(10) Plaintext : 10000001

Key : 11111 00000

P_{10} : 1110101000

LS-1 LS-1

11011 10000

1 2 3 4 5 6 7 8 9 10

P_8 : 10010100

K_1 : 10010100

→ 1101110000

LS-2 LS-2

01111 00010

1 2 3 4 5 6 7 8 9 10

P_8 : 01010101

K_2 : 01010101

P : 10000001

IP : 00010100

L : 0001 R : 0100

Ep : 00101000

K_1 : 10010100

⊕ 10111100

Row=11→3 Row=10→2

Col=01→1 Col→10→2

S_0 : 01 S_2 : 01

0101

P_4 : 1100

L : 0001

⊕ 1101

P_{10}

3 5 2 7 4 10 1 9 7 6

P_8

6 3 7 4 8 5 10 9

IP_8

2 6 3 1 4 8 5 7

IP^{-1}

4 1 3 5 7 2 8 6

Ep

4 1 2 3 2 3 4 1

P_4 :

2 4 3 1

L : 0100   R : 1101

Ep : 11101011

K_2 : 01010101

$\oplus$ 10111110

L : 1011   R : 1110

r = 11 → 3   r = 10

c : 01 → 1   c = 11

S_0 : 01 S_1 : 00

→ 0100

P_4 : 1000

L : 0100

$\oplus$ 1100

11001101

k2 3

$I\bar{p}^{1}$: 01010111

Cipher text : 01010111

(14)

(a) Plaintext = 1001

K_1 : 01

K_2 : 11

$P_1 = E(P, K_1) = E(1001, 01)$

$= 1001$

$E(P_1, K_2) = E(1001, 11)$

$C_1 = 1000$

$D(C, K_1) = (1000, 01) = 1111$

$D(C, K_2) = (1000, 11) = 1001$

$K_0(1001) = 1111$

$K_1(1001) = 1001$

$K_2(1001) = 0001$

$K_3(1001) = 1000$

there decryption for $D(C, K_2) = 1001$ and it is matched with $K_1(1001) = 1001$ which is K_1 (Plain text)

This is colled meet in the middle attack.

b) (i) Time Complexity or possible keys for DES = 2^{56}
for 2DES is $2 \times 2^{56} = 2^{57}$

(ii) Time Complexity of brute force attack on double encryption is $2^{56+56} = 2^{112}$.