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

КТбо2-8

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).

**Востановление паролей**

**SHA1-Hash**

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

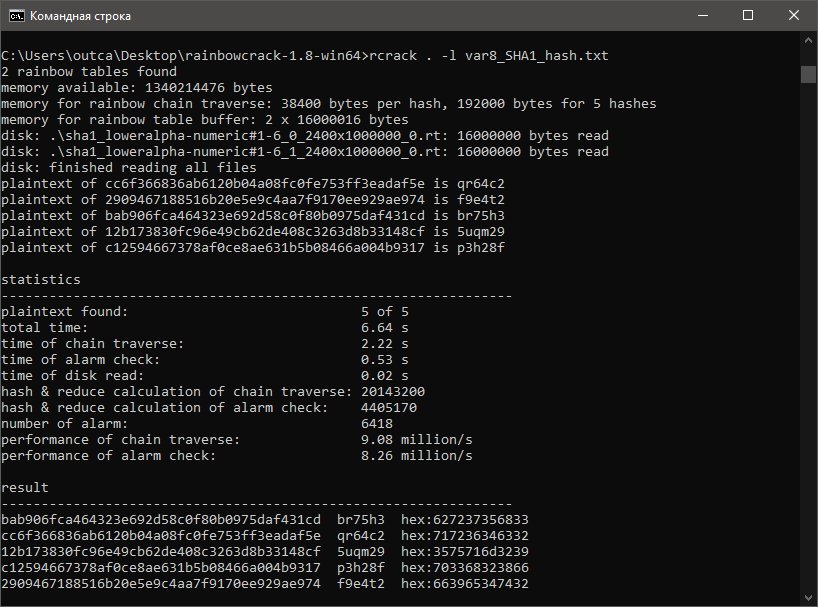


Рисунок 1 – Результат работы rainbowcrack

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.

