Project Description

The server and client program designed attempts to simulate Paillier encryption to

create an electronic voting algorithim which uses socket programming concepts..

Upon users entering a port number for the server and they will be prompted to enter

any two numbers which would then be multiplied and their product used in the

generation of two keys, a private key which the server should keep and a public key

that is sent to clients that are connected. The server also sends messages to clients

indicating the options for the candidates to vote for and poll opening.The clients

would then send the server a scrambled message back to the server containing the

candidate chosen. The server would then unscramble this message and tally the votes

for each candidate; sending a message to the clients with the winning candidate. The

clients and server would then terminate.

Program Design

Server:

The server is designed to take in take in a port number inputted from the command

line by the user. Upon starting the server prompts for two numbers which are used in

the generation of two keys(public and private key). A Socket is then created to bind

the port number entered by the user to the server and to accept incoming connections

from clients.The server then sends messages to the clients after they connect. The

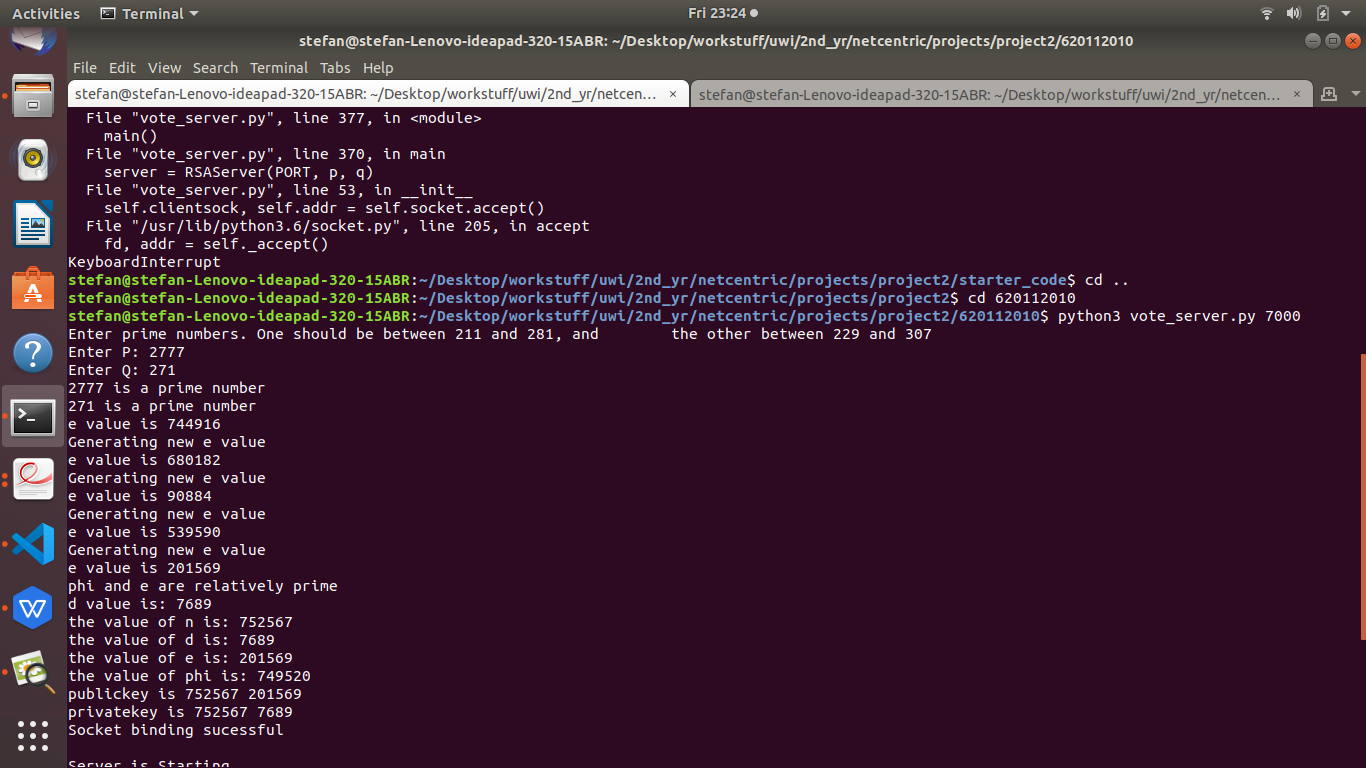
server then listens for replies from clients.

