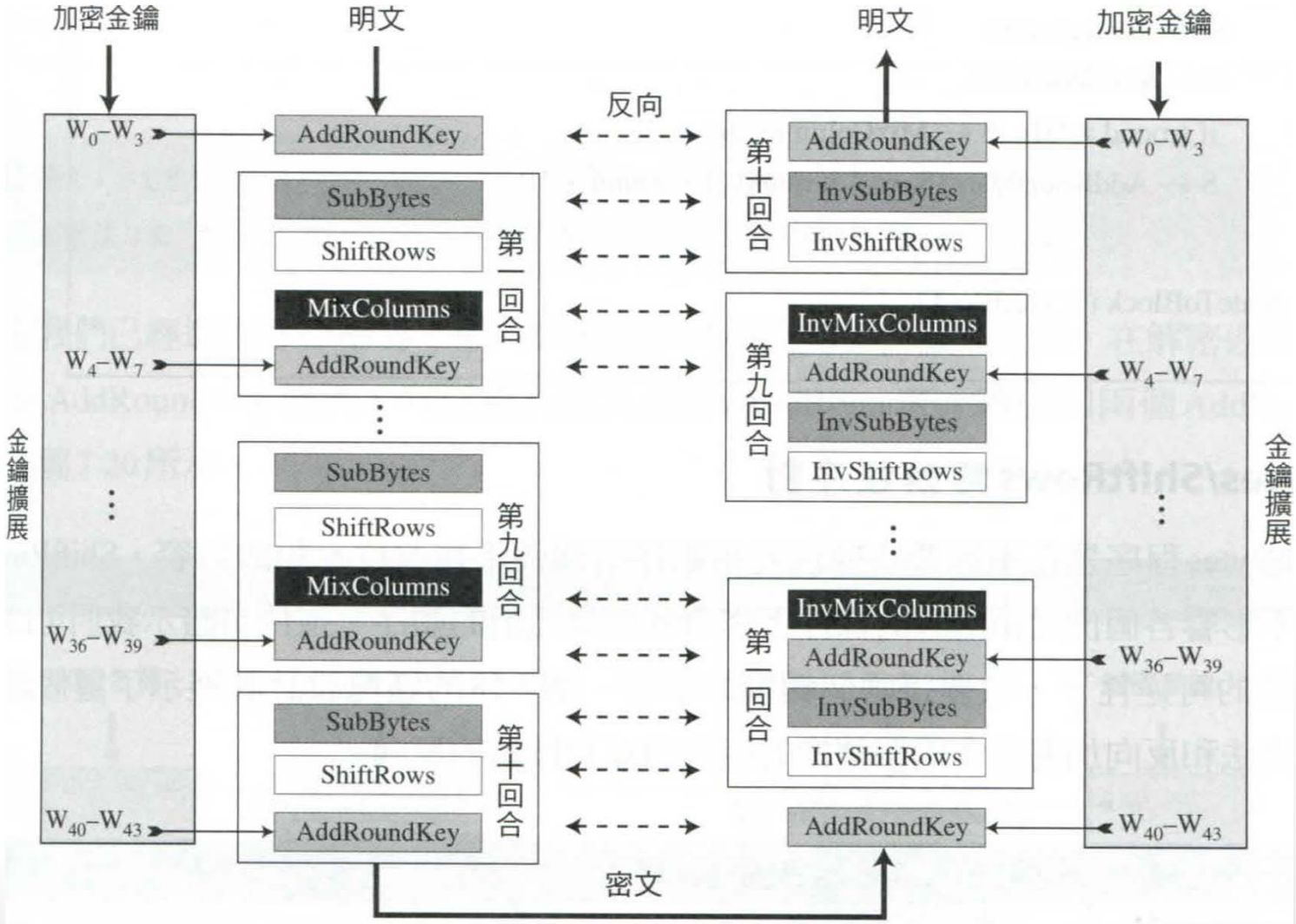
- 即使加密金鑰差異很小，所求出來的兩組回合金鑰的差異也很明顯。

R.	第一組回合金鑰	第二組回合金鑰	*B. D.*
—	1245A2A1 2331A4A3 B2CCAA34 C2BB7723	1245A2A1 2331A4A3 B2CCAB34 C2BB7723	01
1	F9B08484 DA812027 684D8A13 AAF6FD30	F9B08484 DA812027 684D8B13 AAF6FC30	02
2	B9E48028 6365A00F 0B282A1C A1DED72C	B9008028 6381A00F 0BCC2B1C A13AD72C	17
3	A0EAF11A C38F5115 C8A77B09 6979AC25	3D0EF11A 5E8F5115 55437A09 F479AD25	30
4	1E7BCEE3 DDF49FF6 1553E4FF 7C2A48DA	839BCEA5 DD149FB0 8857E5B9 7C2E489C	31
5	EB2999F3 36DD0605 238EE2FA 5FA4AA20	A2C910B5 7FDD8F05 F78A6ABC 8BA42220	34
6	82852E3C B4582839 97D6CAC3 C87260E3	CB5AA788 B487288D 430D4231 C8A96011	56
7	82553FD4 360D17ED A1DBDD2E 69A9BDCD	588A2560 EC0D0DED AF004FDC 67A92FCD	50
8	D12F822D E72295C0 46F948EE 2F50F523	0B9F98E5 E7929508 4892DAD4 2F3BF519	44
9	99C9A438 7EEB31F8 38127916 17428C35	F2794CF0 15EBD9F8 5D79032C 7242F635	51
10	83AD32C8 FD460330 C5547A26 D216F613	E83BDAB0 FDD00348 A0A90064 D2EBF651	52

