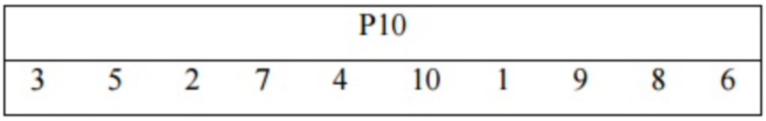
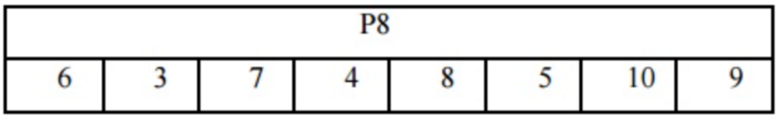
KEY: 1010101010

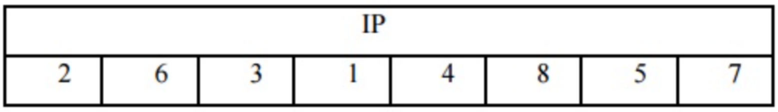


P10									
3	5	2	7	4	10	1	9	8	6

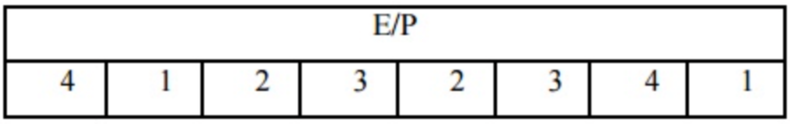


P8							
6	3	7	4	8	5	10	9

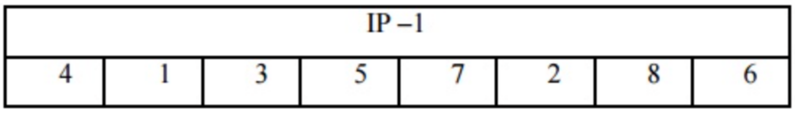
Plaintext: 10111101



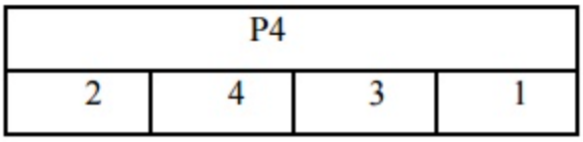
IP							
2	6	3	1	4	8	5	7



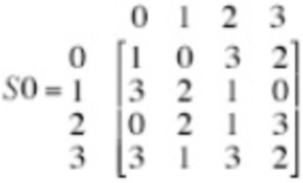
E/P							
4	1	2	3	2	3	4	1



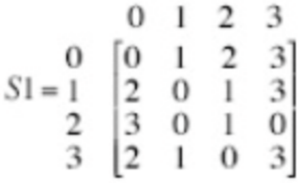
IP –1							
4	1	3	5	7	2	8	6



P4			
2	4	3	1



$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array}$$



$$S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

Key Generation

Step 1: Performed Permutation P10
Step 2: divided into two equal 2 parts
Step 3: perform left shift
Step 4: Perform Permutation P8 - Generated key 1
Step 5: Repeat steps 1, 2, & 3
Step 6: perform left two left shift
Step 7: perform Permutation P8 - Generated key 2

Encryption

Step 1: Performed Initial Permutation
Step 2: Divided into two equal 2 parts
Step 3: Take the Right value and perform E/P
Step 4: Perform XOR with KEY1
Step 5: Divided into two equal 2 parts perform SBOX
Step 6: Performed P4
Step 7: Perform XOR with the left value from Step 2
Step 8: Take the Right value from Step 2 and merge it with Step 7 left value

Step 9: Perform shift operation to left and right
Step 10: Divided into two equal 2 parts
Step 11: Take the Right value and perform E/P
Step 12: Perform XOR with KEY2
Step 13: Divided into two equal 2 parts perform SBOX
Step 14: Performed P4
Step 15: Perform XOR with the left value from Step 10
Step 16: Take the Right value from Step 2 and merge it with Step 15 left value
Step 17: Perform IP^{-1}

Key Generation

KEY: 1010101010

Step1 : Perform permutation

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

STEP 2:

1	1	0	1	0	0	1	1	0	0

STEP3: PERFORM LEST SHIFT

1	1	0	1	0

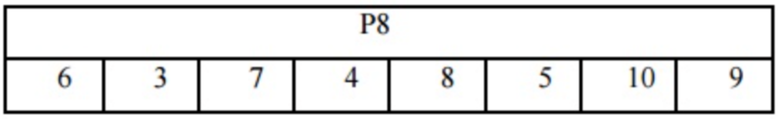
1	0	1	0	1

0	1	1	0	0

1	1	0	0	0

1	0	1	0	1	1	1	0	0	0

STEP4: PERMUTAION



P8							
6	3	7	4	8	5	10	9

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

Key 1: 11100100

STEP 5 : PERFORM TWO LEFT SHIFT IN STEP3

1	0	1	0	1	1	1	0	0	0

1	0	1	1	0	0	0	0	1	1

STEP 6 : PERMUTATION

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

Key 2: 01010011

ENCRYPTION

PT: 10111101

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

IP: 26314857

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

Right: 1110

E/P

4	1	2	3	2	3	4	1
0	1	1	1	1	1	0	1

	01111101
KEY 1	11100100
XOR	10011001

1	0	0	1	1	0	0	1
S0 -> 11,00 -> 3,0 -> 3				S1 -> 11,00 -> 3,0 -> 2			

S0 : 11 S1 :10
1110

P4

2	4	3	1
1	0	1	1

	1011
LEFT	0111
XOR	1100

1	1	0	0	1	1	1	0

Shift left & Right

1	1	1	0	1	1	0	0

Right : 1100

E/P

4	1	2	3	2	3	4	1
0	1	1	0	1	0	0	1

	01101001
KEY 2	01010011
XOR	00111010

0	0	1	1	1	0	1	0
S0 -> 01,01 -> 1,1				S1 -> 10,01 -> 2,1			

S0 : 10 S1 :00

1000

P4

2	4	3	1
0	0	0	1

	0001
LEFT	1110
XOR	1111

1	1	1	1	1	1	0	0

IP^{-1}

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

Encryption: 11110101