

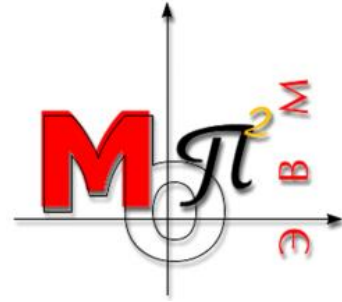
МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждения высшего
образования

«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт компьютерных технологий и информационной безопасности

Кафедра математического обеспечения и применения ЭВМ



ЛАБОРАТОРНАЯ РАБОТА № 5

по дисциплине

«Безопасность информационных технологий»

на тему:

«Hash-функции»

Вариант № 1

Выполнил:

Студент группы

КТбo2-8

Нестеренко П. А.

Проверил:

доцент кафедры

ИБТКС

Петров Д. А.

Оценка

«____» _____ 2020 г.

Введение

Данный лабораторный практикум преследует две цели:

- 1) закрепить навыки обучающихся по правильному формированию паролей пользователей путём сравнения эффективности восстановления паролей, имеющих различные параметры;
- 2) показать, как неправильное использование стойких криптографических алгоритмов может привести к созданию слабозащищённых систем идентификации и аутентификации пользователей (на примере LM-хэшей).

В ходе выполнения данного лабораторного практикума обучающийся получит навыки по самостоятельному формированию различных хэш-функций от паролей пользователей, получит возможность сравнить эффективность двух различных подходов к восстановлению паролей пользователей: на основе методов перебора (полного, по словарю, с мутациями символов и т.д.) и на основе техники криптоанализа по размену «время — память» (с использованием радужных таблиц).

Практическое задание

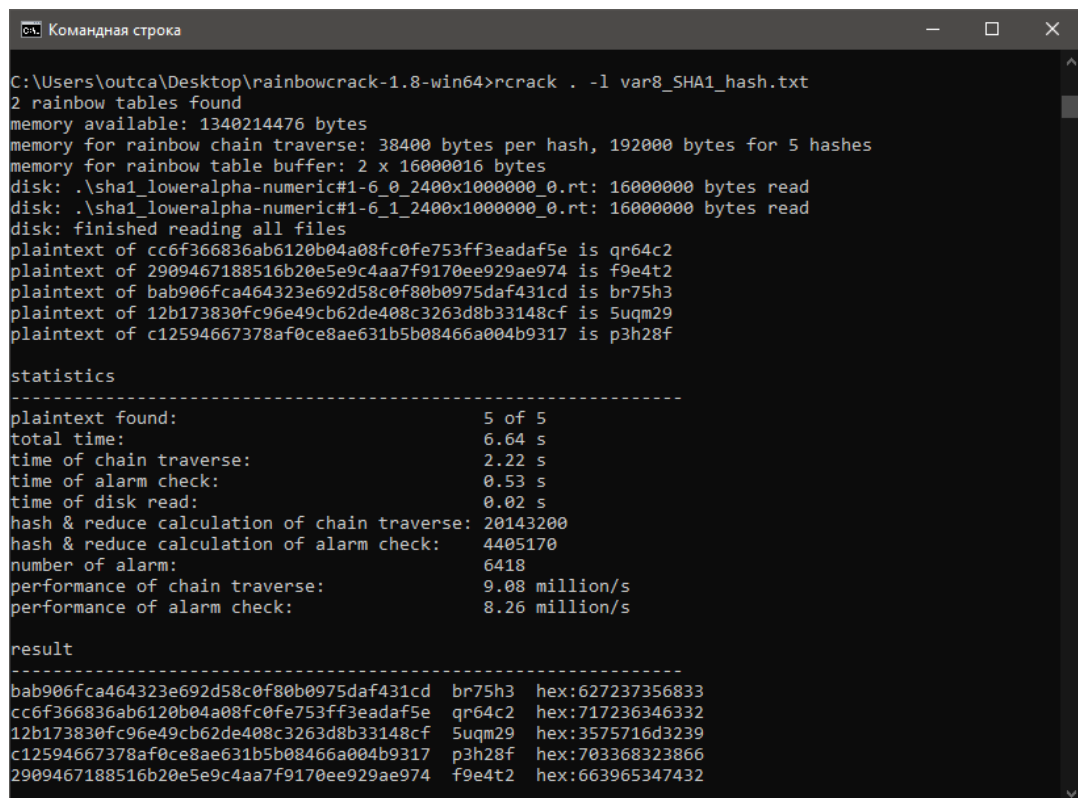
Вариант №1.

1. По заданным значениям хэш-функций восстановить пароли пользователей, результаты занести в таблицу. Указать долю правильно восстановленных паролей.
2. Дополнительно сформировать пароли и соответствующие им sha1-хэши, состоящие из русских символов и цифр (длиной не более 6 символов).
3. Сформировать радужную таблицу с использованием символов русского алфавита и набора цифр. Приложить её к отчёту (в электронном виде).

