Procedural report (project phase III)

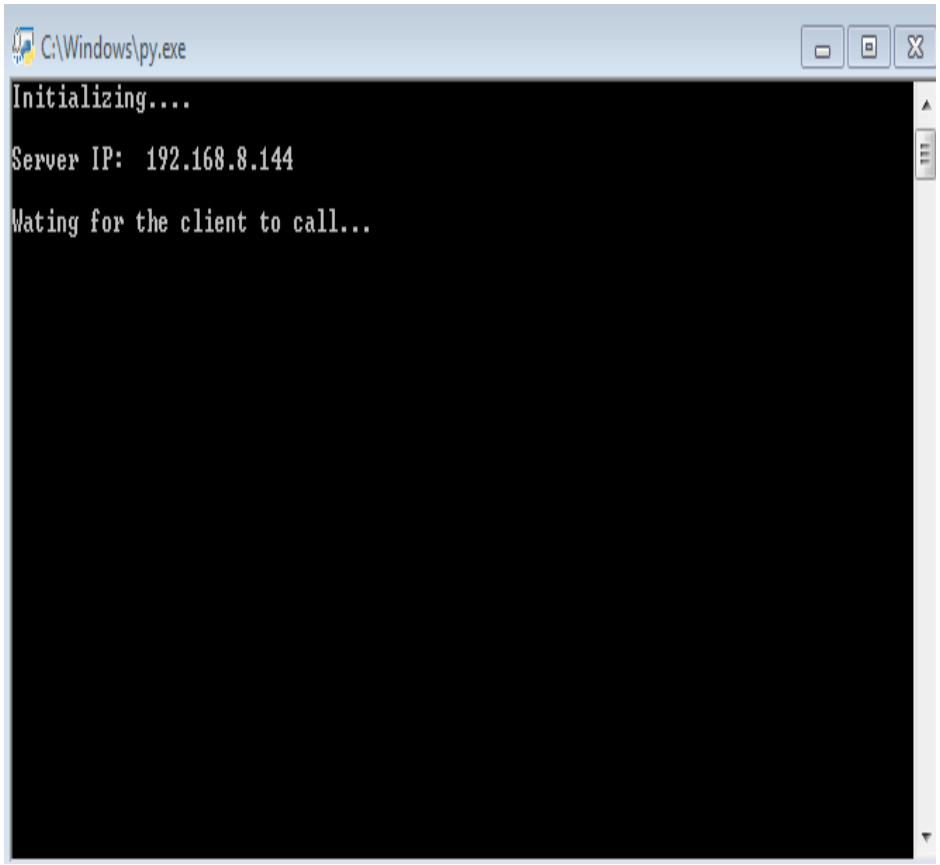
Name: Abdulwahab Hassan Alzahrani
ID: 201337310

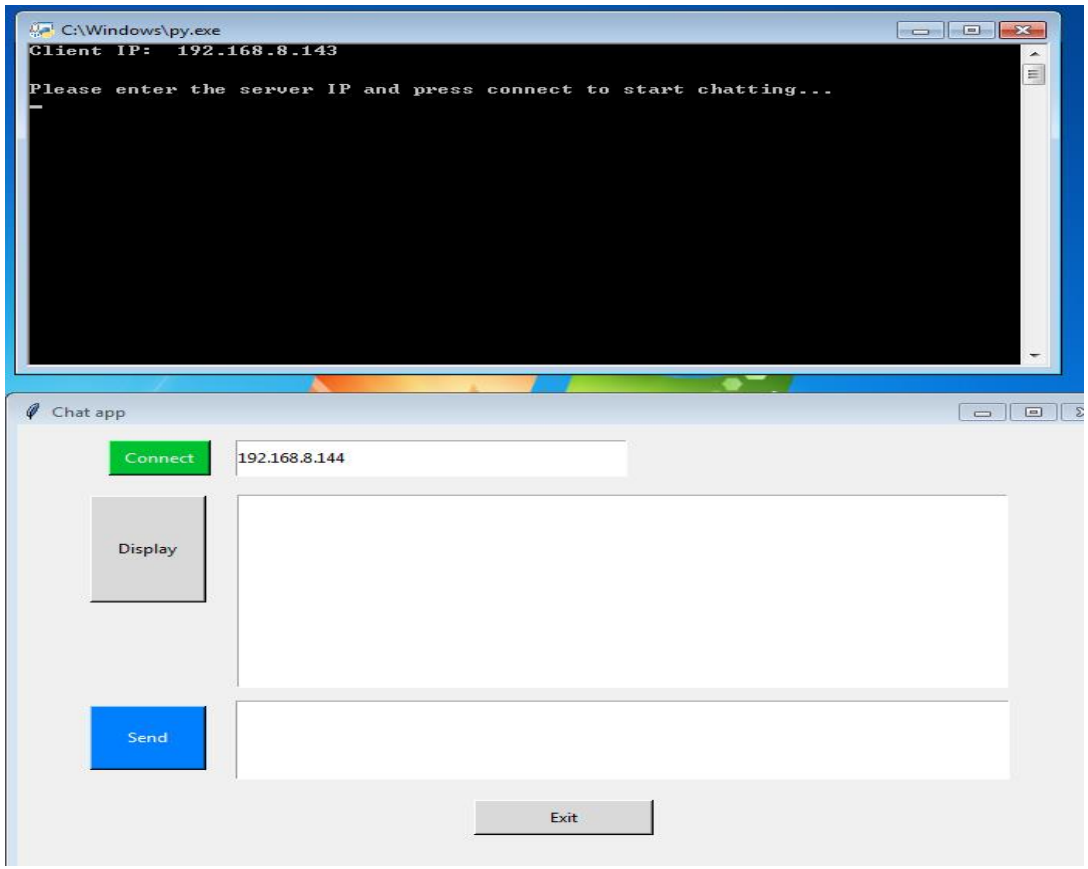
Abstract

This report shows the procedural process of the modified SSH protocol along with AES_256_CBC cryptosystem.

