NAME: JAWAD AHMED

RollNo: 20P-0165

Section: BCS - 7A

Information Security

Assignment # 01

X————X

NAME : JAWAD AHMED

ROLL NO : 20P-0165

SECTION : BCS-7A

SUBJECT : INFORMATION-SECURITY

Assignment # 01

X———————————X

Q:- Perform complete encryption/decryption using S-DES?

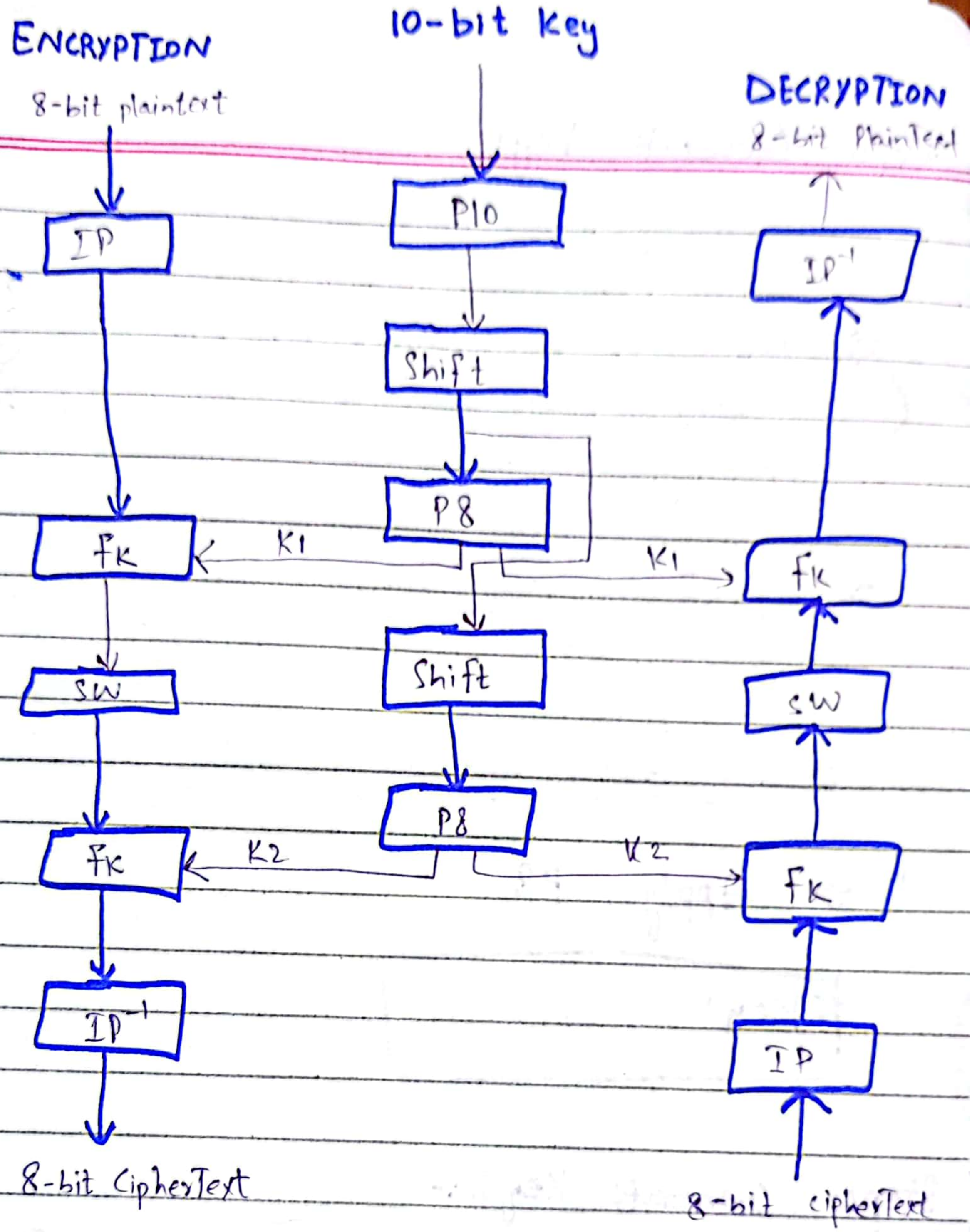
Ans:- SDES (Simplified Data Encryption Standard). is a simple encrypting algorithm. It is used for educational purposes and has limited security applications.

Encryption using S-DES.

Input: 1 0 1 0 0 1 0 1 (8-bit)

Key: 0 0 1 0 0 1 0 1 1 1 (10-bit)

The figure: 1 shows an main idea how S-DES encryption and decryption works.



Example :-

Given Data

Input : 1 0 1 0 0 1 0 1

Key : 0 0 1 0 0 1 0 1 1 1

Step1: Generate Key1

orignal-key = 0 0 1 0 0 1 0 1 1 1
1 2 3 4 5 6 7 8 9 10

⇒ Apply P10 on orignal-key
(P10 is shifting of bits based on rules or may be given)

P10-orignal-key = 1 0 0 0 0 1 0 1 1 1

⇒ Shift $ First and Last 5 bits by one left

shifted-P10-orignal-key = 00001 01111
1 2 3 4 5 6 7 8 9 10

⇒ Apply P8

Key1 = 00101111

Step2: Generate Key2 :-

Take shifted-P10-orignal key and shift first and last 5 bits by 2 left.