Восстановление паролей

SHA1-Hash

Результат работы программы **rainbowcrack** представлен на рисунке 1. Как видим, найдены 3 из 5 паролей. Занесем результаты в таблицу 1.



```
C:\Users\outca\Desktop\rainbowcrack-1.8-win64>rcrack . -l var8_SHA1_hash.txt
2 rainbow tables found
memory available: 1340214476 bytes
memory for rainbow chain traverse: 38400 bytes per hash, 192000 bytes for 5 hashes
memory for rainbow table buffer: 2 x 16000016 bytes
disk: .\sha1_loweralpha-numeric#1-6_0_2400x1000000_0.rt: 16000000 bytes read
disk: .\sha1_loweralpha-numeric#1-6_1_2400x1000000_0.rt: 16000000 bytes read
disk: finished reading all files
plaintext of cc6f366836ab6120b04a08fc0fe753ff3eadaf5e is qr64c2
plaintext of 2909467188516b20e5e9c4aa7f9170ee929ae974 is f9e4t2
plaintext of bab906fca464323e692d58c0f80b0975daf431cd is br75h3
plaintext of 12b173830fc96e49cb62de408c3263d8b33148cf is 5uqm29
plaintext of c12594667378af0ce8ae631b5b08466a004b9317 is p3h28f

statistics
-----
plaintext found:          5 of 5
total time:              6.64 s
time of chain traverse:   2.22 s
time of alarm check:     0.53 s
time of disk read:       0.02 s
hash & reduce calculation of chain traverse: 20143200
hash & reduce calculation of alarm check:    4405170
number of alarm:         6418
performance of chain traverse: 9.08 million/s
performance of alarm check:  8.26 million/s

result
-----
bab906fca464323e692d58c0f80b0975daf431cd  br75h3  hex:627237356833
cc6f366836ab6120b04a08fc0fe753ff3eadaf5e  qr64c2  hex:717236346332
12b173830fc96e49cb62de408c3263d8b33148cf  5uqm29  hex:3575716d3239
c12594667378af0ce8ae631b5b08466a004b9317  p3h28f  hex:703368323866
2909467188516b20e5e9c4aa7f9170ee929ae974  f9e4t2  hex:663965347432
```

Рисунок 1 – Результат работы rainbowcrack

Результат работы программы **BruteHash** по восстановлению пароля из последнего хэша представлен на рисунке 2. Все результаты занесем в таблицу 2. Как видим, не восстановлено ни одного пароля – это объясняется тем, что в словаре, который мы выбрали, не содержится паролей, имеющих введенные хэши.

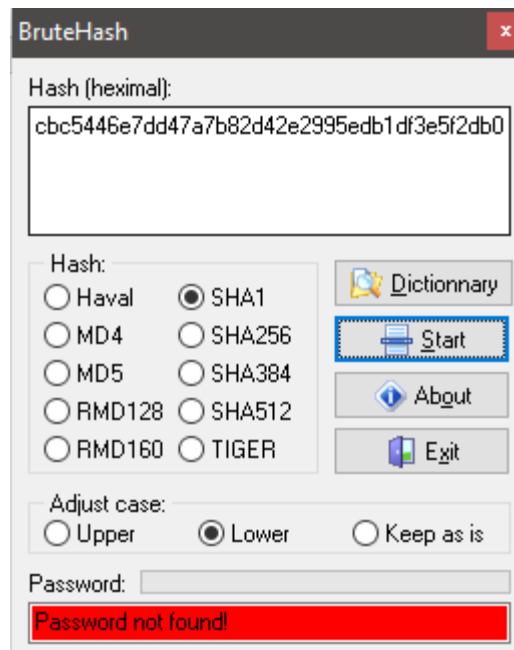


Рисунок 2 – Результат восстановления пароля по последнему хэшу в BruteHash

Таблица 1. Результат работы rainbowcrack

| SHA1-хэш | Пароль |
|--|-----------------|
| cbc5446e7dd47a7b82d42e2995edb1df3e5f2db0 | Не восстановлен |
| 6a5912c3781eede62390786fbd43d69c9cca3dc9 | fw42t7 |
| aaf044a02f19b365db04873cda6481b175c54141 | Не восстановлен |
| 8a058c61af5dd9d91ffa6007f1499a9154113a34 | h4t86q |
| 9af733a383a885f7c07325d71a49c9ae857b53f8 | x26kv9 |

Таблица 2. Результат работы BruteHash

| SHA1-хэш | Пароль |
|--|-----------------|
| cbc5446e7dd47a7b82d42e2995edb1df3e5f2db0 | Не восстановлен |
| 6a5912c3781eede62390786fbd43d69c9cca3dc9 | Не восстановлен |
| aaf044a02f19b365db04873cda6481b175c54141 | Не восстановлен |
| 8a058c61af5dd9d91ffa6007f1499a9154113a34 | Не восстановлен |
| 9af733a383a885f7c07325d71a49c9ae857b53f8 | Не восстановлен |

