AES 密碼標準

- 進階加密標準 (Advanced Encryption Standard, AES)
  - 美國 NIST 標準。
  - 採用 Rijndael 演算法 ：
    - 區塊長度：128, 192, 256 個位元。
    - 鑰匙長度：AES-128、AES-192、AES-256 密碼系統。
    - 編碼演算法：『反覆區段編碼』(Iterated Block Cipher, IBC)

AES 基本架構

- AES 演算法參數
  - 明文區段數目 (N_b)：32 bits 加密區段的數目。
  - 鑰匙區段數目 (N_k)：32 bits 鑰匙區段的數目。
  - 重覆次數 (N_r)：加密/解密編碼的次數。

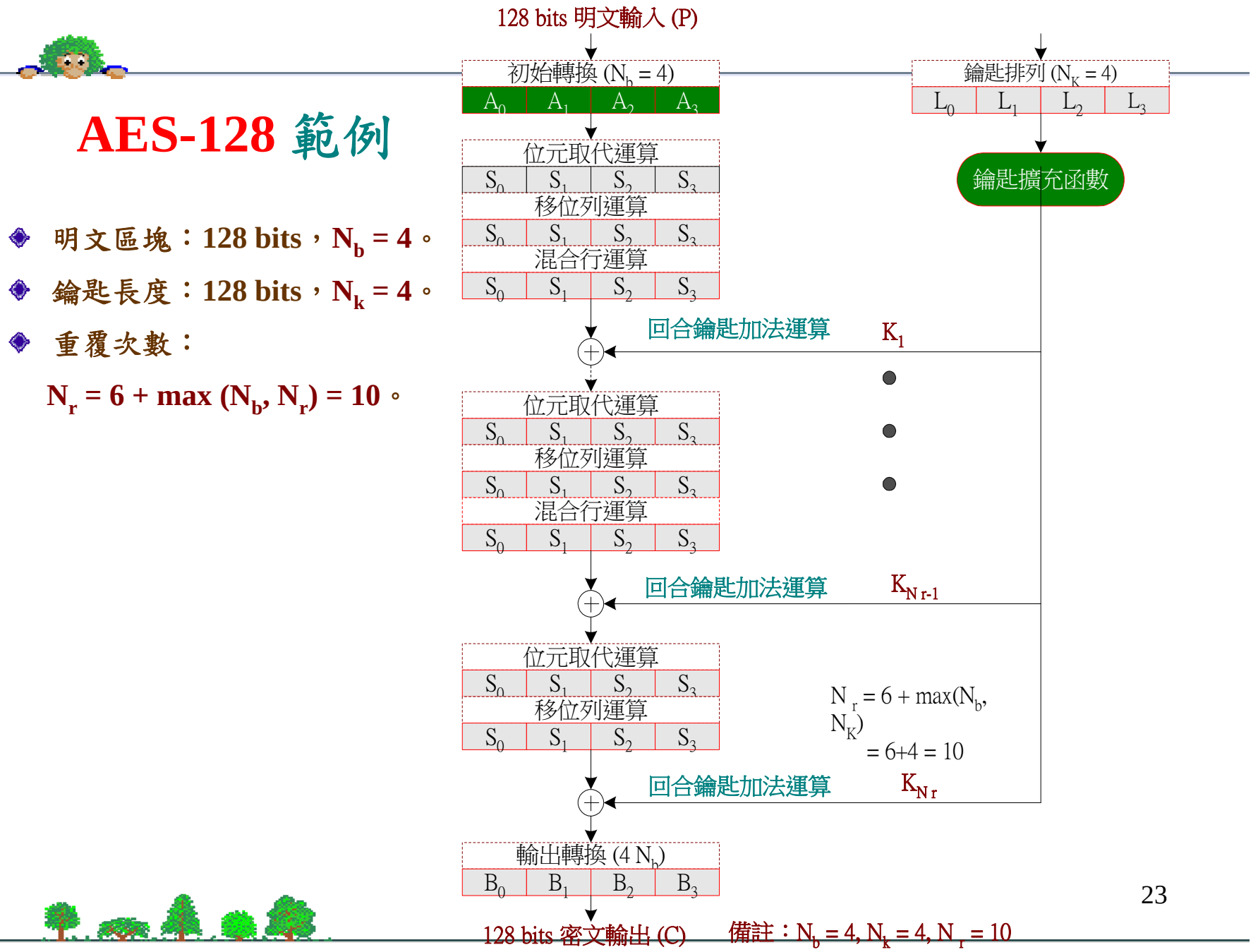
    $N_r = 6 + \max(N_b, N_r)$
  - 標準規範：
    - AES-128
    - AES-192
    - AES-256
    - 明文及密文長度：128 bits