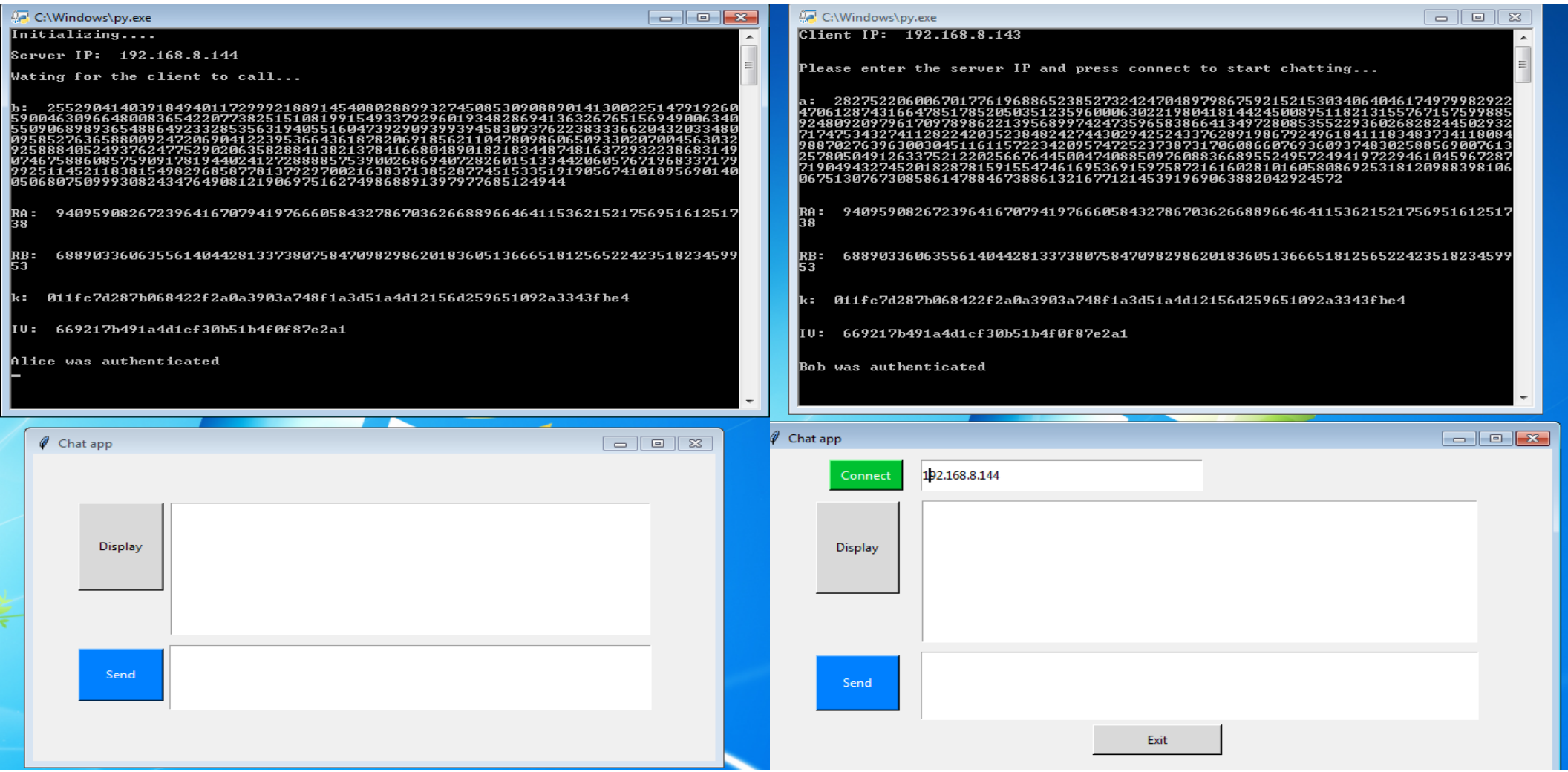
Left pictures are for Bob(server) and right pictures are for Alice(Client)

Test case 1_Session 1:

