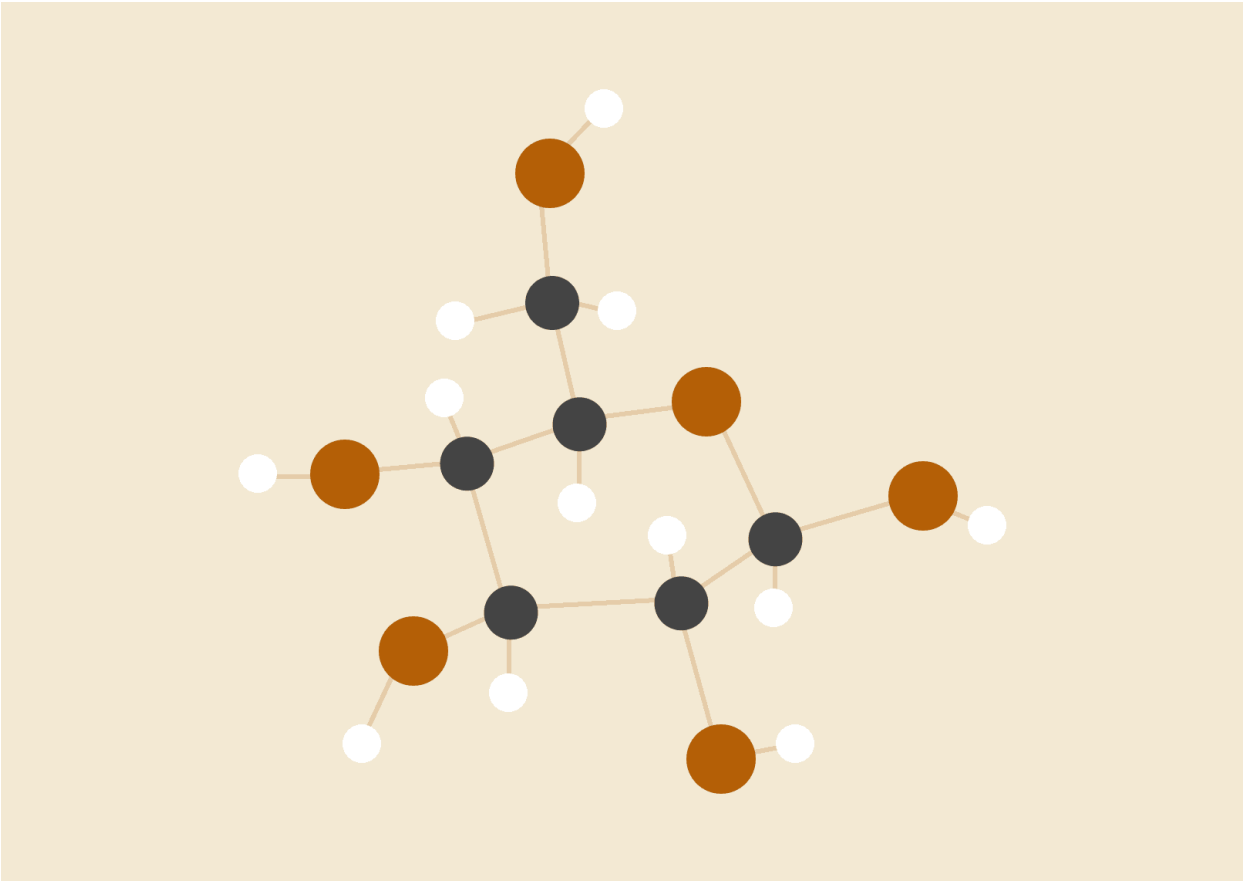
CSS IA 1

RAINBOW CRACK- PASSWORD CRACKING USING RAINBOW TABLES



Swastik Kar(1911086)

Mitali Sharma(1911094)

Computer Engineering, B2

INTRODUCTION

The passwords in a computer system are not stored directly as plain texts but are hashed using encryption. A hash function is a 1-way function, which means that it can't be decrypted. Whenever a user enters a password, it is converted into a hash value and is compared with the already stored hash value. If the values match, the user is authenticated.

