Patrick O’Brien, Marco Rojas

4/18/2019

CSC 160 Combo

Final Project Proposal

For our final project, we would like to design a program that serves as a tool to perform brute force password attacks against a list of unknown hashes. It will also serve as a tool that will allow a user to securely check if their password appears in the top 10,000 passwords used.

In order to design a program that can accomplish these tasks, we will need to read in two text files, one is the list of 10,000 most common passwords (Passwords.txt), the other is a list of hashes that we are attempting to determine the plaintext of (Hashes.txt). We will have a class that will take information from the Passwords.txt file and create a two-field object out of each line: one field containing the plaintext password, the other containing the hash of the password. We will create one class for MD5 and look at using a second as well. After we have the hashes of the Passwords.txt passwords, we can compare the unknown hashes in Hashes.txt to of Passwords.txt hashes to determine what the plaintext is of our unknown hashes. To allow for a user to check their password against our list of known passwords, we will hide the user text so any onlookers cannot see it.

Patrick will complete

* + A
  + A
  + a

Marco will complete

* + A
  + A
  + a