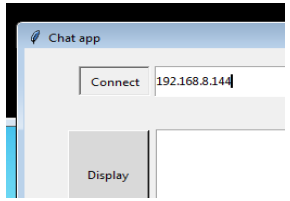


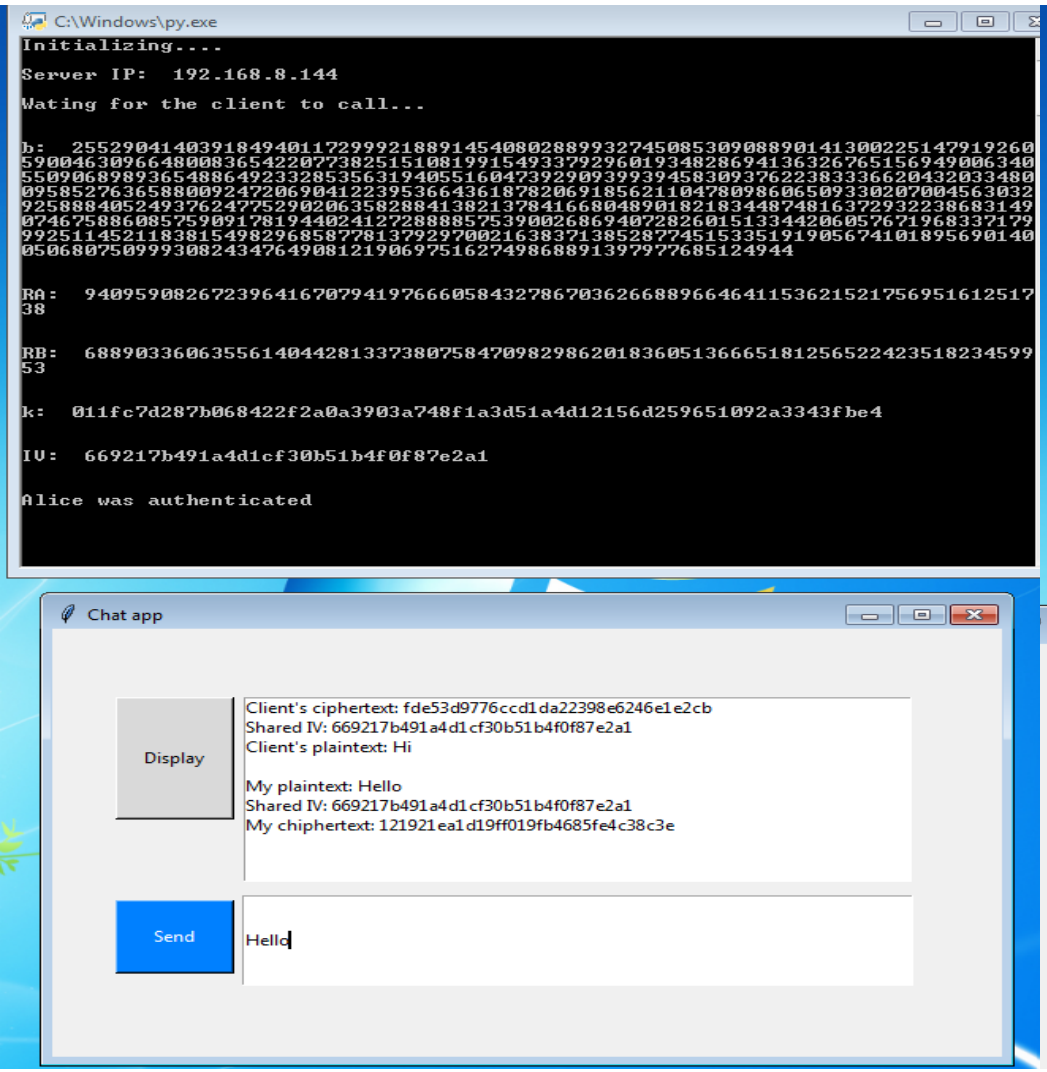


- Before clicking connect (same case for all remaining sessions)