- AES-128 範例 (1)
  - 明文區塊：128 bits，$N_b = 4$。
  - 鑰匙長度：128 bits，$N_k = 4$。
  - 重覆次數：$N_r = 6 + \max(N_b, N_r) = 10$。

AES-128 範例

- 明文區塊：128 bits，$N_b = 4$。
- 鑰匙長度：128 bits，$N_k = 4$。
- 重覆次數：

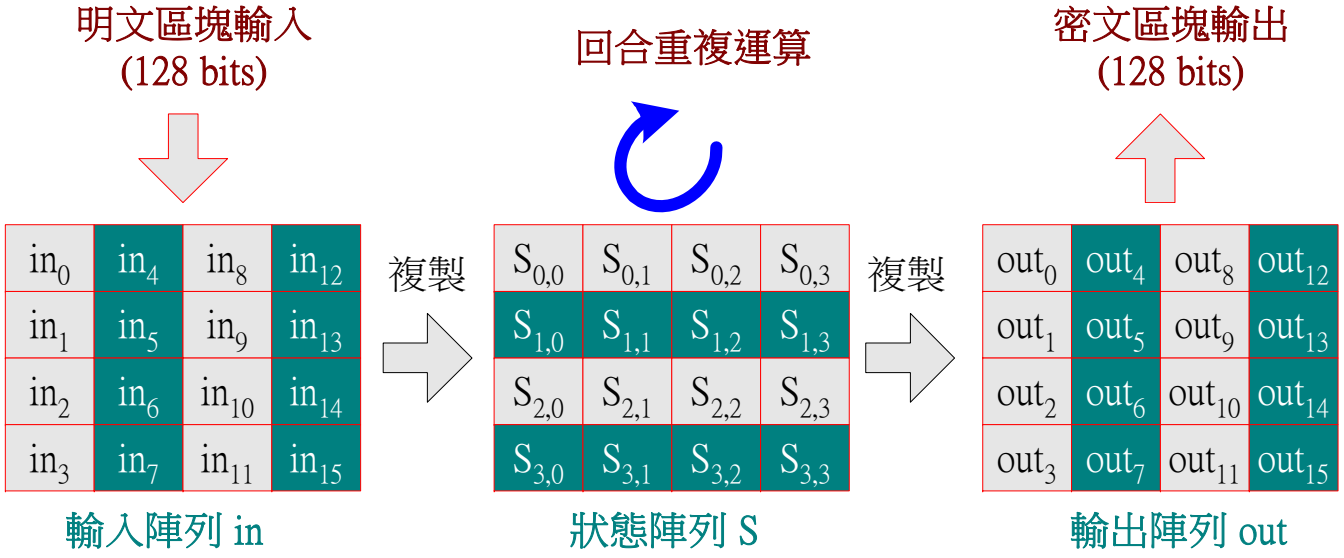
  $N_r = 6 + \max(N_b, N_r) = 10$。



AES基本元素

- 位元組(Byte)
- 位元組陣列(Array of Bytes)
- 狀態 (State)
- 行陣列狀態

- 運作程序
  - 每區段為 8 bits
  - 輸入陣列 in
  - 狀態陣列 (State) S
  - 輸出陣列 out



AES 數學基礎

- 『有限場』（Finite Field）運算
- 加法
- 乘法
- GF(2^8) 多項式係數

AES加密演算法

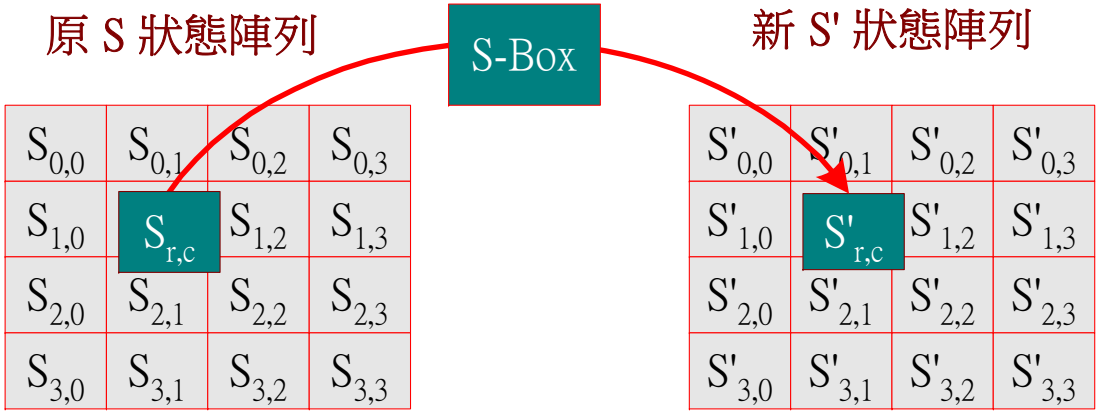
- **AES 加密編碼**
  - **回合鑰匙加法運算：AddRoundKey()**
  - **位元組取代：SubBytes()**
  - **列移位運算：ShiftRows()**
  - **混合行運算：MixColumns()**

```
Cipher (byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