MD5-Hash

Результат работы программы **Rainbowcrack** представлен на рисунке 3. Как видим, 5 из 5 паролей найдено. Занесем результаты в таблицу 3.

```
C:\Users\User\Desktop\mop_evm\BIT\lab5(Passwords)\lr1\data\progs\rainbowcrack-1.6.1-win64\rainbowcrack-1.6.1-win64\rainbowcrack-1.6.1-win64>rcrack md5_loweralpha-numeric#1-6_0_2400x4000000_0.rt -l xexam.txt
1497706905 bytes memory available
1 x 64000000 bytes memory allocated for table buffer
192000 bytes memory allocated for chain traverse
disk: md5_loweralpha-numeric#1-6_0_2400x4000000_0.rt: 64000000 bytes read
searching for 5 hashes...
plaintext of 72cf870a0290c931e39d1c814bbcb0fc is 23ea4h
plaintext of 357b1a263fa0ea406f73f7d16b8532bb is 3tvz72
plaintext of 3446a71cc08e28516943567df4676d82 is c6en43
plaintext of 3dc11bbdbcb578a8cc28c371430489a48 is 8dc3n4
plaintext of 2aa1010cc58d6d3fcf6cad27737c8f6e is 4st27h
disk: thread exited

statistics
-----
plaintext found: 5 of 5
total time: 1.11 s
time of chain traverse: 0.84 s
time of alarm check: 0.19 s
time of wait: 0.00 s
time of other operation: 0.00 s
time of disk read: 0.06 s
hash & reduce calculation of chain traverse: 14388000
hash & reduce calculation of alarm check: 4047813
number of alarm: 11392
speed of chain traverse: 17.03 million/s
speed of alarm check: 21.53 million/s

result
-----
2aa1010cc58d6d3fcf6cad27737c8f6e 4st27h hex:347374323768
357b1a263fa0ea406f73f7d16b8532bb 3tvz72 hex:3374767a3732
3446a71cc08e28516943567df4676d82 c6en43 hex:8336666e4433
3dc11bbdbcb578a8cc28c371430489a48 8dc3n4 hex:386461336e34
72cf870a0290c931e39d1c814bbcb0fc 23ea4h hex:323365613468

C:\Users\User\Desktop\mop_evm\BIT\lab5(Passwords)\lr1\data\progs\rainbowcrack-1.6.1-win64\rainbowcrack-1.6.1-win64>
```

Рисунок 3 – Результат работы Rainbowcrack

Результат работы программы **BruteHash** по восстановлению пароля из последнего хэша представлен на рисунке 4. Все результаты занесем в таблицу 4. Как видим, не восстановлено ни одного пароля – это объясняется тем, что в словаре, который мы выбрали, не содержится паролей, имеющих введенные хэши.

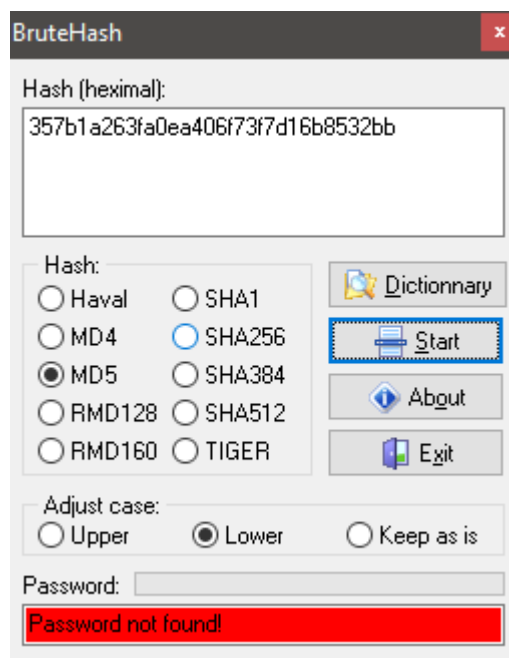


Рисунок 4 - Результат восстановления пароля по последнему хэшу в BruteHash

Таблица 3. Результат работы Rainbowcrack

| MD5-хэш | Пароль |
|-----------------------------------|--------|
| 2aa1010cc58d6d3fcf6cad27737c8f6e | 4st27h |
| 357b1a263fa0ea406f73f7d16b8532bb | 3tvz72 |
| 3446a71cc08e28516943567df4676d82 | c6en43 |
| 3dc11bbdbcb578a8cc28c371430489a48 | 8dc3n4 |
| 72cf870a0290c931e39d1c814bbcb0fc | 23ea4h |

