Class Activity # 03

Name: *M.ARSLAN AHMAD KHAN*
RollNumber: *P176089*

Question # 01:

Find Cipher text for the first 2 rounds of DES. After receiving L_2R_2 reverse their order and apply inverse permutation.

plaint text: 11010000 11110000 10101010 11001010 11100001 10 111101 10101111 11110010

Key: 00111010 01010101 11100001 00111100 10100000 00011110 10111111 00001011

Round1:

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

Round 2:

L0 = 10011011 10100011 01100000 01110000

R0 = 11111111 11110110 01101100 11001100

K1+E(R0) =110110110101000011010010111110010010000010010001

L1=11111111 11110110 01101100 11001100

R1=11000100 11100110 10000110 11001111

L2=11000100 11100110 10000110 11001111

R2=00111011 00101111 11001010 11100111

R2L2=00111011 00101111 11001010 11100111 11000100 11100110 10000110 11001111

IP^{-1}= 01010011 01111111 10111011 01010110 01000000 01110001 10100111 10101111