Rainbow Table Generation and Sort

Introduction

The RainbowCrack software cracks hashes by rainbow table lookup. Rainbow tables are ordinary files stored on hard disk.

This document explains the rtgen and rtsort programs. The rtgen program generate rainbow tables based on parameters specified by user, and the rtsort program post processing the rainbow tables to enable fast lookup.

After the two steps above, rainbow tables can be used to crack hashes with rcrack program.

Generate Rainbow Table with rtgen Program

Command line syntax of rtgen program:

```
rtgen hash_algorithm charset plaintext_len_min plaintext_len_max
table_index chain_len chain_num part_index
```

An example to generate a rainbow table set with 6 rainbow tables:

```
rtgen md5 loweralpha-numeric 1 7 0 3800 33554432 0

rtgen md5 loweralpha-numeric 1 7 1 3800 33554432 0

rtgen md5 loweralpha-numeric 1 7 2 3800 33554432 0

rtgen md5 loweralpha-numeric 1 7 3 3800 33554432 0

rtgen md5 loweralpha-numeric 1 7 4 3800 33554432 0

rtgen md5 loweralpha-numeric 1 7 5 3800 33554432 0
```

Options:

hash_algorithm	Rainbow table is hash algorithm specific. Rainbow table for a certain hash algorithm only helps to crack hashes of that type. The rtgen program natively support lots of hash algorithms like lm, ntlm, md5, sha1, mysqlsha1, halflmchall, ntlmchall, oracle-SYSTEM and md5-half. In the example above, we generate md5 rainbow tables that speed up cracking of md5 hashes.
charset	The charset includes all possible characters for the plaintext. "loweralpha-numeric" stands for "abcdefghijklmnopqrstuvwxyz0123456789", which is defined in configuration file charset.txt.
plaintext_len_min **plaintext_len_max**	These two parameters limit the plaintext length range of the rainbow table. In the example above, the plaintext length range is 1 to 7. So plaintexts like "a" and "abcdefg" are likely contained in the rainbow table generated. But plaintext "abcdefgh" with length 8 will not be

	contained.
table_index[1]	The table_index parameter selects the reduction function. Rainbow table with different table_index parameter uses different reduction function.
chain_len[1]	This is the rainbow chain length. Longer rainbow chain stores more plaintexts and requires longer time to generate.
chain_num[1]	Number of rainbow chains to generate. Rainbow table is simply an array of rainbow chains. Size of each rainbow chain is 16 bytes.
part_index	To store a large rainbow table in many smaller files, use different number in this parameter for each part and keep all other parameters identical.

[1] To fully understand the meaning of reduction function and the structure of rainbow table, reading of Philippe Oechslin's paper is necessary.

There are many rainbow table characteristics determined implicitly by table generation parameters:

Table Size	With .rt rainbow table format, file size of a rainbow table equals to chain_num parameter multiplied by 16.
Key Space	Key space is the number of possible plaintexts, calculated based on number of characters in charset and plaintext length range parameters. In the example above, key space is $36^1 + 36^2 + 36^3 + 36^4 + 36^5 + 36^6 + 36^7 = 80603140212$
Success Rate	The time-memory tradeoff algorithm is a probabilistic algorithm. Whatever the parameters are selected, there always exist many plaintexts (within the selected charset and plaintext length range) missing from the rainbow table generated. In the example above, success rate is 99.9% with all 6 rainbow tables. Success rate is determined by all table generation parameters except the hash_algorithm parameter.

To start generating the first rainbow table, run following command in a command window:

```
rtgen md5 loweralpha-numeric 1 7 0 3800 33554432 0
```

CPU will be busy computing rainbow chains. On system with multi-core processor, all cores are fully utilized.

To pause table generation, just press Ctrl+C and rtgen program will exit. Next time if the rtgen program is executed with exactly same parameters, table generation is resumed.

This command takes hours to complete with ordinary processor.

When finished, a file "md5_loweralpha-numeric#1-7_0_3800x33554432_0.rt" sized 512 MB is in current directory. The file name stores all table generation parameters.

Now generate the remaining 5 rainbow tables:

```
rtgen md5 loweralpha-numeric 1 7 1 3800 33554432 0

rtgen md5 loweralpha-numeric 1 7 2 3800 33554432 0
```

```
rtgen md5 loweralpha-numeric 1 7 3 3800 33554432 0
rtgen md5 loweralpha-numeric 1 7 4 3800 33554432 0
rtgen md5 loweralpha-numeric 1 7 5 3800 33554432 0
```

Finally, there are 6 rainbow tables generated:

```
536,870,912 md5_loweralpha-numeric#1-7_0_3800x33554432_0.rt
536,870,912 md5_loweralpha-numeric#1-7_1_3800x33554432_0.rt
536,870,912 md5_loweralpha-numeric#1-7_2_3800x33554432_0.rt
536,870,912 md5_loweralpha-numeric#1-7_3_3800x33554432_0.rt
536,870,912 md5_loweralpha-numeric#1-7_4_3800x33554432_0.rt
536,870,912 md5_loweralpha-numeric#1-7_5_3800x33554432_0.rt
```

Sort Rainbow Table with rtsort Program

Rainbow table is an array of rainbow chains. Each rainbow chain has a start point and an end point. The rtsort program sorts the rainbow chains by end point to make binary search possible.

Run following command to sort all .rt rainbow tables in current directory:

```
rtsort .
```

Never interrupt the rtsort program; otherwise the rainbow table being sorted may be damaged.

If free memory size is smaller than the size of rainbow table being sorted, temporary hard disk space as large as the rainbow table size is needed to store intermediate results.