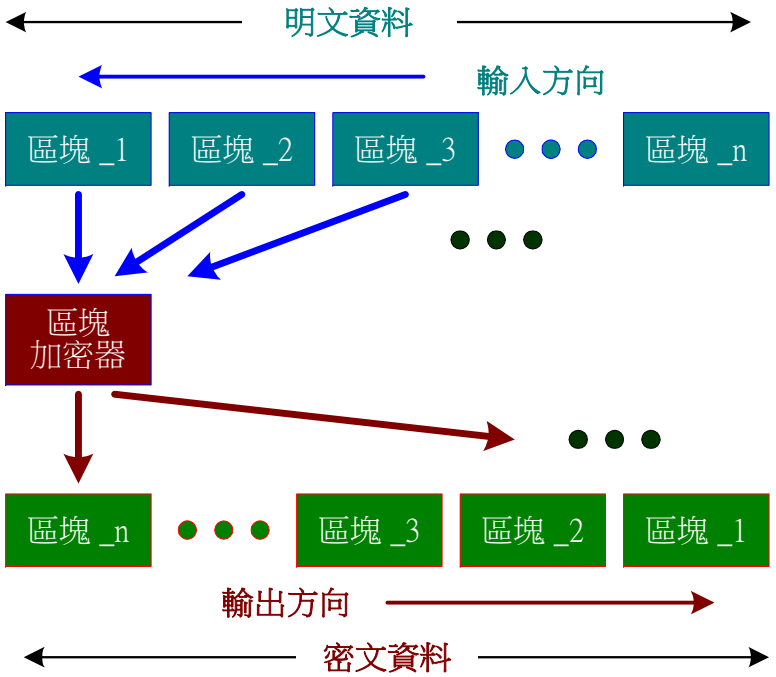
DES 操作模式

- 電子密碼書 (Electronic Code Book, ECB) 模式
- 密文區段串接 (Cipher Block Chaining, CBC) 模式
- k-位元密文反饋 (k-bits Cipher Feedback, CFB) 模式
- k-位元輸出反饋 (k-bits Output Feedback, OFB) 模式



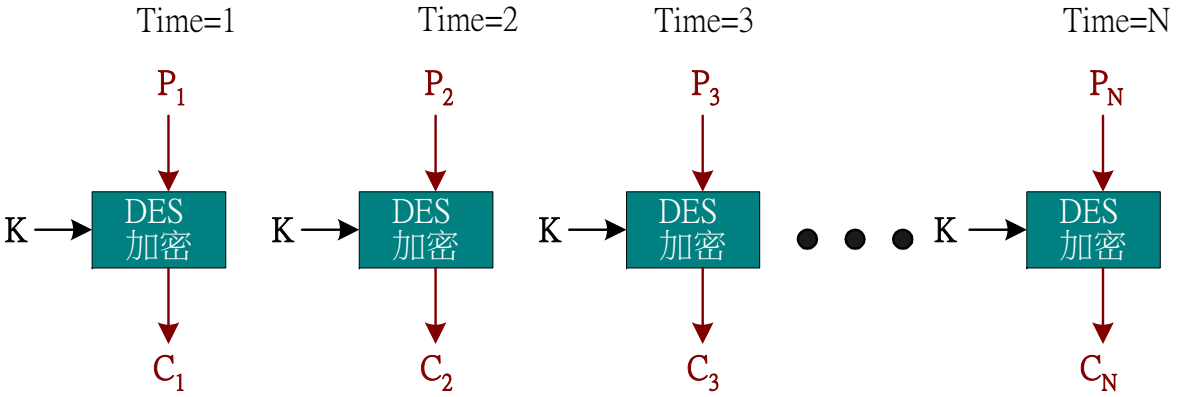
DES電子密碼書模式

電子密碼書模式 (ECB)

