**159.342 Assignment 2**

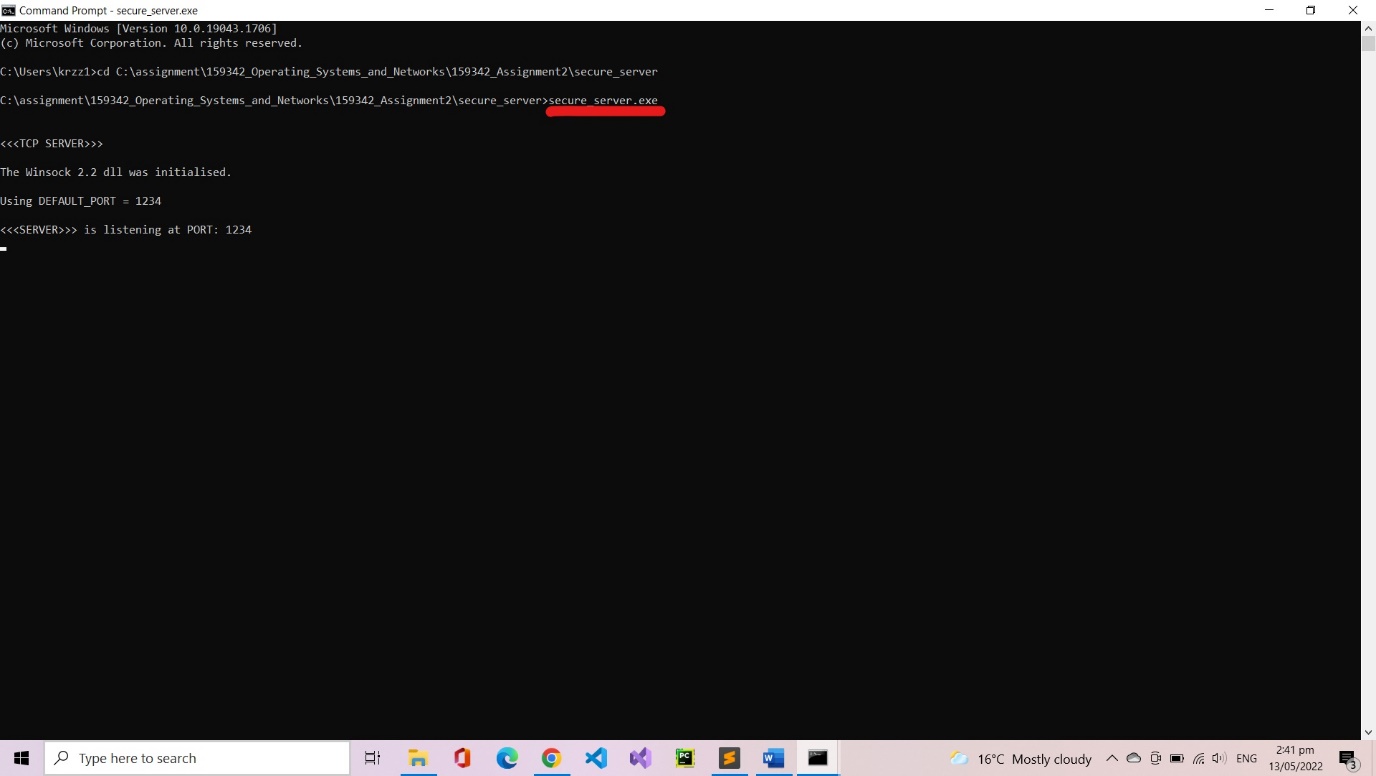
**RSA algorithm with Cipher Block Chaining**

Name: Mark Lee ID: 08493227

**Brief instructions of RSA program**

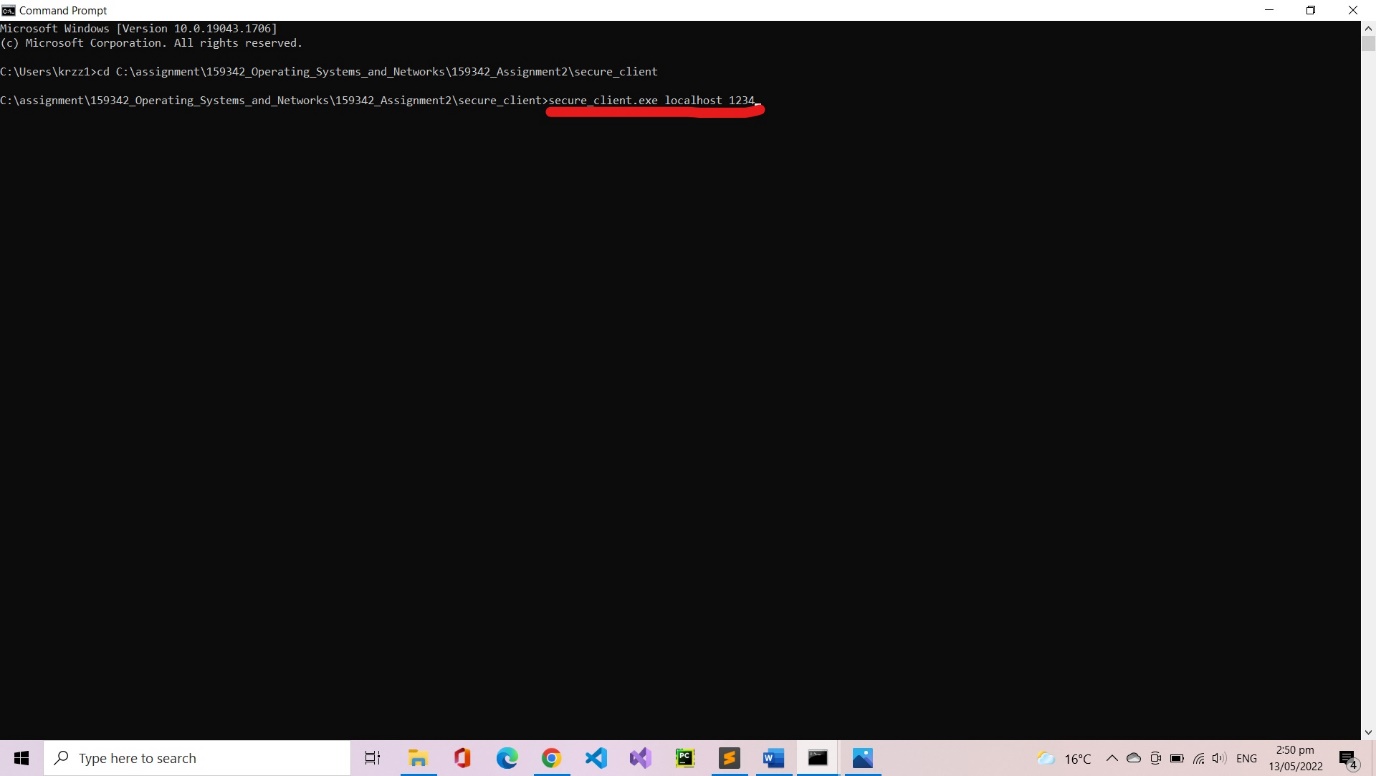
<<Server Side>>

Execute the program by ‘secure\_server.exe’. Server is up and running and is waiting for a client to join. As you can see port number is ‘1234’ which is default port number.



