- Assignment No: 01
- Name: Muhammad Sherjeel Akhtar
- ROLL NO: 2af-0101
- Section: BCS-7

Submitted To Respected Sir: Dr. Muhammad Amin.

key = 1010000010

Step → 1 0 1 0 0 0 0 0 1 0

1 2 3 4 5 6 7 8 9 10

Step → Permutation (P_{10})

3 5 2 7 4 10 1 9 8 6

1 0 0 0 0 0 1 1 0 0

Step 1:

Left Half	Right Half
10000	01100

Step 2 ⇒ One Round

00001	11000

Step → Combine

0 0 0 0 0 1 1 1 0 0 0

Step 5 → P_8 table (6 3 7 4 8 5 b

• 1 0 1 0 0 0 | 0 0 → key 1st

Step b

→ Previous Combine key → 0 0 0 0 1 1 1 0 0 0

• 0 0 0 0 1 | 1 1 0 0 0

→ perform 2 Round right

• 0 0 1 0 0 | 0 0 0 1 1

⇒ Combine → 0 0 1 0 0 0 0 0 1 1

Step → P_8 Permute

• 0 1 0 0 0 0 1 1 → K_2

→ Plain TXT → Cipher.

Plain text 8-bit:

0 1 1 1 0 1 0

(i) IP-8 permutate (2 6 3 1 4 8 5 7)

→ 1 0 1 0 0 0 1

③ LH | RH

1010 | 1001

④ Take right 4-bits (expand to 8 bits)

1 0 0 1

Number →	1	2	3	4	5	6	7	8
Expand →	4	1	2	3	2	3	4	1
o/p →	1	1	0	0	0	0	1	1

⑤ XOR

Expanded → 11000011

10100102

01100111

S_0 → 10 → 011

SBox

S_1 → 11

LH → 0110

RH → 0111

	0	1	2	3
0	01	00	11	10
1	11	10	01	00
2	00	10	01	11
3	11	01	11	10

S_0 Box

R → 00101

C → 11(3)

left half

	0	1	2	3
0	00	01	10	11
1	10	00	01	11
2	11	00	01	00
3	10	01	00	11

S_1 Box

R → 01

C → 11

right half

→ Apply P_4 . Permutate (2431)

1011 → P_4 (permutate)

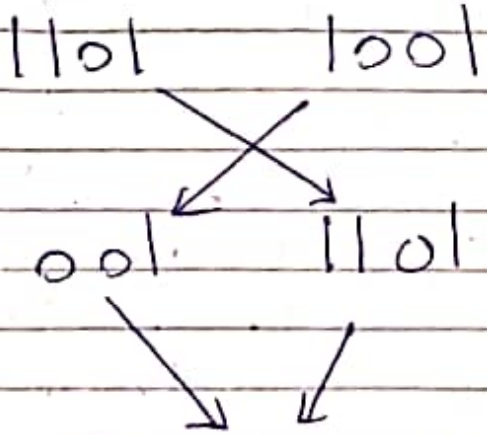
0111

Take left half initial permutation

0111
1010

1101 → Combine it with Right half of initial permutation.

(9)



key 2 → Treat it as plain text and apply key 2

IP → Table → 10100011

Output