A rainbow table is a database that is used to gain authentication by cracking the password hash. It is a precomputed dictionary of plaintext passwords and their corresponding hash values that can be used to find out what plaintext password produces a particular hash. Since more than one text can produce the same hash, it's not important to know what the original password really was, as long as it produces the same hash.

RainbowCrack is a computer program that generates rainbow tables that are used in password cracking. Since it makes use of these precomputed rainbow tables, the length of time needed to crack a password reduces drastically, when compared to traditional brute force cracking methods.

FEATURES

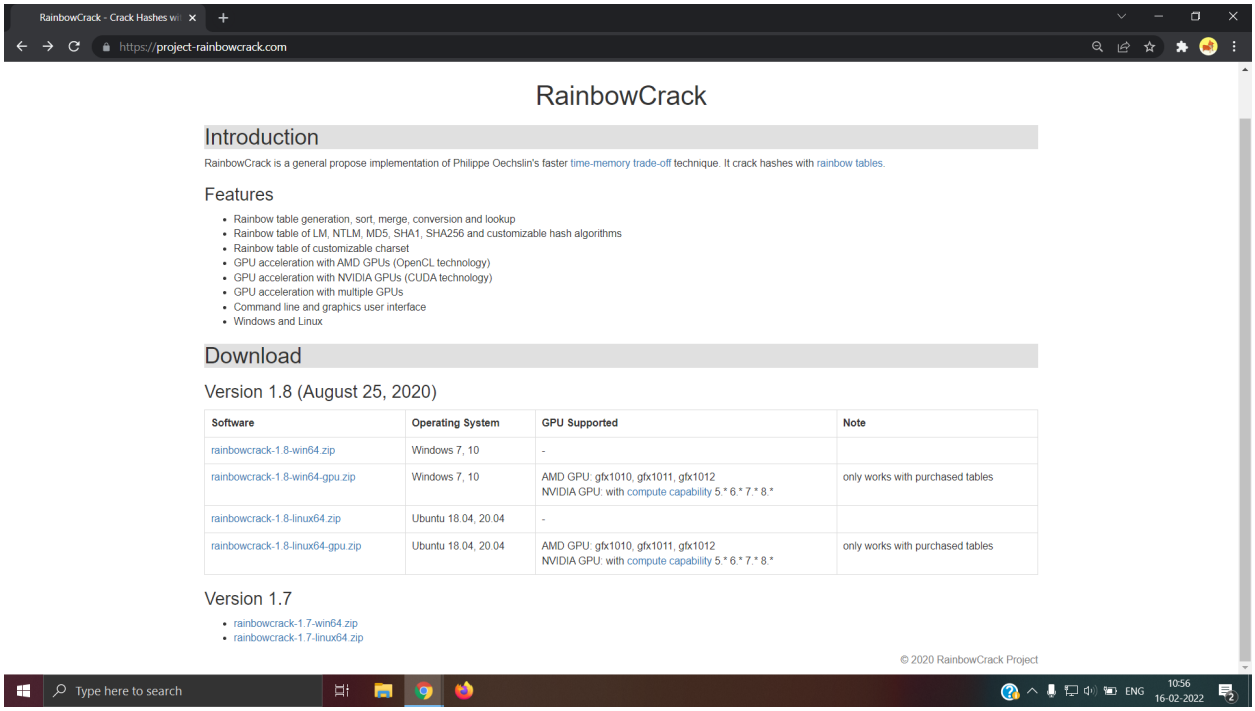
- Rainbow table generation, sort, merge, conversion and lookup
- Rainbow table of LM, NTLM, MD5, SHA1, SHA256 and customizable hash algorithms
- Rainbow table of customizable charset
- GPU acceleration with AMD GPUs (OpenCL technology)
- GPU acceleration with NVIDIA GPUs (CUDA technology)
- GPU acceleration with multiple GPUs
- Command line and graphics user interface
- Windows and Linux