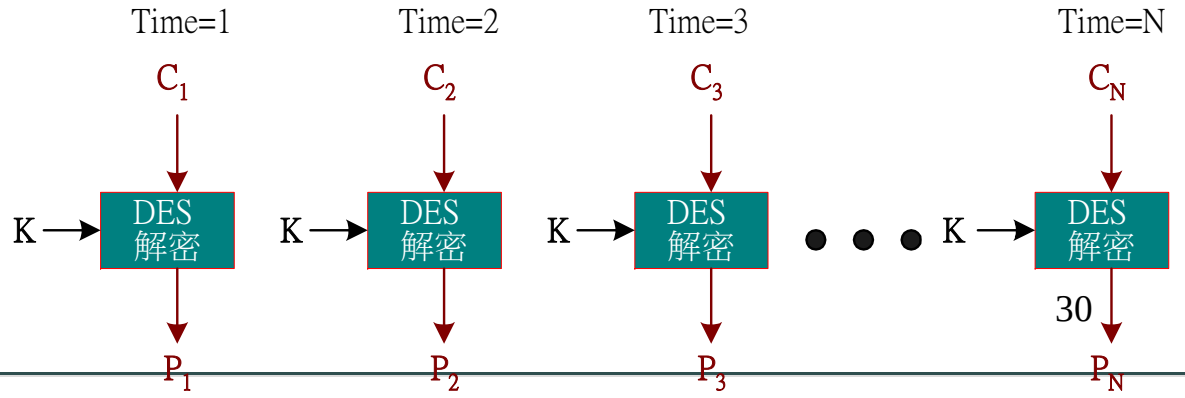
- 加密處理：
  - 明文：$P = P_1 \| P_2 \| P_3, \ldots, \| P_N$
  - 密文：$C = E_K(P) = E_K(P_1) \| E_K(P_2) \| E_K(P_3) \| \ldots \| E_K(P_N)$
- 容易遭受明文攻擊

- 解密處理：
  - 密文：$C = C_1 \| C_2 \| C_3, \ldots, \| C_N$
  - 明文：$P = E_K(C) = E_K(C_1) \| E_K(C_2) \|, \ldots, \|$

(a) ECB 加密操作 $C = E_K(P)$



(b) ECB 解密操作 $P = D_K(C)$



DES 密文區塊串接模式 (1)

密文區塊串接模式(Cipher Block Chaining , CBC)

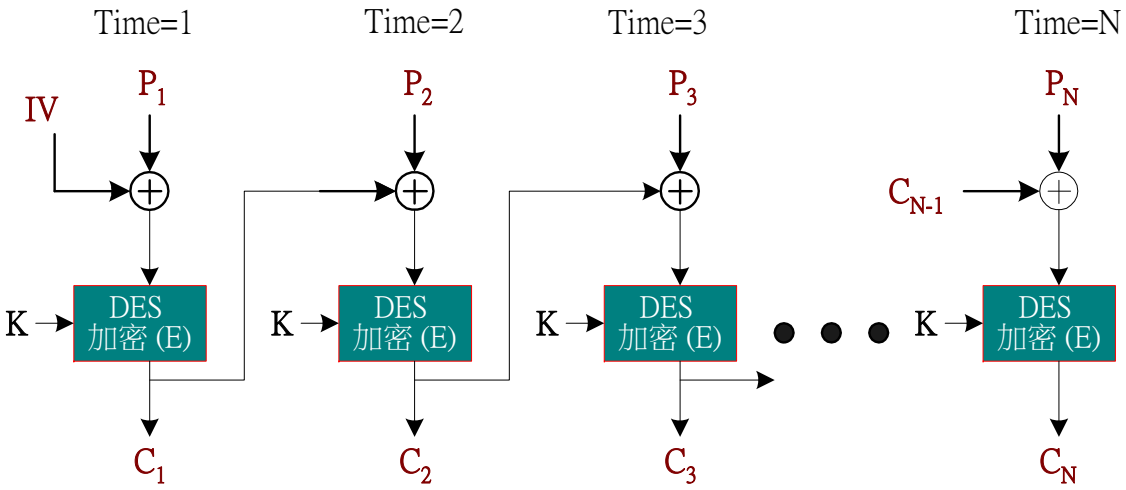
- 增加『初始向量』(Initialization Vector, IV)
- 加密程序：
  - $C_1 = E_K(IV \oplus P_N)$
  - $C_i = E_K(C_{i-1} \oplus P_i)$； $i = 2, 3, 4, \ldots N$
  - $C = C_1 \| C_2 \| C_3, \ldots, C_N$
- 解密程序：
  - $P1 = D_K(C_1) \oplus IV$
  - $Pi = D_K(C_i) \oplus C_{i-1}$ ； $i = 2, 3, 4, \ldots N$
  - $P = P_1 \| P_2 \| P_3, \ldots, P_N$
- 驗證：
  - $D_K(C_i) = D_K(E_K(C_{i-1} \oplus P_i))$； $i = 2, 3, 4, \ldots N$

