**Class Activity # 04**

**Name: M. Arslan** **Roll Number: p176089**

**Question # 01:**

Find Cipher text for the first 2 rounds of DES in Output Feedback Mode (Stream Size=1 byte). After receiving L2R2 reverse their order and apply inverse permutation.

Note: Make the necessary assumptions and state them clearly. Also specify any vectors used.

Key: 00111010 01010101 11100001 00111100 10100000 00011110 10111111 00001011

Plain Text: 11010000 11110000 10101010 11001010 11100001 10111101 10101111 11110010

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | P1 | P2 | P3 | P4 | P5 | P6 | P7 | P8 |
| Plain Text: | 11010000 | 11110000 | 10101010 | 11001010 | 11100001 | 10111101 | 10101111 | 11110010 |
| RN | 00001000 | 10110011 | 00010111 | 00011011 | 00110000 | 11100110 | 11111011 | 10000001 |
|  | P1 **⊕** RN1 | P1 **⊕** RN1 | P1 **⊕** RN1 | P1 **⊕** RN1 | P1 **⊕** RN1 | P1 **⊕** RN1 | P1 **⊕** RN1 | P1 **⊕** RN1 |
| CN | 11011000 | 01000011 | 10111101 | 11010001 | 11010001 | 01011011 | 01010100 | 01110011 |
| key | 00111010 | 01010101 | 11100001 | 00111100 | 10100000 | 00011110 | 10111111 | 00001011 |

C0 = 0101010 0000001 1001011 1010110

D0 = 1110000 1011010 1011101 0011011

C1 = 1010100 0000011 0010111 0101100

D1 = 1100001 0110101 0111010 0110111

C2 = 0101000 0000110 0101110 1011001

D2 = 1000010 1101010 1110100 1101111

C1D1 = 0101000 0000110 0101110 1011001 1000010 1101010 1110100 1101111

C2D2 = 0100000 0011001 0111010 1100101 0001011 0101011 1010011 0111110

K1 = 000100010000011100100111100111001100101111001110

K2 = 111000010001100010100101110101001101011011010001

ROUND2:

L0 = 11111011111111010000010010111110

R0 = 00011101100001000010010110100010

L1 = 00011101100001000010010110100010

R1 = L0 + F(R0,K1)

K1+E(R0) =110000011001000010001110010001110110010000110110

R1 = 10000001 00011001 10001010 11001100

L2 = 10000001 00011001 10001010 11001100

R2 = 10010010 11111010 11001111 01101111

R2L2 =10010010 11111010 11001111 01101111 10000001 00011001 10001010 11001100

=00100101 11111101 10001101 00010101 11111010 00110001 10110111 01010100