**Project 2**

* Due Dec 12 by 11:59pm
* Points 100
* Submitting a file upload

**CS455 Cryptography and Network Security**

Project 2

**Tasks**

In this project, you are asked to implement the authentication system for an Internet based service.

1. User interface

In the client program, provides an interface so that the user can choose to sign up (register), log in, or changing password. This could be as simple as a command line interface such as asking the user to choose one of the three options: sign up, log in, or changing password.

1. Sign up/registration

The main requirements:

(1) The client program allows one to start registering an account. The detailed information to be provided for registration include: selected user id, selected password, user’s full name, and email address.

(2) The server will check the registration message and reject it if either of the following conditions appear:

a. The user id already exists.

b. There is an existing user id for this user (with the same email address)

c. Password length is shorter than 8

If a registration request is turned down, the reason should be displayed to the user. Then it displays the user interface as stated in task 1.

If none of the above conditions in (2) appear, the server will accept the registration information and save it in a file called “UserProfile.txt”. Note that the password will be hashed together with salt (a 8-digit random number specific to this user). The hashed password together with the plaintext salt will be saved in the “UserProfile.txt” file.

After the registration succeeds, the client will display the success message to the user and allow user to play a simple game (such as case conversion). If one decides to finish the game, the user will be logged out automatically and the main menu will display (ask user to choose one of the three options).

3. Changing the password

The main requirements:

* If a user choose to change the password, he/she should provide the following information: username, original password, and new password.
* The server will verify the username exist and the original password is correct.

(a) If the username exisit and the original password is correct, the server will check whether the password is at least 8 characters long. If yes, the server will update the hashed password in the UserProfile.txt file and notify the client that the operation succeeded.

(b)Otherwise, the changing password operation failed. In this case the client program just need to notify the user that the password changing operation failed  for the detailed reason that the server found out. Then it displays the user interface as stated in task 1. No need to press the user to re-input information to change the password.

4. Login

You can use the login codes in Assignment 6 as the basic code. But you need to revise them to support the use of hashed password and salt in the password file. Also when login failed, just displays the user interface as stated in task 1.

**General requirements**

* All registration/login/password changing request and response message need to be encrypted to ensure security, with the exception of the method name (e.g. “RegistrationRequest”, “RegistrationResponse”).
* The protocol need to defend replay attacks.
* Use methods for each major task in client and server programs. Make sure the main method is clean and easy to read.
* Write sufficient comments so that your codes are easy to understand.

**Submission**

Upload the client and server programs (just the source files, no project or class files) to Canvas.