    $= (C_{i-1} \oplus P_i)$
  - 則：$D_K(C_i) \oplus C_{i-1} = (C_{i-1} \oplus P_i) \oplus C_{i-1} = P_i$ 得證之。

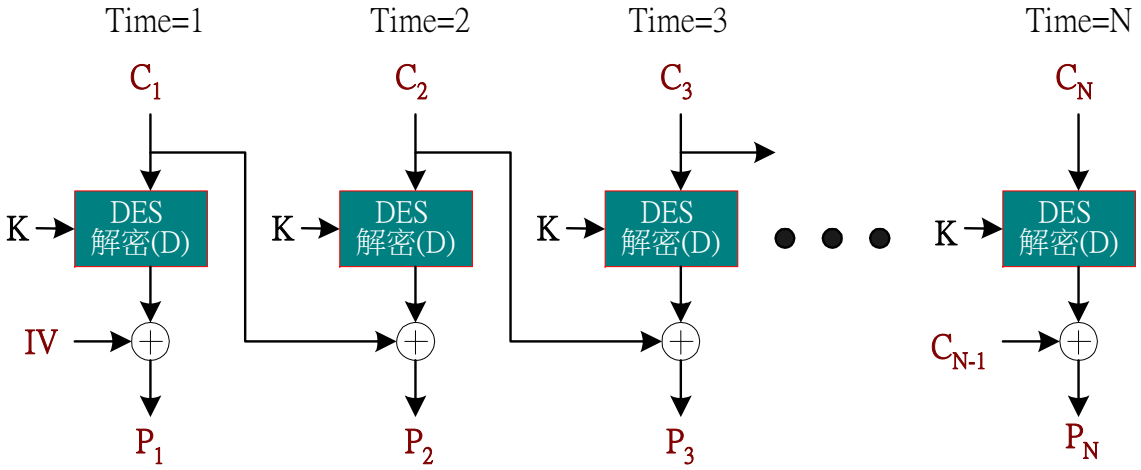
DES 密文區塊串接模式 (2)

- CBC 運作程序

(a) CBC 加密操作 $C = E_K(P)$



(b) CBC 解密操作 $P = D_K(C)$



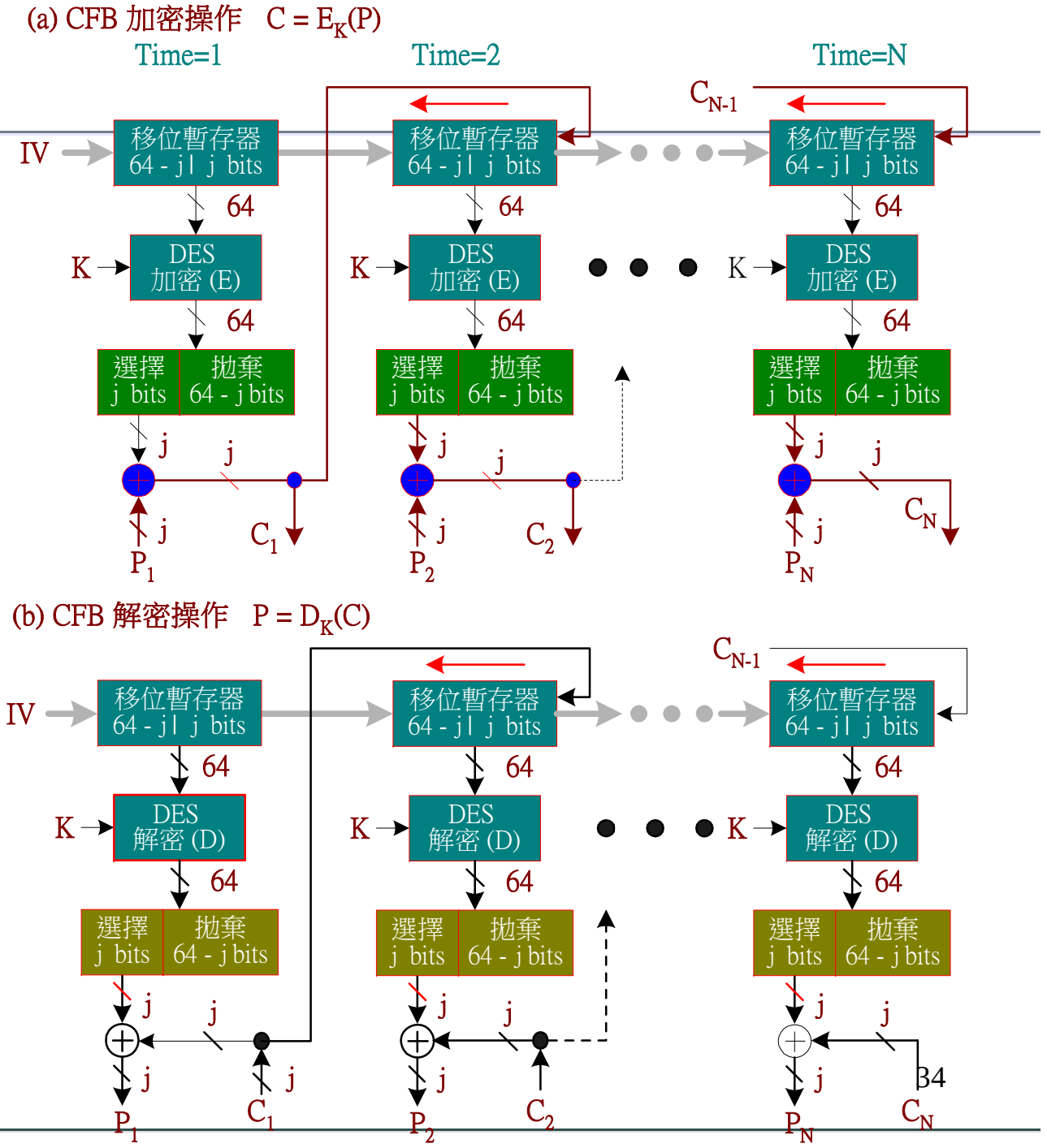
DES J-位元密文反饋模式(1)