- *R*回合數， *B.D.*不同的位元數。

AES進階加密法

- 進階加密法的加密



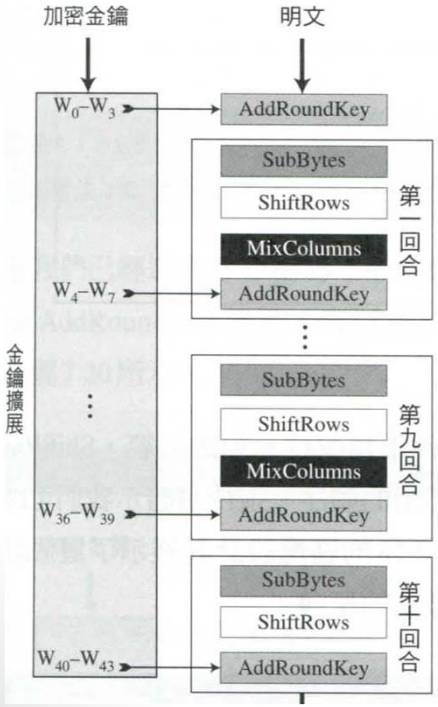
AES範例

- 範例 3.9 以下使用一個隨機選擇加密金鑰將明文加密後產生的密文區塊。

明文： 00 04 12 14 12 04 12 00 0C 00 13 11 08 23 19 19

加密金鑰： 24 75 A2 B3 34 75 56 88 31 E2 12 00 13 AA 54 87

密文： BC 02 8B D2 E0 E3 B1 95 55 0D 6D FB E6 F1 82 41



回合	輸入狀態	輸出狀態	回合金鑰
預先回合	00 12 0C 08 04 04 00 23 12 12 13 19 14 00 11 19	24 26 3D 1B 71 71 E2 89 B0 44 01 4D A7 88 11 9E	24 34 31 13 75 75 E2 AA A2 56 12 54 B3 88 00 87

AES範例

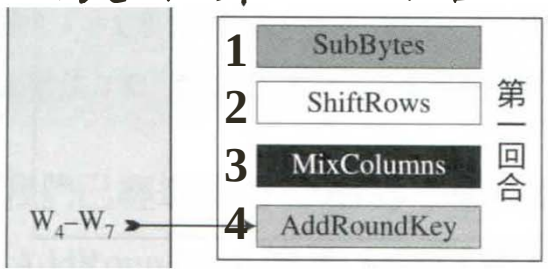
1	24 26 3D 1B 71 71 E2 89 B0 44 01 4D A7 88 11 9E	6C 44 13 BD B1 9E 46 35 C5 B5 F3 02 5D 87 FC 8C	89 BD 8C 9F 55 20 C2 68 B5 E3 F1 A5 CE 46 46 C1
2	6C 44 13 BD B1 9E 46 35 C5 B5 F3 02 5D 87 FC 8C	1A 90 15 B2 66 09 1D FC 20 55 5A B2 2B CB 8C 3C	CE 73 FF 60 53 73 B1 D9 CD 2E DF 7A 15 53 15 D4
3	1A 90 15 B2 66 09 1D FC 20 55 5A B2 2B CB 8C 3C	F6 7D A2 B0 1B 61 B4 B8 67 09 C9 45 4A 5C 51 09	FF 8C 73 13 89 FA 4B 92 85 AB 74 0E C5 96 83 57
4	F6 7D A2 B0 1B 61 B4 B8 67 09 C9 45 4A 5C 51 09	CA E5 48 BB D8 42 AF 71 D1 BA 98 2D 4E 60 9E DF	B8 34 47 54 22 D8 93 01 DE 75 01 0F B8 2E AD FA
5	CA E5 48 BB D8 42 AF 71 D1 BA 98 2D 4E 60 9E DF	90 35 13 60 2C FB 82 3A 9E FC 61 ED 49 39 CB 47	D4 E0 A7 F3 54 8C 1F 1E F3 86 87 88 98 B6 1B E1

