Question

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

P8 = 6 3 7 4 8 5 10 9

IP = 2 6 3 1 4 8 5 7

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

EP = 4 1 2 3 2 3 4 1

S_0 =

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S_1 =

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

P4 = 2 4 3 1

plain text = 0010 1000 key = 11000 11110

find the cipher text.

Step 1: key Generation

$K_1 = P8 \circ shift \circ P10 \circ key$

$K_2 = P8 \circ shift^3 \circ P10 \circ key$

	1	2	3	4	5	6	7	8	9	10
key =	1	1	0	0	0	1	1	1	1	0

↓ P10

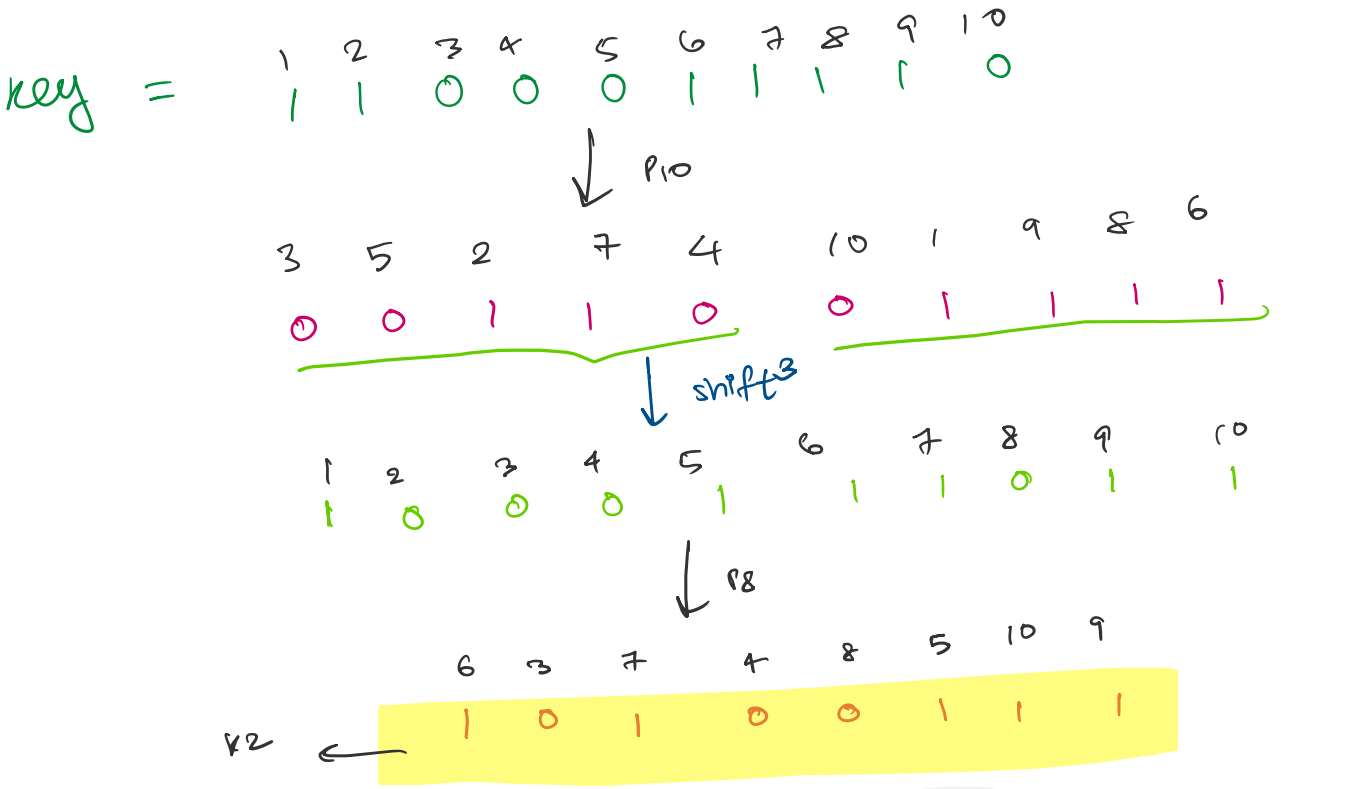
	3	5	2	7	4	10	1	9	8	6
	0	0	1	1	0	0	1	1	1	1

