Assignment - 1

Q1. Establish a connection between the client computers and develop a chat interface between both clients. Use socket programming for the same.
Q2. Use a Diffie hellman key exchange algorithm to communicate the private key between the client and the server.
Q3. Use an RC4 encryption methodology and try to encrypt the messages from the sender's end and decrypt them on the receiver's end. You can assume that the private key is known to both the receiver and sender before establishing the communication. (Through the Diffie Hellman algorithm).
Q4. Implement the man-in-the-middle attack. In this case, you can assume that the attacker is able to receive the stream of messages. Assume that the range of private keys is very limited so that you can use brute force attack. Use this information to decrypt the messages.

Note :-

1. Attach screenshots of all the outputs and these should be done in a group of two students and do it by yourself.
2. In case of any discrepancy you will be awarded "0" marks.