Connor Opderbeck

2/15/17

Project 2

Password Encryption

This application will take passwords that you give it to remember and will return a random three digit integer to you. The three numbers represent values that correspond to how the encryption works. For example the encryption could be $3x-y^2+2z$ and each variable corresponds to the three digits you receive respectively. The application would apply the encryption equation to each character and change its value saving it as a string with a value that is different from the actual password to prevent theft of the password.

The application can hold different users and mutable passwords for each user. To find a password you would have to enter your account name and the password you want to find (you can name passwords anything such as “g-mail” so you know what it is the password too). Once you have the password selected you must input the three digits and the encryption will run in revers with those values. If the values are the same as the one the application gave you earlier then the password that you get back will be the correct one. If you enter the wrong parameters for the equation then an incorrect password will be returned.

Example:

Lets say the password for your email is “password”. The encryption for the application is 3x+y-2z and the integers it generated are 1,5, and 3. The application would then save the password as “rcuuyqtf”, because the encryption would be to move each character 2 positions forward sense 3(1)+(5)-2(3)=2. The actual encryption will be more complex.

If you want to receive that password you must input 1,5, and 3 back to the application and it will move each charter back two positions to the original password and print it in the console. If you put 1,5, and 2 in the application, the password that it sends back to you would be “nxqqumpb” since 3(1)+(5)-2(3)=4 and the reverse encryption will move each charter back 4 positions instead of 2 and the incorrect password is returned.