Таблица 4. Результат работы BruteHash

| MD5-хэш | Пароль |
|----------------------------------|-----------------|
| 2aa1010cc58d6d3fcf6cad27737c8f6e | Не восстановлен |
| 357b1a263fa0ea406f73f7d16b8532bb | Не восстановлен |

| | |
|----------------------------------|-----------------|
| 3446a71cc08e28516943567df4676d82 | Не восстановлен |
| 3dc11bbdbc578a8cc28c371430489a48 | Не восстановлен |
| 72cf870a0290c931e39d1c814bbcb0fc | Не восстановлен |

LM-Hash

Количество возможных комбинаций для подбора:
 $36^1 + 36^2 + 36^3 + 36^4 + 36^5 + 36^6 + 36^7 + 36^8 + 36^9 + 36^{10} + 36^{11} + 36^{12} =$
4873763662273663092

Поскольку количество возможных комбинаций становится слишком большим, использовать данный метод (генерация таблиц и поиск в **Rainbowcrack**) становится нецелесообразно.

Воспользуемся программой **Ophcrack**. Результат ее работы представлен на рисунке 5. Как видим, для всех LM-хэшей восстановлены слова (причем за 13 секунд). В качестве таблицы использовалась **tables_xp_free_small**.

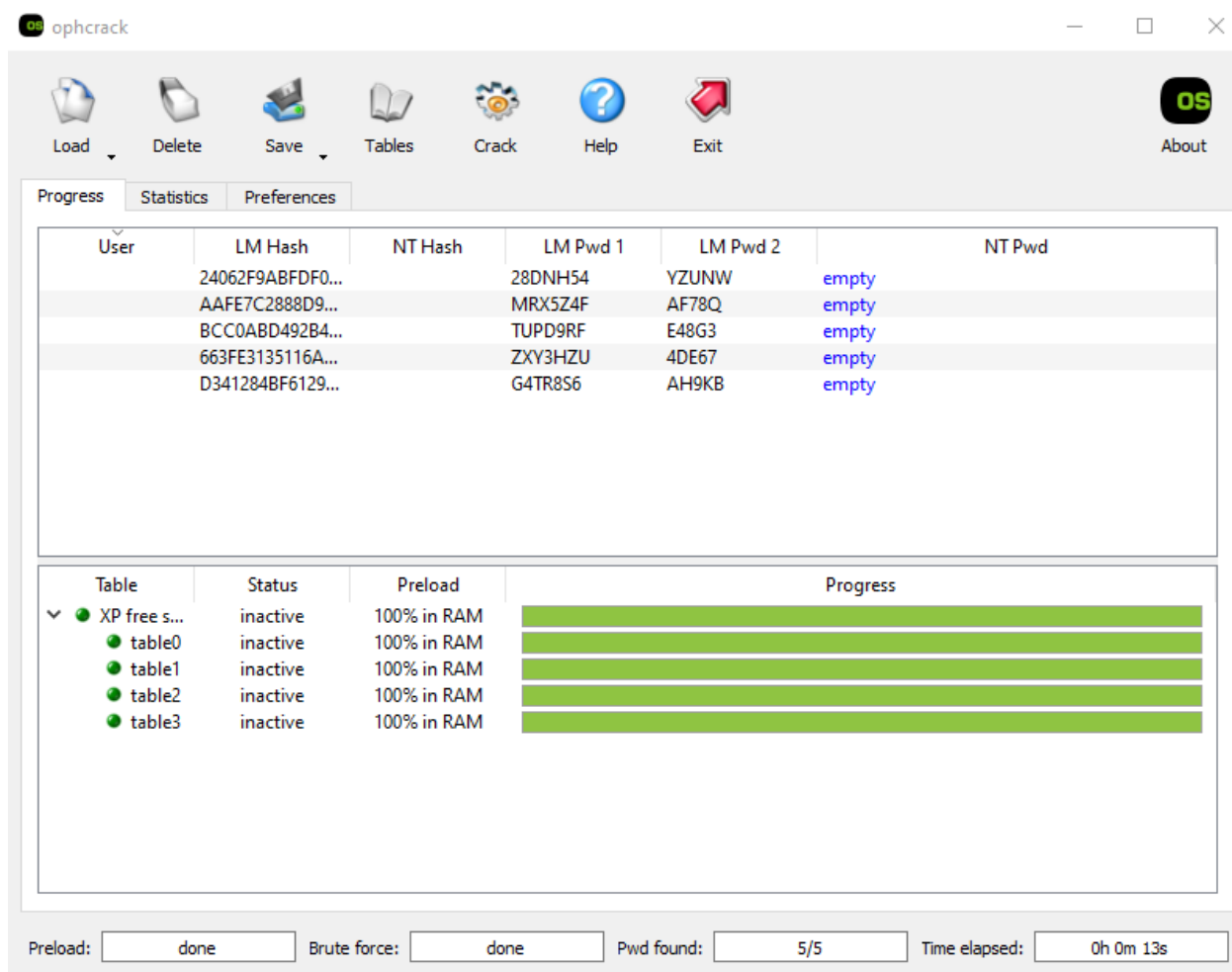


Рисунок 5 – Результат работы ophcrack

Также с LM-хэшами позволяет работать программа **SAMInside**. Результаты ее работы представлены на рисунках 6 (метод BruteForce) и 7 (атака по словарю). Как видим, пароли не восстановлены – это можно объяснить отсутствием в

