# June 21, Class Project – Hashing and Encryption

Goal:

Create a security application that accomplishes the following task:

1. Allows a user to enroll in the application setting up a userid, password, forgot password answer and storing their phone number
2. When logging in, the user is asked for their userid and password or can optionally click the forgot password button. The user id is not case sensitive, but password is.
3. Forgot password should ask the simple question “In what city / town / village were you born?”
4. After logged in, the user can see and change their phone number or can change password forgot password
5. When the user types their password or forgot password, the password should not be shown on the screen
6. The userid is stored as a clear text, base64 encoded and must be unique in the table (no duplicates)
7. The user’s “forgot password answer” should be stored as a on way hash + salt, is not case sensitive and must be at least 2 characters long.
8. The user’s password must be stored as a one way hash + salt and must be at least 8 characters at setup and must contain: lower case characters, upper case characters and numbers
9. The user’s phone number must be stored in an encrypted form that can be decrypted
10. All user data must be stored in a unique MySQL table, but not the configuration data
11. Configuration data, both the salt and the private and public encryption keys should be kept in a JSON file with your app
12. You can use either Winforms or Console app for this project and you can use .Net Core or .Net Framework. No web service is required

Hints:

* You will need to generate the public and private key once and then store them in the JSON
* On a textbox in WinForms, you can set the property “UseSystemPasswordChar”: <https://docs.microsoft.com/en-us/dotnet/api/system.windows.forms.textbox.usesystempasswordchar?view=netcore-3.1>
* Remember we can log into the MySQL host using ssh or putty userid: student, hostname: sql.saye.org, password: LearnSQL
* The connection string to our MySQL is: "server=sql.saye.org;uid=class;pwd=LearnSQL;database=classicmodels;SslMode=Required;"
* Regex can be used to search for a range of numbers in a string
* Need help creating a table: <https://www.mysqltutorial.org/mysql-create-table/>
* When creating a table, put your name in the table so others do not alter your table, example: kevinusers
* You can use the classicmodels database or create your own database
* For visual reference, consider the following to help you understand the goal (note you are free to design your own UI)