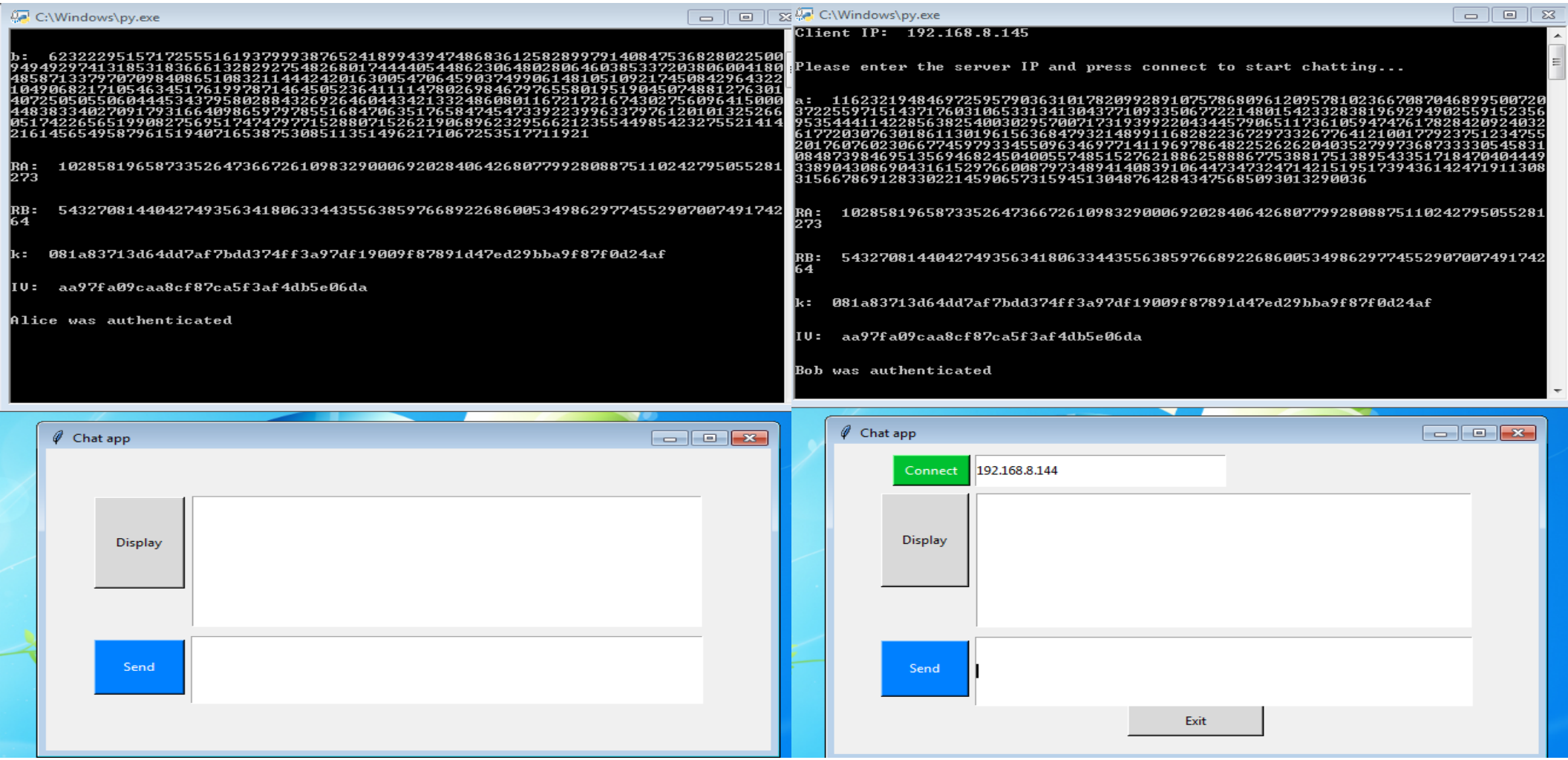
- After clicking connect, it will take few seconds (6 s) as delay for buffers to be loaded correctly.
- Alice prints the following (a, RA, RB, K, IV and if Bob was authenticated or not)
- Bob prints the following (b, RA, RB, K, IV and if Alice was authenticated or not)