REQUIREMENTS

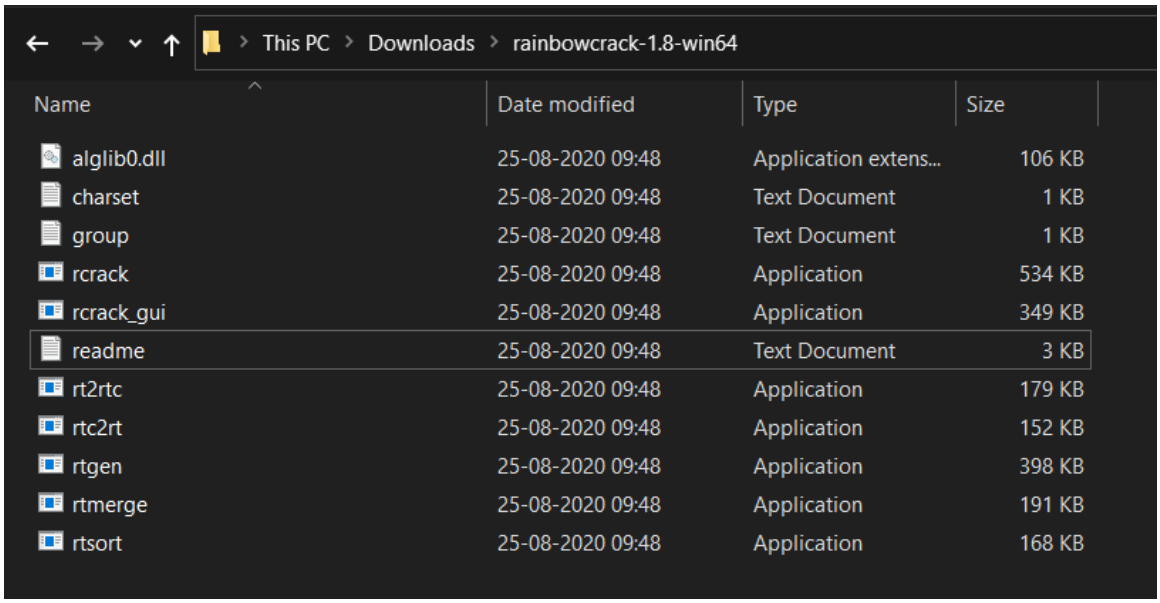
- Windows, Mac, or Linux OS
- Root or Admin access

INSTALLATION STEPS

1) Visit https://project-rainbowcrack.com/ , and download the version suitable for your operating system.



2) Unzip or extract the files that you just downloaded.

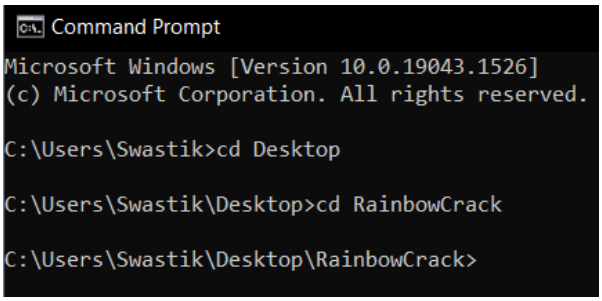


3) Use the Rainbow Crack GUI, or command line.

PROCEDURE

1) First, you'll need to make a rainbow table. To do that, you can make use of either the command line, or use some rainbow table generation software, such as Winrtgen.
    a) Using Command line

    First, change directory to where your RainbowCrack is located



    Next, run the rtgen command. The table will be generated based uponA inputs provided by the user. The rtgen command will provide the parameters, which the user will have to fill.

    hash_algorithm: This is the hash algorithm that we want our rainbow tables to use. You can see a list of available algorithms under *hash algorithms implemented* in the return text. For our example, we will use MD5, but RainbowCrack is just as capable of making perfect SHA1 and NTLM tables, and I will provide the code for the tables for all three.

