Feistel 密碼演算法 – 系統概念

Feistel 系統概念

- XOR(⊕)的的基本特性
- 0⊕0 = 0, 0⊕1 = 1, 1⊕0 = 1, 1⊕1 = 0,
- A⊕0 = A

Feistel 密碼演算法

Feistel 演算法

- 加密器輸入：M = {LEi || REi}
- 加密器輸出：
  - LEi+1 = REi
  - REi+1 = LEi⊕ F(Ki+1，REi)
  - C = {REi+1 || LEi+1}
- 解密器輸入：C = {LDi || RDi}

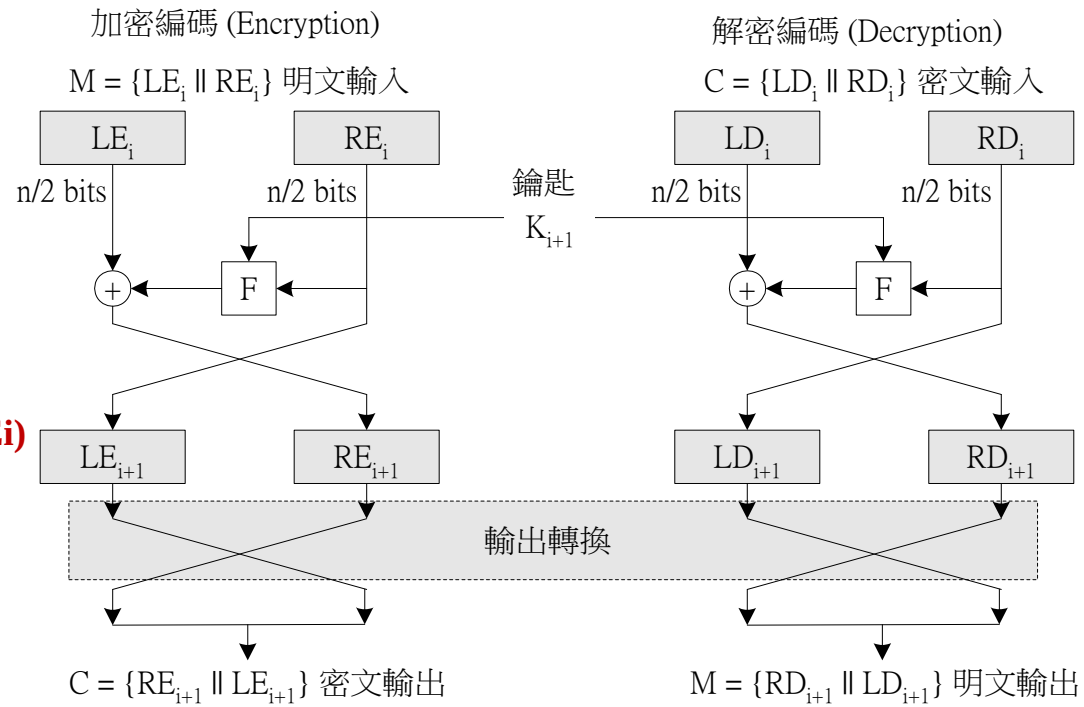
  LDi = REi+1 = LEi⊕ F(Ki+1，REi)

  RDi = LEi+1 = REi
- 解密器輸出：
  - LDi+1 = RDi

    = REi
  - RDi+1 = LDi⊕ F(Ki+1，RDi) = LDi⊕ F(Ki+1，REi)

    = LEi⊕ F(Ki+1，REi) ⊕ F(Ki+1，REi)

    = LEi ⊕ = LEi
  - M = {RDi+1 || LDi+1} = {LEi || REi}



Feistel 密碼演算法 – 範例

- 我們用一個範例來驗證 Feistel 架構是否可行。
- 假設 $M = \{4, 8\}$、$k_i = 6$、$F = \oplus$。則加密過程為：

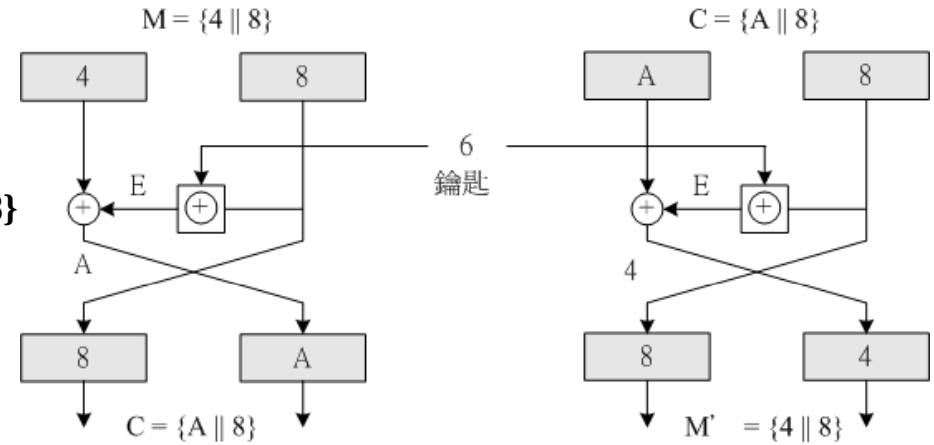
  $LE_i = 4$、$RE_i = 8$

  $RE_{i+1} = LE_i \oplus F(RE_i, K_i)$

  $=4 \oplus 8 \oplus 6 = A$

  $LE_{i+1} = RE_i = 8$

  則密文為：$C = \{RE_{i+1}, LE_{i+1}\} = \{A, 8\}$



- 解密過程為：

  $LD_i = A$、$RD_i = 8$

  $LD_{i+1} = RD_i = 8$

  $RD_{i+1} = LD_i \oplus F(RD_i, K_i)$

  $=A \oplus 8 \oplus 6 = 4$

  則明文為：$M = \{RD_{i+1}, LD_{i+1}\} = \{4, 8\}$

Feistel 密碼演算法 – 架構

Feistel 系統架構