Project Description

Assigned Project: Designing Your Smartest Strategy to Crack Passwords

In this project, you are given a password file "passwords.txt", the file lists a number of passwords, however, in SHA-1 hashed version. Each line of the file has the following format: [Uer ID] [SPACE] [SHA-1 Hash of The User's Password]. For example: the first two lines of the file is

1 7c4a8d09ca3762af61e59520943dc26494f8941b
2 5baa61e4c9b93f3f0682250b6cf8331b7ee68fd8
…

First, please verify User 1's password is "123456" using this website:
http://www.sha1-online.com/

Your goal in this project is to crack the passwords in the file as many as possible. You are given the following knowledge about the (bad!) practice of people setting up their passwords:

- Some people tend to use only a few digits as passwords
    - Examples: 0000, 123456, 012, 20170101,
- Some people tend to use English words or phrases or short sentences as passwords (not safe!)
    - Examples: university, good, password, reallygood, greatday
- Some people combine English words and digits, but they generally place few digits after the English words.
    - Examples: university17, password123, great007

In this project, you can safely assume that all English words are lower-case, and all of them are chosen from a given dictionary file "dictionary.txt". You can use any computer language (Java, C/C++, Python, R, Matlab, …) and leverage any existing open-source software, tools, or commands (e.g., sha1sum in Linux) to design the cracking system.

You must detail your strategy and give the results in the report. Generally, you may need to run your code on a (faster?) computer for a (large?) number of days. It really depends on your cracking strategy!!!

Don't not disclose your results to other groups!

Grading (Total: 100 pts)

- Report, Code, Readme file: 50 pts
- Crack Results:
    - Crack 50% of the passwords, 30 pts
    - Crack 75% of the passwords, 40 pts
    - Crack 100% of the passwords, 50 pts