Name : Harsh verdhan singh
Roll no : 20mcs009

Sample output format

Client Side:

Input Plaintext: 0b1010100110111001

Input Cipher key: 0b110011100111101

After Pre-round transformation: 0b100001000011100

Round key K0: 0b1110101110100101

After Round 1 Substitute nibbles: 0b1101101001001100

After Round 1 Shift rows: 0b1101110001001010

After Round 1 Mix columns: 0b1000110110101001

After Round 1 Add round key: 0b110011000001100

Round key K1: 0b1110101110100101

After Round 2 Substitute nibbles: 0b1000100010011100

After Round 2 Shift rows: 0b1000110010011000

After Round 2 Add round key: 0b110011100111101

Round Key K2: 0b1110101110100101

Cipher text: 0b110011100111101

Server Side:

Input Cipher text: 0b110011100111101

Input Cipher key: 0b1110101110100101

After Pre-round transformation: 0b100001000011100

Round key K2: 0b1110101110100101

After Round 1 InvShift rows: 0b1000100010011100

After Round 1 InvSubstitute nibbles: 0b110011000001100

After Round 1 InvAdd round key: 0b1000110110101001

Round key K1: 0b1110101110100101

After Round 1 InvMix columns: 0b1101110001001010

After Round 2 InvShift rows: 0b1101101001001100

After Round 2 InvSubstitute nibbles : 0b100001000011100

After Round 2 Add round key:

Round Key K0: 0b1110101110100101

Plaintext: 0b1010100110111001