Clients:

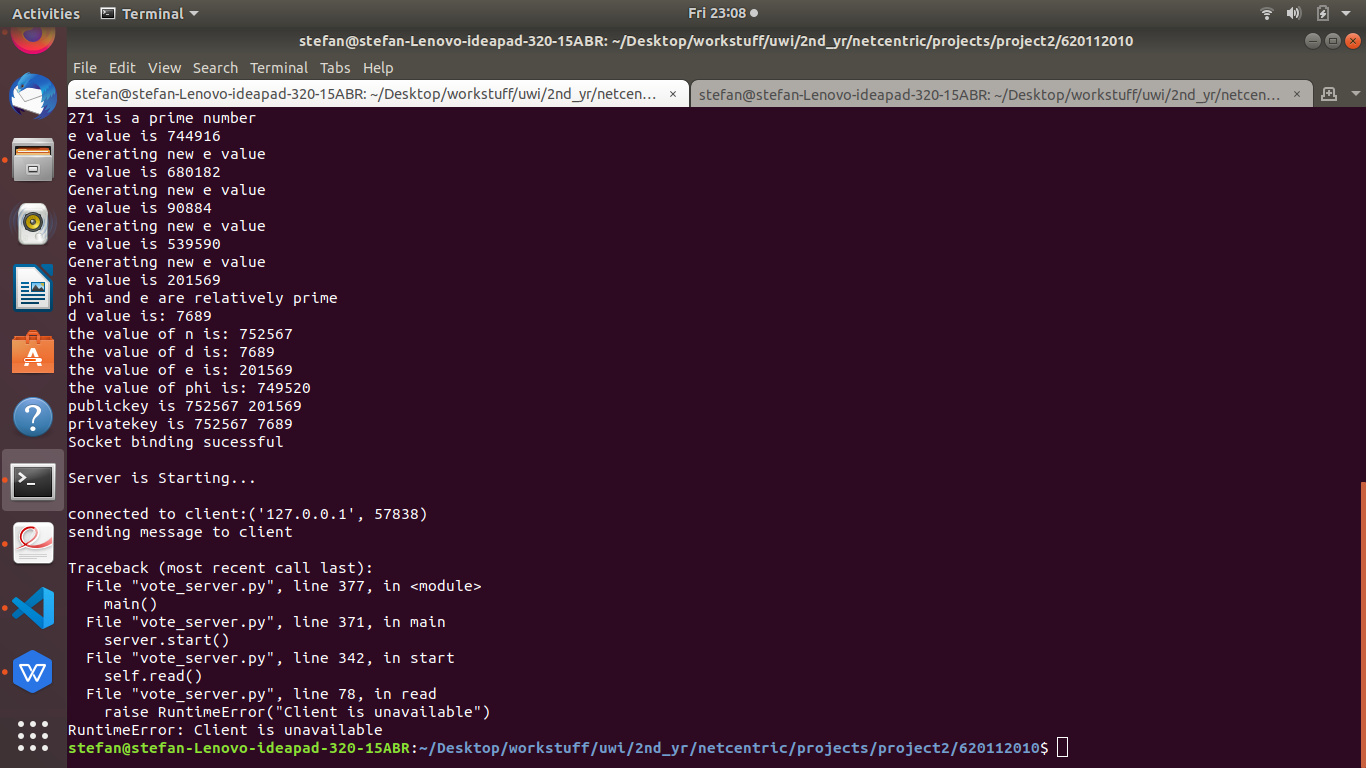
The clients are also designed to take in port number and host from the terminal to

connect to the server. Upon entering the port number and host it will connect to the

