**T.C.**

**MARMARA UNIVERSITY**

**FACULTY of ENGINEERING**

**COMPUTER ENGINEERING DEPARTMENT**

CSE4057 Information System Security

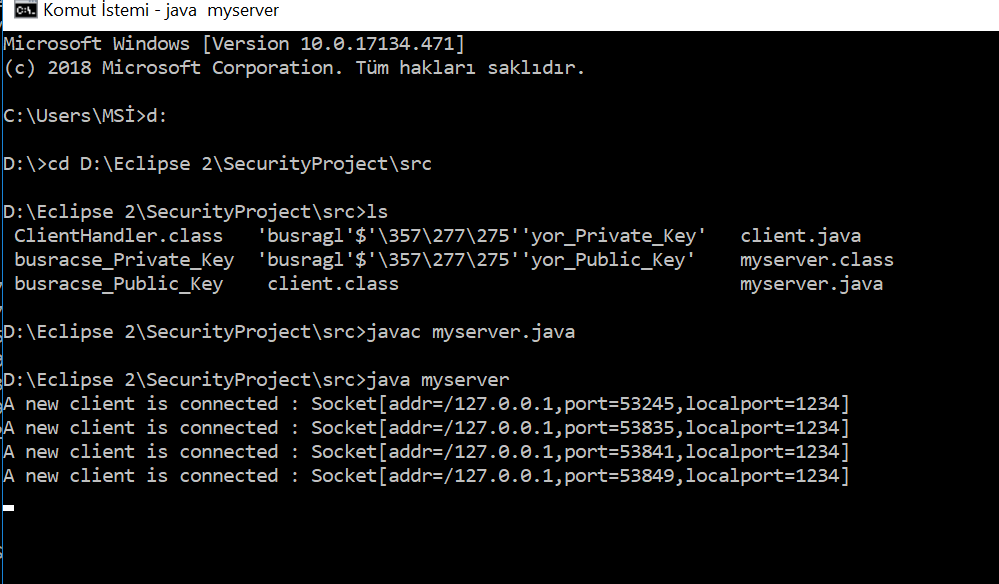
Project#1

Büşra YAŞAR-150114063

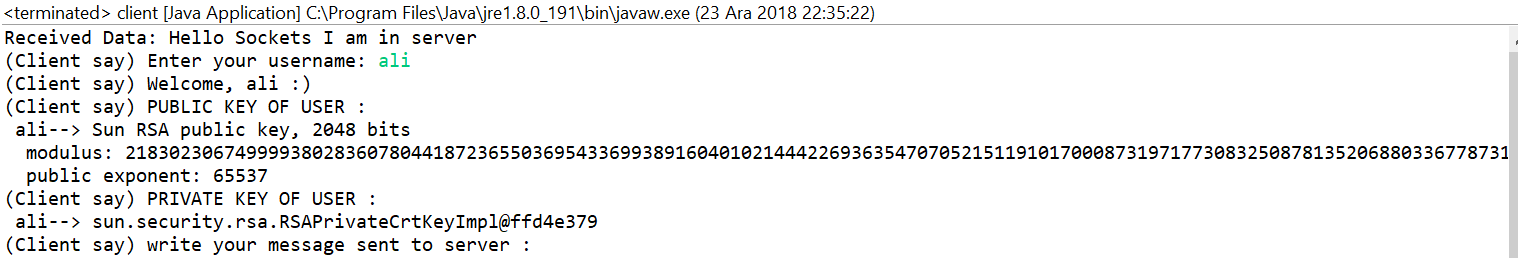
**Registration and Public Key Certification**.

I couldn’t implement this project completely. When user connect to server, the public and private keys of the user generated and keep in a file. Also when server starts to listen the port the public private key of the server also generated. I tried to create digital signature but I couldn’t send users key file through server to digital signature.

