Quiz 6

Q.1 What is key 2?

key = 1010000010

P10 = 3, 5, 2, 7, 4, 10, 1, 9, 8, 6

P8 = 6, 3, 7, 4, 8, 5, 10, 9

$\overset{1\,2\,3\,4\,5\,6\,7\,8\,9\,10}{1010000010}$

$\downarrow$ P10

$\underbrace{10000}\underbrace{01100}$

$\downarrow$ LS1

$\overset{1\,2\,3\,4\,5}{00001}\ \overset{6\,7\,8\,9\,10}{11000}$

$\downarrow$ P8

$\boxed{1010\ 0100}$ key1

$\downarrow$ LS2

$\overset{1\,2\,3\,4\,5}{00100}\ \overset{6\,7\,8\,9\,10}{00011}$

$\downarrow$ P8

$\boxed{0100\ 0011}$ key 2

Q.2 What is the output of the first round after the SW?

Plaintext = 10111101

IP = 2, 6, 3, 1, 4, 8, 5, 7

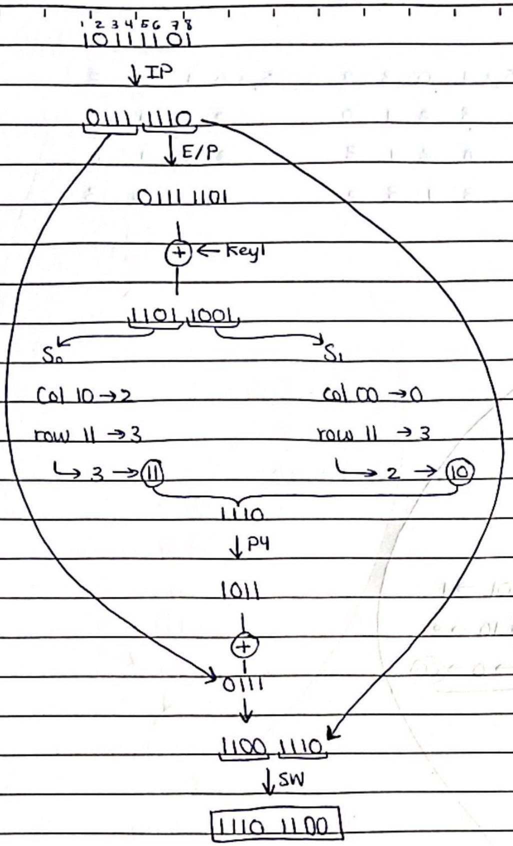
E/P = 4, 1, 2, 3, 2, 3, 4, 1

P4 = 2, 4, 3, 1

Key1 = 10100100 key2 = 0100 0011

$$S_0 = \begin{matrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{matrix}$$

$$S_1 = \begin{matrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{matrix}$$



Q.3 What is the IP^{-1} of IP = 3,4,1,2,5,6,7,8

1	2	3	4	5	6	7	8
3	4	1	2	5	6	7	8

1	2	3	4	5	6	7	8	
3	4	1	2	5	6	7	8	← IP^{-1}

Q.4 What is the ciphertext?

Round ① Text = 11101100

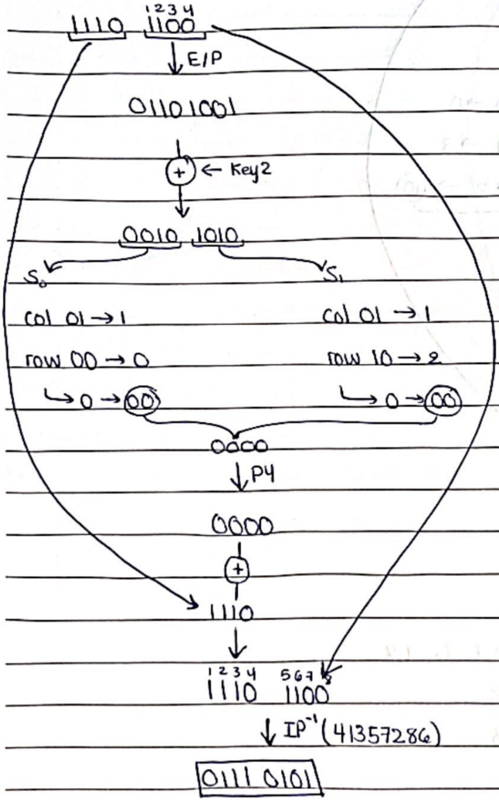
IP = 26314857

E/P = 41232341

P4 = 2,4,3,1

Key 2 = 01000011

$$S_0 = \begin{matrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{matrix} \qquad S_1 = \begin{matrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{matrix}$$



1110 1100
1234
E/P
01101001
← Key2
0010 1010
S_0
S_1
col 01 → 1
row 00 → 0
↳ 0 → 00
col 01 → 1
row 10 → 2
↳ 0 → 00
0000
P4
0000
1110
1234 5678
1110 1100
IP⁻¹(41357286)
0111 0101