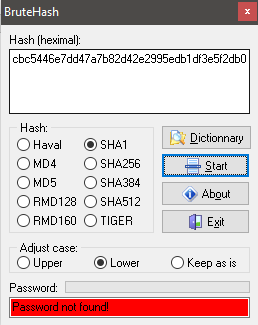


Рисунок 2 – Результат восстановления пароля по последнему хэшу в BruteHash

Таблица 1. Результат работы rainbowcrack

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

Таблица 2. Результат работы BruteHash

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

**MD5-Hash**

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

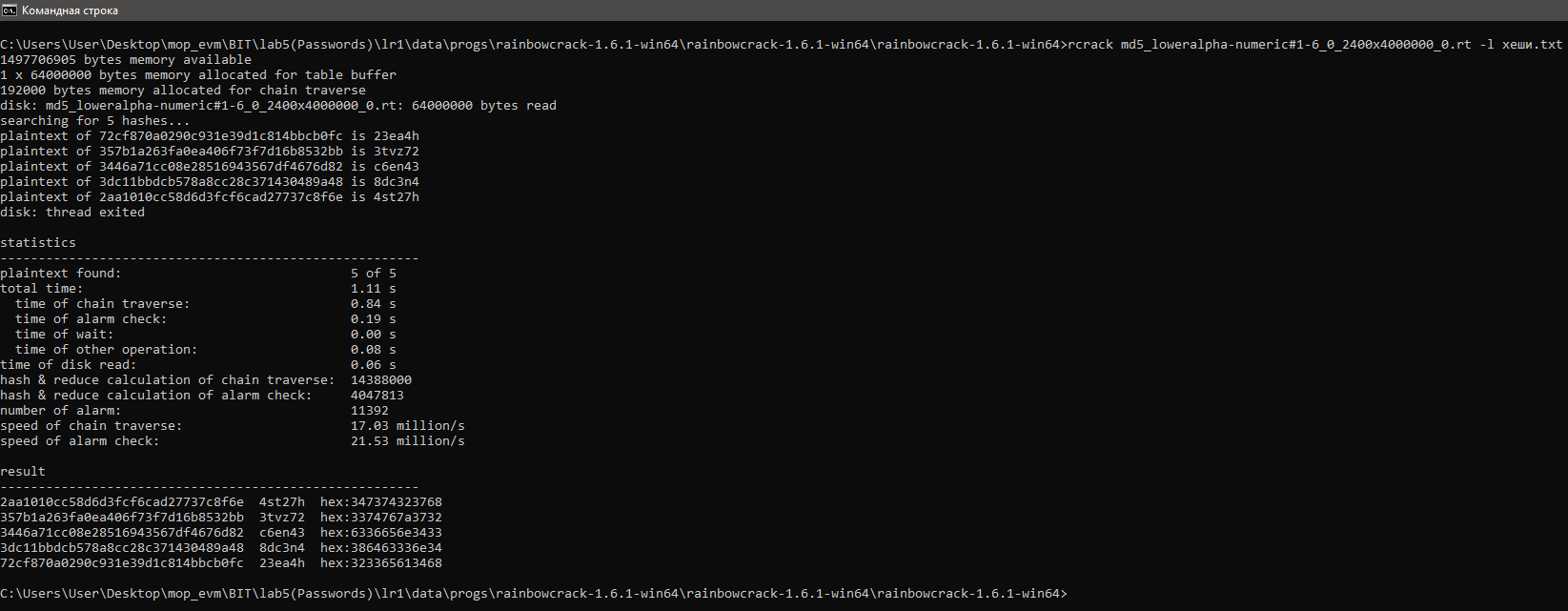


Рисунок 3 – Результат работы Rainbowcrack

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.

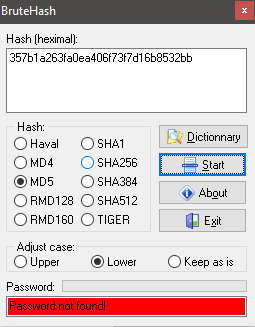


Рисунок 4 - Результат восстановления пароля по последнему хэшу в BruteHash

Таблица 3. Результат работы Rainbowcrack

|  |  |
| --- | --- |
| **MD5-хэш** | **Пароль** |
| 2aa1010cc58d6d3fcf6cad27737c8f6e  357b1a263fa0ea406f73f7d16b8532bb  3446a71cc08e28516943567df4676d82  3dc11bbdcb578a8cc28c371430489a48  72cf870a0290c931e39d1c814bbcb0fc | 4st27h  3tvz72  c6en43  8dc3n4  23ea4h |

Таблица 4. Результат работы BruteHash

|  |  |
| --- | --- |
| **MD5-хэш** | **Пароль** |
| 2aa1010cc58d6d3fcf6cad27737c8f6e  357b1a263fa0ea406f73f7d16b8532bb  3446a71cc08e28516943567df4676d82  3dc11bbdcb578a8cc28c371430489a48  72cf870a0290c931e39d1c814bbcb0fc | Не восстановлен  Не восстановлен  Не восстановлен  Не восстановлен  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 возможный 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 секунды). В качестве таблицы использовалась **tables\_xp\_free\_small**.

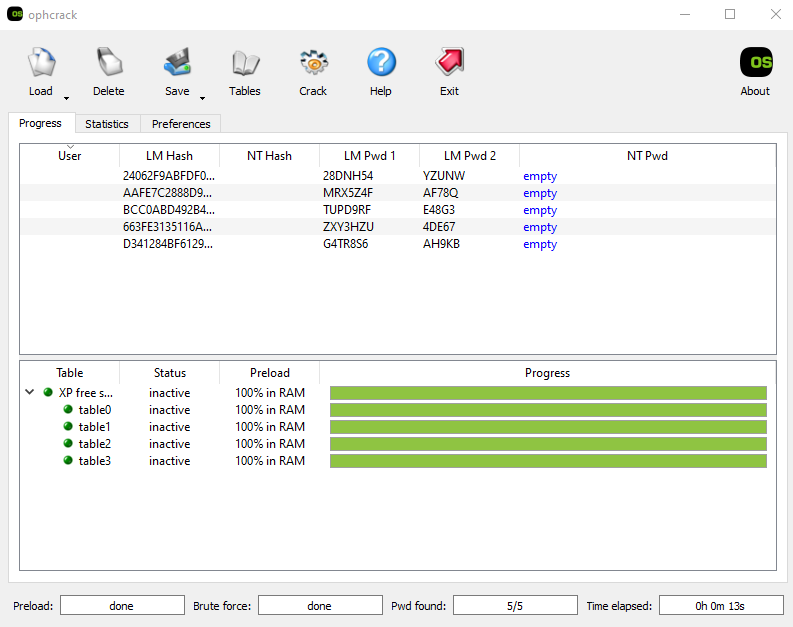


Рисунок 5 – Результат работы ophcrack

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)