J-位元密文反饋模式(J-bits Cipher Feedback , CFB)

- J 位元串流加密 (Stream Cipher)
- 加密運算程序：
  - $SR_1 = IV$
  - $C_1 = F_j\,(E_K(SR_1)) \oplus P_1$
  - $SR_m = S_j\,(SR_{m-1}) \,||\, C_{m-1}$ ； $m = 2, 3, 4, \ldots, N$
  - $C_m = F_j\,(E_K(SR_m)) \oplus P_m$ ； $m = 2, 3, 4, \ldots, N$
  - $C = C_1 \,||\, C_2 \,||\, C_3, \ldots, C_N$
- 解密運算程序：
  - $SR_1 = IV$
  - $P_1 = F_j\,(D_K(SR_1)) \oplus C_1$
  - $SR_m = S_j\,(SR_{m-1}) \,||\, C_{m-1}$ ； $m = 2, 3, 4, \ldots, N$
  - $P_m = F_j\,(D_K(SR_m)) \oplus C_m$ ； $m = 2, 3, 4, \ldots, N$
  - $P = P_1 \,||\, P_2 \,||\, P_3, \ldots, P_N$

DES J-位元密文反饋模式(2)

- CFB 運作程序



DES J-位元輸出反饋模式(1)

- **J-位元輸出反饋模式(J-bits Output Feedback, OFB)**
  - J-位元串流加密
  - 加密運算乘程序：
    - $SR_1 = IV$
    - $O_1 = F_j (E_K(SR_1))$
    - $C_1 = P_1 \oplus O_1$
    - $SR_m = S_j (SR_{m-1}) \| O_{m-1}$ ； $m = 2, 3, 4, \ldots, N$
    - $O_m = F_j (E_K(SR_m))$ ； $m = 2, 3, 4, \ldots, N$
    - $C_m = O_m \oplus P_m$ ； $m = 2, 3, 4, \ldots, N$
    - $C = C_1 \| C_2 \| C_3, \ldots, C_N$
  - 解密運算程序：
    - $SR_1 = IV$
    - $O_1 = F_j (D_K(SR_1))$
    - $P_1 = O_1 \oplus C_1$
    - $SR_m = S_j (SR_{m-1}) \| O_{m-1}$ ； $m = 2, 3, 4, \ldots, N$
    - $O_m = F_j (D_K(SR_m))$ ； $m = 2, 3, 4, \ldots, N$
    - $P_m = O_m \oplus C_m$ ； $m = 2, 3, 4, \ldots, N$
    - $P = P_1 \| P_2 \| P_3, \ldots, P_N$

DES J-位元輸出反饋模式(2)

- OFB 運作程序