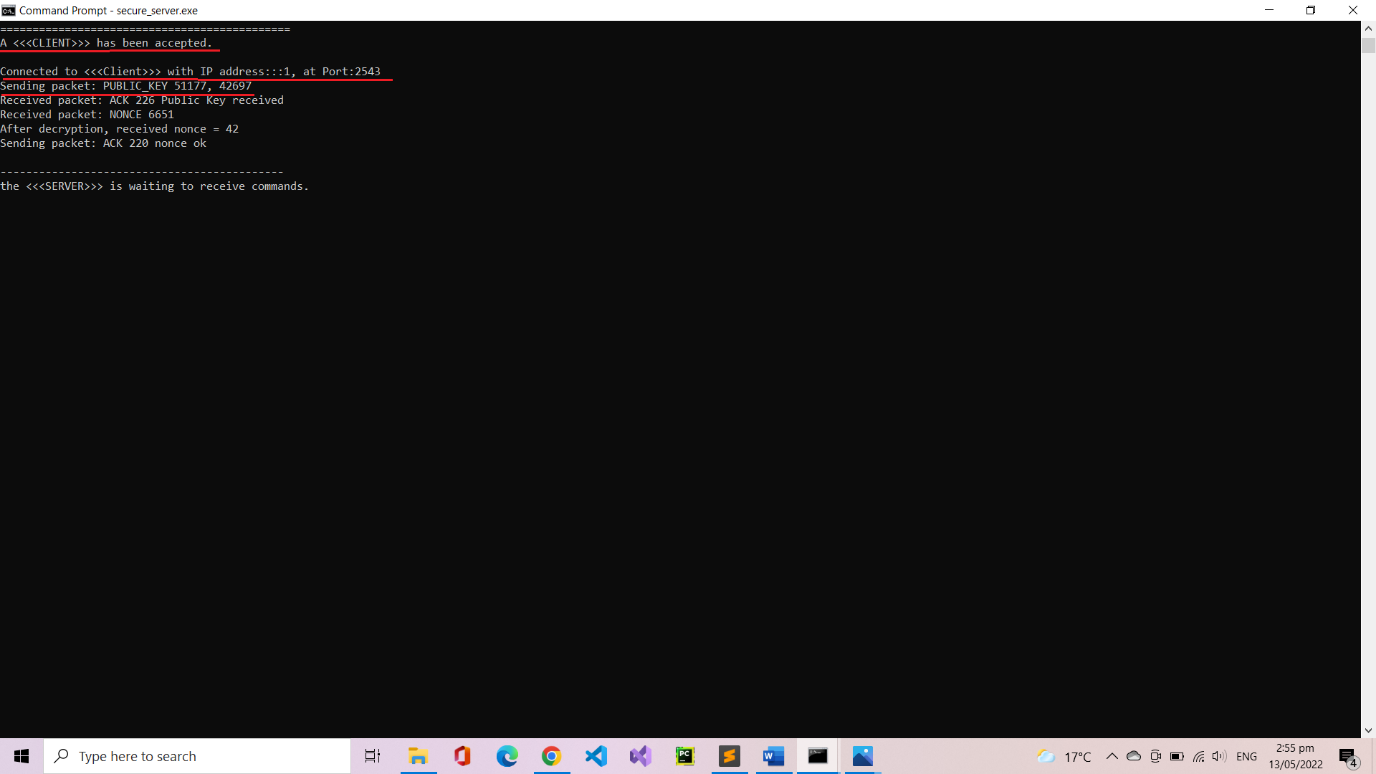
<<Client Side>>

Client connects to the server by typing ‘secure\_client.exe localhost 1234’.



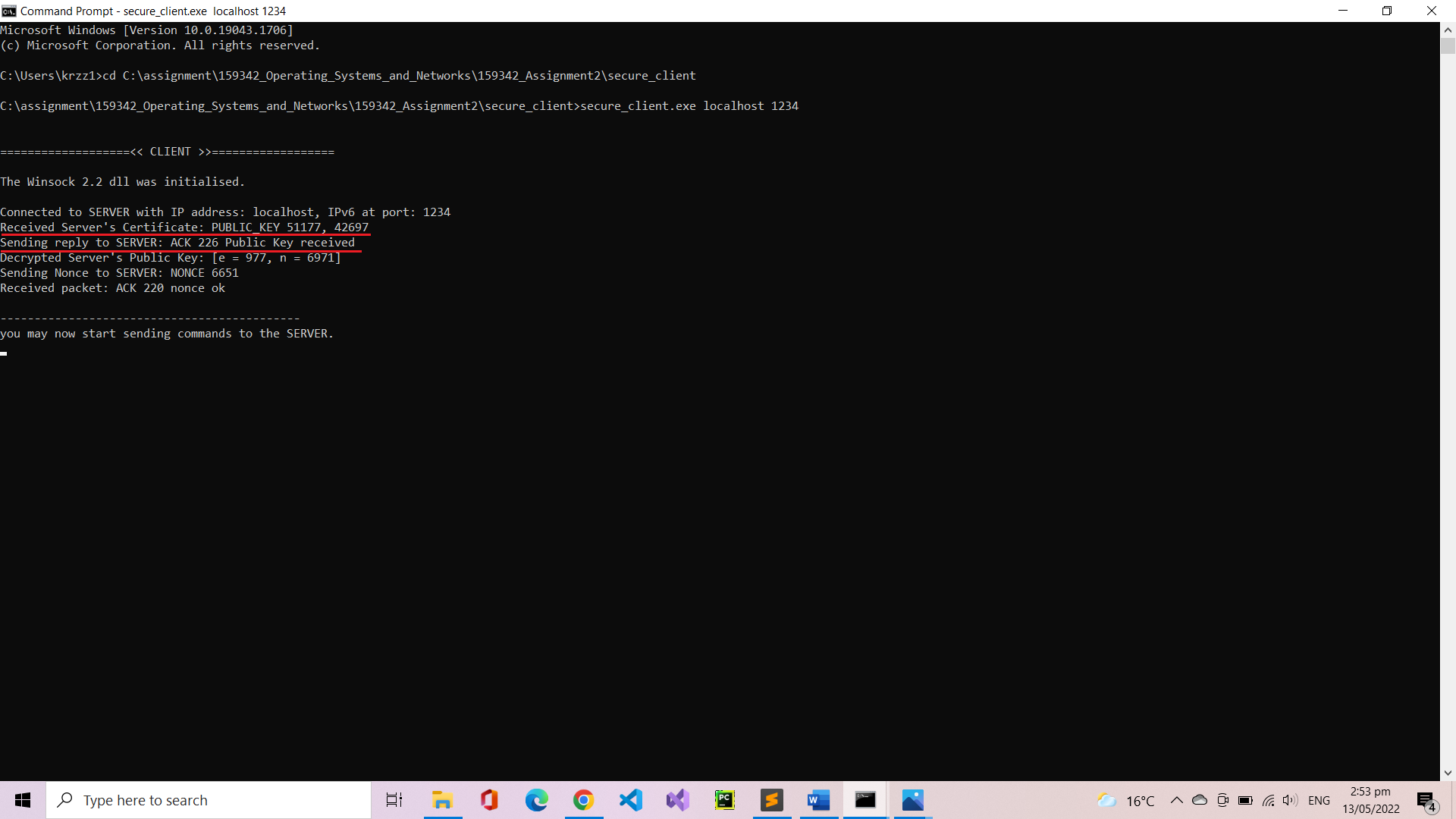
<<Server Side>>

Once connection has been established server acknowledges client and sends encrypted public key to client. (e = 51177, d = 42697)

