#### COMP 3061 Assignment 1 Topic 3 : Use an Online Rainbow Table Cracker

# Nooran El-Sherif 100695733

## Objective

The objective of this report is to use an online rainbow table to answer the following questions:

1. How long does it take this online rainbow table to crack a given hash?
2. What’s the difference between a salted and unsalted hash value?

## Process

To answer these questions, I will use the online rainbow table <https://crackstation.net>.  
I will additionally be using and MD5 hash generator <https://www.md5hashgenerator.com> for generating salted and unsalted hashes.

To collect a variety of data, I will be using 12 types of passwords, in both salted and unsalted hash forms.

The passwords used will be in the following formats:

1. letters only, a dictionary word, lowercase
2. letters only, dictionary word, uppercase
3. letters only, dictionary word, mixed-case
4. letters only, non-dictionary word, lowercase
5. letters only, non-dictionary word, uppercase
6. letters only, non-dictionary word, mixed-case
7. numbers only
8. two numbers followed by dictionary word
9. dictionary word followed by two numbers
10. dictionary word with some letters replaced with numbers and special characters (i.e. 1337$p3@k)
11. alphanumeric, non-dictionary
12. alphanumeric, non-dictionary, special characters

For the sake of simplicity, the passwords will be the same length (excluding passwords 9 and 10). The salt will be added to the end of the password. It will be made up of 8 randomly generated alphabet characters, both lowercase and uppercase. To generate the alphanumeric, non-dictionary passwords I will use an online password generator: <https://passwordsgenerator.net/>

## Results

It took an average of 4.065 seconds for the online rainbow table to crack the unsalted passwords. For the unsalted passwords that were not successfully cracked, the average time for a result of “not found” was 4.938 seconds. For the complete table of data on time to crack the passwords, see Figure 1: Results Table below.

An unsalted hash value is a hash value created from just the plaintext password. A salted hash value has any number of characters either added to the front or the back of the password before it is hashed. The salted hashes were unable to be cracked by the online rainbow table. This is because the rainbow table uses a lookup of common passwords and their hashes; the lookup does not contain hashes of random strings of characters. In Figure 1 below, it is apparent that uncommon passwords (do not contain dictionary words, are random mixtures of alphanumeric characters) are not able to be cracked by a rainbow table cracker.

## Summary

Given the way that rainbow tables work, a password that has been salted before being hashed cannot be cracked. An unsalted, common password is easily cracked within 5 seconds. Unsalted, uncommon passwords of mixed case alphanumeric characters are also less likely to be cracked, because it is less likely they will be stored in the lookup table. Salt refers to adding a random string of characters either before or after the password before it is hashed.

# Figures

#### Results Table: Time to Crack Unsalted and Salted Hashes of Various Passwords

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Plain-Text Password** | **Unsalted Hash** | **Time (s)** | **Cracked** | **Salted Hash** | **Time (s)** | **Cracked** |
| password | 5f4dcc3b5aa765d  61d8327deb882cf99 | 4.40 | Yes | 90dfda96c344a4c66  1ba1a192865aabd | 5.01 | No |
| PASSWORD | 319f4d26e3c536b5dd8  71bb2c52e3178 | 4.73 | Yes | 43885e558dd88c217  af8872ae1fa1e47 | 5.43 | No |
| pAsSwOrD | ec7a43ecf46bbaa8c  808f4ce0cdedceb | 5.09 | Yes | d877d40dcbdb6ce02  865176d43177258 | 5.85 | No |
| mlgtherg | a07aff6ff6e003bdd5  755785b9cc9e1c | 5.34 | No | 03df43f5c715f0ee441c2  a6375a213f9 | 5.80 | No |
| MLGTHERG | 4e02532329d9ca224e342  93477377e91 | 4.96 | No | 23d1f0550f38f7cbc2a9c29f9da9555e | 5.89 | No |
| mLgThErG | 621104d412d42a64  2b6f591dda1591e0 | 5.23 | No | 8ed72e2ec12a840ae2b5f69143e231f6 | 5.86 | No |
| 99password | e3ba13361d172357  89a70bd899274c30 | 5.08 | Yes | 1c2e2d058a244a2559129139a9ddb6a4 | 5.73 | No |
| password99 | 2484b2d1aec71de2  ca87f88af401a6af | 4.65 | Yes | 27b8d9fef03bdac4b48f9c5d75d61ce9 | 4.83 | No |
| p@$$w0rd | b7463760284fd067  73ac2a48e29b0acf | 4.50 | Yes | 8bbedab8456d6ea4db8ed542b63fac83 | 5.19 | No |
| 7K4YQEvv | 74f44dcb26051b8a5a  38b79ce890cde7 | 6.33 | No | b168338dac6c871177bc98b029fa984b | 6.66 | No |
| V@Q%7)rX | 19c44a49f2f0bc978  3a3f7c81a822b99 | 4.83 | No | fb6183a6a77cfd32dab8b93f04147985 | 5.39 | No |

#### Figure 1