2-left-shifted-P10-orignal-key = 00100 11101
1 2 3 4 5 6 7 8 9 10

=> Apply P8

Key2 = 11101010

Step3: ENCRYPTION

$$\text{orignal-input} = \begin{array}{cccccccc} 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{array}$$

=> Apply IP

IP-orignal-key = 0 1 1 1 0 1 0 0

=> Apply Fkey1:

$$F_K(L, R) = (L \oplus F(R, SK), R)$$

L = 0111

R = 0100

SK = key 1

First solve F(R, SK)

R = 0100 => $n_1 \; n_2 \; n_3 \; n_4$

E/P = 0010 1000

$$= \begin{array}{c|cc|c} n_4 & n_1 & n_2 & n_3 \\ n_2 & n_3 & n_4 & n_1 \end{array}$$

⊕ => In Equality Detector
00 → 0
01 → 1

Key 1 = 0 0 1 0 1 1 1 1

Key 1 =	0	0	1	0	1	1	1	1
	k_{11}	k_{12}	k_{13}	k_{14}	k_{15}	k_{16}	k_{17}	k_{18}

$k_{11} \oplus n_4$	$n_1 \oplus k_{12}$	$n_2 \oplus k_{13}$	$n_3 \oplus k_{14}$
$k_{15} \oplus n_2$	$n_3 \oplus k_{16}$	$n_4 \oplus k_{17}$	$n_1 \oplus k_{18}$

Put values

$0 \oplus 0$	$0 \oplus 0$	$1 \oplus 1$	$0 \oplus 0$
$1 \oplus 1$	$0 \oplus 1$	$0 \oplus 1$	$0 \oplus 1$
r	c	c	r
= 0	0	0	0
0	1	1	1

Check values in matrix S0

row (00) & column (00)

= 1 => 01

Check values in matrix S1

row (01) & colum (11)

① ③

= ~~0~~ 3 => 11

So,

$F(R, SK) = P4(\underset{1}{0}\underset{2}{1}\ \underset{3}{1}\underset{4}{1})$

Now Apply P4

$$\boxed{F(R, SK) = 1110}$$

$Fk(L, R) = (0111 \oplus 1110, 0100$

$= (1001, 0100)$

$Fk(L, R) = 10010100$

Now Apply Sandwich Function

$$\boxed{SW = 01001001}$$

Step 4: Apply Fkey2 on SW

$Fkey(01001001) = (L \oplus F(R, key2), R)$

$\longrightarrow$ Ⓐ

$L = 0100$

$R = 1001$

$key2 = 11101010$

Apply E/P

= 1100 00 11

R = 1001
$n_1 n_2 n_3 n_4$

$$= \begin{array}{c|c} 1 & 1 \\ 0 & 0 \end{array} \qquad \begin{array}{c|c} 0 & 0 \\ 1 & 1 \end{array}$$

Apply key $\textcircled{2}$

$$= \begin{array}{c|c} \textcircled{r} & \textcircled{c} \\ 0 & 0 \\ 1 & 0 \end{array} \qquad \begin{array}{c|c} \textcircled{c} & \textcircled{r} \\ 1 & 0 \\ 0 & 1 \end{array}$$

⇒ Check 0 row 1 column of S1

= 00

⇒ Check 3 row 0 colum of S2

⇒ 10

$\overset{1\,2\,3\,4}{=0010}$

Apply P4

= 0010

Put values in Eq (A)

$$(0100 \oplus 0010 , 1001)$$

$$= \underset{1\,2\,3\,4}{0110}\ \underset{5\,6\,7\,8}{1001}$$

(5) Apply IP^{-1}

$$\boxed{\text{Encrypted Text} = \underset{1\,2\,3\,4\,5\,6\,7\,8}{0\,0\,1\,1\,0\,1\,1\,0}}$$

Decryption Algorithm.

We have key1, key2 (as calculate back)
The reciever can calculate it with
key let's apply it to decrypt
'cipher text to plain text.

Apply IP on encrypted-text (cipher-text)

$$\boxed{IP = 0\,1\,1\,0\,1\,0\,0\,1}$$

Now apply f_{K_2} with K_2

$L = 0110$

$R = 1001$

$= (0110 \oplus f(1001, K_2) , 1001)$ $\textcircled{F}$

$F(1001, K_2) = 1001 = n_1\ n_2\ n_3\ n_4$

$$= \begin{array}{c|cc|c} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{array}$$

$\text{Key } 2 = (1\ 1\ 1\ 0\ 1\quad 0\ 1\quad 0)$

$$= \begin{array}{c|cc|c} 1 \oplus 1 & 1 \oplus 1 & 0 \oplus 1 & 0 \oplus 0 \\ 0 \oplus 1 & 0 \oplus 0 & 1 \oplus 1 & 1 \oplus 0 \\ \textcircled{v} & \textcircled{c} & \textcircled{c} & \textcircled{y} \end{array}$$

$$= \begin{array}{c|cc|c} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array}$$

$= \overset{1}{0}\overset{2}{0}\overset{3}{1}\overset{4}{0}$

Apply P4

= 0010 Put in (B)

$$= \left(0110 \oplus 0010 , 1001\right)$$

= 0100 1001

Now Apply SW

= 1001 0100

Again apply fk with key1

L= 1001

R= 0100

Key1= 0010 1111

$$= \left(1001 \oplus f_{K1}(0100, k_1) , 0100\right) \rightarrow (D)$$

∘ 0100 = $n_1 \; n_2 \; n_3 \; n_4$

$$= \begin{array}{c|cc|c} 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{array} \longrightarrow (C)$$

Apply key (1) on (C)

(a)

$$= \begin{array}{c|cc|c} r & c & c & r \\ 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{array}$$

- Check matrix S0 & S1

= 0111 → put in (P)

(1001 ⊕ 0111, 0100)

= 11100100
  1 2 3 4 5 6 7 8

Now Apply IP^{-1}

= ~~01100101~~

= 10100101

↑

Plain-Text