/* in 為輸入陣列、out = 輸出陣列、w = 鑰匙字元陣列 */
Begin
Byte state[4, Nb]
/* 明文陣列複製到狀態陣列上 */
state = in
/* 第 0 回合編碼 */
AddRoundKey(state, w[0, Nb-1])
/* 第 1 到 Nr – 1 回合編碼 */
for round = 1 step 1 to Nr-1
SubBytes(state)
ShiftRows(state)
MixColumns(state)
AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
end for
/* 第 Nr 回合編碼 */
SubBytes(state)
ShiftRows(state)
AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
/* 密文陣列輸出 */
out = state
end
```

AES 位元組取代運算

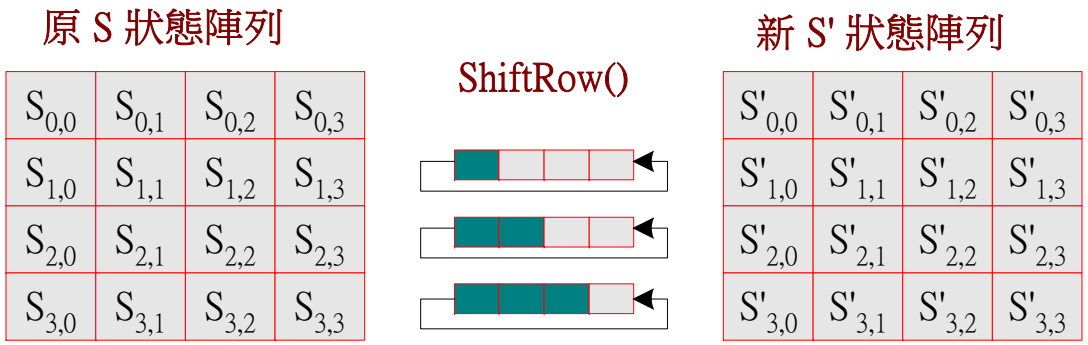
- **S-box 取代盒**
- **程式請參考書本**

$$\begin{bmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{bmatrix} = \begin{bmatrix} 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \\ 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$



