Winter 2020
Sébastien Combéfis

SE507μ Hacking Password Hashes with Rainbow Tables

Coding 2: Hash chain

This assessment evaluates the following competencies:

- *CS502 – Understand how rainbow table can be used to find a password given the hashed passwords database* *(+2)*
- *CS501 – Write a program that tries to guess the password corresponding to a hash value given the hashed passwords database* *(+1)*

In this coding assessment, you have to write a program that computes hash chains with the SHA-256 secure hash algorithm, assuming 8-character passwords that are only composed of lowercase letters (`[a-z]`) and digits (`[0-9]`). You have to use 8 reduction functions R_i that will take one chunk of the SHA-256 hash, represented as a hexadecimal number. The reduction function R_i is defined as:

$$\begin{array}{rrcll} R_i: & C^{64} & \to & C^8 & \\ & h & \mapsto & R_i(h) = & h_i h_{i+1} ... h_{i+7} \end{array}$$

where $C = \{a, ..., z, 0, ..., 9\}$.

Your program must generate randomly 10 passwords, and compute one hash chain for each of them. Theoretically, you should have $10 \times (8+1) = 90$ SHA-256 hashes, with the corresponding clear password, stored with the 10 hash chains. To succeed the assessment, you have to:

1. Write the application that computes 10 hash chains with the SHA-256 hash function and the R_i reduction functions.
2. Measure if you got any collisions by counting how many distinct hashes you have.
3. Explain to the teacher how you wrote your program, how it works and make a demonstration.