Hacettepe University
Department of Computer Engineering
BBM465 Information Security Laboratory
Experiment 2

Subject	:	Cyrpt Messenger
Language	:	Java
Due Date	:	18/11/2020

1 Experiment

You are expected to develop a simple file client-server encryption/decryption messaging application.

The requirements are below:

- The program must support three encryption modes (CBC, OFB) and two encryption algorithms (AES, DES).
- Padding mode must always set to "PKCS5 Padding"
- The program must be executed as follows:

  Server: The server applications should be started first and wait for incoming connections. All encrypted messages received by the server will be distributed to clients directly. Besides, when the server starts, it will produce a random key and random initialization vector (IV) and send these key and vector to all the clients. Finally, the server must write, produced random key, produced IV and the encrypted message sent to itself with information about user name who sent the message to it's console and must create/update a log file (log.txt) whenever a message is sent to itself (**All these informations must be in Base64 Encoded (except "username", username will be displayed as normal text**)

  Client: Client application should have similar GUI showed in Figure-1. In the GUI There are three textboxes. First and the biggest textbox is for messages. Incoming messages will be displayed in this textbox. Second textbox titled **text** is for message writing. After typing a message user will press encrypt button to cipher the message. The encryption method and mode can be selected by using radio buttons top of the window. Then user should press send button to send encrypted message to server.

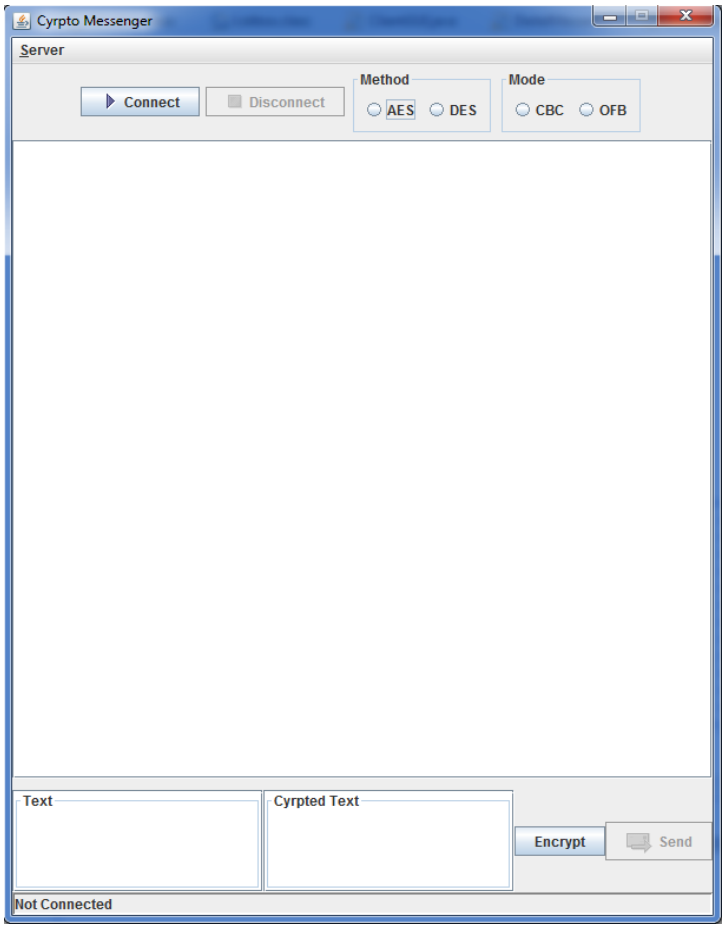

Figure-1 GUI of the application.

Software usage.

First Client application has to connect to server via TCP/IP sockets. Then users should enter his/her nickname that will be used in chatting. The dialog box opened after pressing connect is displayed in Figure-2. The encrypted texts and decrypted texts should be displayed in message area as shown in Figure-3