shift → circular left shift of 2 halves separately

	1	2	3	4	5	6	7	8	9	10
	0	1	1	0	0	1	1	1	1	0

↓ P8

	6	3	7	4	8	5	10	9
K_1 ←	1	1	1	0	1	0	0	1



Step 2 : cipher text generation

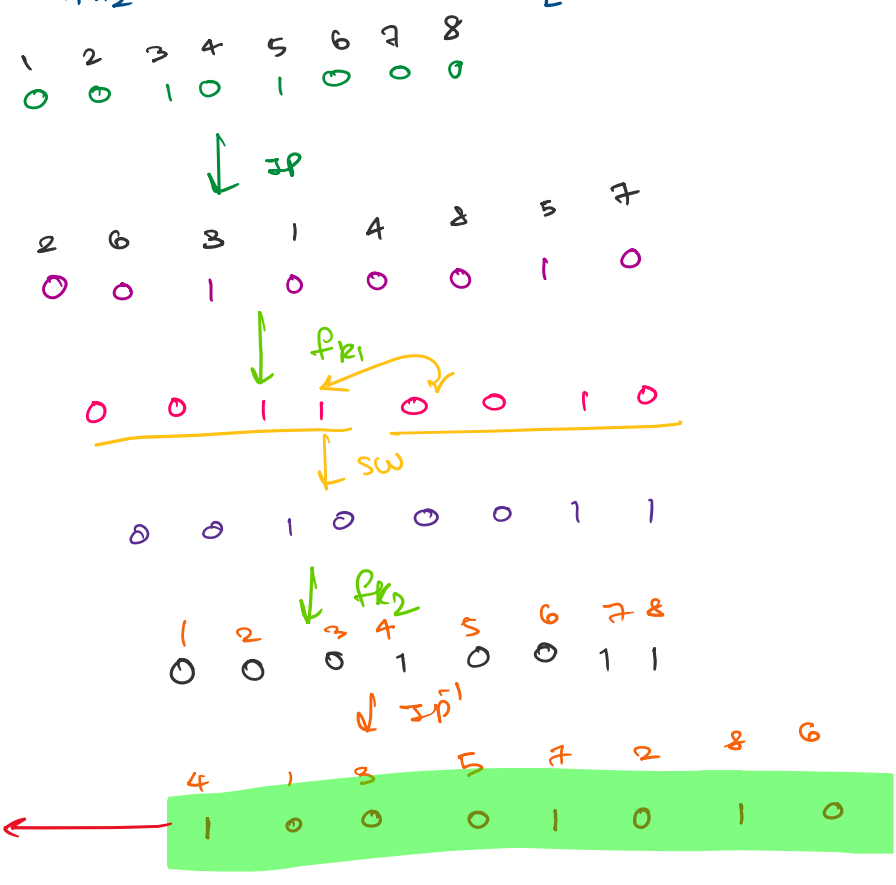
switching

$cipher = IP^{-1} \circ f_{K_2} \circ SW \circ f_{K_1} \circ IP\ (plain)$

$f_K(L, R) = [L \oplus F(R, K)]\ [R]$ — left & right half; R retained as such

$F(R, K) = P4 \circ S\text{-box} \circ XOR_K \circ EP(R)$

$cipher = IP^{-1} \circ f_{K_2} \circ SW \circ f_{K_1} \circ IP\ [0010\ 1000]$



f_{K1} (0010 0010)