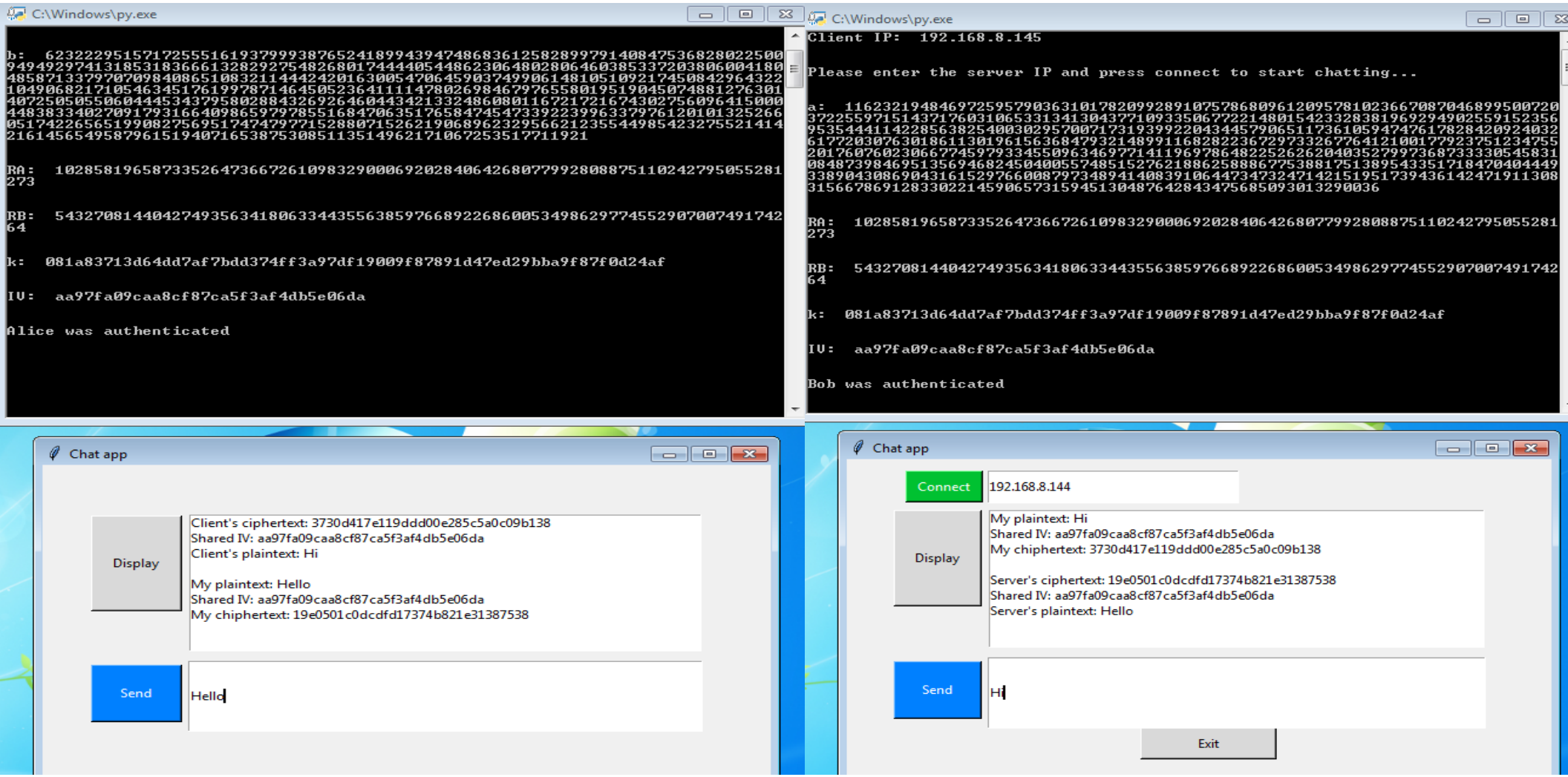


- They can chat as in phase II but with the key k

Test case 1_Session 2:



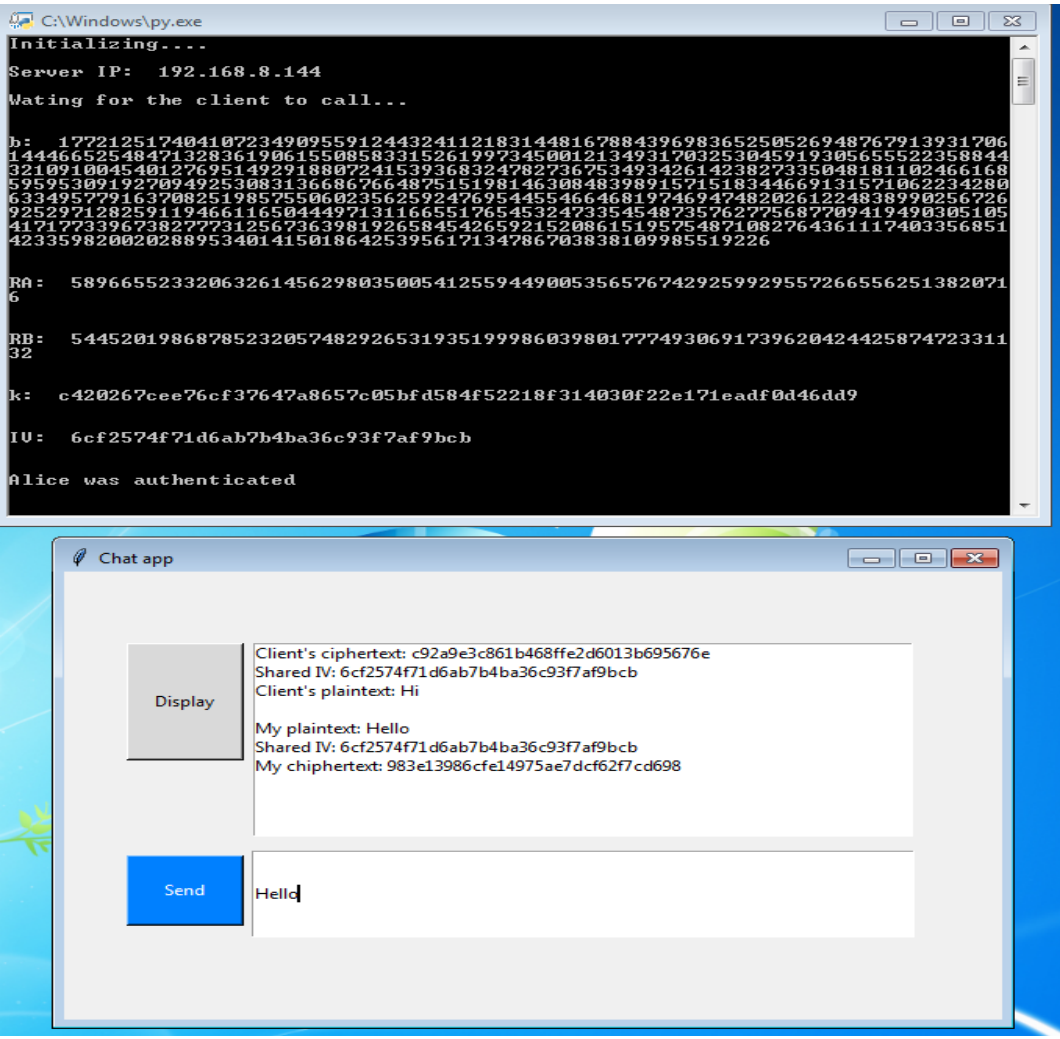
- After clicking connect, as you can see the values have changed



