

## 進階程式設計課程 程式作業#1

(請使用 C 或 C++ 語言撰寫解決下列問題之程式)

## S-BOX

DES 是一套對稱式加解密系統，其中有一個環節是將輸入的 6 位元資料  $b_1b_2b_3b_4b_5b_6$  透過 S-BOX 轉換成 4 位元資料  $x_1x_2x_3x_4$ ，其轉換方法會用到以下 S-BOX 轉換表，步驟如下：

1. 取  $b_1b_6$  之十進位值為列座標值  $r$ ，也就是  $(b_1b_6)_2 = (r)_{10}$ ，取  $b_2b_3b_4b_5$  之十進位值為行座標值  $c$ ，也就是  $(b_2b_3b_4b_5)_2 = (c)_{10}$ 。

2. 到 S-BOX 轉換表中查詢第  $r$  列的第  $c$  行的值並以二進位 4 位元方式輸出。

行 列	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
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-BOX 轉換表

因為在 S-BOX 轉換表中的值均介於 0 至 15 之間，所以只要用 4 位元便可以表示，例如輸入的資料  $(b_1b_2b_3b_4b_5b_6)_2 = (011001)_2$ ，則  $(b_1b_6)_2 = (01)_2 = (1)_{10}$  且  $(b_2b_3b_4b_5)_2 = (1100)_2 = (12)_{10}$ ，而 S-BOX 轉換表中的第 1 列的第 12 行的值為 9，所以  $(9)_{10} = (1001)_2$  因此輸出的結果為  $x_1x_2x_3x_4 = 1001$ 。

輸入說明：

每一列有一 6 位元資料串

輸出說明：

輸出經 S-BOX 轉換後之 4 位元資料串。

範例輸入：

011001

110011

範例輸出：

1001

1011