BCS7A P20-0130 Sharif Ali

Date: Day:

S-DES Encryption | Decryption

P10

input =	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

1 0 1 0 0 0 0 0 1 0

P10

1 0 0 0 0 0 0 1 1 0 0

Now LS 1

1 0 0 0 0 | 0 1 1 0 0

0 0 0 0 1 | 1 0 0 0

Apply p8

0 0 0 0 1 1 1 0 0 0

1 0 1 0 0 1 0 0 Key 1 obtained

Now for K2 we do LS-2

LS-1

LS-2 = 0 0 1 0 0 | 0 0 0 1 1

Now p8

K2 = 0 1 0 0 0 0 1 1

p.t.o

Date: Encryption Day:

Now we encrypt

EP = 4 1 2 3 2 3 4 1

IP = 2 6 3 1 4 8 5 7

P4 = 2 4 3 1

Pt = 1 0 0 1 0 1 1 1

IP = 0 1 0 1 1 1 0 1

Taking last 4 bits

1 1 0 1 now EP

1 1 1 0 1 0 1 1 after EP

take XOR with key 1

1 1 1 0 1 0 1 1

1 0 1 0 0 1 0 0

---

0 1 0 0 1 1 1 1

So row = 00 → 0

So col = 10 → 2

S1 row = 11 → 3

S1 Col = 11 → 3

So & S1 matrix

SoS1 = 1 1 1 1

XOR b/w

So S1 P4 and IP

PT 10

Date: Day:

1 1 1 1
1 1 1 1
0 1 0 1
1 0 1 0 1 1 0 1

→ the last 4 bit ip

first part done

swap

1 1 0 1 1 0 1 0

Now take right 4

1 0 1 0 ep2 0 1 0 1 0 1 0 1

now XOR with key2

0 1 0 1 0 1 0 1
0 1 0 0 0 0 1 1
0 0 0 1 0 1 1 0
S0 S1

S0 row = 01 = 1
S0 col = 00 = 0
S1 row = 00 = 0
S1 col = 11 = 3

S0S1 = 1 1 1 1
take p4 = 1 1 1 1
XOR
1 1 1 1
1 1 1 1
1 1 0 1
0 0 1 0 1 0 1 0

→ Take IP = 0 0 1 1 1 0 0 0
→ cypher text

Decryption

0 0 1 1 1 0 0 0

IP

0 0 1 0 1 0 1 0

1 0 1 0

Ep → 0 1 0 1 0 1 0 1

XOR with k2

0 1 0 1 0 1 0 1
0 1 0 0 0 0 1 1
0 0 0 1 0 1 1 0

p.T.O

Date: Day:

S_0 row = 01 = 1
S_0 col = 00 = 0
S_1 row = 00 = 0
S_1 col = 11 = 3
$S_0 S_1$ = 11 11
P_4 = 11 11

XOR
11 11
11 11
00 10
11 01 10

Swap
10 01 10
take nyb 1101
Ep
11 10
row
11 11 10 11
1010 0100
0100 1111

S_0 row = 00 = 0
S_0 col = 10 = 2
S_1 row = 11 = 3
S_1 col = 11 = 3
$S_0 S_1$ = 11 11
row P_4 11 11

P.T.O

Date:

Day:

XOR

```
 1 1 1 1
 1 1 1 1
 1 0 1 0
---------
 0 1 0 1 1 1 0 1
```

→ right of IP

now IP

1 0 0 1 0 1 1 1 = ptext

✓