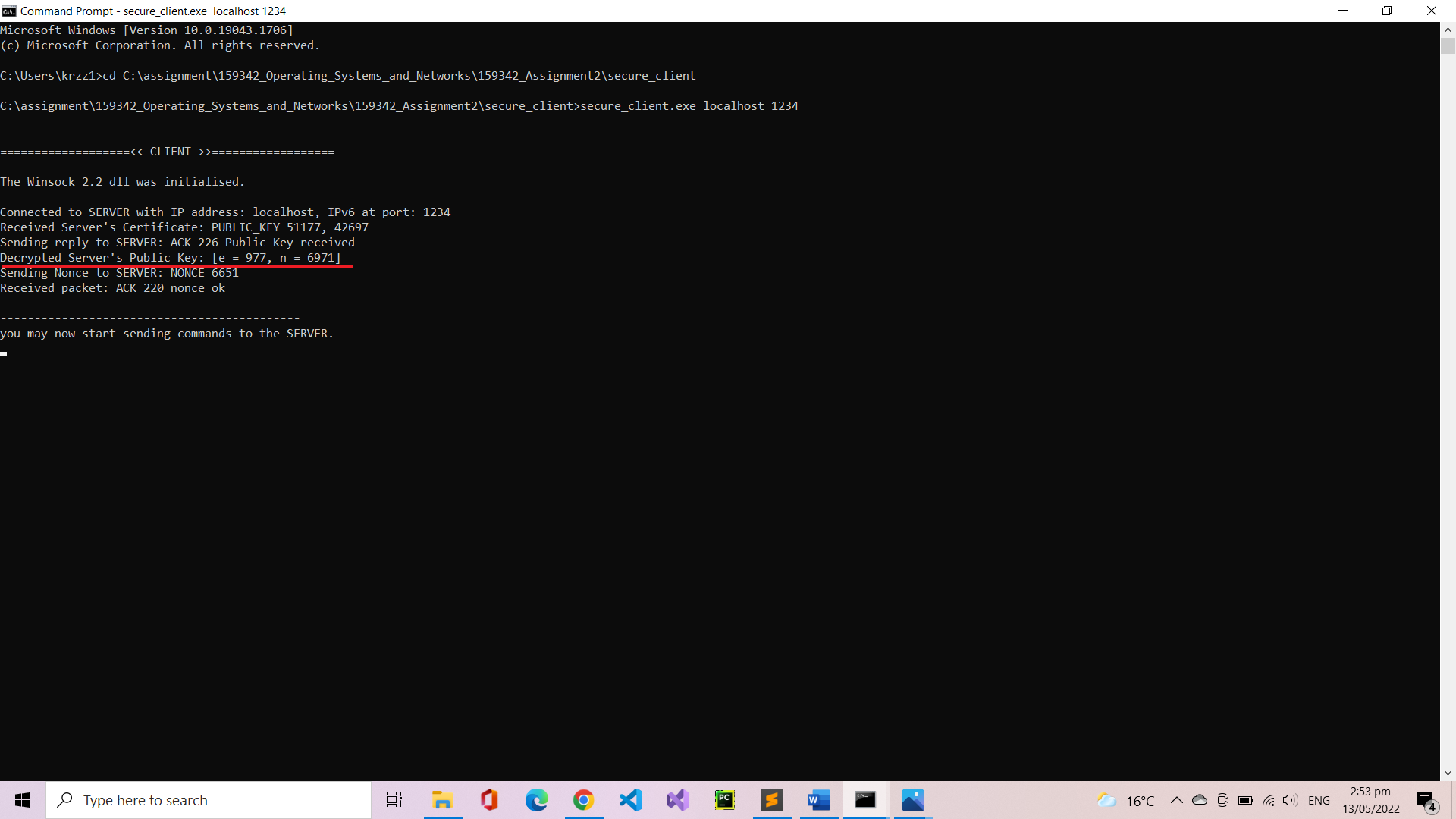


<<Client Side>>

Client receives encrypted public key (e = 51177, d = 42697) from server and send back 226 acknowledgement.