AES範例

6	90 35 13 60 2C FB 82 3A 9E FC 61 ED 49 39 CB 47	18 0A B9 B5 64 68 6A FB 5A EF D7 79 8E B2 10 4D	86 66 C1 32 90 1C 03 1D 0B 8D 0A 82 95 23 38 D9
7	18 0A B9 B5 64 68 6A FB 5A EF D7 79 8E B2 10 4D	01 63 F1 96 55 24 3A 62 F4 8A DE 4D CC BA 88 03	62 04 C5 F7 83 9F 9C 81 3E B3 B9 3B B6 95 AD 74
8	01 63 F1 96 55 24 3A 62 F4 8A DE 4D CC BA 88 03	2A 34 D8 46 2D 6B A2 D6 51 64 CF 5A 87 A8 F8 28	EE EA 2F D8 61 FE 62 E3 AC 1F A6 9D DE 4B E6 92
9	2A 34 D8 46 2D 6B A2 D6 51 64 CF 5A 87 A8 F8 28	0A D9 F1 3C 95 63 9F 35 2A 80 29 00 16 76 09 77	E4 0E 21 F9 3F C1 A3 40 E3 FC 5A C7 BF F4 12 80
10	0A D9 F1 3C 95 63 9F 35 2A 80 29 00 16 76 09 77	BC E0 55 E6 02 E3 0D F1 8B B1 6D 82 D3 95 F8 41	DB D5 F4 0D F9 38 9B DB 2E D2 88 4F 26 D2 C0 40

AES範例

- 展示第一回合的狀態值變化。



回合	輸入狀態	輸出狀態	回合金鑰
1	24 26 3D 1B 71 71 E2 89 B0 44 01 4D A7 88 11 9E	6C 44 13 BD B1 9E 46 35 C5 B5 F3 02 5D 87 FC 8C	89 BD 8C 9F 55 20 C2 68 B5 E3 F1 A5 CE 46 46 C1

- 1. 首先將輸入狀態對應SubByte轉換表

24	26	3D	1B
71	71	E2	89
B0	44	01	4D
A7	88	11	9E

輸入狀態

表 7.1 SubBytes 轉換表

	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

36	F7	27	AF
A3	A3	98	A7
E7	1B	7C	E3
5C	C4	82	0B

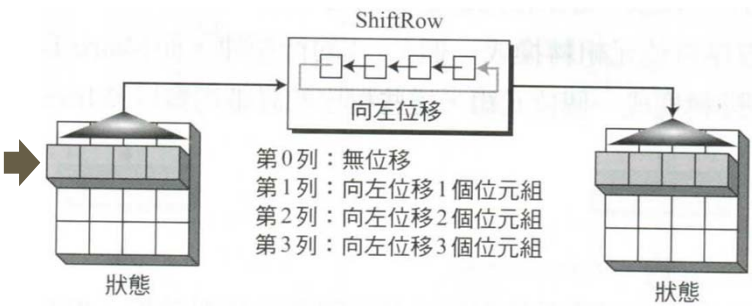
SubByte程序後

AES範例

- 2.經ShiftRows左移位元組

36	F7	27	AF
A3	A3	98	A7
E7	1B	7C	E3
5C	C4	82	0B

SubByte程序後



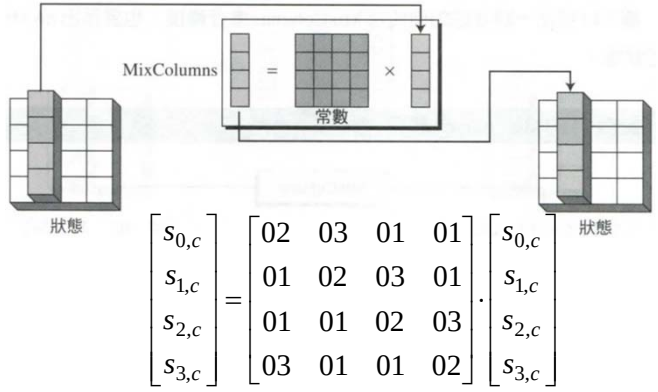
36	F7	27	AF
A3	98	A7	A3
7C	E3	E7	1B
0B	5C	C4	82

ShiftRows程序後

- 3.使用MixColumns計算值

36	F7	27	AF
A3	98	A7	A3
7C	E3	E7	1B
0B	5C	C4	82

ShiftRows程序後

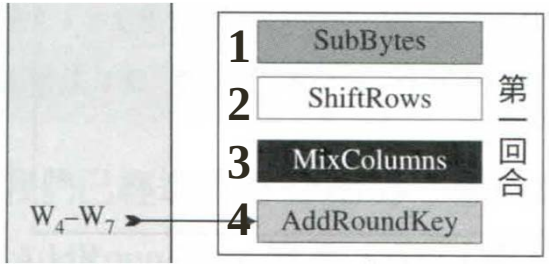


E5	F9	9F	22
E4	BE	84	5D
70	56	02	A7
93	C1	BA	4D

MixColumns程序後

AES範例

- 4. 最後加入回合金鑰(第一回合金鑰W_4-W_7)，且第一回合的密文輸出。



E5	F9	9F	22
E4	BE	84	5D
70	56	02	A7
93	C1	BA	4D

MixColumns程序後

⊕ (第一回合金鑰W_4-W_7)

回合	回合金鑰
1	89 BD 8C 9F 55 20 C2 68 B5 E3 F1 A5 CE 46 46 C1

輸出狀態
6C 44 13 BD
B1 9E 46 35
C5 B5 F3 02
5D 87 FC 8C

$$E5 \oplus 89 = 11100101 \oplus 10001001 = 01101100$$

$$56 \oplus E3 = 01010110 \oplus 11100011 = \underline{10110101}$$

B 5