Given the plaintext [**01101101**] and **K_1: 10100100, K_2: 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) → (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 | 0110**

IP							
2	6	3	1	4	8	5	7

2. $L_0 = 1110$, $R_0 = 0110$
3. Find L_1 and R_1, according the following rules:
   a) $L_1 = R_0$ → 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) $F(0110, 10100100) = P_4 \circ S_{Boxes} \circ ((E/P(0110) \oplus 10100100)$

$$(1110 \oplus F(E/P(0110) \oplus \textbf{10100100})$$
$$(1110 \oplus F(\textbf{00111100} \oplus \textbf{10100100})$$
$$(1110 \oplus \textbf{10011000})$$
$$(1110 \oplus \textbf{1001} \mid \textbf{1000})$$
$$(S_0 \mid S_1)$$
$$(\textbf{11} \mid \textbf{11})$$
$$(1110 \oplus P_4\ (\textbf{1111})$$

E/P							
4	1	2	3	2	3	4	1

S_0		C_0	C_1	C_2	C_3
	R_0	1	0	3	2
	R_1	3	2	1	0
	R_2	0	2	1	3
	R_3	3	1	3	2

S_1		C_0	C_1	C_2	C_3
	R_0	0	1	2	3
	R_1	2	0	1	3
	R_2	3	0	1	0
	R_3	2	1	0	3

5. So now we have the outcome of F as 1111

$$(1110 \oplus \textbf{1111})$$
$$(0001)$$

P4			
2	4	3	1

- $f_K(L,R) = (L \oplus F(R,SK),R)$.
- $f_K(L,R) = (0001, 0110)$.

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 = 0110 0001

9. Round # 2: Now do the calculation of f_{k2} (L,R) = f(**01000011**)(01100001) = (0110 ⊕ F(0001, **0100001**0), 0001))

(0110 ⊕ F(E/P(0001) ⊕ **01000011)**
(0110 ⊕ F(10000010 ⊕ **01000011)**
(0110 ⊕ 11000001)

(0110 ⊕ **1100** | **0001**)

(S_0 | S_1)

(**01** | **10**)
(0110 ⊕ P_4 (**0110**)
(0110 ⊕ 1010)
(1100)

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)	2	6	3	1	4	8	5	7
Step 1: Add indices	1	2	3	4	5	6	7	8
Step 2:Swap contents	1	2	3	4	5	6	7	8
and indices	2	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