IAS-Assignment 4

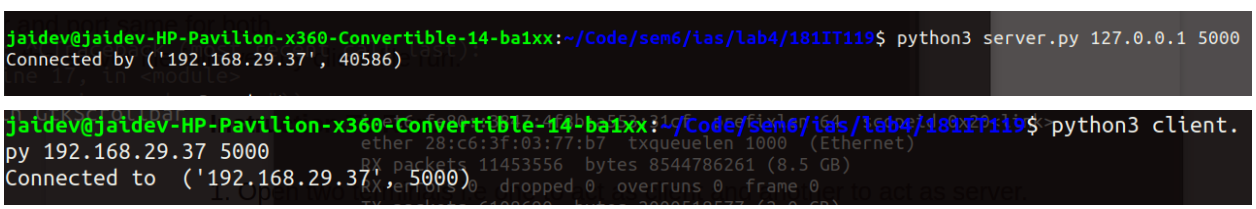
Name: Jaidev Chittoria

Roll No.: 181IT119

Instruction To Run:

1. Open two terminals i.e one to act as client and another to act as server.
2. Use the server machine IP address(your machine's IP) in client and localhost address in server and port same for both.
3. Run the server file followed by client file run.

Example:



Or if you don't know your machine's IP you can just use 0.0.0.0 for both client and server (stands for all non local addresses)

Algorithm :

Client side

- Take 2 prime numbers P and Q
- Then compute N=P*Q
- Select a random number r
- If r is between 0 and N-1 continue the process
- Else print the error message
- Enter the private key S for the client
- If S is between 0 and N-1 continue the process
- Else print the error message

- Compute V=(S^2)mod N where S is the Secret key between 0 to N-1
- **Value of N and V will be public to both Client and Server
- Compute X= (r^2)mod N and send it to the server.

Server side

- Server in response sends challenge C={0,1} to the client.
- Client on receiving challenge(C) computes y=r*(S^C)mod N called response and then sent it back to the server.
- Server checks if Y^2= X.V^C mod N
- If Y^2 == X.V^C mod N
- Then the client proved himself and secret is verified
- Else
- Then client hasn't proved himself and secret is not verified