Hacettepe University
Department of Computer Engineering
BBM465 Information Security Laboratory
Experiment 1

Subject	:	Cyrpt Messenger
Language	:	Java
Due Date	:	07/11/2018
Advisors	:	Assoc. Prof. Dr. Ahmet Burak Can, Dr. Ali Seydi Keçeli

1 Experiment

You are expected to develop a simple 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).
- 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.

  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.

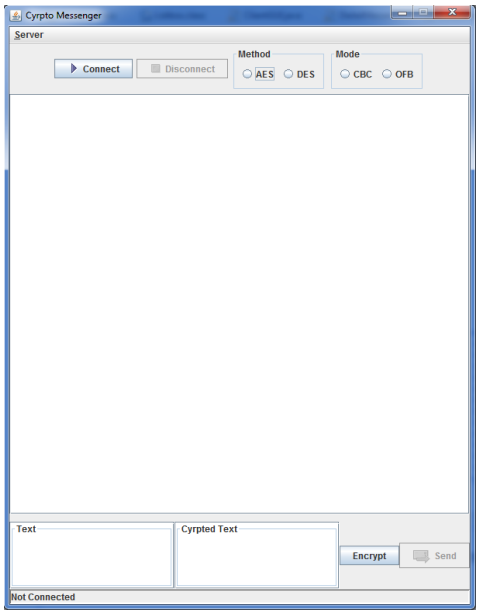

Figure-1 GUI of the application.

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

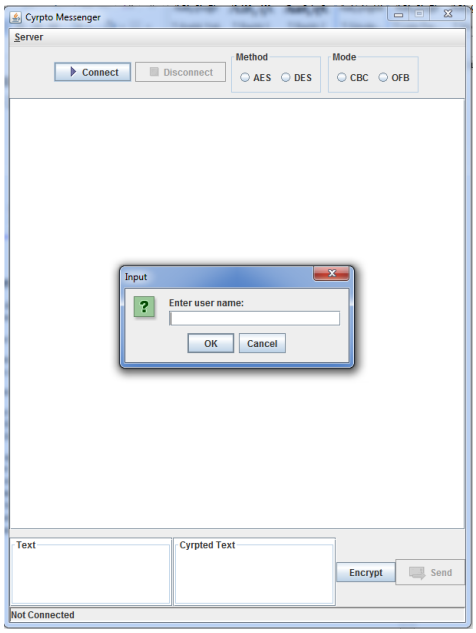

Figure-2 Username dialog box.

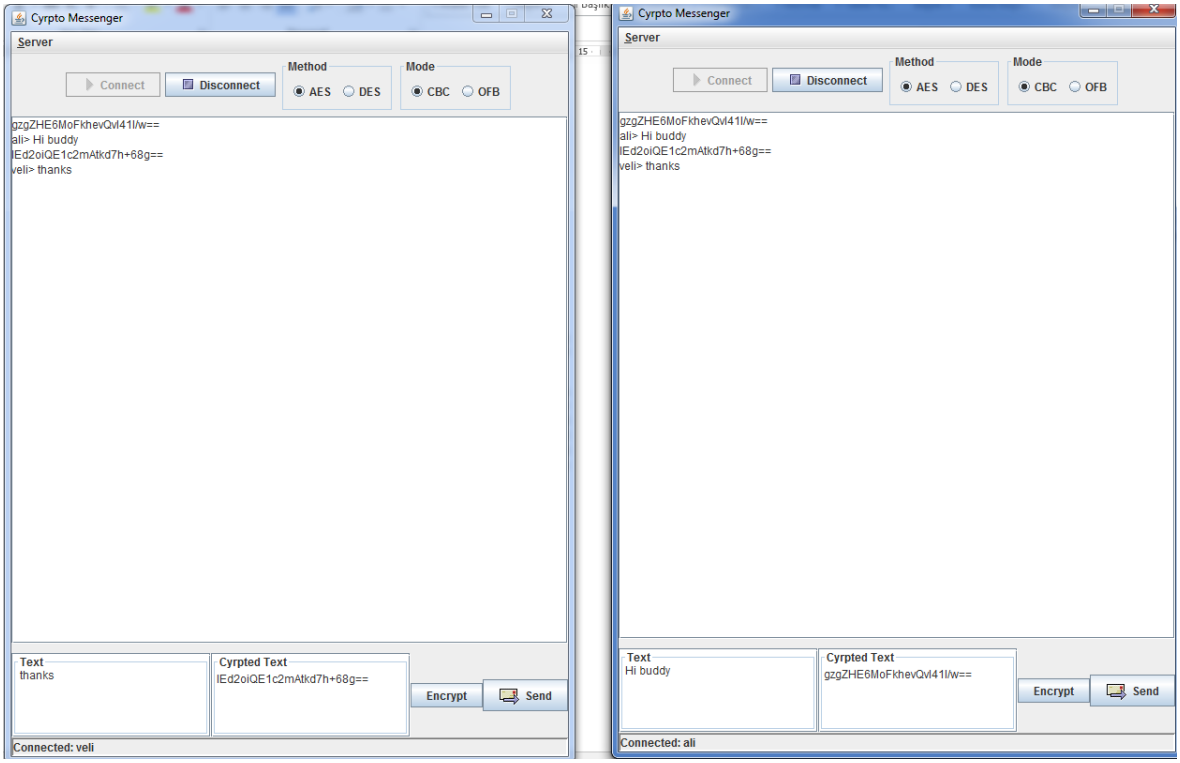

Figure-3 Sample messages

All messages should be send to all clients. Encrypted and decrypted messages should be displayed on message textbox.

2 Notes

1. The same method and mode should be selected in all clients.
2. Key can be embedded to client applications or can be distributed via server. (All clients should use the same key)
3. In Java, you can use standard crypto API [1].
4. You can ask questions about the experiment via Piazza group (piazza.com/hacettepe.edu.tr/fall2018/bbm465).
5. Late submission will not be accepted!
6. You must compile your program on Centos 7 before submission.
7. You are going to submit your experiment to online submission system: www.submit.cs.hacettepe.edu.tr

   The submission format is given below:
   <Student id>.zip
   −[src]/

--*.[java]
-[report]
-Report.pdf

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 elses 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.

Grading policy: %90 code, %10 report

References

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

[2]"Crypto++ Library 5.6.5." https://www.cryptopp.com/.