    charset: The set of characters used to generate the plain-text strings for the rainbow tables. **Numeric** is digits 0–9, **loweralpha** is alphanumeric (all letters and digits 0–9), but only in lowercase. For a full list of charsets that

you can use, see "charset.txt" that comes with RainbowCrack.

plaintext_len_min: The minimum length of plaintext strings. For example, if we choose a numeric charset and a min and max of 1, our table will contain all digits 0–9 and their hashed equivalent.

plaintext_len_max: The maximum length of plaintext strings. For example, if we choose a min of 1 and a max of 2, we get all digits 0–9 and 00–99 and their hashed equivalents in our table.

table_index: This parameter selects the reduction function. A reduction function is a math formula that trims the number of combinations by removing combinations that are incredibly unlikely to be used. By doing so, it lowers computational time drastically. But the flip-side is that there is a tiny possibility that any given reduction function will skip the combination we're looking for, so "perfect" tables use multiple runs with different reduction functions to make tables that are "perfect," containing every possible combination.

chain_len: This controls the length of each table. The larger this number is, the more plaintexts are hashed and stored in the table. This is why the reduction function mentioned above matters — it will reduce possible combinations to the chain length you picked. The flip-side of having a long chain length is generation time. If you want a table that is "perfect" and vast, it can take months.

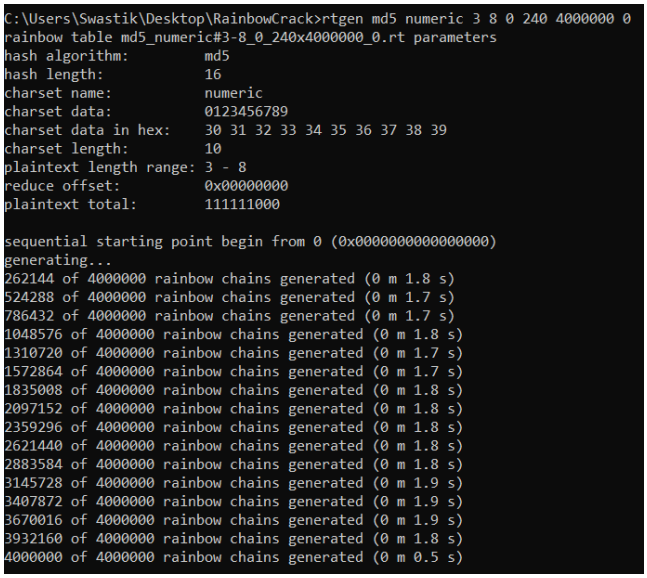
chain_num: This is the number of chains to generate. Each chain will be 16 bytes.

part_index: This is for situations where your hard disk space or computing power is limited, or when your filesystem is unable to address extraordinarily large files. We can change this from the 0 that it should normally be to segment the table file into smaller parts.

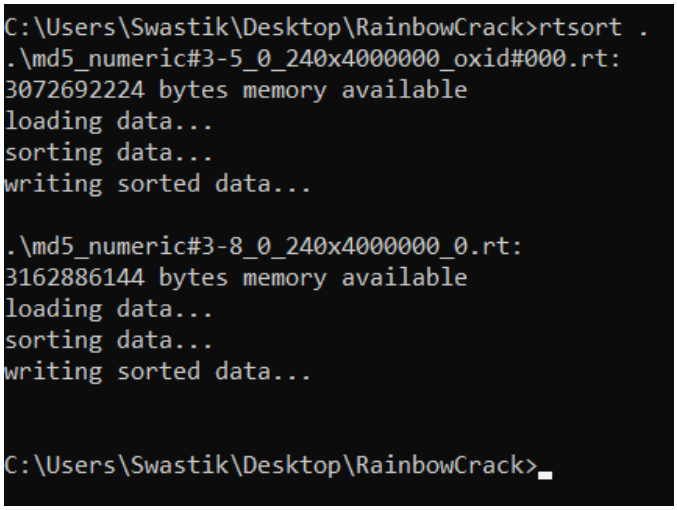
-bench: This is a flag that you can add to do a benchmark on the settings that you have selected. It will not actually create any rainbow tables, it will just determine some numbers that you can use to determine how fast you can generate table entries. Based off of that, you can determine how long table generation will actually take.

