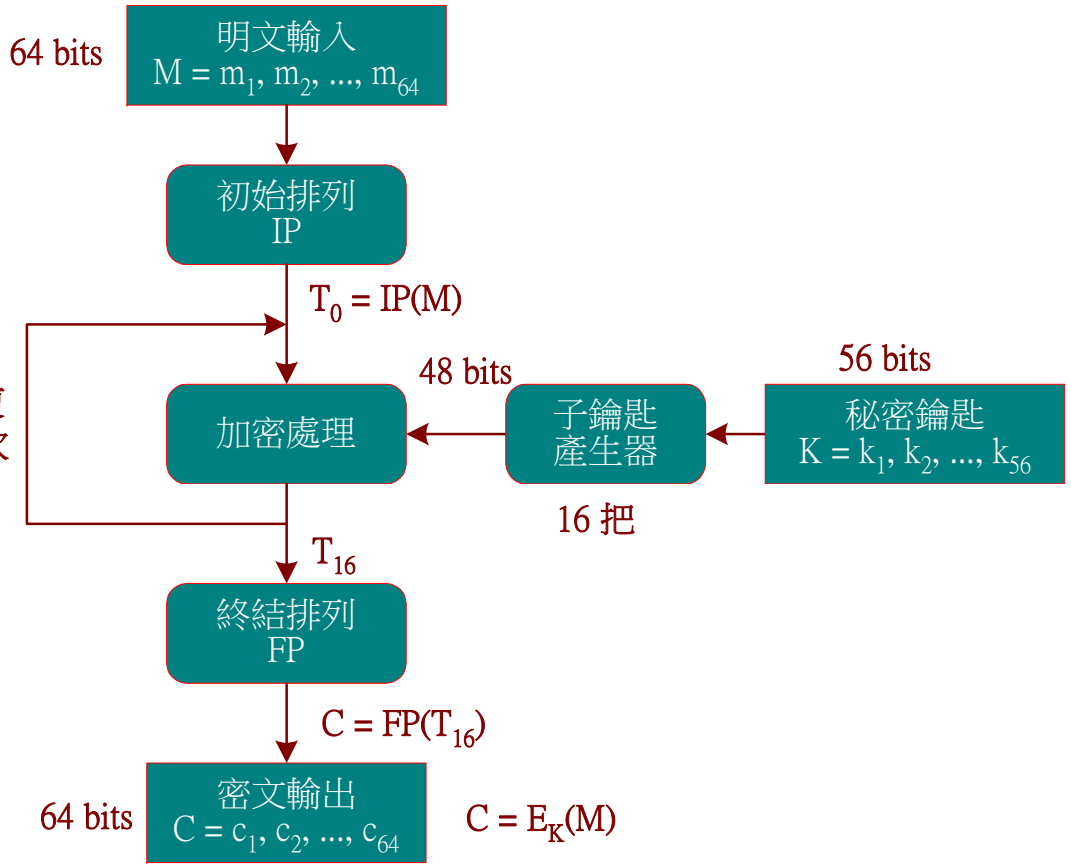
DES 密碼系統(1)

- **Data Encryption Standard (DES)**
  - 美國國家標準
  - 區塊長度：**64 bits**
  - 重複次數：**16** 次 **(**每次一支子鑰匙**)**
  - 母鑰匙長度：**56 bits**
  - 子鑰匙產生：**16** 把**/48 bits**
  - 演算法：加密/解密演算法相容

DES 演算法流程

DES 演算法流程

1. 明文資料分割
2. 初始變換 (Initial Permutation, IP)
3. 選擇子鑰匙，共有 16 把。
4. 加密處理
5. 重複加密處理 16 次，每次使用不同的子鑰匙。
6. 終結變換 (Final Permutation)



DES 初始與終結排列

- 初始與終結排列 (換位加密)