словаре подходящих паролей (для атаки по словарю) и размерностью перебора (для метода BruteForce)

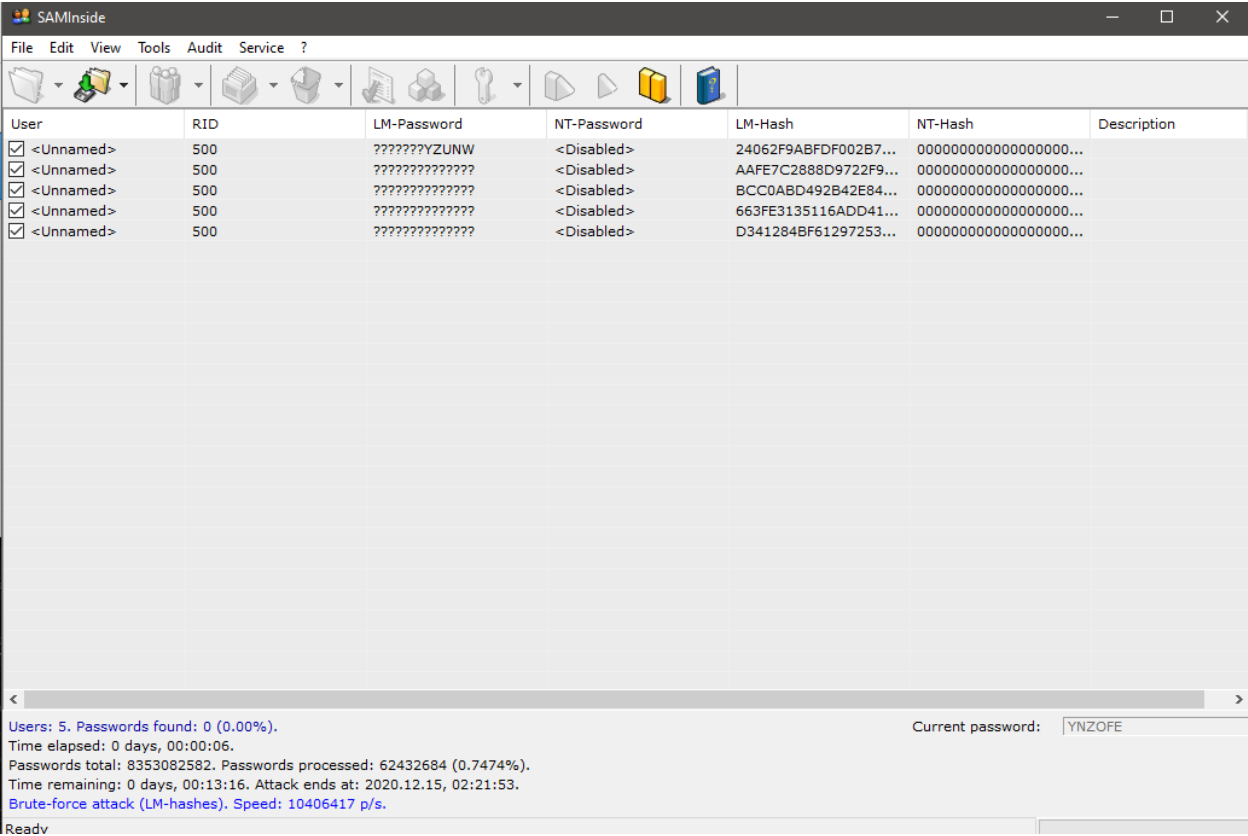


Рисунок 6 – Результат работы SAMInside (BruteForce)