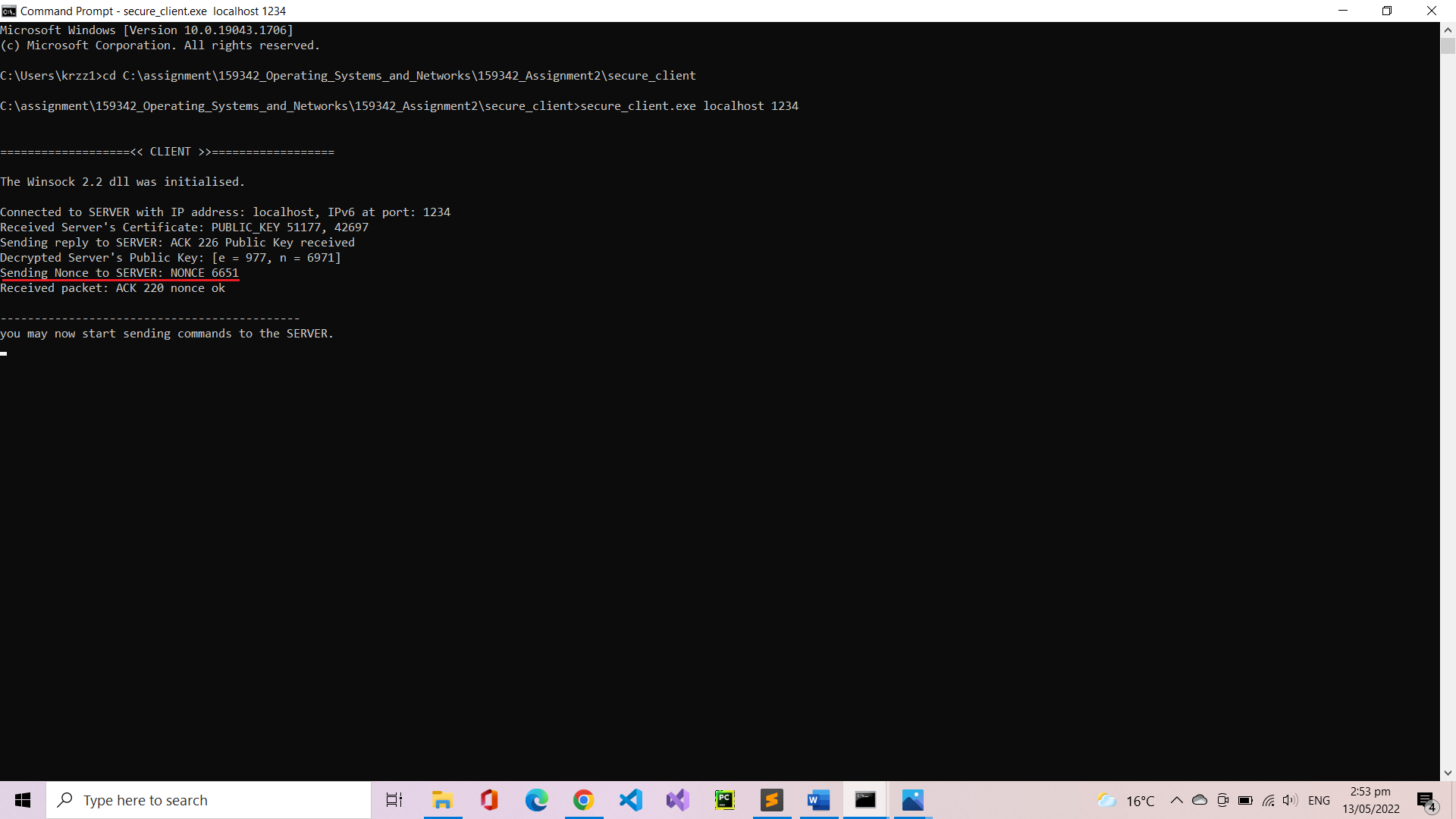


Client decrypts public key and gets [e = 997, n = 6971].



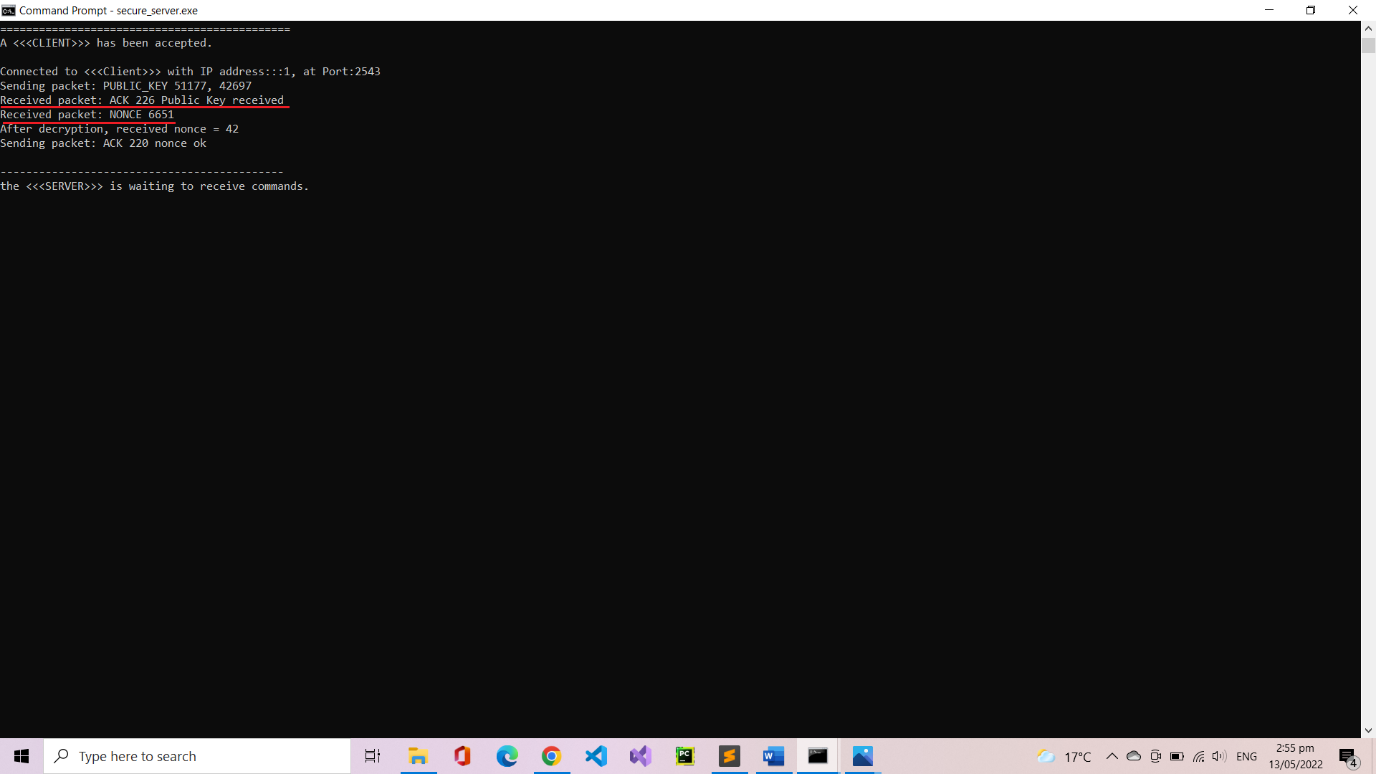
<<Client Side>>

Generates random nonce and encrypt it, sends the encrypted nonce to server.



