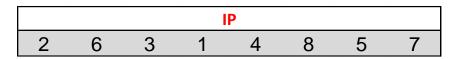
Given the plaintext [01101101] and K₁: 10100100, K₂: 01000011

Functions f_K, SW, K

- The function f_k is defined as follows. Let P = (L,R), then $f_K(L,R) = (L \oplus F(R,SK),R)$.
- The function SW just switches the two halves of the plaintext, so $SW(L,R) \rightarrow (R,L)$
- The function f (P, k) takes a four-bit string P and eight-bit key k and produces a four-bit output.

Applying the functions, we must perform the following steps: $IP^{-1} \circ f_{K2} \circ SW \circ f_{K1} \circ IP$

1. Apply the initial Permutation on [01101101] and split it into two groups. We have calculated $IP(P) = 1110 \mid 0110$

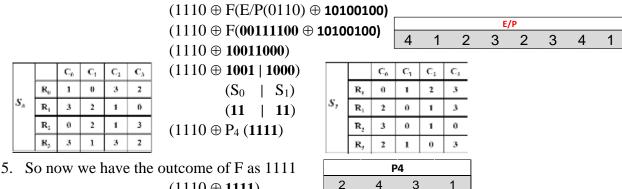


- 2. $L_0 = 1110$, $R_0 = 0110$
- 3. Find L_1 and R_1 , according the following rules:
 - a) $L_1 = R_0 \rightarrow 0110$
 - b) $R_1 = (L_0 \oplus f(R_0, K_1))$

$$(L_0 \oplus f(R_0,K_1)$$

$$(1110 \oplus f(0110 \oplus \textbf{10100100})$$

- 4. Applying the next functions:
 - a) $F(0110, 10100100) = P_4 \circ S_{Boxes} \circ ((E/P(0110) \oplus 10100100))$



- 5. So now we have the outcome of F as 1111 (1110 \oplus 1111) (0001)
- $f_K(L,R) = (L \oplus F(R,SK),R)$.
- $f_K(L,R) = (0001, 0110)$.
- 6. $L_1 = 0001$ and $R_1 = 0110$
- 7. SW just swaps them so $R_1=0001$ and $L_1=0110$
- 8. Concatenate L and R = 01100001

9. Round # 2: Now do the calculation of f_{k2} (L,R) = f_0 **1000011**)(01100001) = (0110 \oplus F(0001, **01000011**0), 0001))

$$\begin{array}{c} (0110 \oplus F(E/P(0001) \oplus \textbf{01000011}) \\ (0110 \oplus F(10000010 \oplus \textbf{01000011}) \\ (0110 \oplus 11000001) \\ \\ (0110 \oplus \textbf{1100} \mid \textbf{0001}) \\ \\ (S_0 \mid S_1) \\ \\ (\textbf{01} \mid \textbf{10}) \\ (0110 \oplus P_4 (\textbf{0110}) \\ (0110 \oplus 1010) \\ (1100) \end{array}$$

- 10. So now we have the outcome of F as 1100
- 11. $f_K(L,R) = (L_1 \oplus F(R_1,K_2), R_1)$
- 12. Calculating we then have $f_{k2}(L, R) = (1100, 0001)$
- 13. $L_2 = 1100$ and $R_2 = 0001$
- 14. Concatenate L_2 and $R_2 = 11000001$
- 15. perform the IP⁻¹ permutation:

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

Ciphertext = 01000110

Steps for Finding IP⁻¹

IP									
2	6	3	1	4	8 5		7		

Original Table (IP)		6	3	1	4	8	5	7
Step 1: Add indices		2	3	4	5	6	7	8
Step 2:Swap contents		2	3	4	5	6	7	8
and indices		6	3	1	4	8	5	7
Step 3: Sort based on	4	1	3	5	7	2	8	6
indices	1	2	3	4	5	6	7	8
Inverted Table (IP ⁻¹)	4	1	3	5	7	2	8	6