The command that the user will run will look something like this

-



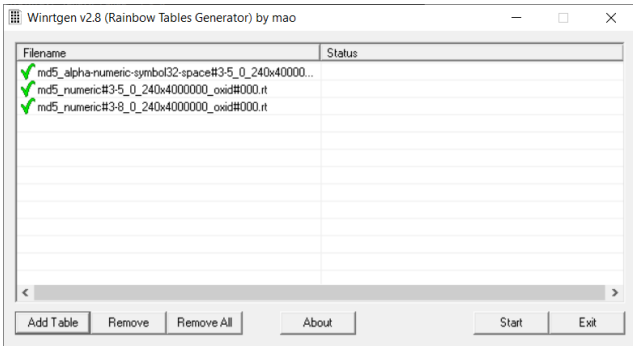
Finally, use the command “rtsort .” to sort the table



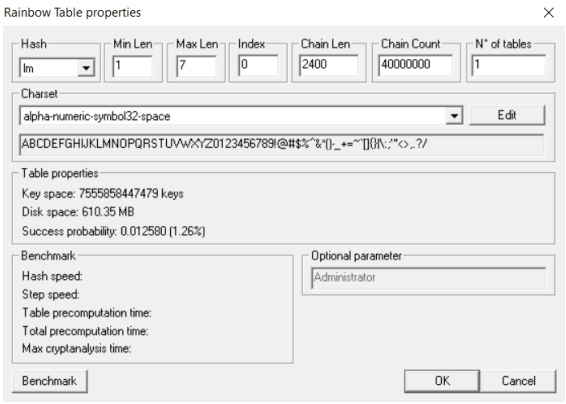
The rainbow tables have been generated and can now be used

b) Using Winrtgen or other software

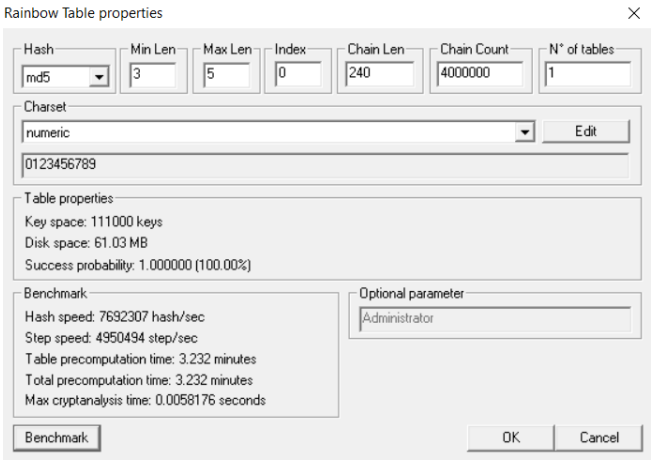
Run the software, which will look like this-