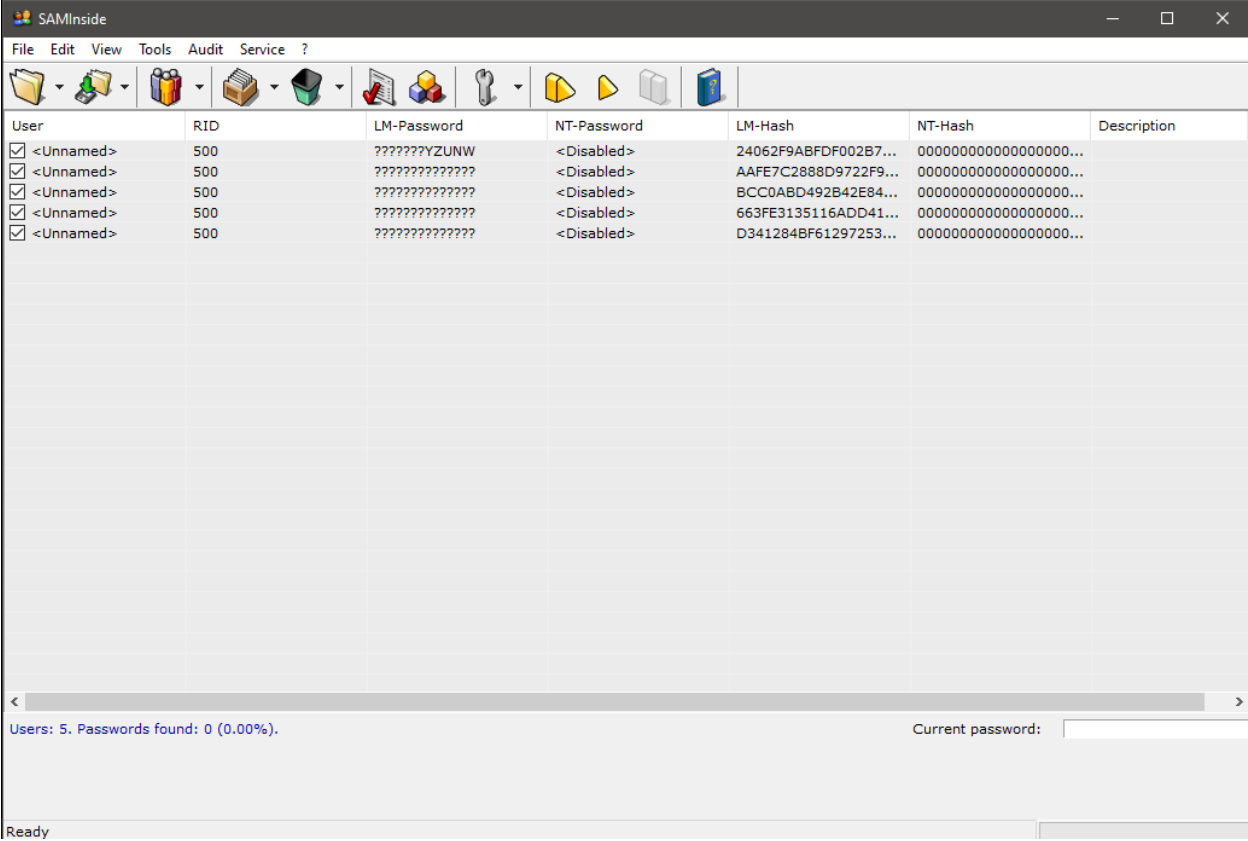


Рисунок 7 – Результат работы SAMInside (Атака по словарю)

Создание русских паролей

Для формирования SHA1-хэшей воспользуемся программой **DAMN Hash Calculator**. Пример формирования SHA1-хэша представлен на рисунке 8. Результаты занесем в таблицу 5 (также имеем возможность сформировать MD5-хэши, отметив соответствующую галочку, и дальше работать с ними).