(a) 初始排列 (IP) 內容

T_0 輸出	明文區塊 M 輸入							
1- 8	58	50	42	34	26	18	10	2
9 - 16	60	52	44	36	28	20	12	4
17 - 24	62	54	46	38	30	22	14	6
25 - 32	64	56	48	40	32	24	16	8
33 - 40	57	49	41	33	25	17	9	1
41 - 48	59	51	43	35	27	19	11	3
49 - 56	61	53	45	37	29	21	13	5
57 - 64	63	55	47	39	31	23	15	7

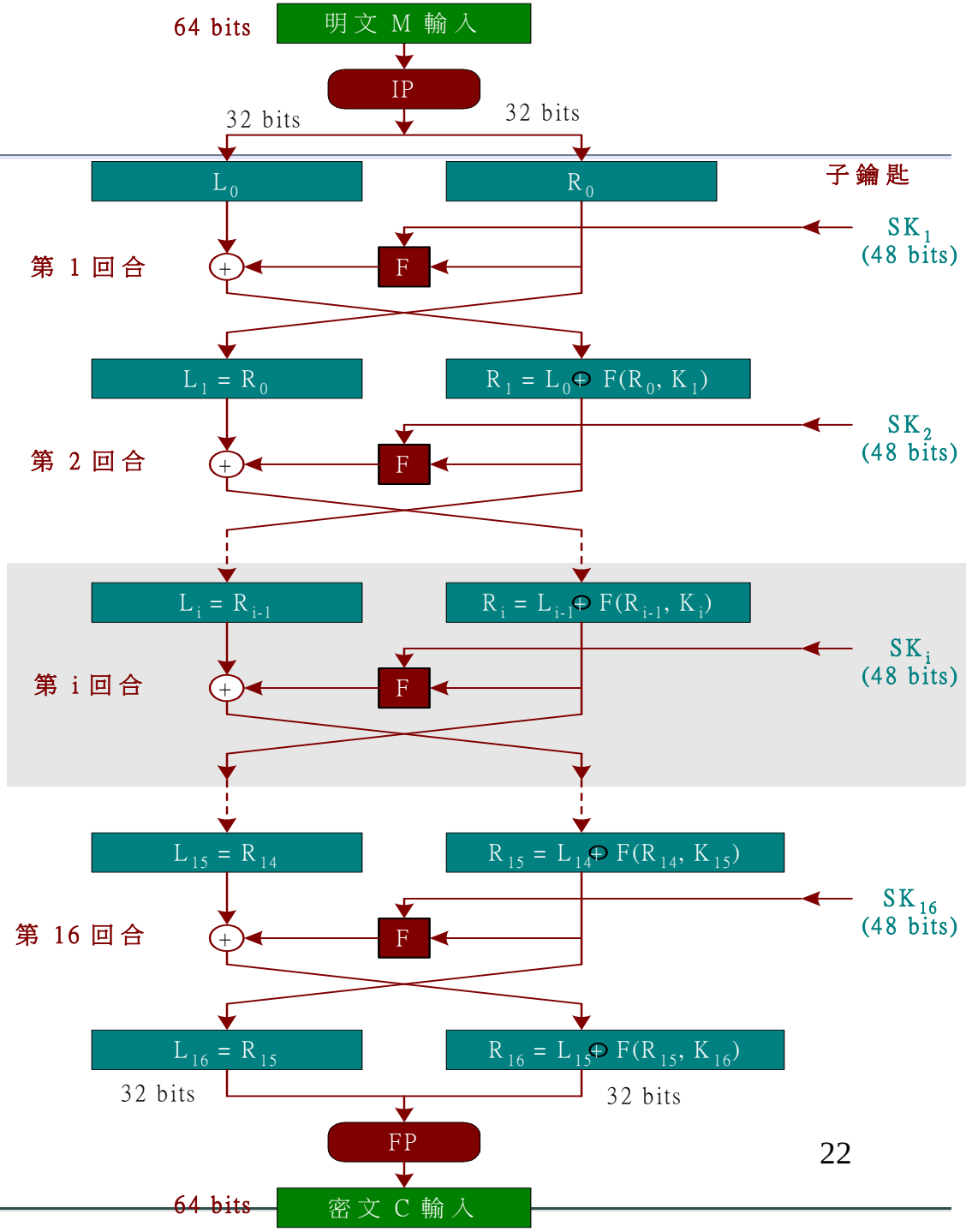
(b) 終結排列 (FP) 內容

密文 C 輸出	T_{16} 輸入							
1- 8	40	8	48	16	56	24	64	32
9 - 16	39	7	47	15	55	23	63	31
17 - 24	38	6	46	14	54	22	62	30
25 - 32	37	5	45	13	53	21	61	29
33 - 40	36	4	44	12	52	20	60	28
41 - 48	35	3	43	11	51	19	59	27
49 - 56	34	2	42	10	50	18	58	26
57 - 64	33	1	41	9	49	17	57	25