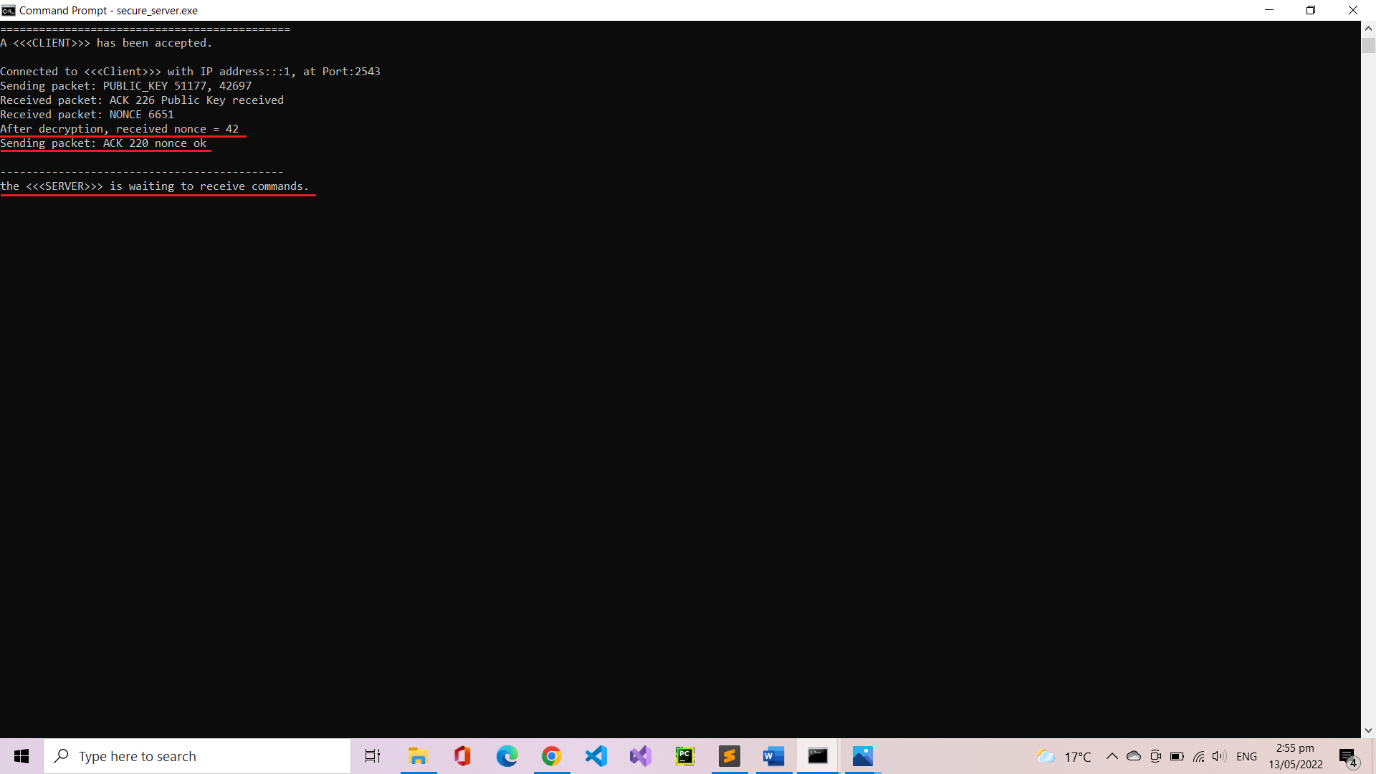
<<Server Side>>

Server receives “ACK 226 public key received” and encrypted nonce(6651).



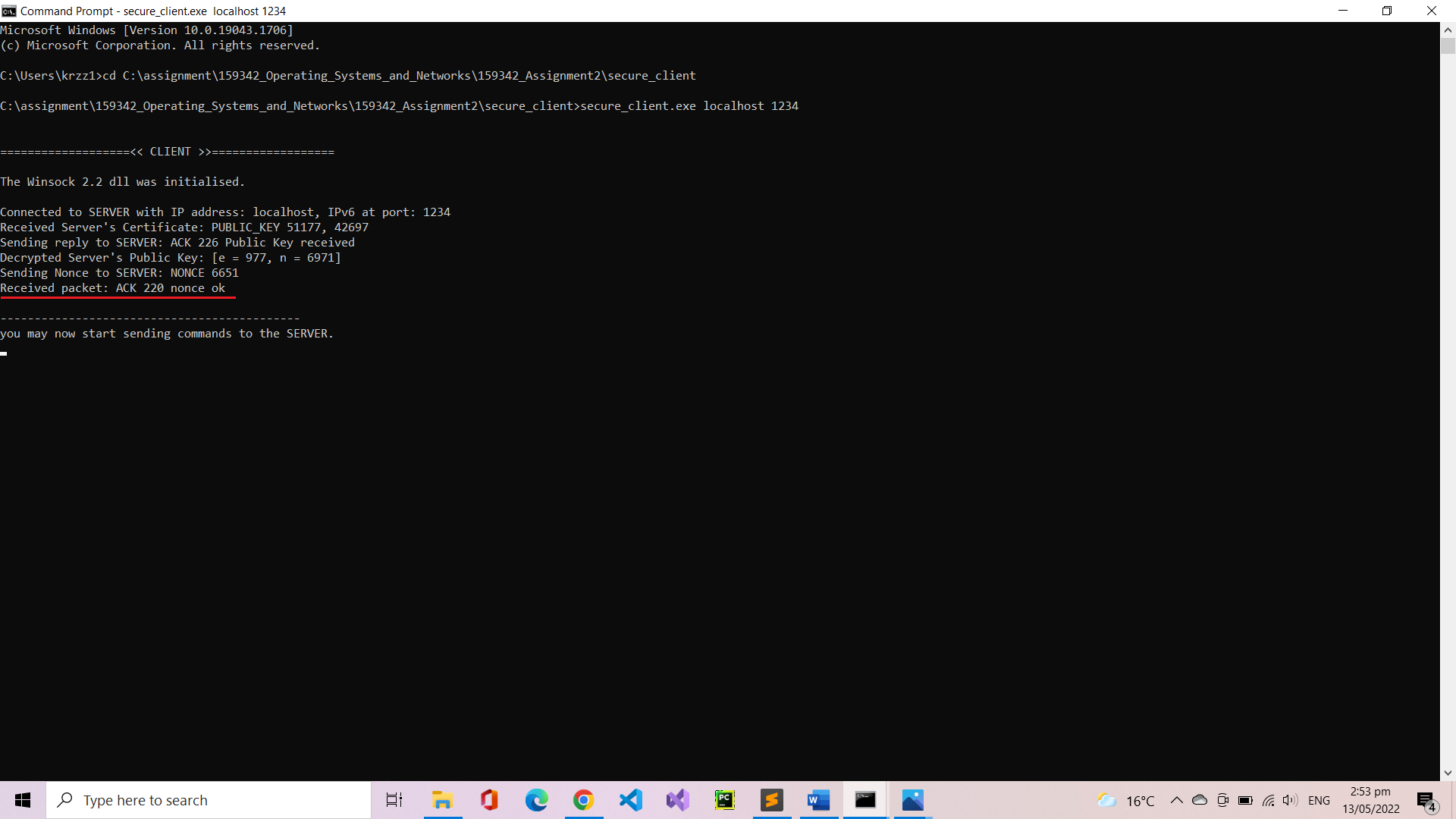
<<Server Side>>

Operates decryption algorithm on nonce(6651) and reveals decrypted nonce = 42. Sends “ACK 220 nonce ok” to the client and waits for input from the client side.