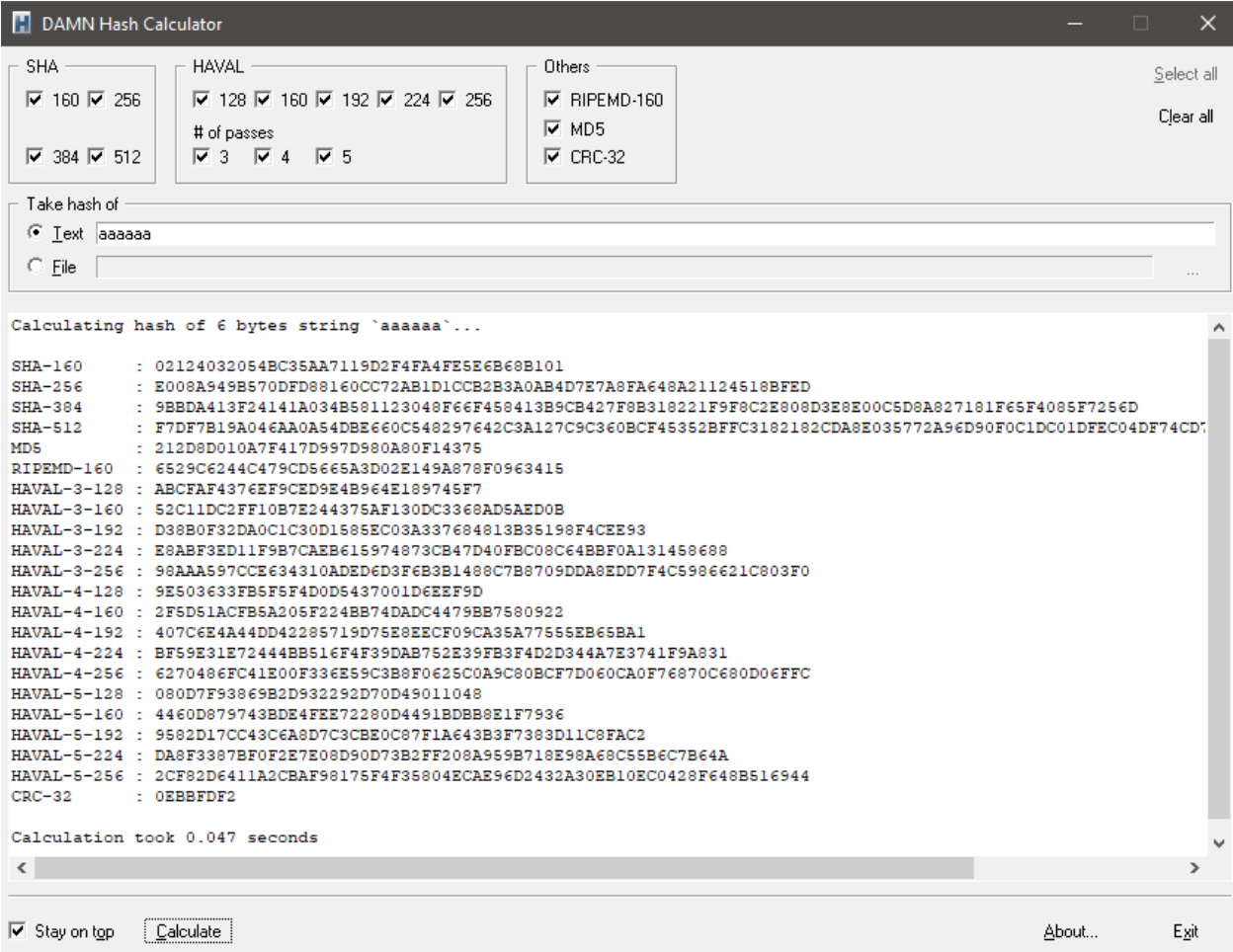


Рисунок 8 – Пример формирования SHA1-хэша в DAMN Hash Calculator

Таблица 5. Результат работы DAMN Hash Calculator

| Пароль | SHA1-хэш |
|--------|--|
| aaaaaa | 02124032054BC35AA7119D2F4FA4FE5E6B68B101 |
| 666666 | 30F7F0ED6010AB6512AD7AC098224D63727650EA |
| cccccc | E65F0CB4BF58DA004C6D491E3250664400A508C1 |
| vvvvvv | 176D312C00496BC44654424C33FBF315BF4D9A2C |
| 123456 | 7C4A8D09CA3762AF61E59520943DC26494F8941B |
| привет | C20431C0A93F36C9540BF21E784C40B8369E62A2 |
| члчлчч | 26B249C212E45767F083A472F0C697ABA79789B0 |
| йцуаоы | F76749FFB35040822D7630DF1ABC8CD9ECFAA03C |
| хжюбът | 707CB529B6255B91F3BA0BB881999ACAF22119B3 |
| фдфдфд | 8F48696A6B60D7BDFD078C9A3D1CE0FFB9B5ABA4 |
| фж21ыф | 5D937524958FCCF55605C310544E42A21FAA36C9 |

| | |
|--------|--|
| parala | 0D0246F914FA3EC4EA404741B2C691A530AEE8EB |
| 918273 | 6A99AA7B1CB8F2D5AFE8F53F99D3E8E61AC21529 |
| 1зй0щ2 | 9A1B7178681733036DA234005310EE4E40CCC75C |

Формирование русской радужной таблицы

Для формирования таблицы составим команду: исходный набор символов содержит 43 объекта: ёйцукенгшщзхъфывапроджэячсмитьбю0123456789.

Определим количество возможных вариантов перебора для паролей длиной не более 6 символов: $43^1 + 43^2 + 43^3 + 43^4 + 43^5 + 43^6 = 6471871692$