DES 系統架構

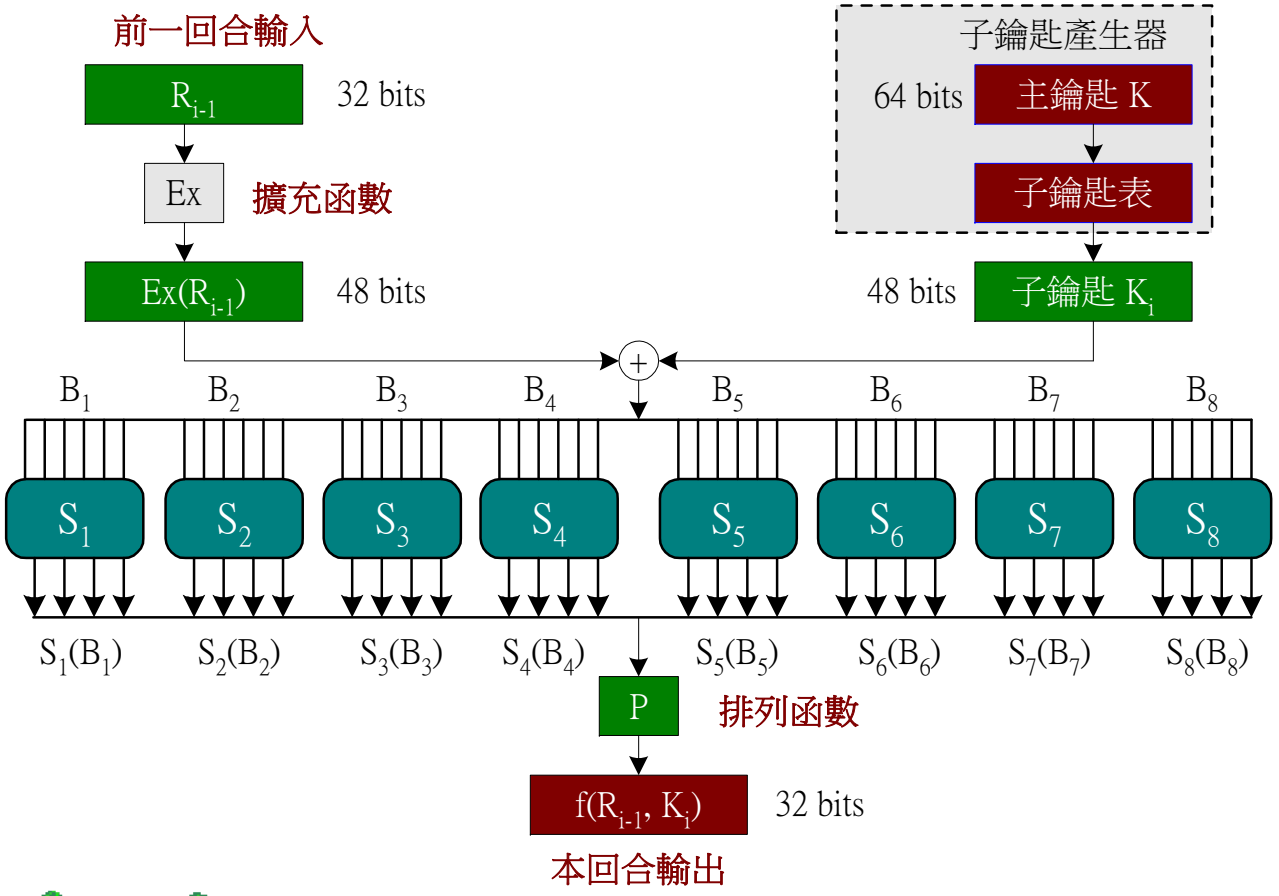
加密處理－演算步驟

- $T_0 = L_0 \| R_0$
- $L_1 = R_0$
- $R_1 = L_0 \oplus F(R_0, K_1)$
- $L_i = R_{i-1}$
- $R_i = L_i \oplus F(R_{i-1}, K_i)$



DES 加密處理 (2)

- 加密處理 (取代加密)
  - $F(R_{i-1}, K_i)$ 函數實現



DES 擴充函數與排列

加密處理

- **(C) Ex(Ri-1) 擴充函數**
- **(D) 排列函數 P**

$Ex(R_{i-1})$ 輸出	R_{i-1} 輸入					
1 - 6	32	1	2	3	4	5
7 - 12	4	5	6	7	8	9
13 - 18	8	9	10	11	12	13
19 - 24	12	13	14	15	16	17
25 - 30	16	17	18	19	20	21
31 - 36	20	21	22	23	24	25
37 - 42	24	25	26	27	28	29
43 - 48	28	29	30	31	32	1

$F(R_{i-1}, K_i)$ 輸出	S(B) 輸入			
1 - 4	16	7	20	21
5 - 8	29	12	28	17
9 - 12	1	15	23	26
13 - 16	5	18	31	10
17 - 20	2	8	24	14
21 - 24	32	27	3	9
24 - 28	19	13	30	6
29 - 32	22	11	4	25