- They can chat as in phase II but with the key k

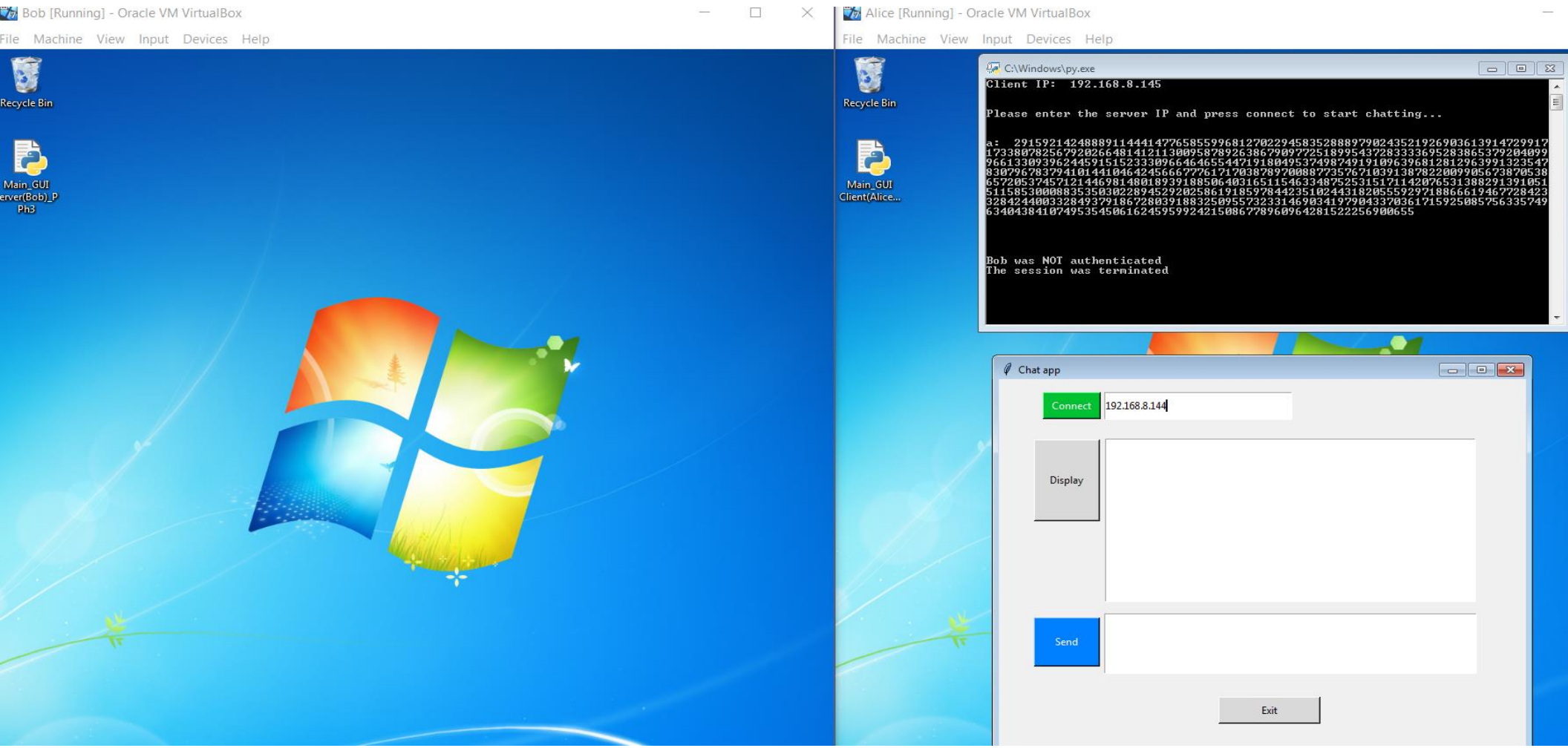
Test case 1_Session 3:

