CS 351: Project: End to End Secure Messaging System

Project Description. Design and implement a basic end to end secure messaging system. There is a central server managing all the account information, user can log in from the clients and send encrypted message to "friends" without worrying others including the server to see the content.

Project Components. There are multiple basic modules any secure messaging system needs to have:

- User registration and authentication via remote password log in.
- Server authentication and user account management (regarding the pwd): when each user tries to connect to the server and send his password to log in, he needs to be sure he is talking to the right server. And server needs a proper management for user accounts for verification etc.
- User secure communication module. Once sender client has all necessary information about the receiver, they establish a secure channel for communication leveraging secure protocols.

Milestone and Final Reports. A one-page milestone report is required to be submitted by **Nov 17** mid-night describing what you already have done for the project and what is your plan how to proceed forward. In particular, in the milestone report, you should at least demonstrate progress with one module.

The final report should contain **detailed description** of your design about each important modules, and how you realize the above functionalities. Also screenshots for critical steps showing the implementation is working are also required in the report.

In particular, screenshots should at least contain evidence showing (1) registration and what is stored at the server backend; (2) user login, including successful log in and rejected failed log in; (3) secure communication of the testing message that I will tell you before the due date. The plaintext, the corresponding ciphertext, the decryption at the receiver end etc.

Grading Criteria. Each component counts for 5% each, and milestone and final report counts for 2.5%, each.

Programing Language Requirements. There is no restriction on which language you use, as long as you have a clear system design and an implementation that realize the functionalities properly.

Bonus Functionalities. There are also other extra features you can add, e.g., dealing with offline clients etc, with a maximum of 5% bonus credits.