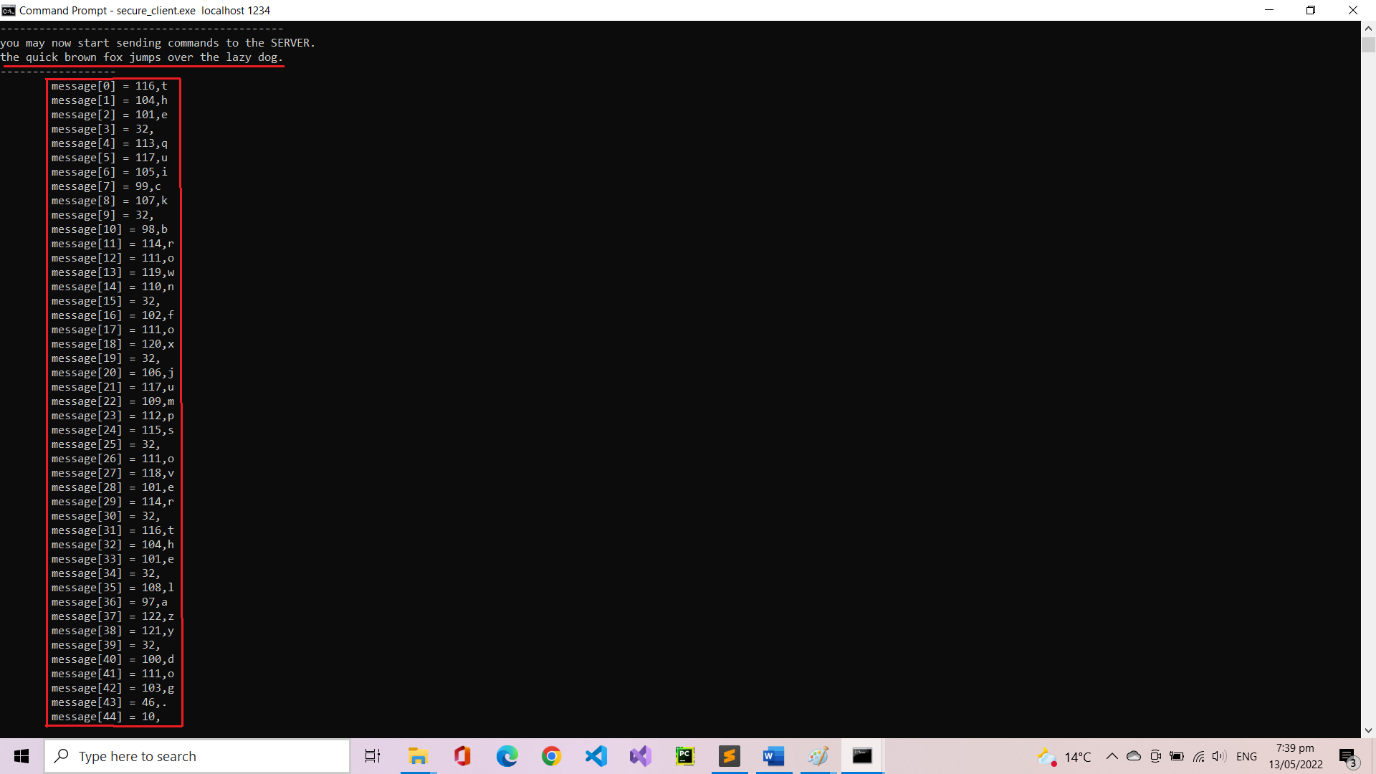
<<Client Side>>

Client receives “ACK 220 nonce ok” from the server and waits for a user input.

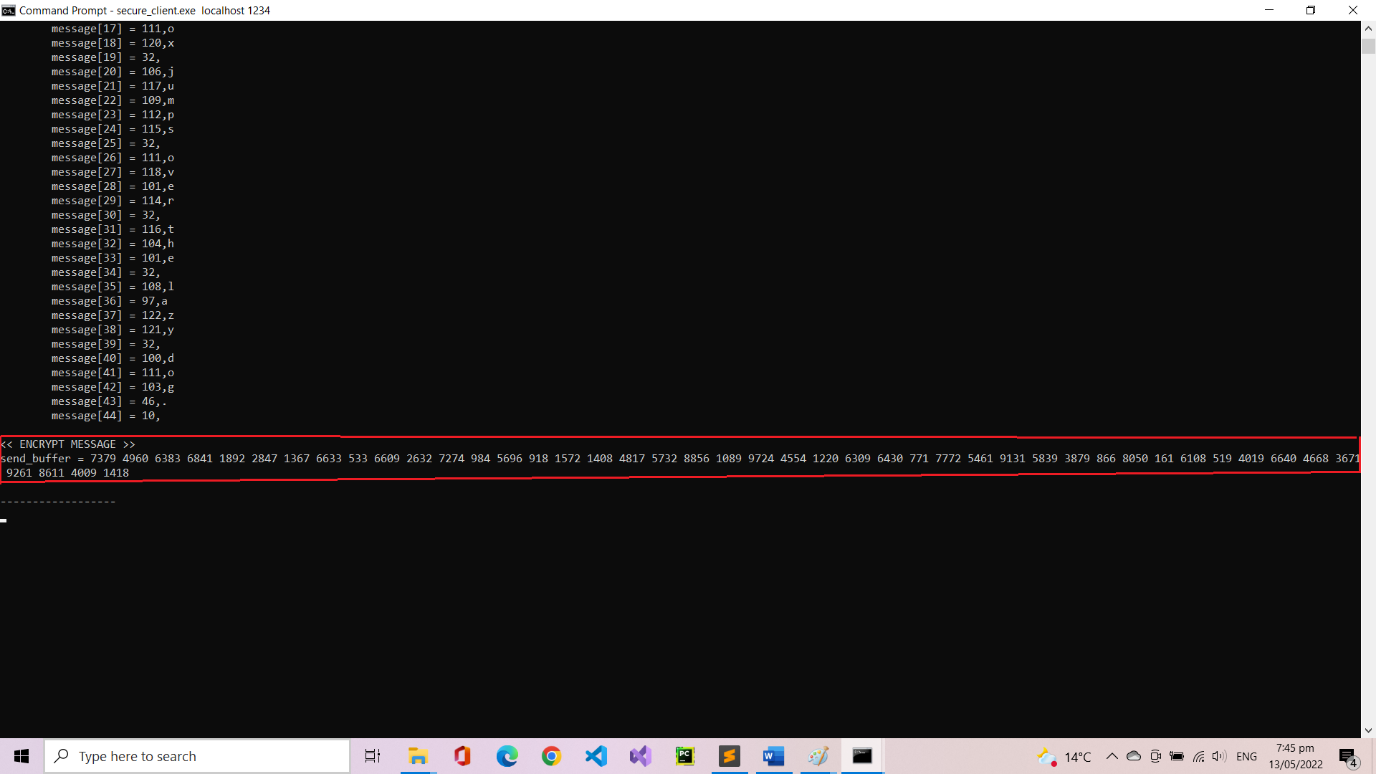


###Testing Input: “the quick brown fox jumps over the lazy dog.”###

Client types “the quick brown fox jumps over the lazy dog.”. Console displays the input string and individual letters with corresponding ascii code.