L R

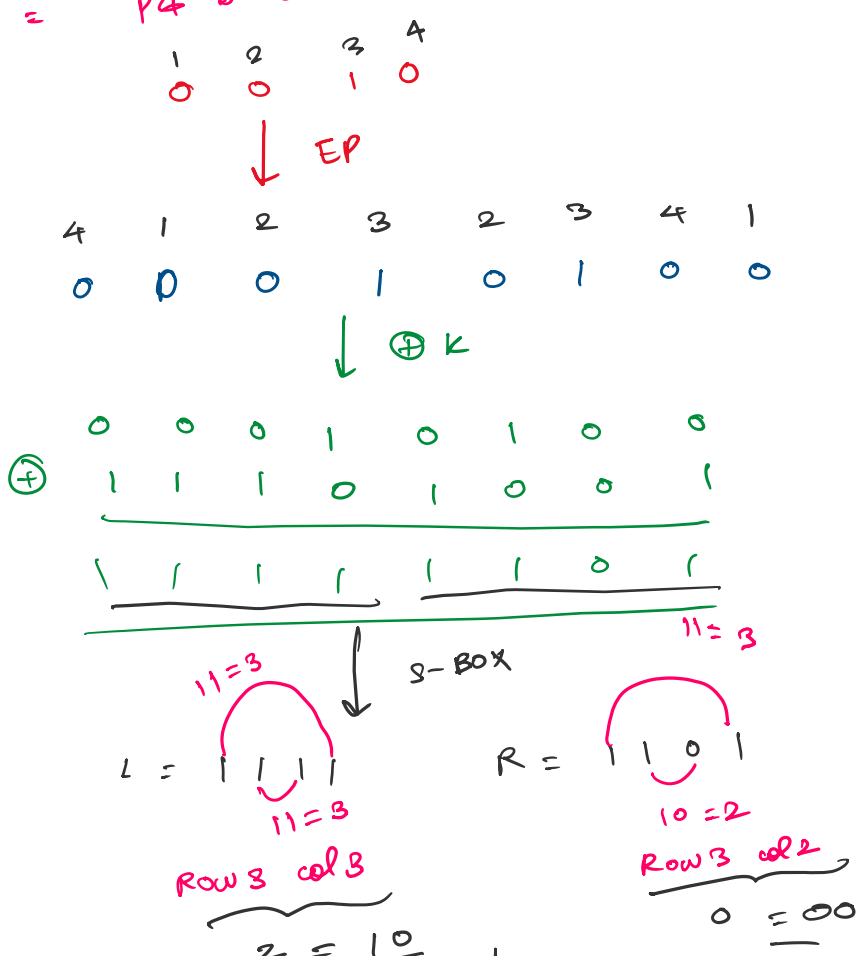
K1 = 1110 1001

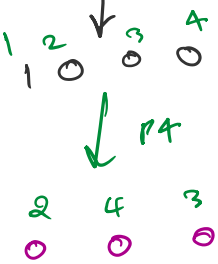
f = [L ⊕ F(R, K1)][R]

R K

F(0010, 1110 1001)

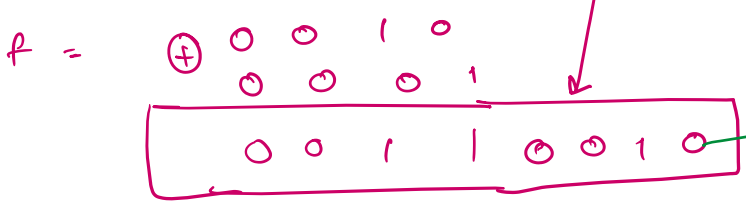
F(R, K) = P4 . sbox . XORK . EP (R)





2 4 3 1
0 0 0 1 => F output

f = [L ⊕ F][R]



→ output of f_{K1}

$f_{k_2}(00\ 10\ 00\ 11)$ (L = 00 10, R = 00 11) $k_2 = 1\ 0\ 1\ 0\ 0\ 1\ 1\ 1$

$f_{k_2}(L, R) = [L \oplus F(R, k_2)][R]$

$F(R, k_2) =$ P4 · S-box · XOR k_2 · EP (R)