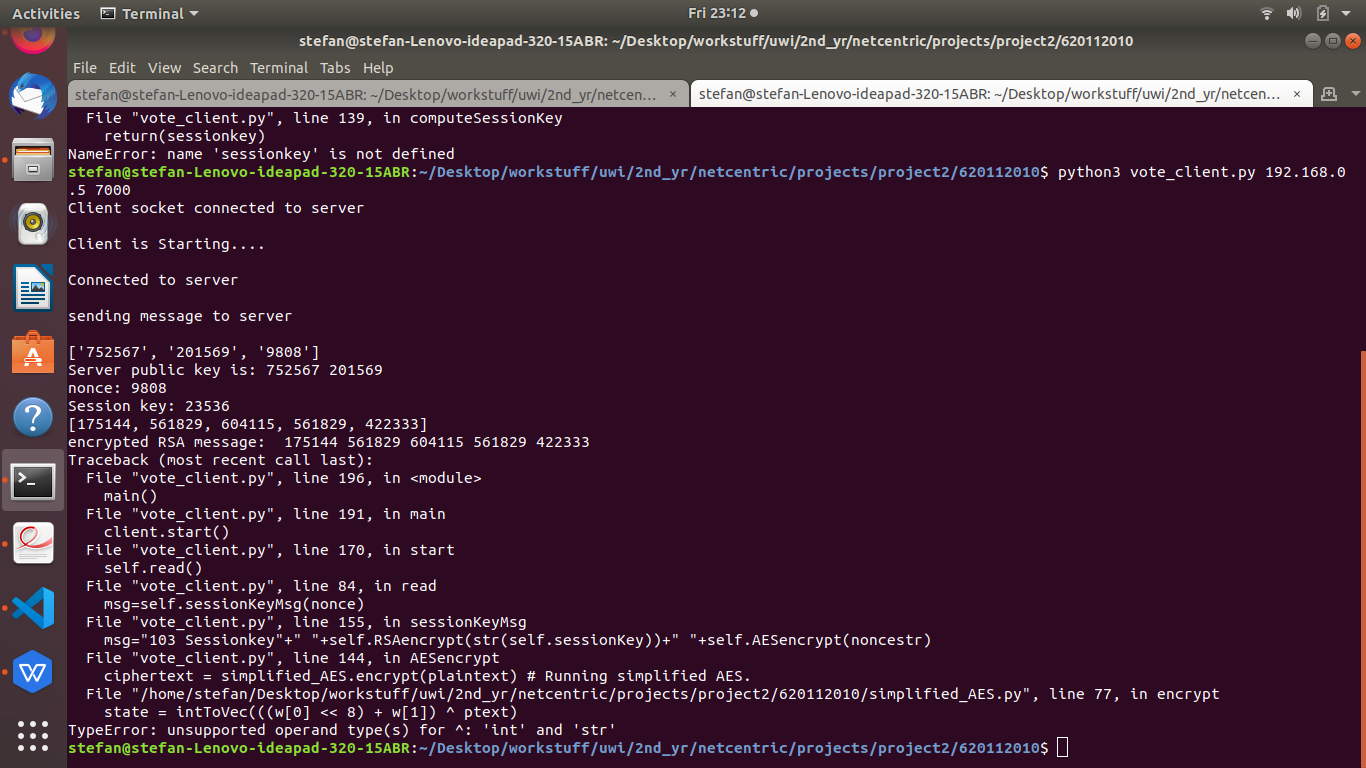
server and send a hello message.



Screenshot showing server sucessfully generating its keys



Screenshot showing server connecting to client



Screenshot showing message being received by client from server with value succesfully with RSA

tests

created a prime number checker function to check if p and q entered are prime.