IS

Input text = 10100101

key = 0010010111

P_{10} on key

0010010111
1 2 3 4 5 6 7 8 9 10

(3,5,2,7,4,10,1,9,8,

= 1000010111

10000 10111

LS-1 => 00001 01111
1 2 3 4 5 6 7 8 9 10

Apply P_8 on it

6,3,7,4,8,5,10,9

$\boxed{K_1 = 00101111}$

Now apply LS-2 on LS-1

1 2 3 4 5 6 7 8 9 10
LS-2 = 00100 11101

Apply P-8 on it

$\boxed{K_2 = 11101010}$

Apply IP on plain text

text = $\underset{1\,2\,3\,4\,5\,6\,7\,8}{10100101}$

(2,6,3,1,4,8,5,7)

IP = $\underbrace{0111}\underbrace{0100}$

R = $\underset{1\,2\,3\,4}{0100}$

Apply EP on R

4,1,2,3,2,3,4,1

EP = 00101000

Now apply ~~XOR~~ EP XOR K_1

$$\begin{array}{r} 0\,0\,1\,0\,1\,0\,0\,0 \\ \underline{0\,0\,1\,0\,1\,1\,1\,1} \\ \underbrace{0\,0\,0\,0}_{S_0}\,\underbrace{0\,1\,1\,1}_{S_1} \end{array}$$

S_0 → row → 00 → 0

S_0 → column → 00 → 0

S_1 → row → 01 → 1

S_1 → column → 11 → 3

looking into S0 & S1 table

S0 1 => 01

S1 3 => 11

$S_0 S_1$ = $\underset{1234}{0111}$

Apply P4 on it

2,4,3,1

P4 = 1110

S_0S_1 = 0111

1st 4-bits of IP = 0111

P4 1 1 1 0

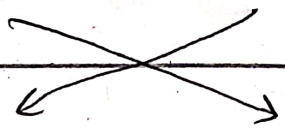
$S_0 S_1$ 0 1 1 1

4-bits IP 0 1 1 1 XOR

1 0 0 1

shift operation

1001 0100 → last 4-bits of IP



0100 1001

= 01001001

$R = \overset{1234}{1001}$

Apply E/P on it

E/P 11000011

Add key 2 in it

$$\begin{array}{rl} & 11000011 \\ \text{XOR} & 11101010 \\ \hline & \underbrace{0010}_{S_0}\,\underbrace{1001}_{S_1} \end{array}$$

S_0 - row → 00 → 0

S_0 - Col → 01 → 1

S_1 - row → 11 → 3

S_1 → Col → 00 → 0

Analyzing through S_0 & S_1 table

$S_0\,S_1$ = 0 2

= $\overset{1\,2\,3\,4}{0010}$

$$\begin{array}{r} 0010 \\ 0000 \\ \hline 0010 \end{array}$$

Apply P4 = $\overset{1234}{0010}\,\overset{5678}{1001}$) 1011 1

IP^{-1} 00110010

XOR = 0 11 0 1001

C.T = 00110110

C·T = 0 0 1 1 0 1 1 0

K_1 = 0 0 1 0 1 1 1 1

K_2 = 1 1 1 0 1 0 1 0

Apply IP on C·T

$$\underset{1\,2\,3\,4\,5\,6\,7\,8}{00110110}$$

(2,6,3,1,4,8,5,7)

IP = $\underbrace{0110}\underbrace{1001}$

R = $\overset{1234}{1001}$

Apply EP on R

4,1,2,3,2,3,4,1

= 11000011

Now apply E/P XoR K_2

$$\begin{array}{rl} & 1\,1\,0\,0\,0\,0\,1\,1 \\ \text{XoR} & 1\,1\,1\,0\,1\,0\,1\,0 \\ \hline & \underbrace{0\,0\,1\,0}_{S0}\,\underbrace{1\,0\,0\,1}_{S_1} \end{array}$$

S_0 — row → 00 → 0

S_0 — Col → 01 → 1

S_1 — row → 11 → 3

S_1 — Col → 00 → 0

By looking into So & S1 table

S_0S_1 = 0 2

= $\underset{1\,2\,3\,4}{0010}$

Apply P_4 on it (2,4,3,1)

= 0010

1st 4 bit of IP = 0 1 1 0

S_0S_1 = 0 0 1 0

P_4 = 0 0 1 0 XOR

0 1 0 0

= $\underbrace{0100}\underbrace{1001}$

Switch them

= 1001 0100

R = $\overset{1\,2\,3\,4}{0100}$

Apply E/P on it 4,1,2,3,2,3,4,1

E/P = 00101000

Add key1 in it

$$\begin{array}{rcccccccc} & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ \text{XoR} & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ \hline & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{array}$$

$$\underbrace{0\ 0\ 0\ 0}_{S_0}\ \underbrace{0\ 1\ 1\ 1}_{S_1}$$

S_0 – row → 00 → 0

S_0 – col → 00 → 0

S_1 – row → 01 → 1

S_1 – col → 11 → 3

S_0S_1 = 1 3

= $\overset{1}{0}\overset{2}{1}\overset{3}{1}\overset{4}{1}$

Apply P_4 = 1110 (2,4,3,1)

P_4 = 1110

Right 4 bits of switch = 1001

0111

$\overset{1}{0}\overset{2}{1}\overset{3}{1}\overset{4}{1}\ \overset{5}{0}\overset{6}{1}\overset{7}{0}\overset{8}{0}$

Apply IP^{-1} (4,1,3,5,7,2,8,6)

= 10100101