Name: 8hoarb Akhlar
Roll No: 20P-0147

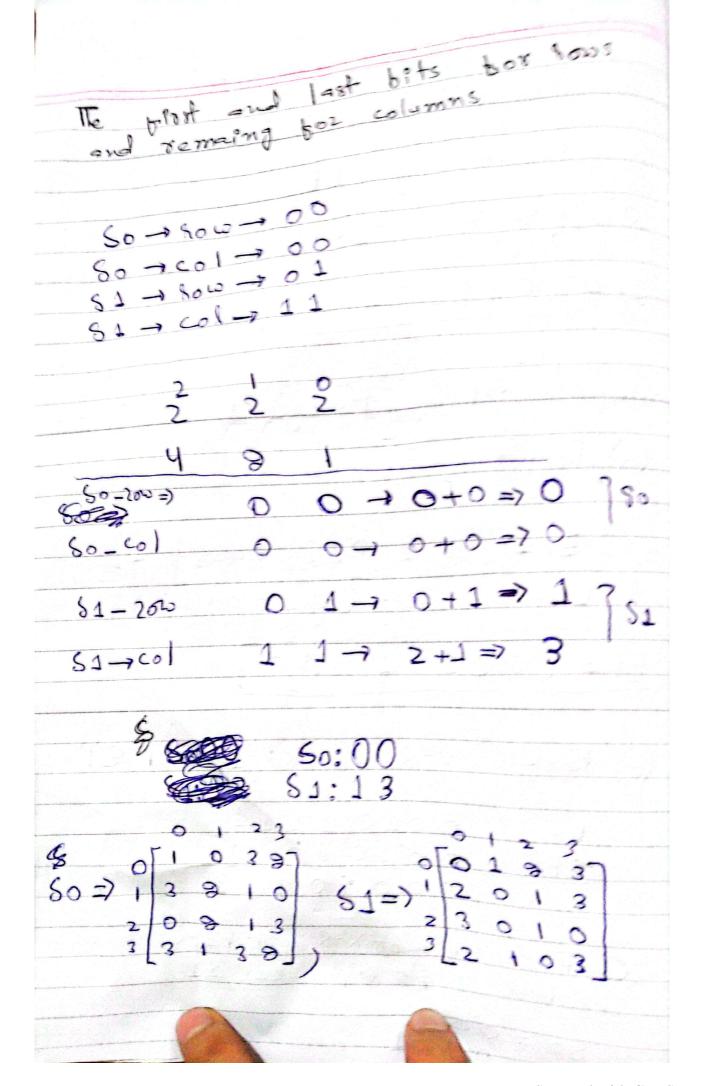
8e C: BS-CS 7B

Submitted to: 8ix Amen 8b.

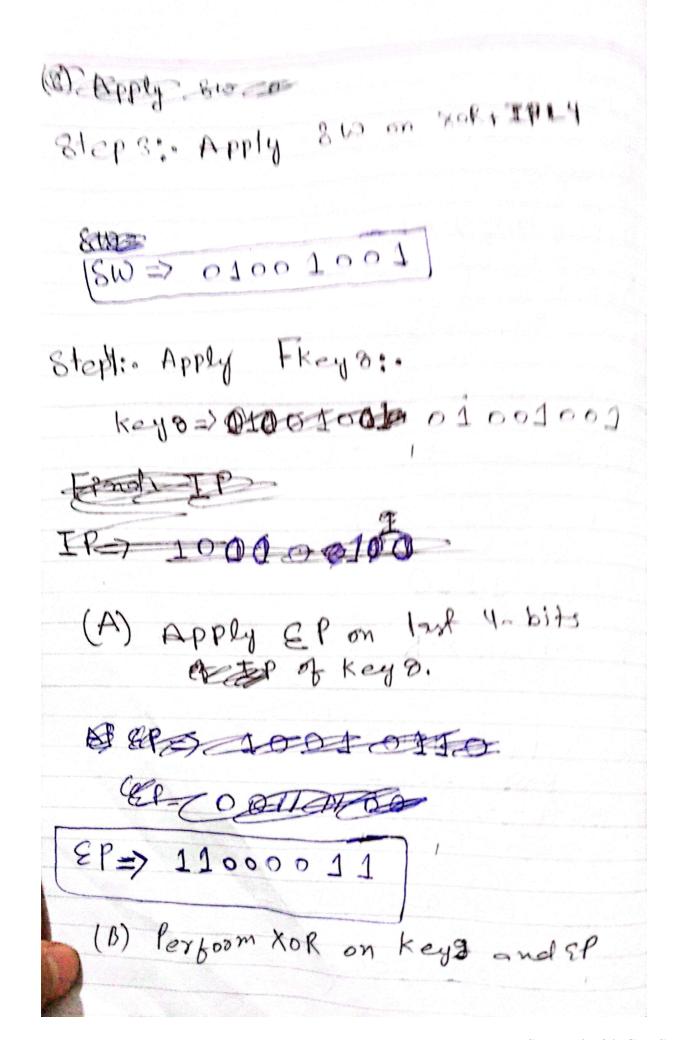
SDES Key Greneralion! Key=0010010111 \$ Step1: Finding Plo Plo = (K3, K5, K9, K7, K4, K10, K1, K9, K8, K6) Plo= (1000010111) Steps: Perborm LS-1 on each 5 bits LG-1 = 00001 01111 Step 3: Find P8 using below Formula. P8 = (K8, K3, K7, K4, K8, K5, K10, K9) P8 = (00101111) -> key 1 Key 1=) 00101111 Step 4: · Perform "LS-9", on 'LS-1" LS-1= 00001 01111 LS-9= 00100 \11101