- After clicking connect, as you can see the values have changed

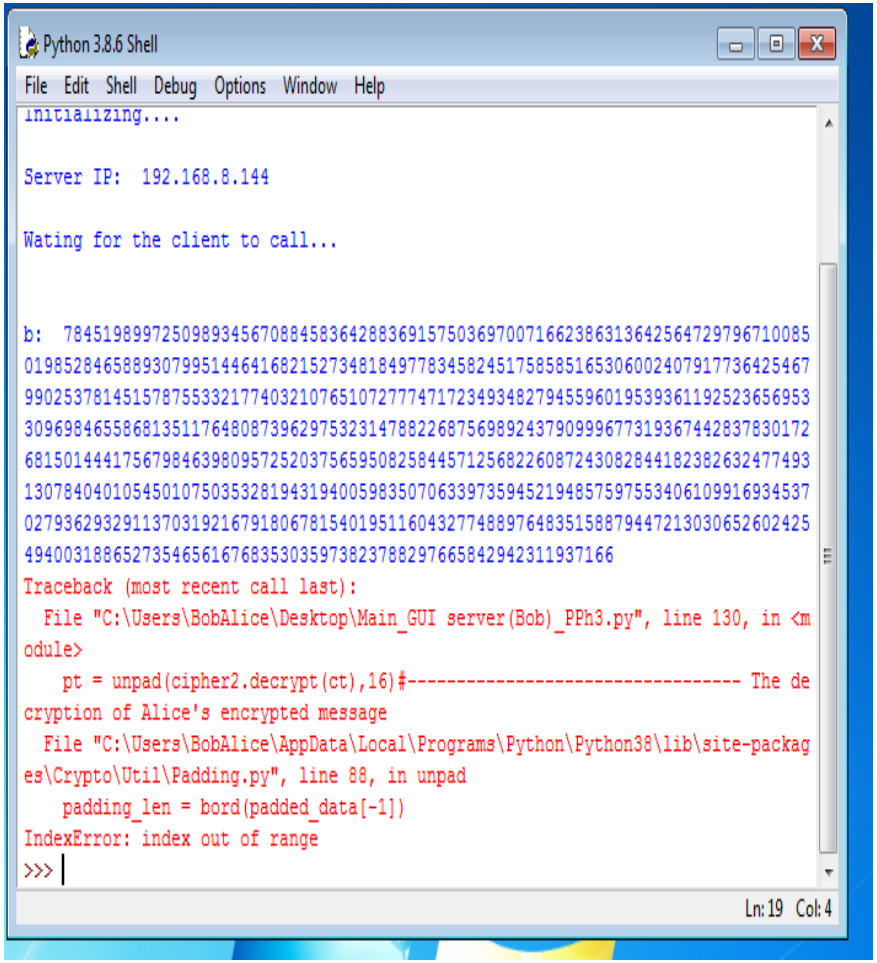


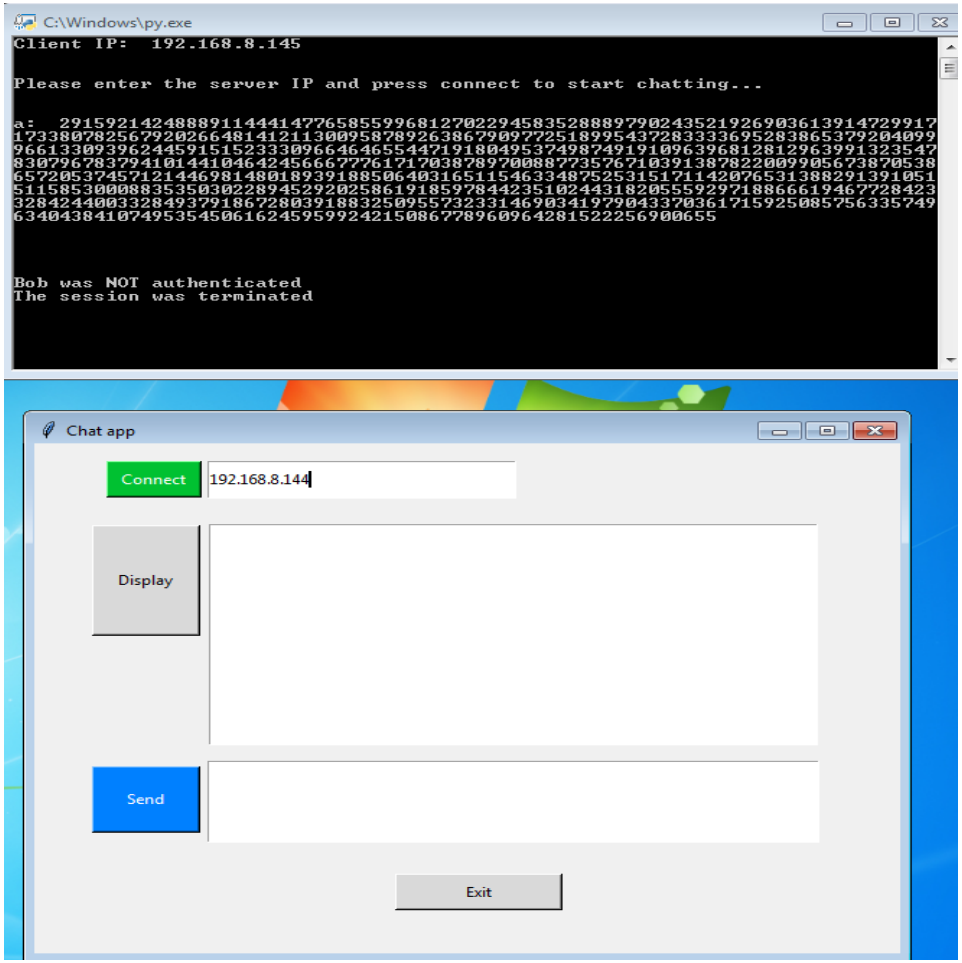
- They can chat as in phase II but with the key k