DES S-Box

(E) S-Box 函數

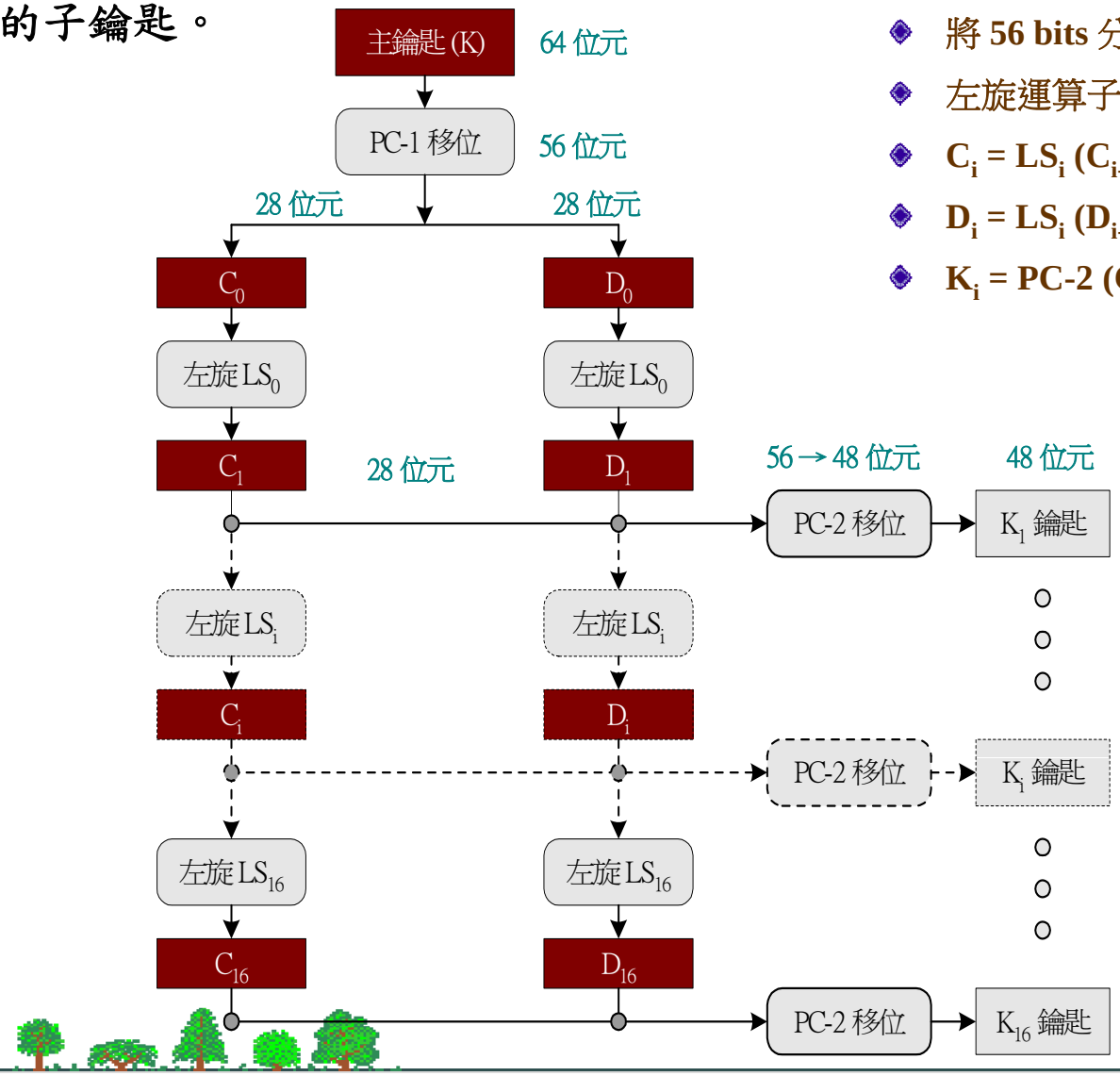
- 將 48 bits 的輸入壓縮為 32 bits 的輸出。
- $B = Ex(R_{i-1}) \oplus K_i$
- $B = B_1 \| B_2 \| \ldots \| B_8$

- $B_i = b_1, b_2, b_3, b_4, b_5, b_6$
- $S_i(B_i) = S_i^{\,b1b6}(b_2\, b_3\, b_4\, b_5)$

(b_1, b_6)	B 輸入，行 (b_1, b_2, b_3, b_4)															
	$b_1\, b_6$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

DES 子鑰匙產生

- 將 56 bits 的主鑰匙產生 16 把 48 bits 的子鑰匙。



- 產生方法：
  - 將 56 bits 分成兩組 28 bits (C_0 與 D_0)
  - 左旋運算子 (LS_i)
  - $C_i = LS_i (C_{i-1})$
  - $D_i = LS_i (D_{i-1})$
  - $K_i = PC\text{-}2 (C_i \| D_i)$； i = 1, 2, 3, …, 16。

DES 子鑰匙產生(2)

- 子鑰匙產生
  - (A) PC-1 移位轉換

56 bits

左區段輸出 C_0

28 bits

右區段輸出 D_0

28 bits

輸出	主鑰匙輸入 (64 bits)
1 - 7	57 49 41 33 25 17 9
8 - 14	1 58 50 42 34 26 18
15 - 21	10 2 59 51 43 35 27
22 - 28	19 11 3 60 52 44 36
1 - 7	63 55 47 39 31 23 15
8 - 14	7 62 54 46 38 30 32
15 - 21	14 6 61 53 45 37 29
22 - 28	21 13 5 28 20 12 4

  - (B) PC-2 移位轉換