AES 移位列運算

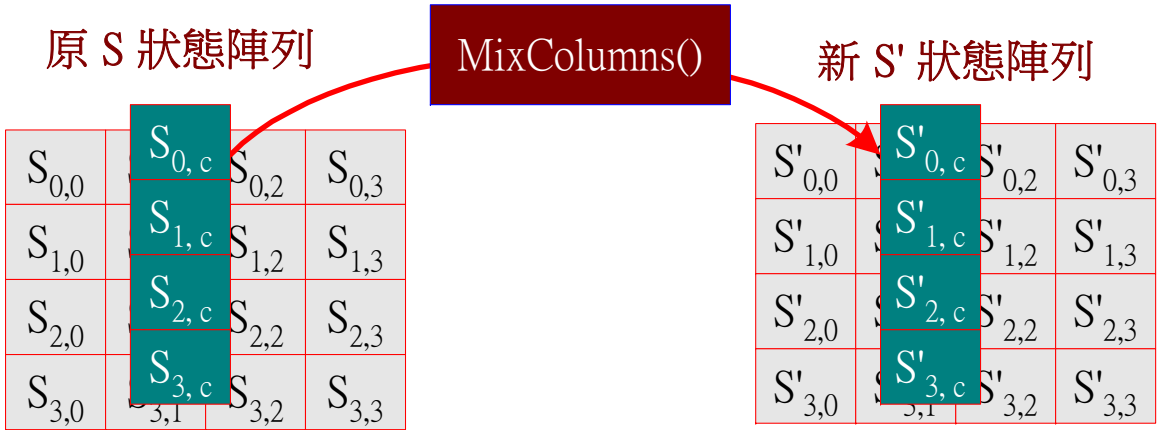
- 位移列運算 (Shift Row Operation)
- 程式解說請參考書本



AES 混合行運算

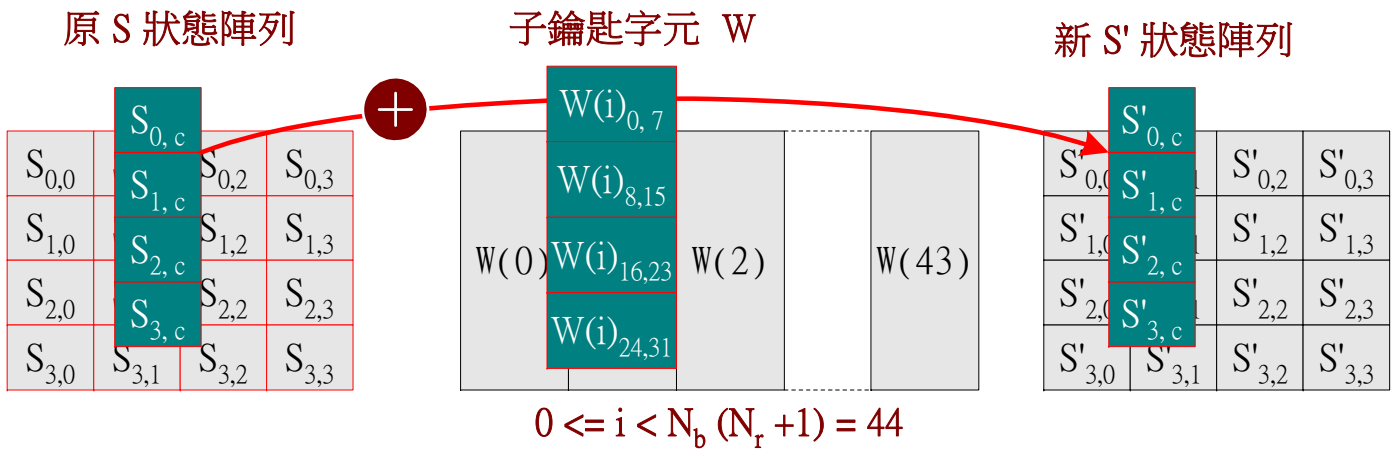
- 混合行運算 (Mix Column Operation)
  - 程式範例請參考書本
- **a(x) = {03}x^3 + (01)x^2 + {01}x +{02}**

$$\begin{bmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \times \begin{bmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{bmatrix}$$



