Henry Hong

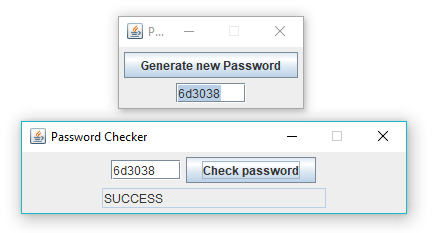
CSS 337 Secure Systems

Assignment 2

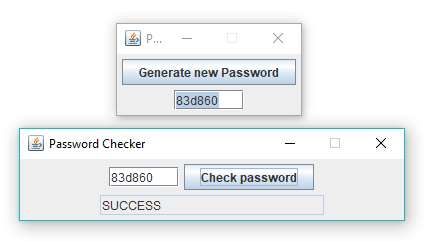
**One Time Password Generation and Authentication**

**Screen caps:**

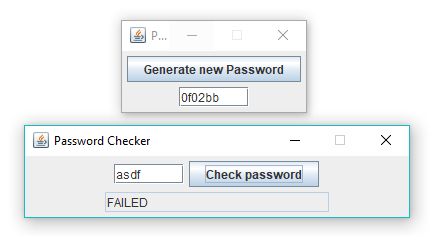
Check 1st password:



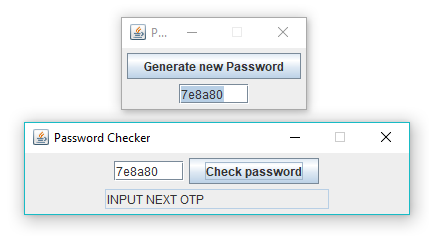
Generate 2nd password, and validate:



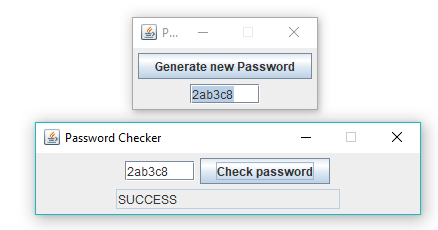
Check incorrect password:



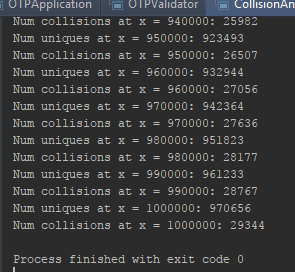
Check Desynchronized password that is valid (within 100 hashes of current OTP)



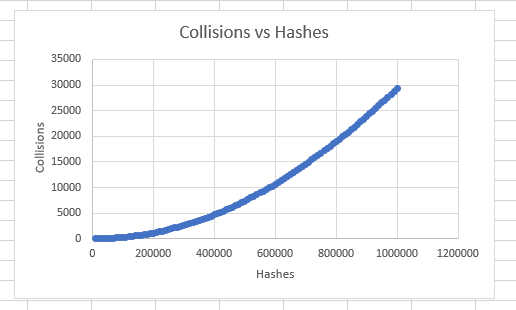
Confirm valid, and resynchronize



# collisions:



**Collision Analysis:**



As the number of hashes increase, the # of collisions increase at what looks to be a rate of logn. After one million Hashes, there were only 29,344 collisions.

If this application were to be used in a very limited setting, there would not be an issue with collisions. However, if the application were used in a setting where many hashes are made, the number of collisions would increase up to the point where theoretically all possible hashes have been made, and every new hash is a collision with a previous hash. Practically speaking though, this would take a long time, and a lot of space.