**Name:**  Hassan El Krytly

Mirsa Casas

**Date:** April 30th, 2018

**Course:** CS 492- 01

**Final Project Topic: Two Steps Authentication & RAS Algorithm**

In our final project we create a sample application that demonstrates two major security concepts. The first one is Two steps authentication to authenticate the user of the application, and second one is the use of RSA algorithm implementation.

**Part 1: Two steps authentication**

* The application will ask the first-time user to register in the app by creating a username and password. Also, the app will ask the user Three security questions that he/she has to answer and remember them. For security purpose, one of the most important things we had to during user registration is hashing the password and store it as hash value in our database.
* In the first step autentication; the user needs to enter the username and password, the application will validate that information with the database, if it is correct, it will continue with the second step authentication, otherwise, the user will get a login error.
* In the second step, the user needs to answer a personal security question that only he/she knows the answer for that question, the application will validate the information provided. If the user enters the correct credentials, the system will let him login and start a communication session otherwise, the user will get a login error.
* **Part 2: RAS Algorithm Implementation**

In this application, we consider two users Alice and Bob.

* In the first step, Alice needs to generate her public and private keys by choosing two available primes numbers that will be used to compute N, E, and D.
* E and N are the public key pair, while D and N are the private key pair
* Alice needs to give her public key pair N and E to Bob
* Bob uses Alice's public key to encrypt a message for her
* Alice uses her private key the decrypt Bob's message

In conclusion, we want to say that since we were able to create a complete system login with most its functionalities such as errors validation and hashing the password, to demonstrate the two-step authentication and the use of GUI front end to implement RSA. We think that the design we have chosen to demonstrate the two security concepts was appropriate to application functionality.