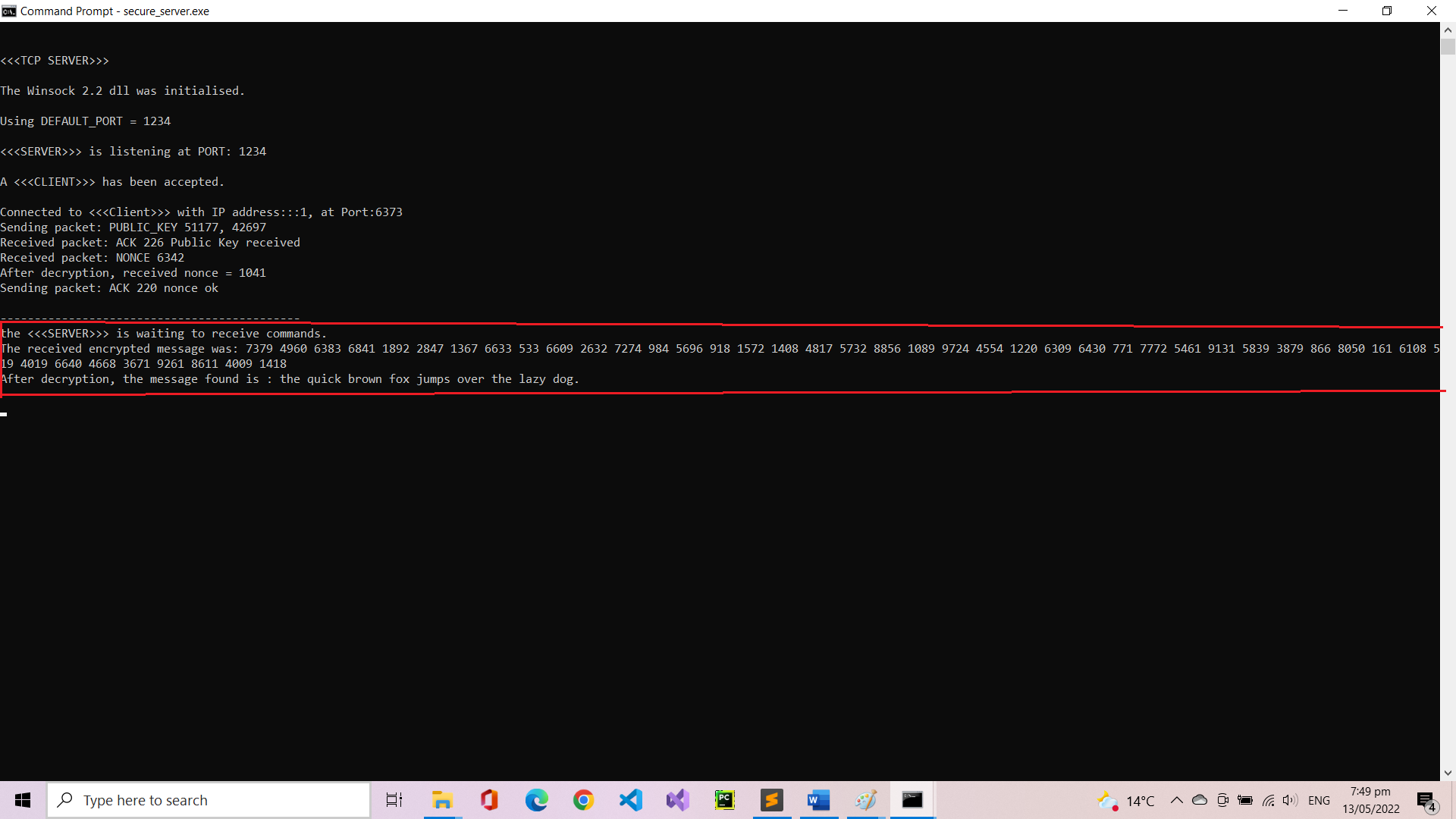


Then, encrypts the message, display the encrypted message and sends it to the server.



<<Server Side>>

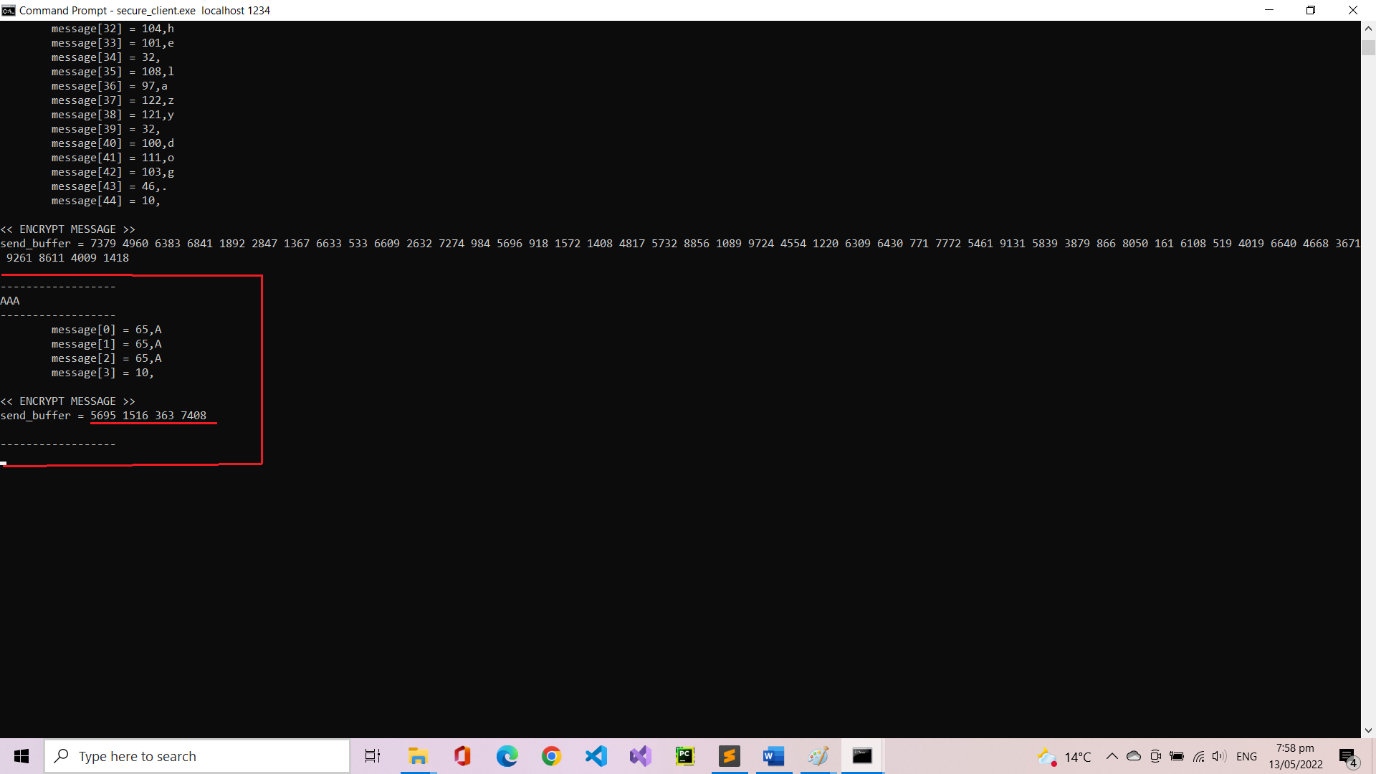
Server receives encrypted message from the client. Displays the encrypted message. Then, compute the decryption algorithm. After decrypting the message display the decrypted message on console, which decrypted the message without any error.