Click add table, which will cause this menu to pop up-

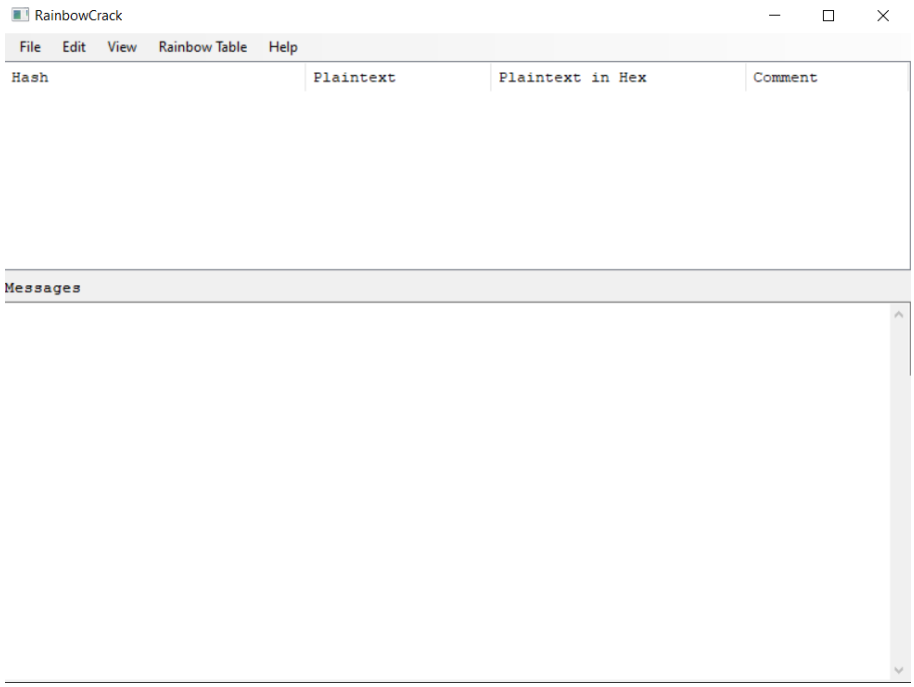


Here, enter the chosen parameters

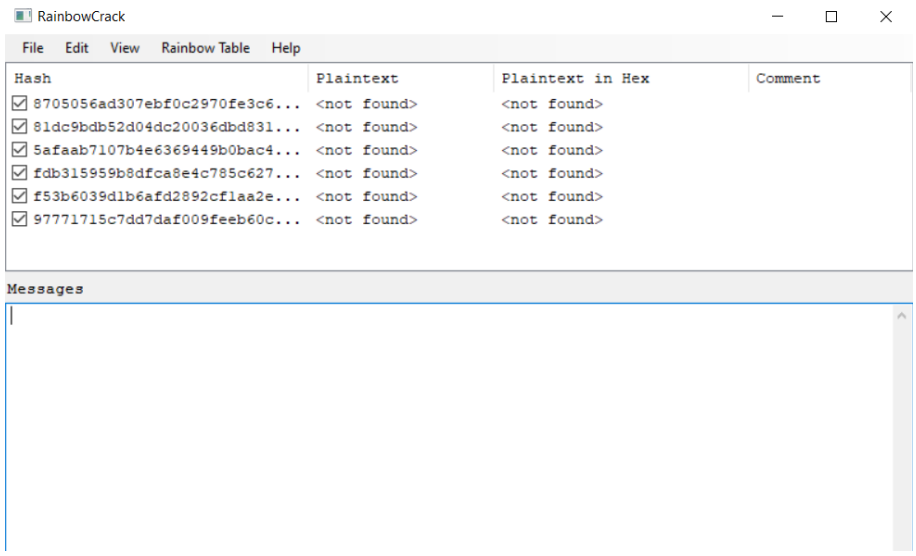


Now click OK, and press start, and wait for the table to generate. The tables are now ready to be used.

