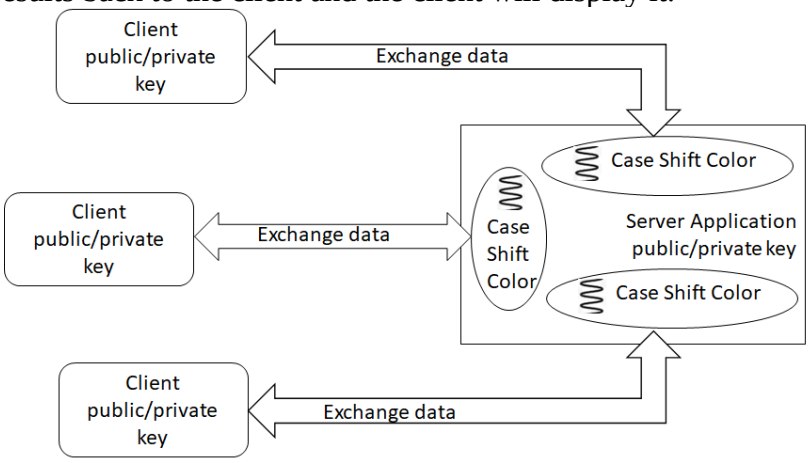
SE375 SYSTEM PROGRAMMING SPRING 2019-2020
Laboratory Assignment
May 27 2020

In this lab you will be making your network enabled application secure. In your last lab the client has sent the HashMap that contained the data to the server and the server performed the transformation and returned the results back to the client. The client then displayed the results. You will make the client server communication secure by using asymmetric (public-private key) cryptography.

a) As a first step make your server multi-threaded so that it can handle multiple clients at the same time. You can use the MultiThreadedServer.java code given to you in the lectures as a starting point.
b) To simplify the lab,
    a. The client will send just a **String** to the server, not the HashMap. The client will read the string from the user and send it to the server for transformation. **Eliminate all the HashMap related code.**
    b. The server will perform **Lower Case**, **Shift 3** characters and **Red** coloring transformations only (You can choose something else too).
c) The server application will have a pair of public/private keys. Run **GenerateKeys.java** program to generate server public private keys. Rename the files properly to indicate they are server keys.
d) Every TCP client application will also have a set of public/private keys of their own. Run **GenerateKeys.java** program to generate client public/private keys. Rename the files properly so that they indicate client keys.
e) From this point on, all data exchanged will be secured using the public-private key cryptography. Use the public and private keys you have generated in parts (c) and (d) when needed. The client will send data encrypted to the server and server will return encrypted results back to the client and the client will display it.



Notes:

1. Case, shift and color will be done within the client threads on the sever sequentially
2. Store the keys in a file both on the server and client.

Submission Guidelines for SE375

ACADEMIC INTEGRITY

This is an individual assignment. All individual assignments must be completed by the student himself/herself only. Plagiarism, copying, cheating, outsourcing the assignment to another person or organization for pay or without pay are considered as actions of academic dishonesty. Failure to maintain academic honesty may result in disciplinary action according to the Izmir University of Economics' **disciplinary bylaw for students of institutions of higher education** (https://www.ieu.edu.tr/en/bylaws/type/read/id/13).

Please Read Carefully. Failure to Follow the Guidelines May Cause Rejection of Your Submission.

1. You will submit your work to **Blackboard/Assignments/SE375 LAB.**
2. Complete your work using at most three **3 java files.**
3. We should be able to compile and run your programs using **javac.exe** and **java.exe** respectively (from a shell command) without using any IDE.
4. Do not use any third-party jar files or packages.
5. Archive java source files only into a **zip** or **rar** file. Name your zip file as follows:
   - **<yourname-lastname>.zip** (Example: SenolGunes.zip, SenolGunes.rar)
   - No such file likes Project*2(1).java, PROJETC1.txt, PROJECT.java, main.java* etc. Do not send any project meta files coming from Eclipse/Netbeans/IntelliJ etc.
   - No links to external repositories or cloud storage such as onedrive/dropbox/ Google Drive
6. Put your name and number in each of your source files as well.
7. Save your lab work.