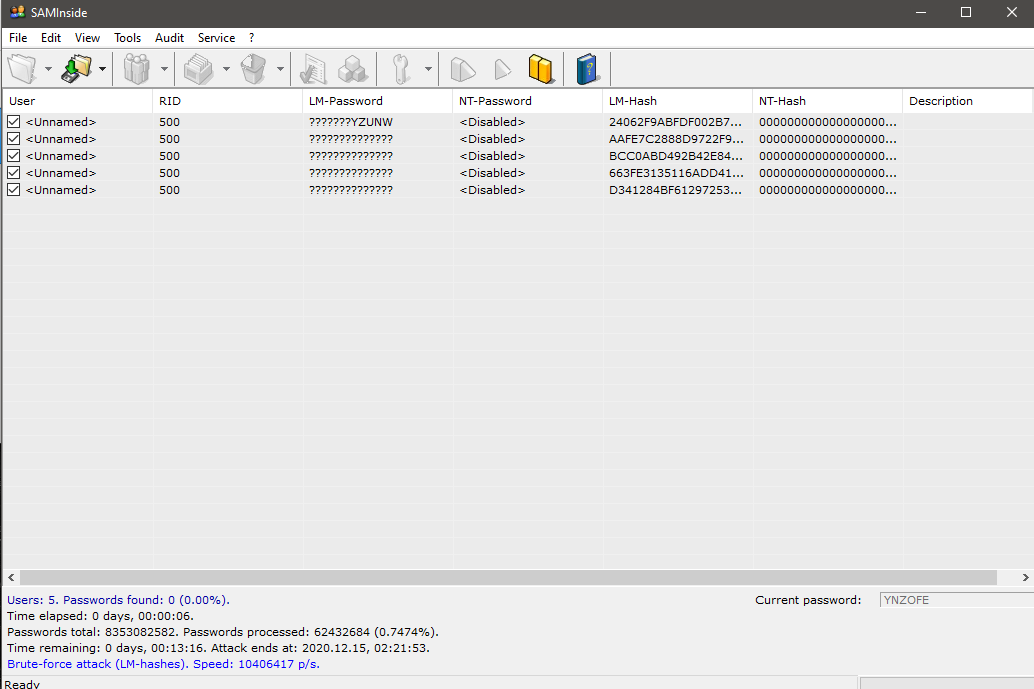


Рисунок 6 – Результат работы SAMInside (BruteForce)

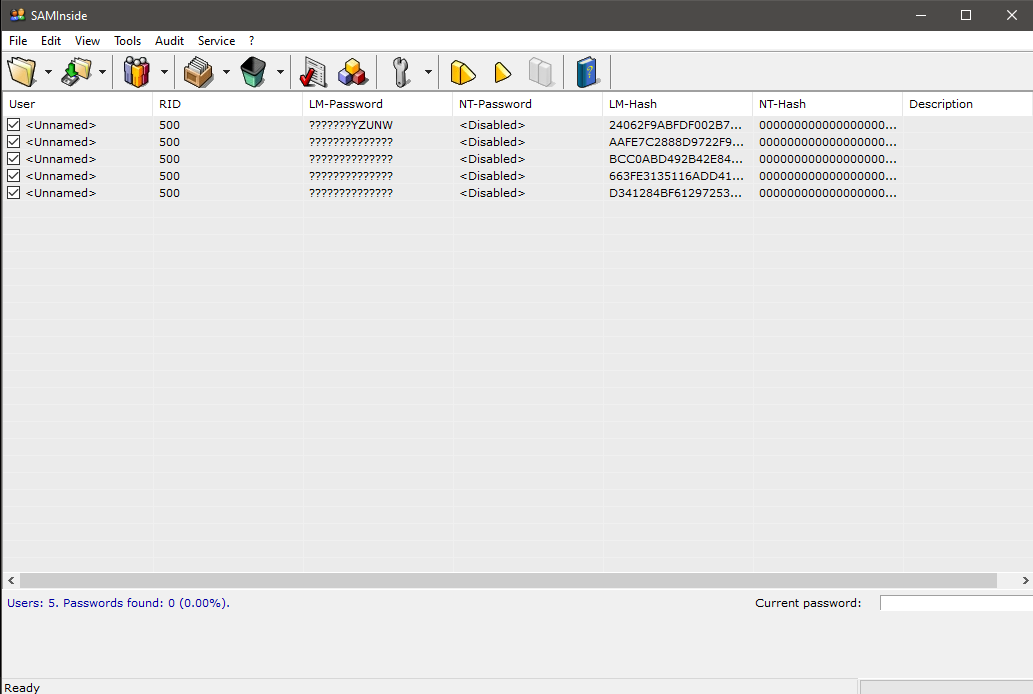


Рисунок 7 – Результат работы SAMInside (Атака по словарю)

