SE375 SYSTEM PROGRAMMING SPRING 2023-2024
Laboratory Assignment 12

May 29-30, 2024

Client-Server Communication with Signatures

Your task is a simplified version of our data communication scheme. This time, we will implement asymmetric encryption with signatures.

The client and server are now going to follow the steps below:

1. The client and server will generate their own key pairs.

2. Each side will create a signature of their **public** keys.

3. Each side will send to the other:
    a. Their public keys,
    b. The signature of their public keys.

4. Each side will verify the signature of the public key they received.

5. The server will encrypt the URL https://homes.izmirekonomi.edu.tr/eokur/sample0.txt, and send it over to the client. Encryption should be done using the client's public key.

6. The client will decrypt the URL using its own private key, display it on the console and read the text inside.

7. The client will encrypt the text using the server's public key and send it over to the server.

8. The server will decrypt the text using its own private key and display it on the console.

Note: All communication is done through the TCP protocol.