Test case 2



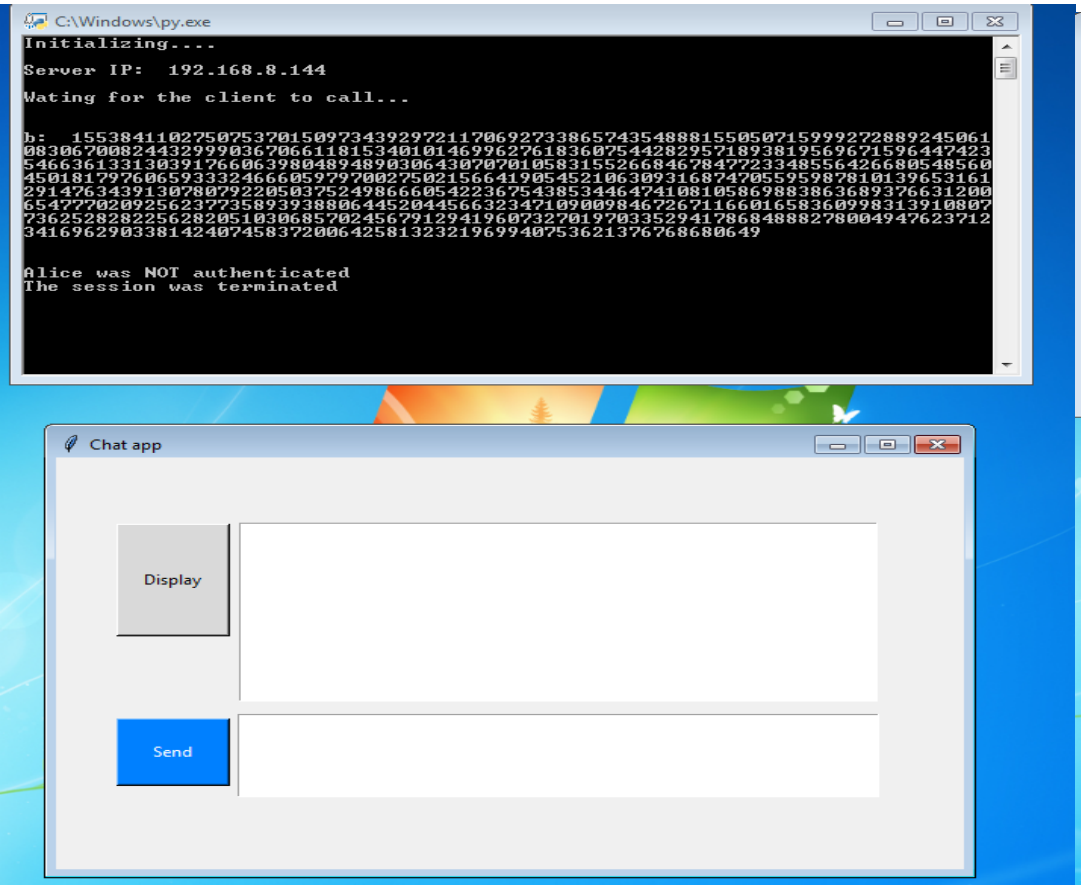
- After connecting to Bob, the following will happen, (a) will be printed at Alice's side and (b) will be printed at Bob's side then the program find that H_Bob is not as H then Alice will terminate the connection.

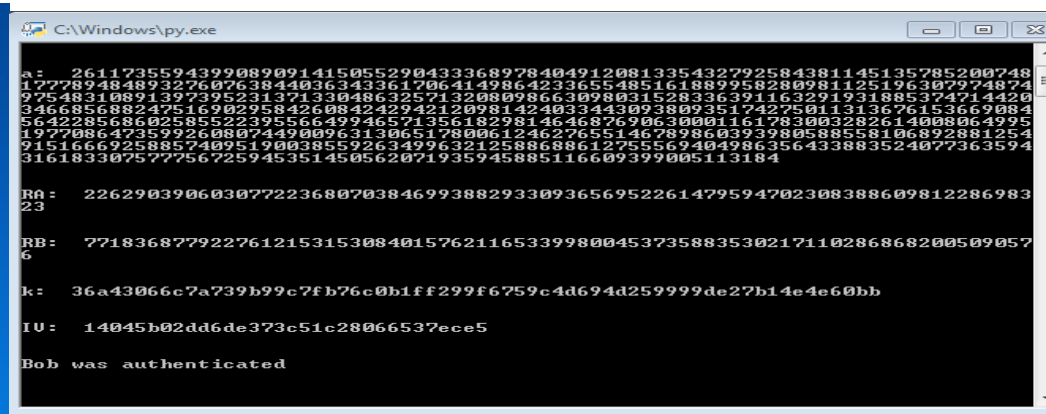


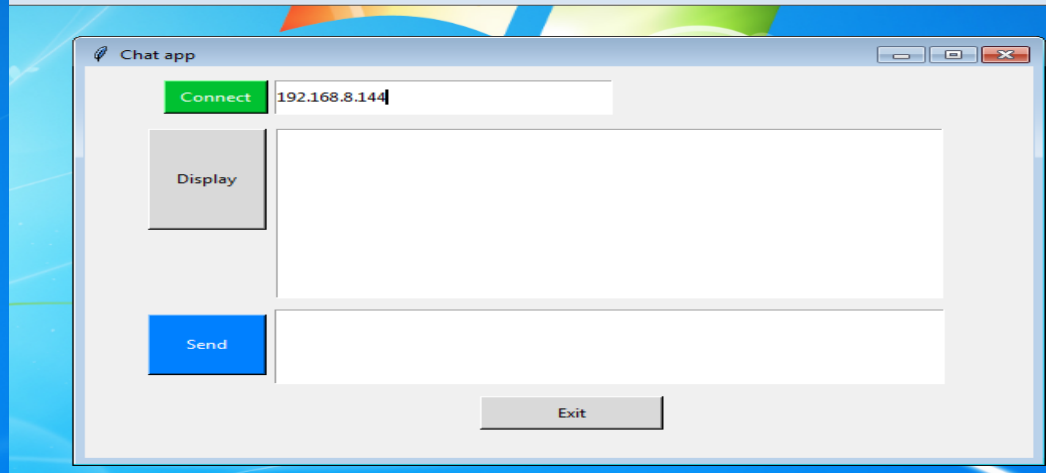


- The same as above but on the shell, so you can see b was printed and the error shown is due to the termination from Alice's side.

Test case 3







- Bob was authenticated by Alice but Alice was not authenticated by Bob so the connection was terminated by Bob after Bob had compared H_Alice with H and he found it not matching.