Project owner - Ankita Tank

This a fully functional project.

In order to run this program, you have to run the file Client.java and Server.java. The server can handle multiple client connection and it will detect the multiple client in a list structure and HashMap.
Based on the list the dropdown menu is populated and clients can choose from the drop down list to send message to another client.

The p and q values should be prime. If the client doesn't provide a correct prime number, the exception will catch the program from crashing and will show dialogue box which will inform them about the error in typing the prime number. The public and private key is generated based on the valid p and q values.

Encrypting message .

The RSA.java is responsible for encrypting and decrypting the message sent from client.
It calculates the d,n,e along with various intermediate values supporting the algorithm.
I have followed the description logic provided in the write up.
After decrypting, the server receives the message as a calculated number which is generated based on the block size of 2 and the client will get the encrypted message. Additionally, the receiving client decrypts the message using their private key in order to obtain the original message.

Decrypting messages

Using bit shifting
I used the reverse logic from encryption of messages from RSA.