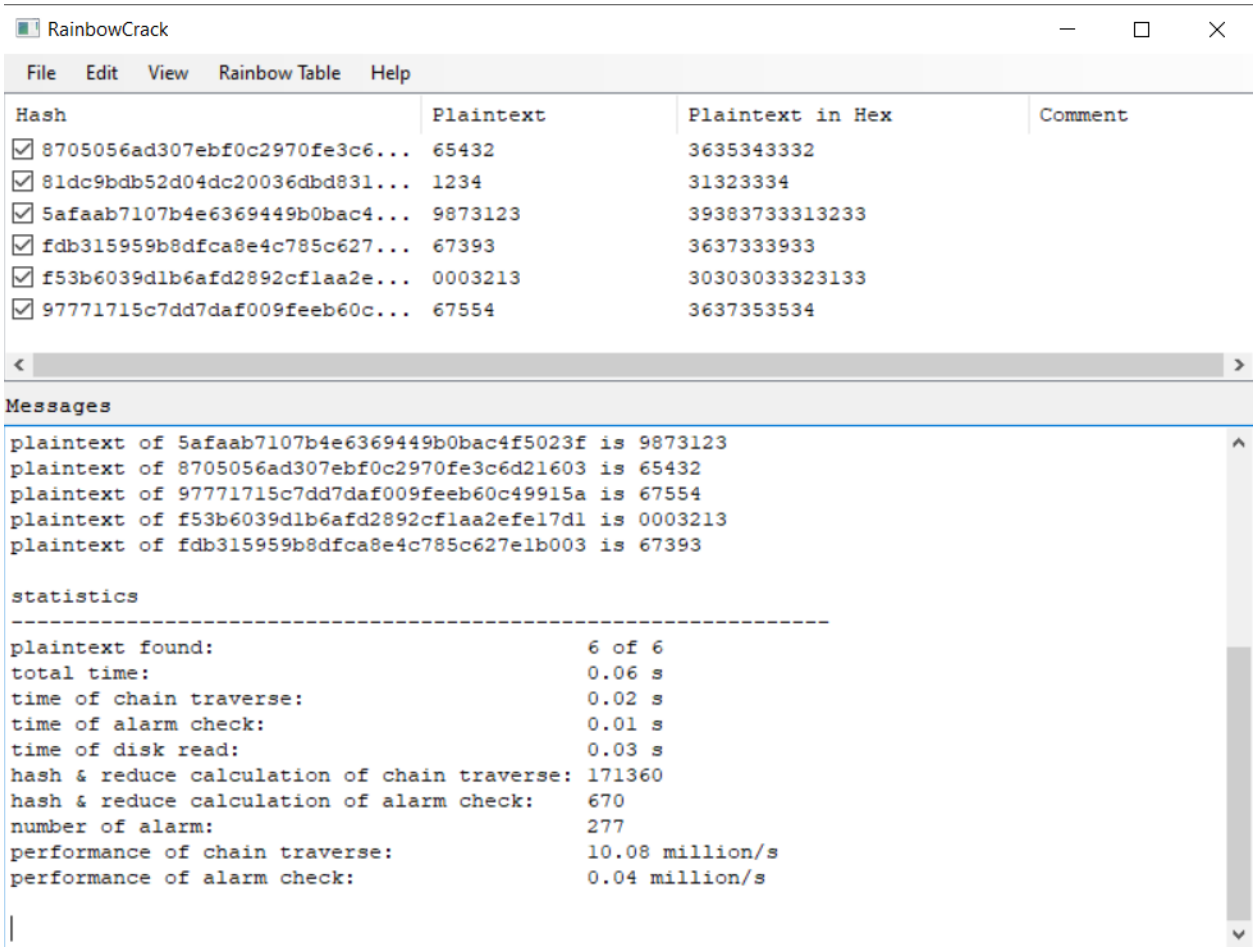
2) Now, run the rcrack_gui



3) Click file and add the hash of the password you want to crack, or make a text document of multiple hashes, each in one like, and open it.



4) Next, select the rainbow table to use.



So, all the passwords were deciphered.

ADVANTAGES

Unlike brute-forcing, performing the hash function isn't the problem here (since everything is precomputed). With all of the values already computed, it's simplified to just a simple search-and-compare operation on the table.

The exact password string isn't needed to be known. If the hash is matched, it doesn't matter if the string isn't the password itself. It will be authenticated.

DISADVANTAGES

A large amount of storage is required for store tables.

Rainbow table attacks can easily be prevented by using salt techniques, which is a random data that is passed into the hash function along with the plain text. This ensures that every password has a unique generated hash and hence, rainbow table attack, which works on the principle that more than one text can have the same hash value, is prevented.

Another technique that helps prevent precomputation attacks is key stretching. Using this, the salt, the password, and some intermediate hash values are run through the hash function multiple times to increase the computation time required to hash each password. An alternative approach, called key strengthening, extends the key with a random salt, but then (unlike in key stretching) securely deletes the salt. This forces both the attacker and legitimate users to perform a brute-force search for the salt value. Therefore, there is no point in by passing salting.