Name : Muhammad Rafay

Roll # 20P-0018

BCS-7A

Topic : S-Des Algorithm.

P10 :

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

P8 :

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

10 bit Key : 1010000010

P10 : 1000001100

Step 1. LS-1 :

10000 => 01100

00001 => 11000

Step 2. Apply P8

0000111000

10100100 -> Key 1

Now -> K2 = (LS2 of LS1)

LS-2 00100 00011 Now

P8 K_2 = 01000011

Encryption.

E_p. 4 1 2 3 2 3 4 1

I_p. 2 6 3 1 4 8 5 7

P_4 = 2431

P_t = 10010111

I_p = 00111101

Taking 4 bit.

1101 now E_p

11101011 after E_p

Taking XOR with key 1.

```
 11101011
 10100100
----------
 01001111
```

row - 00 → 0
col - 10 → 2
row - 11 → 3
col - 11 → 3

from S_0 & S_1 Matrix

S_0S_1 = 1111

P_4 = 1111

XOR b/w S_0 & S_1 P_4 & IP

```
 1111
 1111
 0101
-----
1010 1101
```

Ip of 4 bit.

First part done

Swap

1101 1010

Take right 4 bit

1010 E_p = 01010101

XOR with Key 2.

```
 01010101
 01000011
----------
 00010110
```

So

Row - 01 → 1

Col - 00 → 0

S_1

Row - 00 → 0

Col - 11 → 3

S_0S_1 = 1111

P_4 = 1111

XOR

```
 1111
 1111
 1101
------
 00101010
```

00111000 → encrypt text

DECRYPTION:-

00111000

IP 00101010

1010

E_p = 01010101

Xor with key 2.

```
  01010101
  01000011
  --------
  00010110
```

S_0

row - 01 → 1

col - 00 → 0

S_1

row = 00 → 0

col - 11 → 3

S_0S_1 = 1111

P_4 = 1111

```
XOR -  1111
       1111
       0010
       ----
       1101 1010
```

Swap : 10101101

Taking right 1101

EP

1110 1011

Now XOR with Key 1.

1110	1011
1010	0100
0100	1111

So

row - 00 → 0

col - 10 → 2

S_1

row - 11 → 3

Col - 11 → 3

S_0S_1 = 1111

P_4 = 1111

XOR

1111	
1111	
1010	
0101	1101

Now IP.

10010111

↳ Plain Text.