CT255 Assignment 2

Rainbow Tables

Overview

The objectives of this assignment are as follow:

1. Reinforce your understanding of hash chains and rainbow tables.
2. Algorithmically build rainbow tables.
3. Recover passwords using rainbow tables.

The Java class *RainbowTable* is based on a hash function and a reduction function, which process 8-character long strings (aka passwords) consisting of smaller or capital letters, digits, "!" and "#" (64 possible characters in total).
The reduction function has a second argument ("int round"), therefore providing for a slightly different reduction algorithm for every time the function is called. As a result, hash collisions are less likely as outlined in the lecture notes.

Problem 1: [4 marks]
Complete the code so that it generates rainbow tables with 10,000 chain elements that match the start and end value pairs as shown in the program listing (for example: Kermit12 - lsXcRAuN). Your generated chain would start with the password candidate "Kermit12" and end with the password candidate "lsXcRAuN" after 10,000 hash/reduction cycles.

Problem 2: [6 marks]
Enhance your code in problem 1 to find password matches for the following hash values:
895210601874431214
750105908431234638
111111111115664932
977984261343652499
Use the ten (start - end) value pairs shown in the program listing for your hash chains.
Please note that only two out of the four hash values will actually find a match.

Assignment Submission

Please submit a zipped folder to Blackboard containing:

- Your (well-commented!) source code for problems 1 and 2 in PDF format.
- Screenshots showing your programs being compiled and producing results.
- Your solution for problem 2 (i.e. passwords you found).