IP : 1000 0011

FP : 10010110 ⊗ K = 1001 0110 × 0010 0001

1011 0111

S0 S1

11 01 01 11

r3 c1 r1 c3

1 3

00100001 01 11 with P4

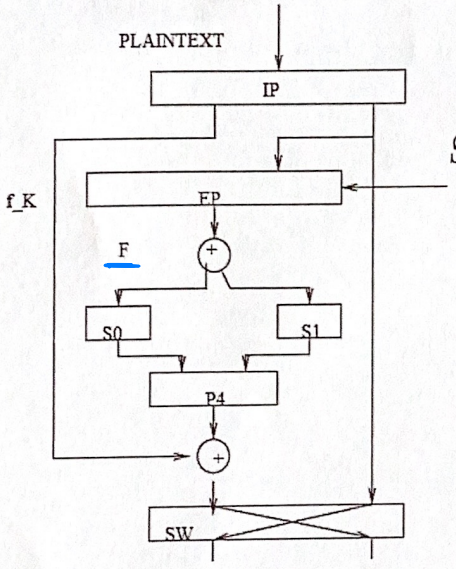
0100 1010

Q1

Given a block $(4A)_{16}$ in simple DES and a key k1 $(21)_{16}$ Find the cipher text for next round(simple iteration)(8 Marks)

$$IP:\begin{pmatrix}2&6&3&1&4&8&5&7\\1&2&3&4&5&6&7&8\end{pmatrix}$$

$$EP\ \begin{pmatrix}4&1&2&3&2&3&4&1\\1&2&3&4&5&6&7&8\end{pmatrix}$$



$$S0=\begin{bmatrix}1&0&3&2\\3&2&1&0\\0&2&1&3\\3&1&3&2\end{bmatrix}\qquad S1=\begin{bmatrix}0&1&2&3\\2&0&1&3\\3&0&1&0\\2&1&0&3\end{bmatrix}$$

P4

$$\begin{pmatrix}2&4&3&1\\1&2&3&4\end{pmatrix}$$

0111

1110 → ⊛ 2

1110
1000
0110 → 6

LR
63

then Switch
36

Q2: Summarize in your language the story of the whole DES

key generation

⇒ make them in binary

1 initial permutation

then we take this output and split to left - right

2 right with Exp to get 8bit the XOR with the key

3 left

5 then keys split to S0 S1 and take 03 12 see the number and enter the matrix for row coulum

then use those numbers to

Key generation

Encryption :

1. make the numbers from hex to binary

2. then number with Intial permutation

3. then take the R with the EP

4. then XOR it the the Key

5. the split them to be S0 S1

and the 0 1 2 3 (row) (colum)

From the matrix

S0 = 2 then S1 = R

turn back to binary

then do XOR with the left from the number

this number will be on left

L R

from

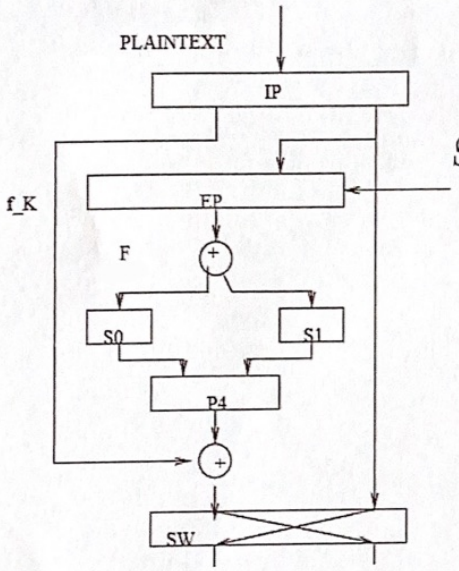
orginal number.

Q1

Given a block $(4A)_{16}$ in simple DES and a key k1 $(21)_{16}$ Find the cipher text for next round(simple iteration)(8 Marks)

$$IP: \begin{pmatrix} 2 & 6 & 3 & 1 & 4 & 8 & 5 & 7 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

$$EP \begin{pmatrix} 4 & 1 & 2 & 3 & 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$



$$S0 = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \quad S1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$$

P4

$$\begin{pmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$