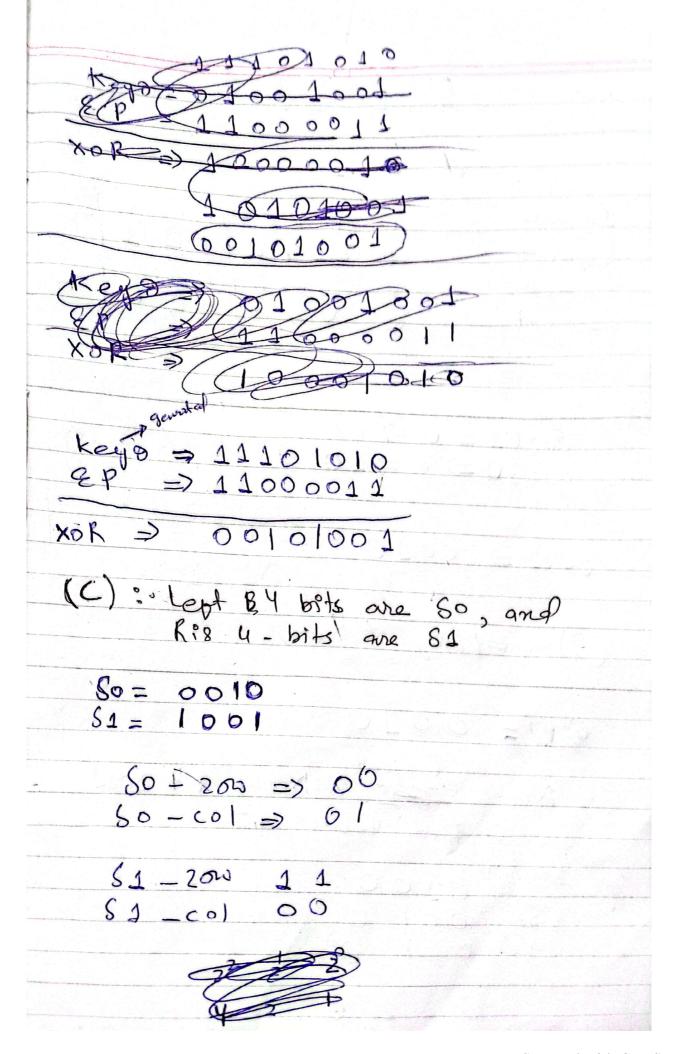
8tep=5: Frmd P8 on "LS-9" LS-9 = 001001101 $P8 \Rightarrow 11101010 \longrightarrow Key 9$ Key 9 = 11101010

S-DES Encruption! 029gend Input/Plaintext=> 10100101 Step1: Apply IP IP= (8,6,3,1,4,8,5,7 IP=> 01110100 Steps: Apply Fkey1: (A) Perform "EP" on Part 4-69ts ob IPO EP= (4,1,8,3,8,3,4,1) Last-4-bits & IP: (0100) EP = 00101000 (B) Perform XOR on key1 and EP key1 = 00101111 2P = 00101006 XOR = 0000011 (C) First 4-bits of XOR will be 80 last 4-bits will be 81 80 = 0000 81 = 0111



Using Matrices, Find the value of So. So:00, S1:13
50,00, 51:23
$S_0:00 \Rightarrow 01 \Rightarrow 01$ $S_1:13 \Rightarrow 3 \Rightarrow 11$
Frally, 8081
8081 => 0111
D: Perborm P4 on 8081
Pu: (9,4,3,1)
Py => 1110
Now Find XOR of PY, 5081 and First-4-694s of IP.
P4 = 1110
8051 = 0111
Firsty-IP= 0111
XOR = 1001
Merge last 4-bits of IP wilk XOR
XXX+IPLY \$ 10010100





2 2 2
$\frac{421}{00070+0=70}$
50-(0) 0 01-10+1=> 3?(1
S1-col 0 0 → 0 + 0 ⇒ 0 01
, 21 - 2 00
$5_0:01 = 0 \Rightarrow 00$ $5_1:30 \Rightarrow 3 \Rightarrow 10$
5051 => 0010
(O) Apply Py
e. Du - 0010
NOW Perform XOR ON P4, SOSI and First 4-bits of IP.
16t-4-6its 0106 501 001 0
24.001.0
0116

Merge last 4-bits. 0 110 1 001 Step 5 Apply 1P IP-1=) (4,1,3,5,7,8,8,6) FIP=> (001101 10) The cipher tor the plain text. :)