Выберем длину цепочки 2400, количество цепочек 40000000

rtgen.exe sha1 lowerrus-numeric 1 6 0 2400 4000000 laba

Восстановление русских паролей

Результат восстановления русских паролей представлен на рисунке 9. Как видим, все пароли восстановлены.

```
C:\Users\User\Desktop\mop_evm\BIT\lab5(Passwords)\всё что нужно\rainbowcrack-1.7-win64>rcrack.exe . -l hash.txt
4 rainbow tables found
memory available: 1991799603 bytes
memory for rainbow chain traverse: 38400 bytes per hash, 537600 bytes for 14 hashes
memory for rainbow table buffer: 4 x 64000016 bytes
disk: .\sha1_lowerrus-numeric#1-6_0_2400x4000000_0.rt: 64000000 bytes read
disk: .\sha1_lowerrus-numeric#1-6_1_2400x4000000_0.rt: 64000000 bytes read
disk: .\sha1_lowerrus-numeric#1-6_2_2400x4000000_0.rt: 64000000 bytes read
disk: .\sha1_lowerrus-numeric#1-6_3_2400x4000000_0.rt: 64000000 bytes read
disk: finished reading all files
plaintext of c20431c0a93f36c9540bf21e784c40b8369e62a2 is \xef\x0\x8\x2\x5\x2
plaintext of 6a99aa7b1cb8f2d5afe8f53f99d3e8e61ac21529 is 918273
plaintext of e65f0cb4bf58da004c6d491e3250664400a508c1 is \xf1\xf1\xf1\xf1\xf1
plaintext of 7c4a8d09ca3762af61e59520943dc26494f8941b is 123456
plaintext of 5d937524958fccf55605c310544e42a21faa36c9 is \xf4\xe621\xfb\xf4
plaintext of f76749ffb35040822d7630df1abc8cd9ecfaa03c is \xe9\xf6\xf3\xe0\xee\xfb
plaintext of 176d312c00496bc44654424c33fbf315bf4d9a2c is \xe2\xe2\xe2\xe2\xe2
plaintext of 9a1b7178681733036da234005310ee4e40ccc75c is 1\xe7\xe90\xf92
plaintext of 8f48696a6b60d7bdfd078c9a3d1ce0ffb9b5aba4 is \xf4\xe4\xf4\xe4\xf4\xe4
plaintext of 0d0246f914fa3ec4ea404741b2c691a530aee8eb is \xf0\xe0\xf0\xe0\xe0
plaintext of 26b249c212e45767f083a472f0c697aba79789b0 is \xf7\xeb\xf7\xeb\xeb\xf7
plaintext of 30f7f0ed6010ab6512ad7ac098224d63727650ea is \xe1\xe1\xe1\xe1\xe1\xe1
plaintext of 02124032054bc35aa7119d2f4fa4fe5e6b68b101 is \xe0\xe0\xe0\xe0\xe0
plaintext of 707cb529b6255b91f3ba0bb881999acaf22119b3 is \xf5\xe6\xfe\xe1\xfc\xf2

statistics
-----
plaintext found:                14 of 14
total time:                     7.28 s
time of chain traverse:         5.86 s
time of alarm check:           1.30 s
time of disk read:              0.88 s
hash & reduce calculation of chain traverse: 46041600
hash & reduce calculation of alarm check:    9154825
number of alarm:                16014
performance of chain traverse:   7.86 million/s
performance of alarm check:     7.06 million/s

result
-----
02124032054bc35aa7119d2f4fa4fe5e6b68b101 \xe0\xe0\xe0\xe0\xe0\xe0 hex:e0e0e0e0e0e0
30f7f0ed6010ab6512ad7ac098224d63727650ea \xe1\xe1\xe1\xe1\xe1\xe1 hex:e1e1e1e1e1e1
e65f0cb4bf58da004c6d491e3250664400a508c1 \xf1\xf1\xf1\xf1\xf1\xf1 hex:f1f1f1f1f1f1
176d312c00496bc44654424c33fbf315bf4d9a2c \xe2\xe2\xe2\xe2\xe2\xe2 hex:e2e2e2e2e2e2
7c4a8d09ca3762af61e59520943dc26494f8941b 123456 hex:313233343536
c20431c0a93f36c9540bf21e784c40b8369e62a2 \xef\x0\x8\x2\x5\x2 hex:eff0e8e2e5f2
26b249c212e45767f083a472f0c697aba79789b0 \xf7\xeb\xf7\xeb\xeb\xf7 hex:f7ebf7ebbf7
f76749ffb35040822d7630df1abc8cd9ecfaa03c \xe9\xf6\xf3\xe0\xee\xfb hex:e9f6f3e0eebf
707cb529b6255b91f3ba0bb881999acaf22119b3 \xf5\xe6\xfe\xe1\xfc\xf2 hex:f5e6fee1fcf2
8f48696a6b60d7bdfd078c9a3d1ce0ffb9b5aba4 \xf4\xe4\xf4\xe4\xf4\xe4 hex:f4e4f4e4f4e4
5d937524958fccf55605c310544e42a21faa36c9 \xf4\xe621\xfb\xf4 hex:f4e63231fbf4
0d0246f914fa3ec4ea404741b2c691a530aee8eb \xf0\xe0\xf0\xe0\xe0 hex:f0e0f0e031e0
6a99aa7b1cb8f2d5afe8f53f99d3e8e61ac21529 918273 hex:393138323733
9a1b7178681733036da234005310ee4e40ccc75c 1\xe7\xe90\xf92 hex:31e7e930f932

C:\Users\User\Desktop\mop_evm\BIT\lab5(Passwords)\всё что нужно\rainbowcrack-1.7-win64>
```

Заключение

В результате выполнения лабораторной работы я научился восстанавливать пароли по их хеш-функциям. Восстановление эффективно работает для коротких паролей, использующих узкий пул возможных символов. Из данного факта можно сделать заключение, что длинные и сложные пароли использующие разные регистры и спец. символы, являются наиболее устойчивыми к восстановлению по хеш-функции.