Lab5 - Exercise

The Caesar Cipher is one of the simplest and oldest methods of encrypting messages, named after Julius Caesar, who reportedly used it to protect his military communications. This technique involves shifting the letters of the alphabet by a fixed number of places. For example, with a shift of three, the letter 'A' becomes 'D', 'B' becomes 'E', and so on.

1. **Implement a Socket Program for the above**
   Objective: Develop a client-server application using TCP socket programming, where:

   a. **Sender Process (Client): Applies the Caesar Cipher (Encrypts) for the text obtained from the user and sends it to the Receiver**
   b. **Receiver Process (Server): Receives the codeword, decrypts it and sends back to the sender in the reverser order.**

For Example :

Sender :

1. **if the Message is "HELLO" and the Shift(Key) = 3; then the message after encrypt will be "KHOOR".**
2. **Now this encrypted message "KHOOR" is sent to the Receiver**

Receiver :

a) **Receiver "KHOOR" and decrypts it back to "HELLO", in turn reverse it as "OLLEH".**
b) **Now this "OLLEH" is sent back to Sender.**