Name:. Shoaib Akhtar

Roll No:- 20P-0147

Sec : BS-CS 7B

Submitted to: Sir Amin Sb.

SDES Key Generation!

Key = 0 0 1 0 0 1 0 1 1 1

(Sol)

Step1:- Finding P10

$P_{10} = (K_3, K_5, K_2, K_7, K_4, K_{10}, K_1, K_9, K_8, K_6)$

$P_{10} = (1 0 0 0 0 1 0 1 1 1)$

Step2:- Perform LS-1 on each 5 bits

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

Step3:- Find P8 using below Formula. on "LS-1".

$P_8 = (K_6, K_3, K_7, K_4, K_8, K_5, K_{10}, K_9)$

P8 = (0 0 1 0 1 1 1 1) → key 1

$\boxed{\text{Key 1} \Rightarrow 0 0 1 0 1 1 1 1}$

Step4:- Perform "LS-2", on "LS-1"

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

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

Scanned with CamScanner

Step 5 :: Find P8 on "LS-2"

LS-2 = 0010011101

P8 ⇒ 11101010 → Key 2

$\boxed{\text{Key 2} = 11101010}$

S-DES Encryption!

Original Input/Plaintext ⇒ 10100101
1 2 3 4 5 6 7 8

Step1:- Apply IP

IP = (2, 6, 3, 1, 4, 8, 5, 7)

$\boxed{\text{IP} \Rightarrow 01110100}$

Step2:- Apply Fkey1:-

(A) Perform "EP" on last 4-bits of IP

EP = (4, 1, 2, 3, 2, 3, 4, 1)

Last-4-bits of IP:- (0100)
1 2 3 4

$\boxed{\text{EP} = 00101000}$

(B) Perform XOR on key1 and EP

key1 = 0010 1111
EP = 0010 1000
XOR = 0000 0111

(C) First 4-bits of XOR will be S0 and last 4-bits will be S1

S0 = 0000
S1 = 0111

The first and last bits for rows and remaing for columns

S0 → row → 00
S0 → col → 00
S1 → row → 01
S1 → col → 11

2^2 2^1 2^0

4 2 1

S0-row ⇒ 0 0 → 0+0 ⇒ 0 } S0

S0-col 0 0 → 0+0 ⇒ 0

S1-row 0 1 → 0+1 ⇒ 1 } S1

S1→col 1 1 → 2+1 ⇒ 3

S0: 00
S1: 13

$$S_0 \Rightarrow \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 1 & 0 & 3 & 2 \\ 1 & 3 & 2 & 1 & 0 \\ 2 & 0 & 2 & 1 & 3 \\ 3 & 3 & 1 & 3 & 2 \end{array}, \quad S_1 \Rightarrow \begin{array}{c|cccc} & 0 & 1 & 2 & 3 \\ \hline 0 & 0 & 1 & 2 & 3 \\ 1 & 2 & 0 & 1 & 3 \\ 2 & 3 & 0 & 1 & 0 \\ 3 & 2 & 1 & 0 & 3 \end{array}$$

Q

Using Matrices, Find the value of $S_0:00$, $S_1:13$

In binary

$S_0:00 \Rightarrow 01 \Rightarrow 01$

$S_1:13 \Rightarrow 3 \Rightarrow 11$

Finally, S_0S_1

$S_0S_1 \Rightarrow 0111$

D: Perform P4 on S_0S_1

P4 : (2, 4, 3, 1)

P4 $\Rightarrow$ 1110

Now Find XOR of P4, S_0S_1 and First_4-bits of IP.

P4 = 1110

S_0S_1 = 0111

First4-IP = 0111

XOR = 1001

Merge last 4-bits of IP with XOR

XOR+IPL4 $\Rightarrow$ 10010100

~~(3). Apply SW on~~

Step 3:- Apply SW on XOR, IPL4

~~SW~~

SW ⇒ 01001001

Step4:- Apply Fkey8:-

key8 ⇒ ~~01001001~~ 01001001

~~Final IP~~

IP ⇒ ~~100000100~~

(A) Apply EP on last 4-bits ~~of IP~~ of key8.

~~EP ⇒ 10010110~~

~~EP - 00110100~~

EP ⇒ 11000011

(B) Perform XOR on key8 and EP

~~1 1 1 0 1 0 1 0~~

~~Key8 = 0 1 0 0 1 0 0 1~~

~~EP = 1 1 0 0 0 0 1 1~~

~~XOR => 1 0 0 0 0 0 1 0~~

~~1 0 1 0 1 0 0 1~~

~~0 0 1 0 1 0 0 1~~

~~Key8 => 0 1 0 0 1 0 0 1~~

~~EP => 1 1 0 0 0 0 1 1~~

~~XOR => 1 0 0 0 1 0 1 0~~

Key8 (generated) => 1 1 1 0 1 0 1 0

EP => 1 1 0 0 0 0 1 1

XOR => 0 0 1 0 1 0 0 1

(C) ∴ Left B4 bits are S0, and Ri8 4-bits are S1

S0 = 0010

S1 = 1001

S0 - row => 00

S0 - col => 01

S1 - row 1 1

S1 - col 0 0

~~2 1 2 4 1~~

2^2 2^1 2^0

4 2 1

S0 - row 0 0 → 0 + 0 ⇒ 0

S0 - col 1 1 → 0 + 1 ⇒ 1

S1 - row 1 1 → 2 + 1 ⇒ 3

S1 - col 0 0 → 0 + 0 ⇒ 0

$\left.\begin{matrix}0\\1\end{matrix}\right\}$ S0 $\left.\begin{matrix}3\\0\end{matrix}\right\}$ S1

S0 : 01 = 0 ⇒ 00

S1 : 30 ⇒ 2 ⇒ 10

S0S1 ⇒ 0010

(D) Apply P4

P4 = 0010.

Now Perform, XOR on P4, S0S1 and First 4-bits of IP.

1st-4-bits 0 1 0 0

S0S1 0 0 1 0

P4 0 0 1 0

0 1 1 0

Merge last 4-bits.

⇒ 0 110 1 001

Step 5 Apply IP^{-1}

IP-1 ⇒ (4, 1, 3, 5, 7, 2, 8, 6)

~~I~~ IP^{-1} ⇒ (0 0 1 1 0 1 1 0)

↓

The cipher for the plain text. :)