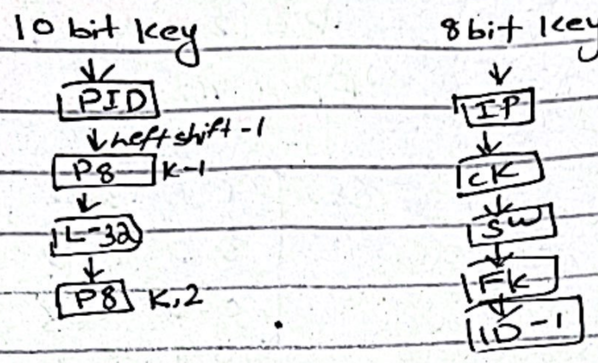
P20-0613

Assignment 1

DES key



S-Desk key generation

10 bit

1010000010

↓ P10

1000001100

Performing left shift (first, Last)

0001 11000

row P10 them

10100100 = key 1

now LS2 on LS1

LS1 =0001 11000

00100 00011

now again

P8

$\boxed{01000011}$ → key 2

P10

3527410198

P8

6374051010

DES Encryption

k1 = 10100100

k2 = 01000011

IP = 26314857

EP = 41232341

PT = 10010111

↓

IP

01011101

↓

0101 1101

1101

↓

1110 1011 : After

XOR with key 1

11101011

10100100

0100 1111

So S1

$$S_0 = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix}$$

$$S_1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$$

S_0 : row = 00(f, S_2) 00 = 0

Col = 10($2 \& 3$) 10 = 2

So = 3

So = 11

for S_1 = 11. 11 { row : 11 : 3
Col = 11 : 3 }

↓

S_1 = 110

S_0, S_1 = 11 11

Now XOR with left of IP

11 11

01 01

1010 1101

1101 1010

Taking right

1010

↓

0101   0101

Now XOR . with K_2

XOR

$$\begin{array}{r} 01010101 \\ 01000011 \\ \hline \underbrace{0001}_{S_0}\ \underbrace{0110}_{S_1} \end{array}$$

$$S_0 \left[\begin{array}{lll} \text{row} & 01 & =1 \\ \text{Col} & 00 & =0 \end{array}\right] = 3 = 11$$

$$S_1 \left[\begin{array}{ll} \text{row} & 00=0 \\ \text{Col} & 11=3 \end{array}\right] = 3 = 11$$

So S_1 = 1111 Now XOR with left of IR

$$\begin{array}{r} 1111 \\ 1101 \\ \hline 0010 \end{array}$$

$\overline{00101010}$

IP^{-1}

$\boxed{00111000}$ cypher text

↓

IP

$\underbrace{0010}\ \underbrace{1010}$

taking

1010

EIR

01010101

now XOR with K_2

01010101
0.1000011

$\underbrace{0001}_{S_0}$ $\underbrace{0110}_{S_1}$

$S_0 = \left\{ \begin{matrix} \text{raw} = 01 = 1 \\ \text{Col} = 00 = 1 \end{matrix} \right\} = 3 = 11$

$S_0 = 11$

$S_1 = \left\{ \begin{matrix} \text{raw} = 00 = 0 \\ \text{col} = 11 = 3 \end{matrix} \right\} = 3 = 11$

$S_0 \; S_1 = 1111$

now XOR with left of IP

111
0010

1101

(1101 ⊗ 10 10) = 1010 = right of P
1010 1101

CT = 00111000
k_1 = 1010100
k_2 = 01000011

$$S_0 = \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix}$$

$$S_1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix}$$

IP = 2 6 3 145054
IP = 41 2 3234
P_4 = 2 4 3 1

e

CIP

1110 1.011

new XOR key 1

1110 1011
1010 0100

$\underbrace{0100}_{S_0}$ $\underbrace{1111}_{S_1}$

$S_0 \left[\begin{matrix} \text{row} & 00 : 0 \\ \text{col} & 10 : 3 \end{matrix} \right] = 3 = 11$

$S_1 \left\{ \begin{matrix} \text{row} & 11 : 3 \\ \text{col} & 11 : 3 \end{matrix} \right\} 3 = 11$

1111

Now P_4
1111

Now XOR with left of IP

1111
1010

0101 1101

Now IP

10010111 : Plaintext
(decrypted)

Hence proved