###Testing Input: “AAA”###

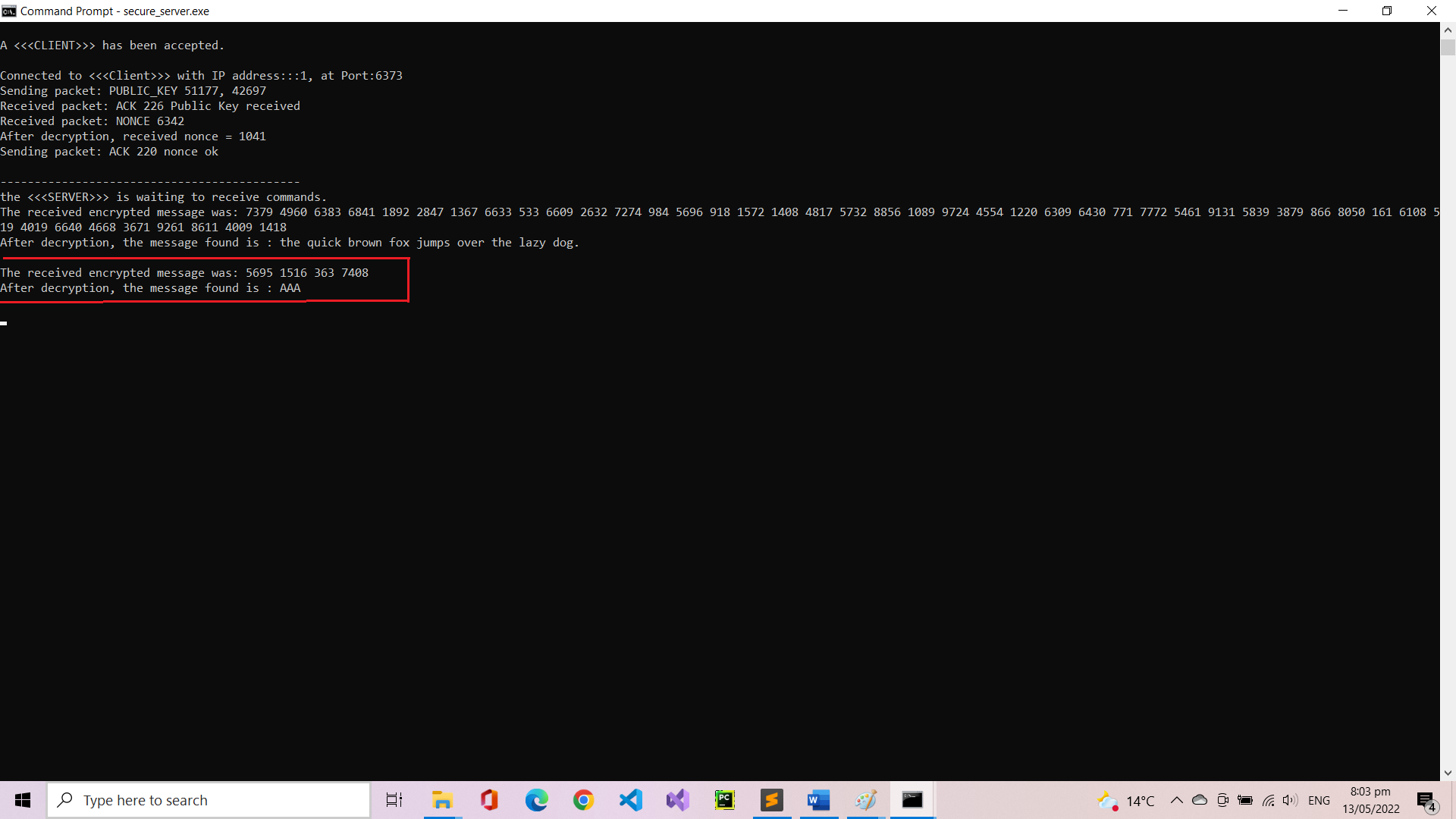
<<Client Side>>

This time client inputs “AAA”, as same as before, displays ascii number with individual letters. The encrypted message show no sign of duplication or pattern. Sends the encrypted message to the server.



<<Server Side>>

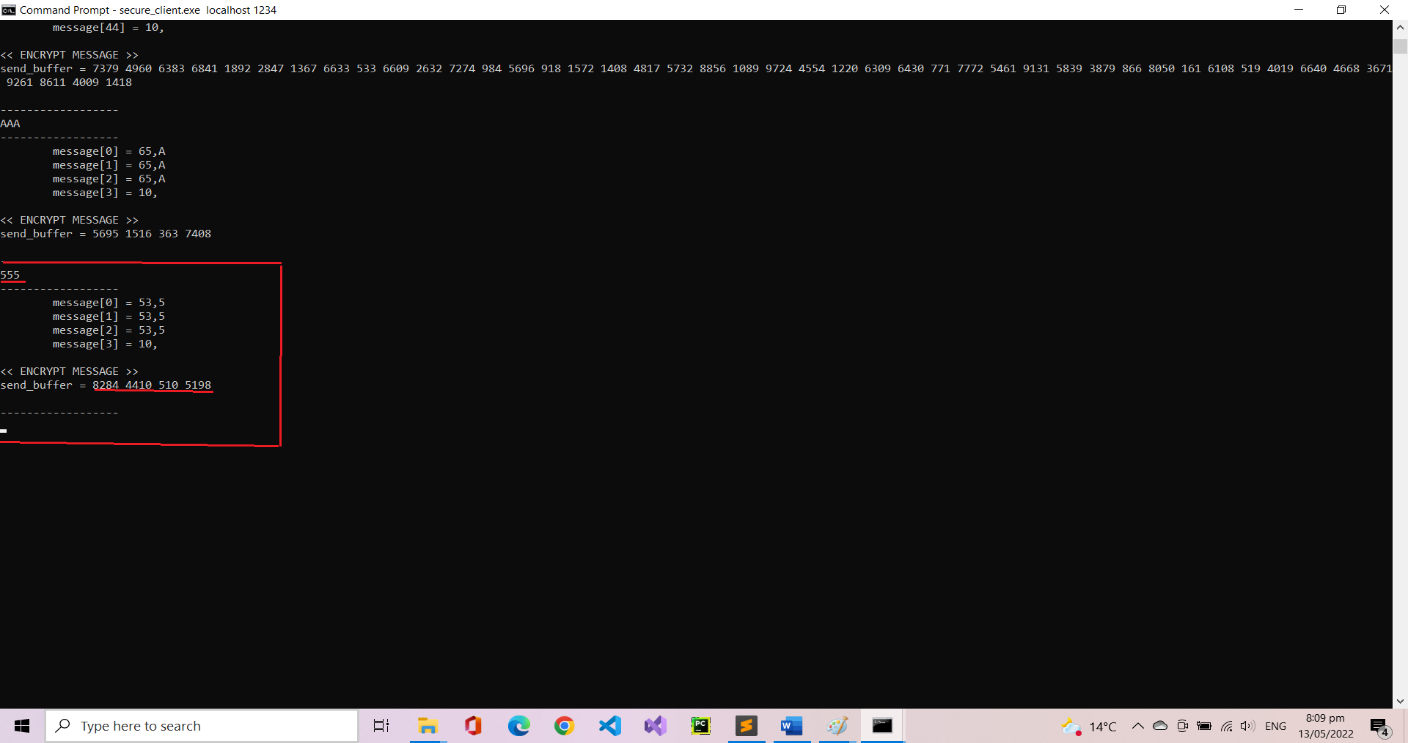
Server receives encrypted message from client. And decrypts using the same algorithm as before. Displays the decrypted message = ‘AAA’



### Testing Input: “555” ###

<<Client Server>>

Lastly, client types ‘555’, same as previously, encrypted message has no pattern or duplication.



<<Server Side>>

Server receives encrypted message, decrypts it, and display plain text ‘555’.

