Logo

Description automatically generated

CSE4057 - Information Systems Security Project 2

150117060 Ahmet Hakan Şimşek

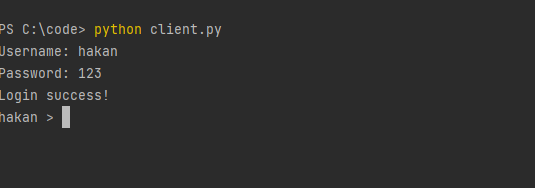
150116062 Muhammed Bera Koç

150119740 Senanur Güvercinoğlu

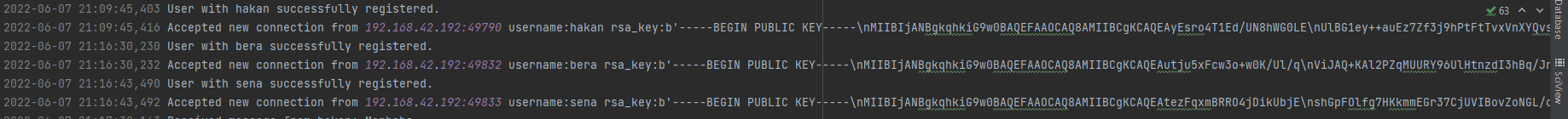
In this project we have built on previous term project, added the project additional security.

To run client we need to run server, by running server, server creates its own public and private RSA key pairs and store them.

To log in to program user need to enter previously registered username and password or if new registration is in process then program creates new user with password that is saved in data.json file



After users logged in to program, then they are in public chat where anyone’s message is seen by everyone. Also after log in, each user creates its own public private RSA key pairs and sends their public key to server to as certificate. In certificate authorithy(server) every users’ public key is store as encrypted with servers public key which mean they are only by decrypted with server itself

Also in server their public keys are written into log file which will serve as certificate authorityText

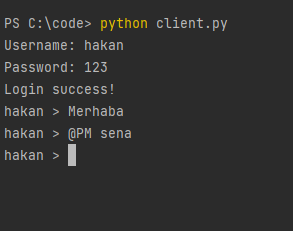
Description automatically generated Graphical user interface, text

Description automatically generatedGraphical user interface, text, application

Description automatically generated

In public chat we did not used any crytology

But users can be get in peer to peer private chat by using “@PM ” with name prefix and handshake phase starts



And user send its public key with nonce to requested user by message as follows

Text

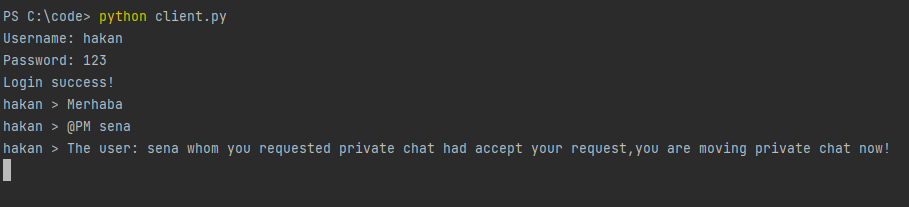
Description automatically generated

If user press y(yes) then, it gets requester’s(hakan) public key by verifying from certificate authority(server) which is encrypted with server’s private key.

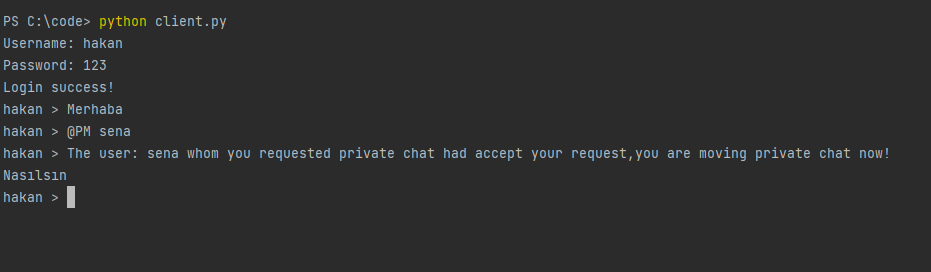
Text

Description automatically generated

When requested user press y(yes), user sends its public key and sends nonce, AES key, IV, HMAC encrypted with pair’s public key which can only be decrypted with pair’s private key.



After AES key is distributed to other side with RSA encryption, then they can send messages each other by using AES encryption and those messages sent with AES are not seen by anyone else. Also messages are hashed with message authentication code(HMAC) to provide integrity.



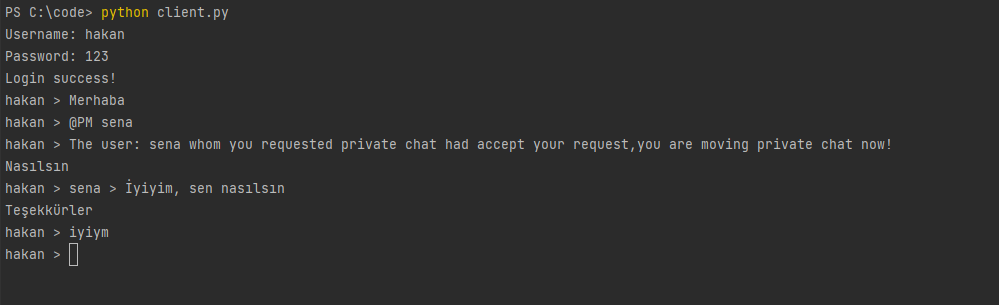
Text

Description automatically generated

Other users cannot see anymore sena and hakan’s private chat

Text

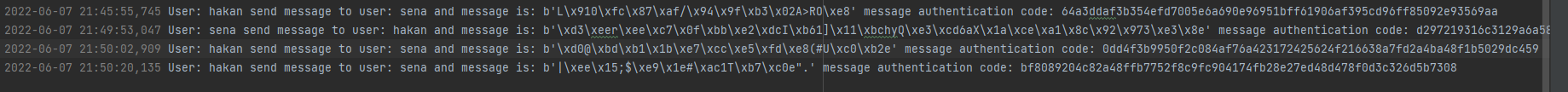
Description automatically generated



Text

Description automatically generated

While they are messaging in private chat their encrypted messages and message authentication code(MAC) logged as follows



While these things happening other users cannot see anything.

Graphical user interface, text

Description automatically generated

Then if one of user writes “PMEXIT” then they return to public chat and all logged in users can send message to each other without encryption.

These is the general way of work of this program.

Security hole

* If any encryption key is known then all messages sent over that key can be seen easily
* Solution to this problem is key update mechanism, to prevent decrypt all other messages, we need to use key update mechanism by using these technique each message encrypted with different key and one key only decrypt one message.