AES 回合鑰匙加法運算

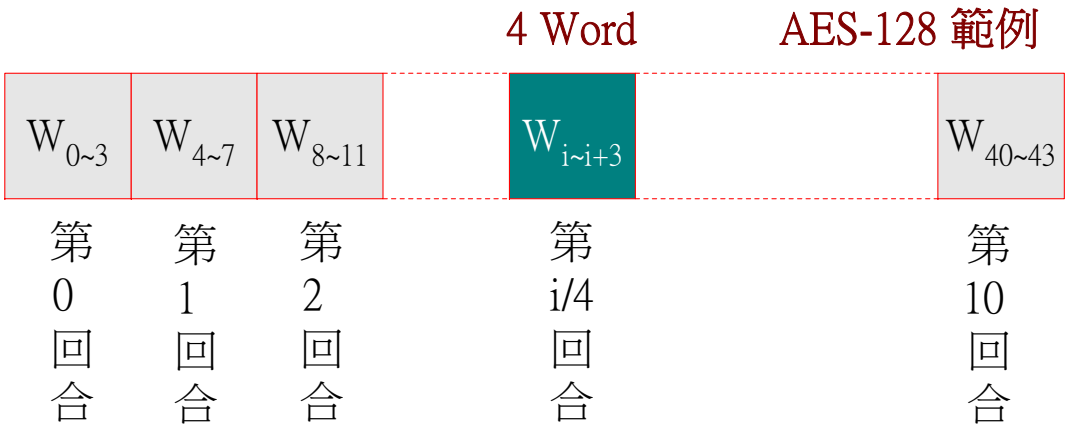
- 回合鑰匙加法 (Round Key Addition)
- 程式範例請參考書本



AES 鑰匙擴充

AES 鑰匙使用量

- 鑰匙字元單位：W[i], 32 bits
- 鑰匙字元數量：Nb * (Nr + 1)
- AES-128 需要：44 個鑰匙字元
- 每一回合使用 4 個字元



AES 鑰匙擴充

- 鑰匙擴充演算法
- 程式範例請參考書本

```
KeyExpansion(byte key[4*Nk], word w[Nb * (Nr+1)], Nk)
/* 主鑰匙輸入 key[]，子鑰匙字元輸出 w[]，鑰匙字元數量輸入 Nr */
/*Nk = 4（AES-128），Nk = 6（AES-192），Nk = 8（AES-256）*/
(1)begin
(2)   word temp
(3)   i = 0
(4)   while (i < Nk)   /*將主鑰匙填入鑰匙區塊，第 0 回合使用 */
(5)      w[i] = word(key[4*i], key[4*i + 1], key[4*i +2], key[4*i + 3])
(6)      i = i +1
(7)   end while
(8)  i = Nk
(9)  while (i < Nb * (Nr + 1))  /* 演算第 1 到 Nr 回合所需鑰匙 */
(10)      temp = w[i –1]
(11)      if (i mod Nk = 0)   /* 子鑰匙區塊週期的開始，如圖 3-18 所示 */
(19)                        temp = SubWord(RotWord(temp)) XOR Rcon[i/Nk]
(19)               else if (Nk > 6 and I mod Nk = 4)  /* 僅 AES-256 適用 */
(19)                        temp = SubWord(temp)
(19)               end if
(19)               w[I] = w[I – Nk] XOR temp
(19)               I = I +1
(18) End while
(19)end
```

AES 鑰匙擴充

- 演算法摘要