表格 5.9: 初始排列表 (Initial Permutation, IP)

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

述：

1). 先將訊息明文以 8 個字母 (64 位元) 爲單位來個別做加密處理，將輸入的 64 位元訊息以表格 5.9 (IP) 之規則做排列重組。例如，重組後的第 2 位元將以將以原訊息中的第 50 位元來替代，重組後的第 20 位元將以將以原訊息中的第 38 位元來替代。重組之後再將其結果分成 L 及 R 二半，其中 L 及 R 各爲 32 位元。

2). 將 L 及 R 分別依下列之函數運算：

$$\begin{aligned} L_j &= R_{j-1} \\ R_j &= L_{j-1} \oplus f(R_{j-1}, K_j) \end{aligned}$$

其中 $j = 1, 2, \cdots, 16$，符號 $\oplus$ 爲互斥或 (Exclusive-or) 運算，K_j 爲 48 位元的第 j 回合金鑰。

3). $f(R_{j-1}, K_j)$ 函數之運算過程可參考圖 5.5 ，說明如下：

(a) 先將 32 位元 R_{j-1} 做位元擴充，使 32 位元得以擴充到 48 位元，其擴充的規則如表格 5.10 (EP) 所示。

(b) 將此擴充後的 48 位元資料與 48 位元的回合金鑰 K_j 做互斥或運算。

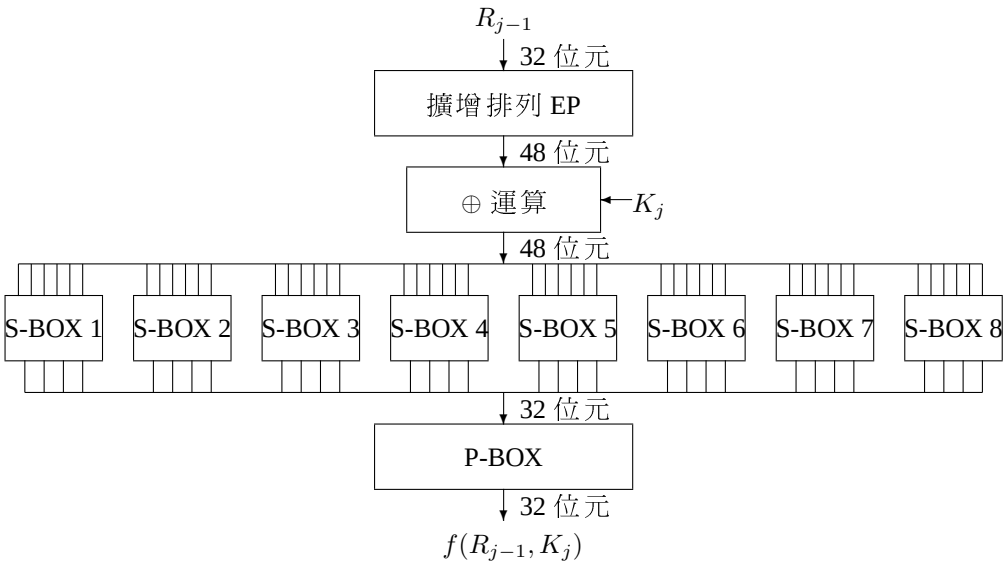

圖 5.5: DES 之 $f(R_{j-1}, K_j)$ 函數運算過程

表格 5.10: 擴增排列表 (Expansion Permutation, EP)

32	1	2	3	4	5	4	5	6	7	8	9
8	9	10	11	12	13	12	13	14	15	16	17
16	17	18	19	20	21	20	21	22	23	24	25
24	25	26	27	28	29	28	29	30	31	32	1

(c) 將做完互斥或運算的 48 位元資料分成 8 個區塊 (S-BOX)，每個 S-BOX 內有 6 位元，分別爲 b_1、b_2、b_3、b_4、b_5、b_6。

(d) 將每個 S-BOX 內的 6 位元資料，依表格 5.11 及 5.12 的規則轉換，每一個 S-BOX 都有一個專屬的轉換規則，經轉換後會產生 4 位元的輸出結果。表格 5.11 及 5.12 的使用方法如下：

i. 將每個 S-BOX 內的 b_1 及 b_6 位元取出，當成是該 S-BOX 的列索引值。

ii. 將每個 S-BOX 內的 b_2、b_3、b_4 及 b_5 位元取出，當成是該 S-BOX 的行索引值。

iii. 利用這行與列的索引值到所屬的 S-BOX 中找出所對應的值。

iv. 將所找到的對應值，轉換成 2 進位表示法後，取代原來 S-BOX 內的 6 位元值。

我們以一例子來作說明，假設原來 S-BOX5 內的值爲 (101011)，取出其前後兩個位元當作是列索引值，中間 4 個位元當作是行索引值，所以其列索引爲 $(11) = 3$，行索引爲 $(0101) = 5$，根據表格 5.12 ，S-BOX5 中列索引爲 3 行索引爲 5 所對應到的值爲 14，轉換成二進位後爲 (1110)，(1110) 就是 S-BOX5 對輸入資料 (110101) 的轉換結果。

(e) 將每個 S-BOX 所輸出的四個位元合併後，共計有 32 位元的輸出，再將此 32 位元的輸出經表格 5.13 (P-BOX) 之重新排列後，即完成一個 $f(R_{j-1}, K_j)$ 函數之運算。

4). 將步驟 2 重復執行 16 次後，再將最後的 R_{16} 及 L_{16}，合併成一 64 位元的輸出。最後將此 64 位元資料依表格 5.14 (IP^{-1}) 做最後的排列重組，所得之結果即爲密文。