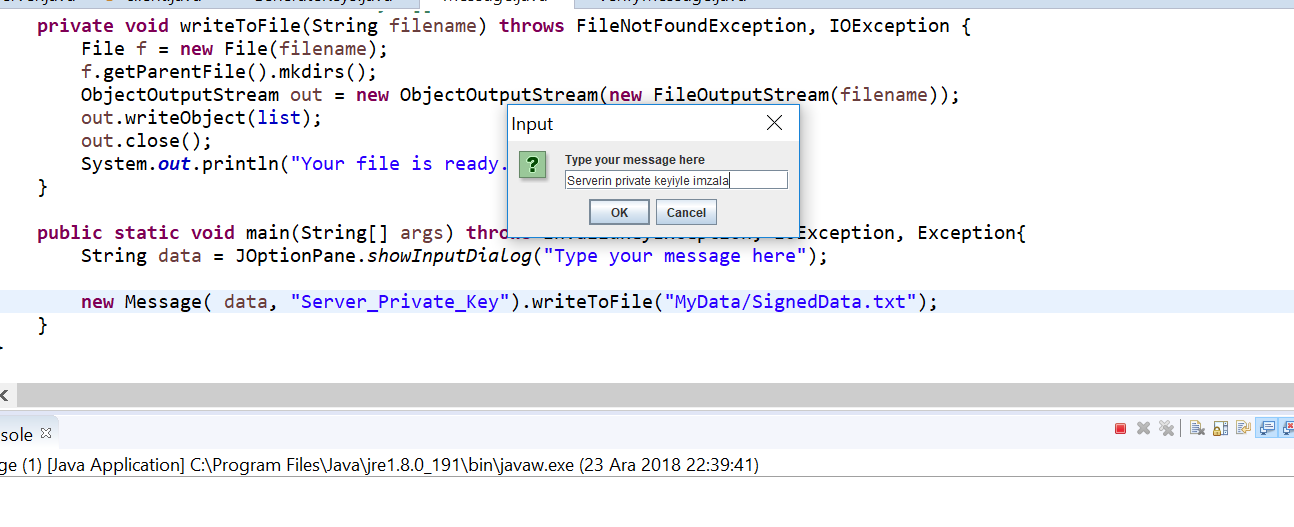
For each user server assign new thread:



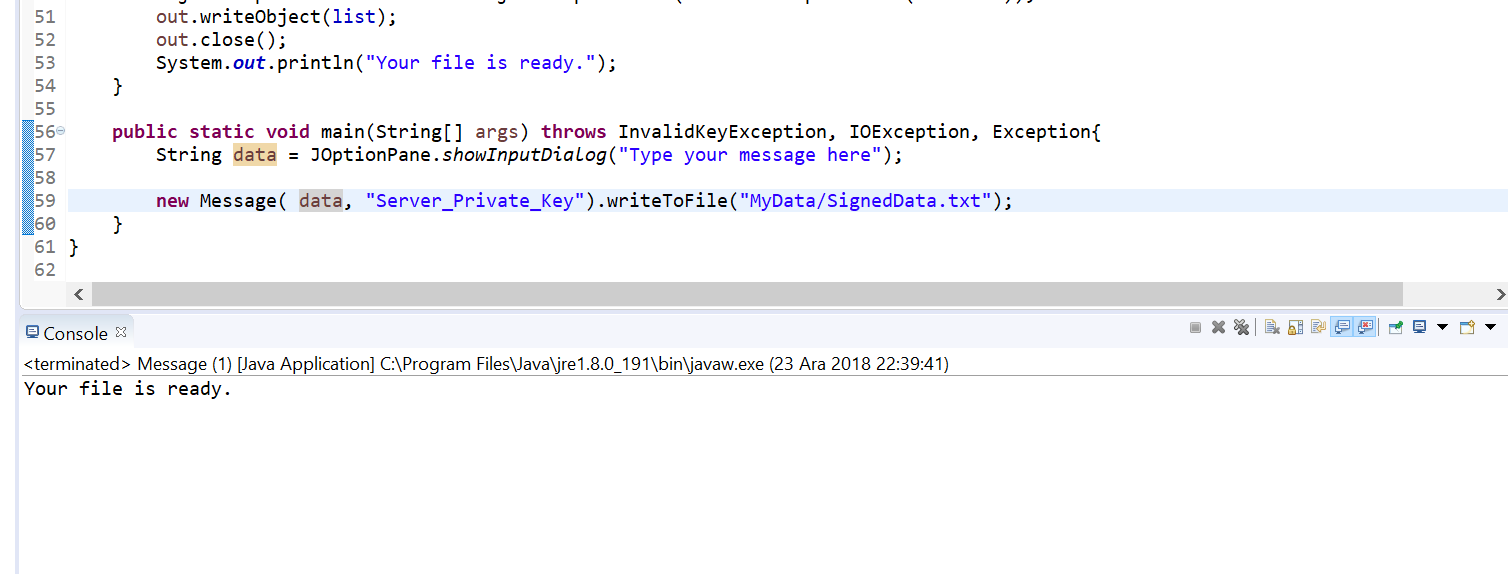
When I run the client side I get:



Also, I can digitally sign a string with Server private key and then I can verify message with Server public key but I can not combine this for cline username with public key.



This string signed with server’s private key :



Then I verified:

