



$$PT = 11110000$$

$$\text{cipher} = IP^{-1} \circ f_{K_2} \circ SW \circ f_{K_1} \circ IP \circ PT$$

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

↓ IP

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

↓  $f_{K_1}$

0 0 1 1 1 0 0 0  
↓ SW

1 0 0 0 0 0 1 1

↓  $f_{K_2}$

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

↓  $IP^{-1}$

4 1 3 5 7 2 8 6

1 0 1 0 1 1 1 0

$$f_{K_1} : I/P = \underbrace{1\ 0\ 1\ 1}_L \underbrace{1\ 0\ 0\ 0}_R \quad K_1 = 1\ 0\ 0\ 0\ 0\ 0\ 1\ 0$$

$$f_{K_1} = [L \oplus F(K_1, R)] [R]$$

$$F(K_1, R) = P4 \cdot S\text{-box} \cdot \text{XOR } K_1 \cdot E_P \cdot R$$

XOR  $K_1$   $\oplus$

4	1	2	3	2	3	4	1
0	1	0	0	0	0	0	1
1	0	0	0	0	0	1	0
1 1 0 0				0 0 1 1			
10				01			

$L = \underbrace{1\ 1\ 0\ 0}_{10}$  Row 2, col 2

$R = \underbrace{0\ 0\ 1\ 1}_{01}$  Row 1, col 1

1  $\rightarrow$  0 1 0 0

$\downarrow P4$

$F(K_1, R) \leftarrow$

2	4	3	1
1	0	0	0

$$f_{K_1}(L, R) = [L \oplus F(K_1, R)] [R]$$

$\oplus$

1	0	1	1
1	0	0	0
xor			
0	0	1	1

concatenate with R

$$f_{K_1}(L, R) = 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0$$

$$f_{K_2} : \text{3/p} = \begin{array}{c} \text{L} \quad \text{R} \\ \hline 1 \ 0 \ 0 \ 0 \ 0 \ 0 \ 1 \ 1 \end{array} \quad K_2 = 000001001$$

$$f_{K_2}(L, R) = [L \oplus F(K_2, R)][R]$$

$$F(K_2, R) = \text{P4} \circ \text{S-box} \circ \text{XOR } K_2 \circ \text{EP} \circ R$$

$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & 1 \end{array}$   
 $\downarrow \text{EP}$   
 $\begin{array}{ccccccccc} 4 & 1 & 2 & 3 & 2 & 3 & 4 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ \text{XOR } K_2 \oplus & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{array}$   


---

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


---

 $\begin{array}{c} 11 \downarrow \text{S-Box} \\ L = \begin{array}{c} \text{Row 3, col 0} \\ \text{③} \end{array} \quad R = \begin{array}{c} \text{Row 3, col 3} \\ \text{③} \end{array}$   
 $\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 1 & 1 & 1 & 1 \end{array}$   
 $\downarrow \text{P4}$   
 $\begin{array}{cccc} 2 & 4 & 3 & 1 \\ 1 & 1 & 1 & 1 \end{array}$   
 $F(K_2, R) \leftarrow \begin{array}{cccc} 1 & 1 & 1 & 1 \end{array}$

$$f_{K_2}(L, R) = [L \oplus F(K_2, R)][R]$$

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

concatenate with R

$$f_{K_2}(L, R) = 01110011$$