**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).

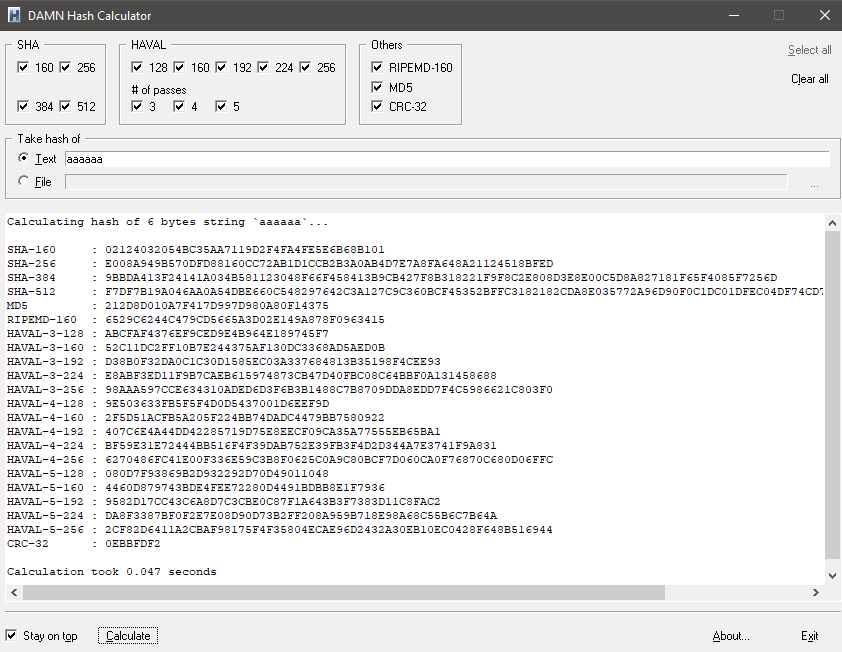


Рисунок 8 – Пример формирования SHA1-хэша в DAMN Hash Calculator

Таблица 5. Результат работы DAMN Hash Calculator

|  |  |
| --- | --- |
| Пароль | SHA1-хэш |
| аааааа  бббббб  сссссс  вввввв  123456  привет  члчллч  йцуаоы  хжюбьт  фдфдфд  фж21ыф  рара1а  918273  1зй0щ2 ||

**Формирование русской радужной таблицы**

Для формирования таблицы составим команду: исходный набор символов содержит 43 объекта: **ёйцукенгшщзхъфывапролджэячсмитьбю0123456789.**

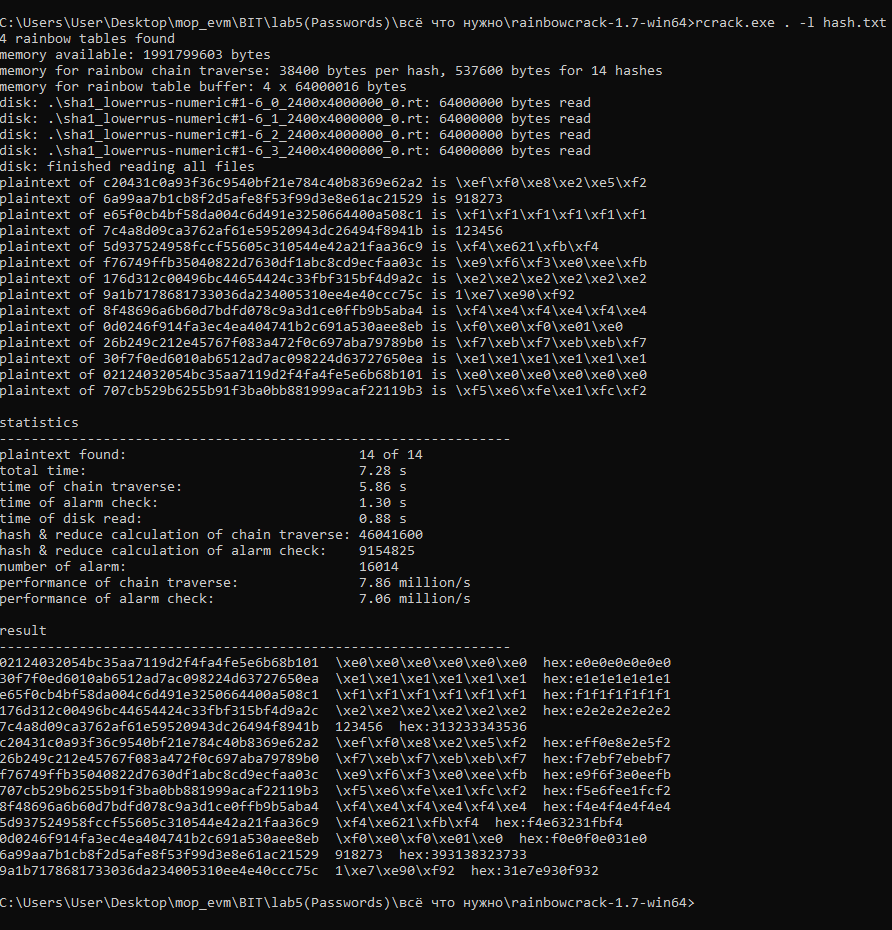
Определим количество возможных вариантов перебора для паролей длиной не более 6 символов: 43^1+43^2+43^3+43^4+43^5+43^6=**6471871692**

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.



**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.