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

$$S0 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ 3 & 3 & 1 & 3 & 2 \end{array} \qquad S_1 = \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 3 \end{array}$$

P4 = 2 4 3 1

plain text = 0010 1000   key = 11000 11110

find the cipher text.

step1 : key Generation

K1 = P8 ∘ shift ∘ P10 ∘ key

K2 = P8 ∘ shift^3 ∘ P10 ∘ 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
K1 ←	1	1	1	0	1	0	0	1

key =

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

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

↓ P8

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

K2 ←

step 2 : cipher text generation

switching

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

$$f_K(\underbrace{L, R}_{\text{left \& right half}}) = \underbrace{[L \oplus F(R, K)]}\ \underbrace{[R]}_{\text{retained as such}}$$

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

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

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

↓ IP

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

↓ fk1

0 0 1 1 | 0 0 1 0

↓ SW

0 0 1 0 0 0 1 1

↓ fk2

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

↓ IP^{-1}

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

(CIPHER TEXT) ←

$fk_1(\underbrace{0010}_{L}\ \underbrace{0010}_{R})$ $K1 = 1110\ 1001$

$f = [L \oplus \underline{F(R, k_1)}][R]$

$F(\overbrace{0010}^{R},\ \overbrace{1110\ 1001}^{K})$

$F(R, K) = P4 \circ sbox \circ XOR_K \circ EP(R)$

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 0 \end{array}$$

$\downarrow$ EP

$$\begin{array}{cccccccc} 4 & 1 & 2 & 3 & 2 & 3 & 4 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{array}$$

$\downarrow \oplus K$

$$\begin{array}{ccccccccc} & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ \oplus & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ \hline & \underline{1} & \underline{1} & \underline{1} & \underline{1} & \underline{1} & \underline{1} & \underline{0} & \underline{1} \end{array}$$

$\downarrow$ S-BOX

$11 = 3$ $11 = 3$

$L = 1111$ $R = 1101$

$11 = 3$ $10 = 2$

Row 3 col 3 Row 3 col 2

$2 = \underline{10}$ $0 = \underline{00}$

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 1 & 0 & 0 & 0 \end{array}$$

$\downarrow$ P4

$$\begin{array}{cccc} 2 & 4 & 3 & 1 \\ 0 & 0 & 0 & 1 \end{array}$$ $\Rightarrow$ F output

$f = [L \oplus F][R]$

$$f = \begin{array}{ccccc} \oplus & 0 & 0 & 1 & 0 \\ & 0 & 0 & 0 & 1 \\ \hline \end{array}$$

$\boxed{0\ 0\ 1\ 1\ 0\ 0\ 1\ 0} \rightarrow$ output of fk_1

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

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

$F(R, k_2) = P4 \circ \text{S-box} \circ \text{XOR}k_2 \circ EP(R)$

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 1 \end{array}$$

↓ EP

$$\begin{array}{cccccccc} 4 & 1 & 2 & 3 & 2 & 3 & 4 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}$$

↓ XOR k_2

$$\begin{array}{ccccccccc} & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ \oplus & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ \hline & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}$$

↓ s-box

$L = \overset{01}{0\ \underset{01}{0\ 1}\ 1}$ $\quad R = \overset{01}{0\ \underset{00}{0\ 0}\ 1}$

Row 1 col 1 $\quad$ Row 1 col 0

o/p = 2 ↳ 10 $\quad$ o/p = 2 ↳ 10

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 1 & 0 & 1 & 0 \end{array}$$

↓ P4

$$\begin{array}{cccc} 2 & 4 & 3 & 1 \\ 0 & 0 & 1 & 1 \end{array}$$

F output ←

$f_K(L, R) = [L \oplus F(R, K)][R]$

$$\begin{array}{ccccc} & 0 & 0 & 1 & 0 \\ \oplus & 0 & 0 & 1 & 1 \end{array}$$

$\boxed{0\ 0\ 0\ 1\ \ 0\ 0\ 1\ 1}$

↳ f_{K_2} output