Cryptography and Network Security (ECSE352L) Lab-4

1) Create a secure client-server chat application using Socket Application Programming Interface.

   a) In this application, client accepts message (M) and, cryptographic key (K) from the user and generates the cipher text using the formula: **C= (M + K) mod 26** then client sends this enciphered message to the server.

   In the destination, server reads the message and prints it. In addition, server should decrypt the received cipher (C) using the symmetric key (K). The decryption process is given by

   D= (C- K+ 26) mod 26.

   b) The communication system will be a bidirectional, client will write first to the server then server will receive the message and print the text. Then server will write the encrypted message to the client using the above symmetric system. Finally, client will receive the encrypted message from server and print the text.