(Comp2190)Netcentric Project 1

Id:620112010
Lecturer:Dr.Fokum

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:

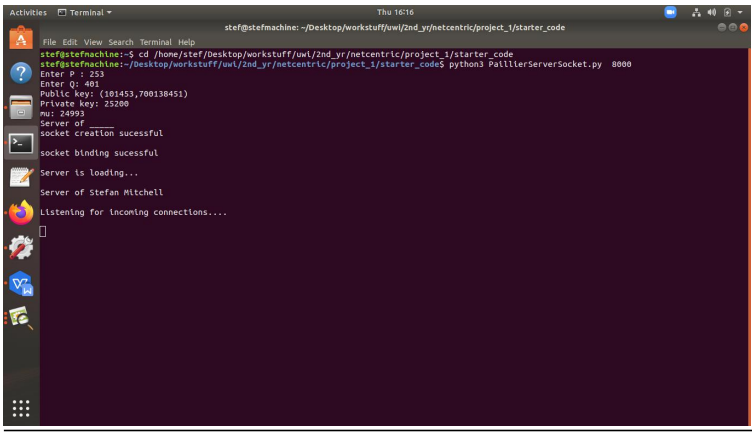
The server is designed to take in take in a port number inputted from the command line by the user. Upon starting the server prompts for two numbers which are used in the generation of two keys(public and private key). A Socket is then created to bind the port number entered by the user to the server 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:

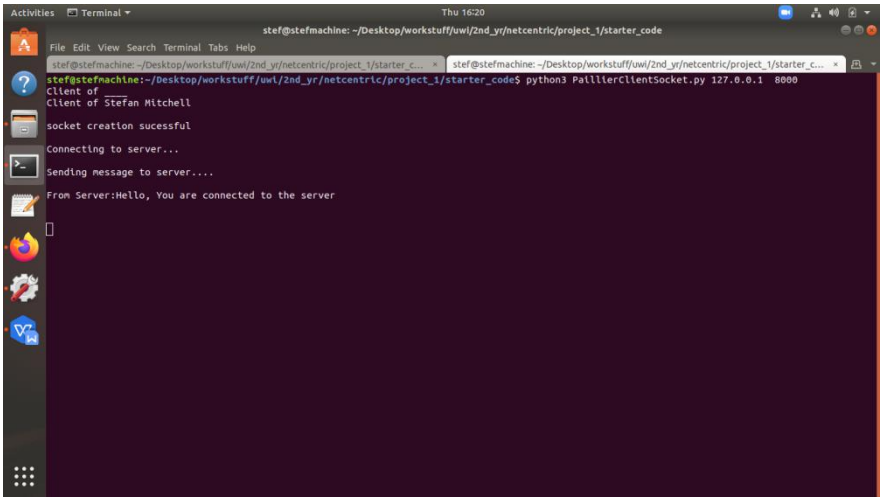
The clients are also designed to take in port number and host from the terminal to connect to the server. Upon entering the port number and host it will connect to the server and send a hello message. Afterwards it listens for messages from the server and replies with a scrambled message(this was not fully implemented in my python code solution, had trouble scrambling message with formula)

Screenshots:

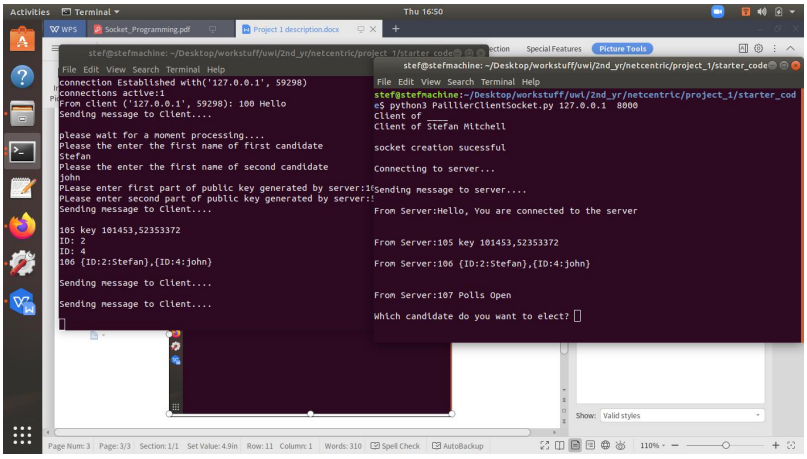
Server starting successfully



Client connecting successfully with server



Client and Server communicating


Activities
Terminal
Thu 16:50
WPS
Socket_Programming.pdf
Project 1 description.docx
Special Features
Picture Tools
stef@stefmachine: ~/Desktop/workstuff/uwi/2nd_yr/netcentric/project_1/starter_code
File Edit View Search Terminal Help
connection Established with('127.0.0.1', 59298)
connections active:1
From client ('127.0.0.1', 59298): 100 Hello
Sending message to Client....
please wait for a moment processing....
Please the enter the first name of first candidate
Stefan
Please the enter the first name of second candidate
john
PLease enter first part of public key generated by server:1
PLease enter second part of public key generated by server:1
Sending message to Client....
105 key 101453,52353372
ID: 2
ID: 4
106 {ID:2:Stefan},{ID:4:john}
Sending message to Client....
Sending message to Client....
stef@stefmachine: ~/Desktop/workstuff/uwi/2nd_yr/netcentric/project_1/starter_code
File Edit View Search Terminal Help
stef@stefmachine:~/Desktop/workstuff/uwi/2nd_yr/netcentric/project_1/starter_code$ python3 PaillierClientSocket.py 127.0.0.1 8000
Client of
Client of Stefan Mitchell
socket creation sucessful
Connecting to server...
Sending message to server....
From Server:Hello, You are connected to the server
From Server:105 key 101453,52353372
From Server:106 {ID:2:Stefan},{ID:4:john}
From Server:107 Polls Open
Which candidate do you want to elect?
Show: Valid styles
Page Num: 3 Page: 3/3 Section: 1/1 Set Value: 4.9in Row: 11 Column: 1 Words: 310 Spell Check AutoBackup
110%