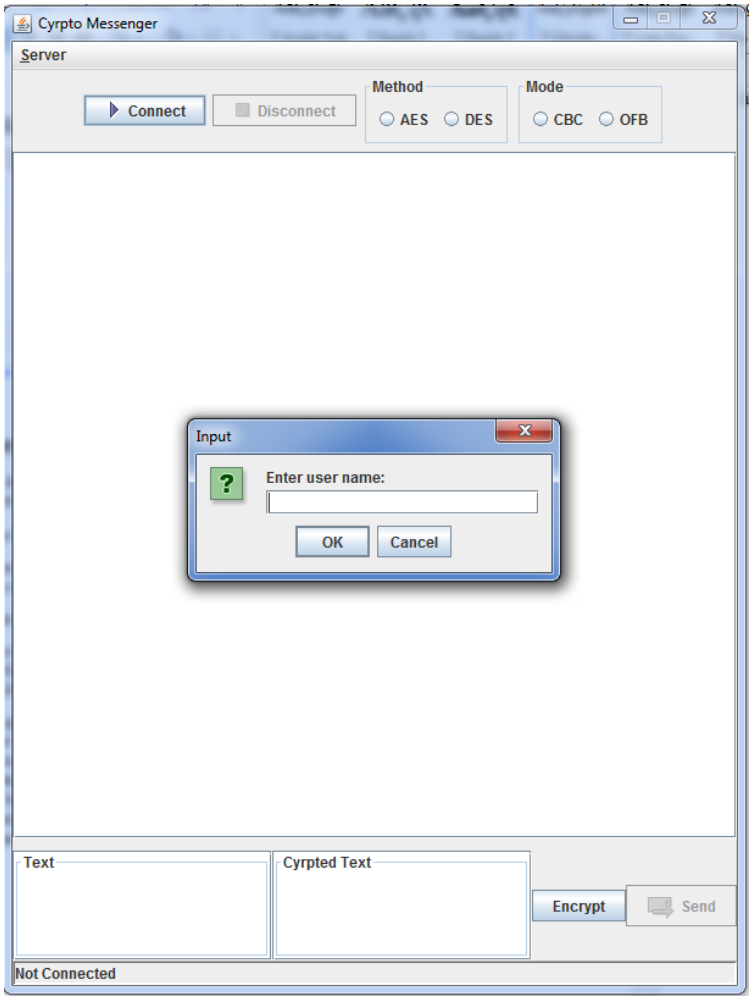

Figure-2 Username dialog box.

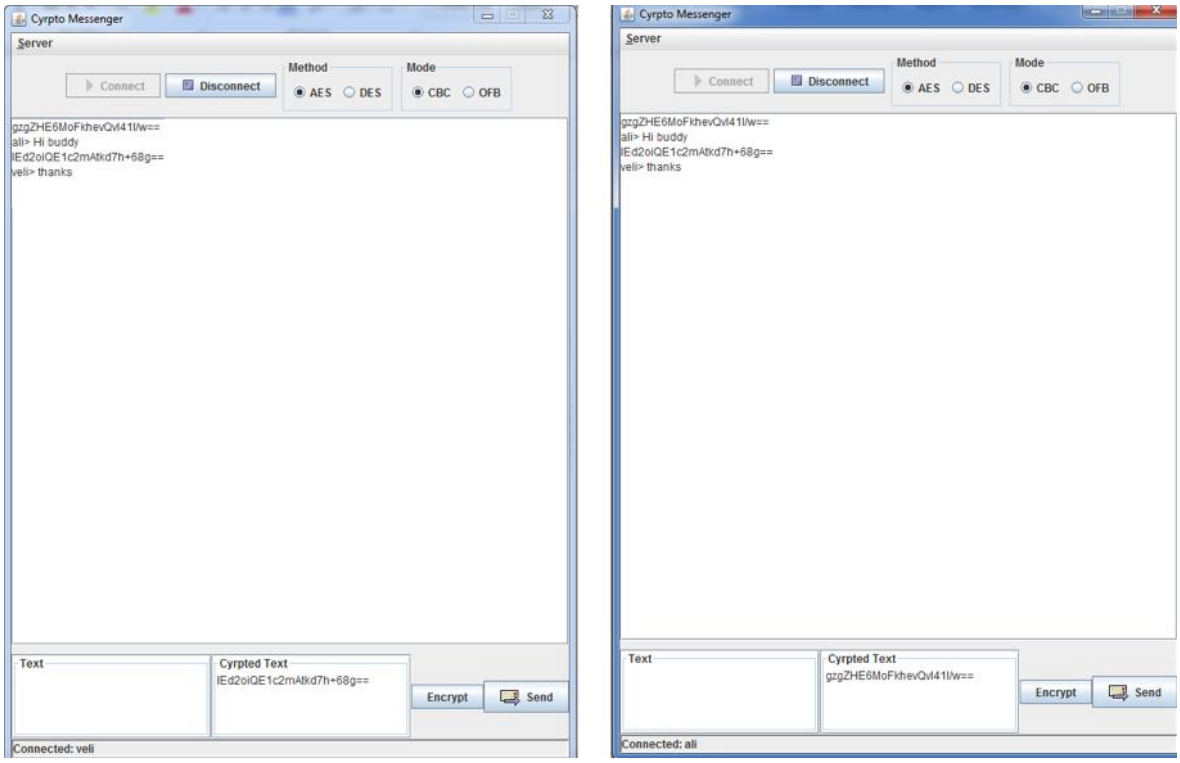

Figure-3 Sample messages

All messages should be send to all clients. Encrypted and decrypted messages should be displayed on message textbox (**crypted message must be displayed with Base64 encoded version**).

The same encryption algorithm and mode should be selected in all clients. Key and IV should be randomly generated by the server and distributed to all clients. All clients should use the same key and IV. You must use Java crypto API [1] for encryption functions.

2 Notes

1. You can ask questions about the experiment via Piazza group (piazza.com/hacettepe.edu.tr/fall2020/bbm465).
2. Late submission will not be accepted!
3. You must compile your program on Java version of the dev machine.
4. You are going to submit your experiment to online submission system:

   http://submit.cs.hacettepe.edu.tr/

   The submission format is given below:

   <Group id>.zip
   −[src]/
   −−*.[java]

3 Policy

All work on assignments must be done with your own group unless stated otherwise. You are encouraged to discuss with your classmates about the given assignments, but these discussions should be carried out in an abstract way. That is, discussions related to a particular solution to a specific problem (either in actual code or in the pseudocode) will not be tolerated. In short, turning in someone else's work(from internet), in whole or in part, as your own will be considered as a violation of academic integrity. Please note that the former condition also holds for the material found on the web as everything on the web has been written by someone else.

References

[1] "Package javax.crypto." https://docs.oracle.com/javase/7/docs/api/javax/crypto/package-summary.html.