Assignment 1

Roll No = 20p-0480.
Topic = S-DES.
Section = BSE -7A
Name = M. Shaheer.

Input = 10100101
Key = 0010010111

Key Generation

Key 1 = 00100111
Key 2 = 11101010

Encryption :-

P_{10} = 3 5 2 7 4 10 1 9 8 6
↳ 1000101111

P_8 = 6 3 7 4 8 5 10 7

Step 1 =
IP = 2 6 3 1 4 8 5 7

Step 2 :-
Plain text = 0111 0100
L R

Step 3:-

E/p ⊕ K1 = 00000111
(S0 = 0000, S1 = 0111)

Step 4:-

R = 0100
P4 = 2431
R = 1110

R ⊕ L = 1001

Step 5 = Switching.

Left	Right
1001	0100
0100	1001

Step 6 = E/p ⊕ K2 = 0010 1001
(S0 = 0010, S1 = 1001)

Step 7 = PL = 0010 ⊕ L
= 0110
= 0110 1001

Step 8 = IP^{-1} = 0011 0110 → Cyphertext.

Decryption:-

Ciphertext = 00110110

Step1 = IP = 26 31 4857

Step2 = $\underbrace{0110}_{L}$ $\underbrace{1001}_{R}$

R = 1001

Step3 = $R \oplus K2 = \underbrace{0010}_{S_0}\ \underbrace{1001}_{S_1}$

Step4 = R = 0010

P4 = 2431
R = 0010

Step5 = Switching.

L R
0100 X 1001
1001 0100

$= \underbrace{1001}_{L}\ \underbrace{0100}_{R}$

Step 6 = E/P $\oplus$ K1 $= \underbrace{0000}_{S_0}\ \underbrace{0111}_{S_1}$

R = 0110

Step 7 = $P_4 = R$

$R = 0110$

$L = L \oplus R$

$= 0110$

$= 0111\ 0100$

Step 8 = P^{-1}

$P^{-1} = 01\ 0001\ 01 \rightarrow$ plaintext.