Password Cracking!

Exercises by Lili Wilson for Willstätter Gymnasium Workshop, 25.01.2024

My email: *LMWILSON@MIT.EDU*

Concept adapted from https://s2.ist.psu.edu/ist451/451-lab1_s06.pdf

*** I am obligated to say: the following exercises are meant to be used as exploration for learning more about passwords, and not to teach you how to break into anything. Password cracking is not ethical, and should not be done to real accounts and real passwords. That being said, in cybersecurity, learning how to break things in a safe and responsible way is important for learning.*

CODING MATERIALS CAN BE FOUND HERE:
https://www.dropbox.com/scl/fo/gd8hw2slbn53itxrytjhw/h?rlkey=f4q8n51ltrb8vxz8j0dvs19g5&dl=0

After learning more about passwords today, you are seriously worried about your friends and their passwords. To prove to your friends that their passwords might be insecure, and to get some practice working with **hash functions**, you try to crack the following passwords using some information you have learned about common password trends.

You will find below a table of people, with some information about who they are, and the **SHA256 hash value** of their password. SHA256 is a very popular hashing algorithm that is used in many places today. Your goal is to use your knowledge of these imaginary people, as well as your knowledge about passwords, to uncover the original passwords.

The passwords get more challenging to crack as you go on! You will need to think *creatively* and use your *programming skills* to solve the harder ones. Some resources you might find helpful for the more challenging questions:

- “replace” method in Java (https://www.w3schools.com/java/ref_string_replace.asp) or Python (https://www.w3schools.com/python/ref_string_replace.asp)

- Reading from a text file in Java (https://www.w3schools.com/java/java_files_read.asp) or Python (https://www.w3schools.com/python/python_file_open.asp)
- Use common password lists and existing wordlists (some have been provided to you)

All passwords except for Olivia's only use lowercase letters, and all passwords except for Kai's do not use numbers.

Name	***Description***	***Hashed password***
Bob	Bob is very lazy and hates remembering any more information than he has to. His password is quite possibly the world's worst password.	5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
Jeremy	Jeremy is a little more creative than Bob, but still chose something in the top 50 most common passwords.	1532e76dbe9d43d0dea98c331ca5ae8a65c5e8e8b99d3e2a42ae989356f6242a
Olivia	Olivia thought that if she changed the casing (uppercase and lowercase letters) of a commonly used password, she'd be safe.	b4b619c0678def23b479283b0b5042c8f9736bf16d137bc349518aba30e34b6b
Kelly	Kelly picked her favorite English word as her password because she thought it would be easy to remember.	3171d89ad00530ffa19a244f040e9401a657903cbbbca724996b90a56df2c189
Kai	Kai took their favorite English word, but replaced some of the letters with numbers that looked similar to make it harder to guess.	8c3eab3a9d70f32824f03ccd2658d5e98ad97b3856a2ca5291cad70f3d4a4577
Marissa	Marissa was inspired by Kelly, and she chose to combine two English words.	403f9b0cae353aa6e0df37d8f0a3e31261072b2c5af892377441877dc142348a

Good luck!

Note: if you want to try another fun game, that requires less coding skill but is still challenging, you should check out this website: https://neal.fun/password-game/ (The Password Game).