Name: Muhammad Shoaib Akhter Qadri
Class & Section: BSE (8B)
Enrollment No: 02-131212-009
Reg No: 79290

Q No. 1

Data Given:

Key = 0111 0110 10
Plain text = 1011 1001

1) Finding K1:

$K_1 = P8(Shift(P10(key)))$

P10

3	5	2	7	4	10	1	9	8	6

Key = 01110 11010
P10 = 10111 00101

Shift = 01111 01010

P8

6	3	7	4	8	5	10	9

P8 = 0111 0101

$K_1 = 01110101$

2) Finding K_2:

$K_2 = P8(\text{Shift}(\text{Shift}(P10(\text{key}))))$

Key = 01110 11010

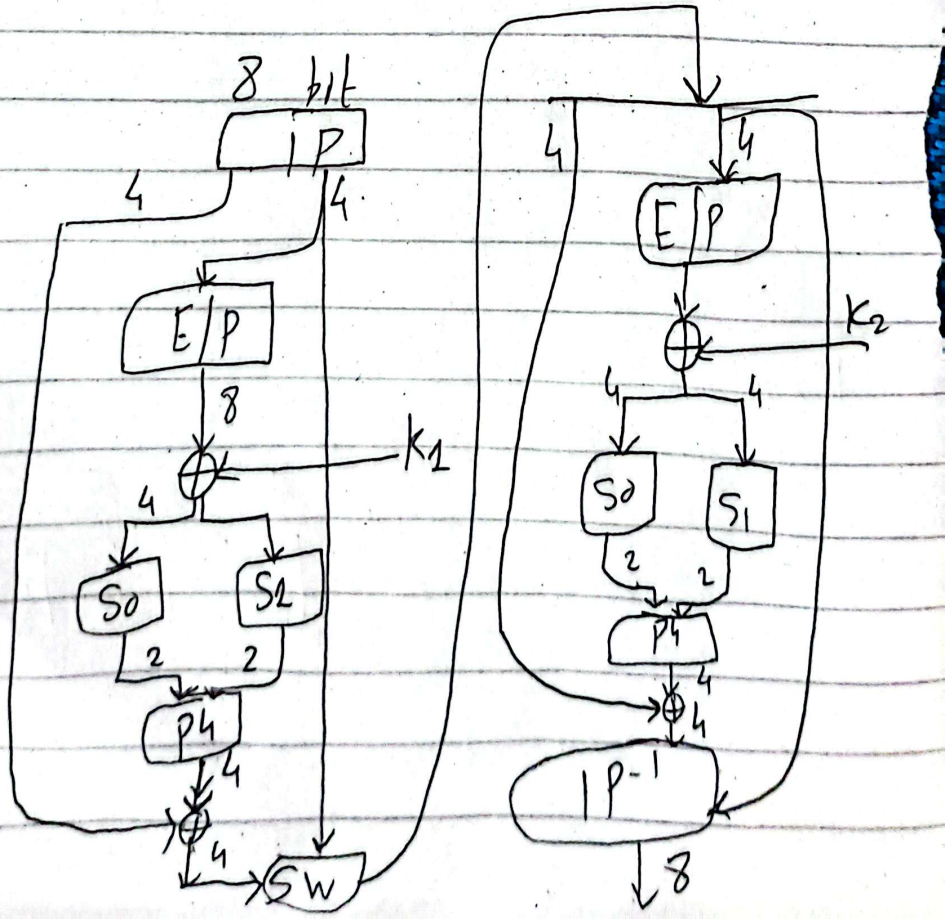
P10 = 10111 00101

LS-I = 01111 01010 ←

LS-II = ~~11110~~ ~~10100~~ 11101 01001

P8 = ~~11011000~~ 01100110

~~$K_2 = 11011000$~~ $K_2 = 01100110$



Plaintext = 1011 1001

Apply Initial Permutation (IP)

IP							
2	6	3	1	4	8	5	7

IP = 0011 1110
L R

Apply Expanded Permutation on right side.

E/P = 0111 1101

E/P							
4	1	2	3	2	3	4	1

Apply XOR Operation on key 1 and E/P

E/P = 0111 1101
K1 = 0111 0101
0000 1000
L R

Apply S0 on L.S

R = 1st & 4th Input = 00 = [0]
C = 2nd & 3rd Input = 00 = [0]

Apply S1 on R.S

1st & 4th Input = 10 = [2]
2nd & 3rd Input = 00 = [0]

S_0 =

	0	1	2	3
0	1	0	3	2
1	3	2	1	0
2	0	2	1	3
3	3	1	3	2

S_1 =

	0	1	2	3
0	0	1	2	3
1	2	0	1	3
2	3	0	1	0
3	2	1	0	3

$S_0 = 2 = 01$

$S_1 = 3 = 11$

P4			
2	4	3	1

$S_0S_1 = 0111$

$P4 = 1110$

Apply XOR of P4 with L.S of IP

$P4 = 1110$

$IP = 0011$

1101

Swap

$1101 \quad 1110$

After Swapping

$\underbrace{1110}_{L} \quad \underbrace{110}_{R}$

$E/P = 1110 \quad 1011$

Apply XOR with E/P and K_2

E/P = 1 1 1 0 1 0 1 1 1 1 1 0 1 0 1 1

K_2 = 0 1 1 0 0 0 0 0 0 1 1 0 0 1 1 0

1 0 0 0 1 1 0 1

S_0 = | S_1

10 01 = [1] 10 ⇒ 2 | 11 01 = [1] 11 ⇒ 3

00 01 = [0] 00 ⇒ 0 | 10 01 = [1] ⇒ 2

S_0 = (2,0) 00 ⇒ 00 | S_2 = (3,0) = 00 ⇒ 00

$S_0 S_2$ = 0000

P4 = 2431

P4 = 0000

XOR = 0 0 0 0
1 1 1 0
1 1 1 0

1110 1101

IP^{-1} = 0111 0111

IP^{-1}							
4	1	3	5	7	2	8	6

~~Cipher Text = 0000 1111~~ Ans

IP^{-1} (Ciphertext) = 0111 0111 Ans

Q2

a) Encrypting All Contents of a folder.

Step 1: Right-click on the folder you want to encrypt.
Step 2: Select Properties from the context menu.
Step 3: In the Properties Window, click on the Advanced button under the General Tab.
Step 4. Check the box that says Encrypt contents to secure data.
Step 5: Click OK to apply the changes.
Step 6: Choose whether to encrypt only the folder or the folder and its contents.
Step 7: Click Ok and then Apply to encrypt the folder.

b) Encrypting All Contents of a Drive.

Step1 = Open File Explorer and right-click on the drive you want to encrypt.

Step2: Select Turn on BitLocker from the context menu.

Step3: Choose how you want to unlock the drive (e.g., password, smart card).

Step4: Save the recovery key to a file or print it for backup.

Step5: Choose whether to encrypt the entire drive or only the used space.

Step 6: Click Next and then Start Encrypting to begin the encryption process.

Step 7: Wait for the encryption process to complete.

Both EFS and BitLocker are effective encryption tools in Windows, but the choice depends on the scope of encryption.

- EFS is best for encrypting individual files and folders.
- BitLocker is ideal for full disk encryption, ensuring complete security of all data on a drive.