SE507μ Hacking Password Hashes with Rainbow Tables

Project 2: My first rainbow table

This assessment evaluates the following competencies:

- *CS007 – Understand why it is important to store passwords carefully*   *(+1)*
- *CS502 – Understand how rainbow table can be used to find a password given the hashed passwords database*   *(+3)*
- *CS901 – Understand how passwords database can be attacked*   *(+1)*
- *CS501 – Write a program that tries to guess the password corresponding to a hash value given the hashed passwords database*   *(+2)*

In this project assessment, you have to write a program that produces a rainbow table for LM hashes. For this, you first have to define seven reduction functions and generate a text file storing 100 hash chains (only store the first and last element of the chain). Then, once you managed to create your first rainbow table, write and test the two following functions:

- The first function reads through the file with the rainbow table, rebuilds the whole hash chains and writes them out in another text file.

- The second function searches for the clear password corresponding to a given hash or indicates that it has not been found in the rainbow table.

To succeed the assessment, you have to:

1. Generate your own rainbow table storing 100 hash chains for passwords hashed with the LM Hash algorithm.

2. Write and test the two aforementioned functions.

3. Explain to the teacher the program you wrote, how it works and make a demonstration.