ЛАБОРАТОРНАЯ РАБОТА №5

**на тему: «ВОССТАНОВЛЕНИЕ И ФОРМИРОВАНИЕ ПАРОЛЕЙ ПОЛЬЗОВАТЕЛЕЙ»**

по дисциплине «Безопасность информационных технологий»

**Вариант 2**

Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

(ФГАОУ ВО «ЮФУ»)

Инженерно-технологическая Академия

Институт компьютерных технологий и информационной безопасности

Кафедра Систем Автоматизированного Проектирования

им. В. М. Курейчика

Выполнили

студенты КТбо2-4 \_\_\_\_\_\_\_\_\_\_\_\_\_ А. А. Воронов, В. С. Якунин

Принял

ст. пр. каф. ИБТКС, к. т. н. \_\_\_\_\_\_\_\_\_\_\_\_\_ Я. К. Миронов

Таганрог 2024

Содержание

[Введение 3](#_Toc182216652)

[1 Практическая часть 4](#_Toc182216653)

[1.1 Восстановление паролей по заданным значениям хэш-функций 4](#_Toc182216654)

[1.2 Формирование паролей, их sha1-хэшей и радужной таблицы 5](#_Toc182216655)

[1.3 Демонстрация восстановления созданных паролей 6](#_Toc182216656)

[Заключение 8](#_Toc182216657)

Введение

Цели лабораторной работы:

* Закрепить навыки по правильному формированию паролей пользователей путём сравнения эффективности восстановления паролей с различными параметрами;
* Продемонстрировать, как неправильное использование стойких криптографических алгоритмов может привести к созданию слабозащищённых систем идентификации и аутентификации пользователей.

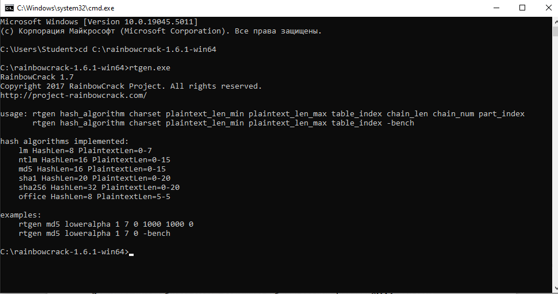
В работе будут получены практические навыки по созданию различных хэш-функций от пользовательских паролей, а также оценить два подхода к восстановлению паролей: методы перебора (полного, по словарю, с мутациями символов и т.д.) и технику криптоанализа с применением метода «время — память» (радужные таблицы).

Используемый в работе инструмент RainbowCrack предоставляет возможность для эффективного восстановления исходного текста на основе хэшей. В отличие от традиционного перебора, RainbowCrack применяет методику предвычисления всех возможных пар «открытый текст — зашифрованный текст» и их сохранения в виде «радужных таблиц». Это позволяет быстро восстанавливать пароли, значительно сокращая время поиска за счёт предварительных вычислений. RainbowCrack работает с популярными хэш-функциями, такими как MD5 и SHA-1, а также поддерживает добавление новых хэш-функций благодаря открытым исходным кодам.

# Практическая часть

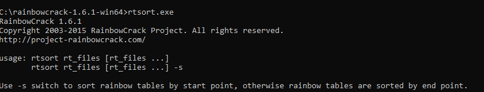
## Восстановление паролей по заданным значениям хэш-функций

Сперва установили программу RainbowCrack, открыли командную строку, перешли в ее директорию и подготовили ее радужные таблицы через команду rtgen.exe (рисунок 1).



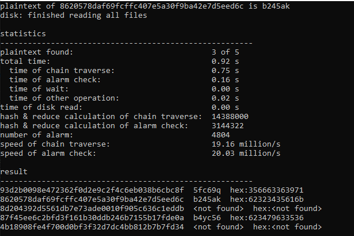
1. — Подготовка радужных таблиц

Для того, чтобы восстановить пароли данные во втором варианте, нам потребовалось сгенерировать радужные таблицы для SHA1 и MD5. Затем их нужно было отсортировать при помощи rtsort.exe (рисунок 2).

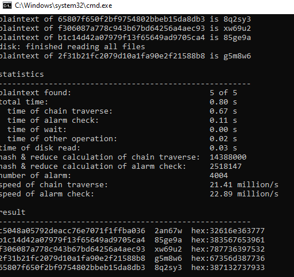


1. — Сортировка таблицы

Далее, используя команду rcrack для соответствующей радужной таблицы (sha1 loweralpha-numeric) и файла, откуда берутся хэшированные данные, расшифровали их (рисунок 3). Повторили то же самое для md5 loweralpha-numeric. В первом случае удалось восстановить только 60% паролей. Во втором — 100% (рисунок 4).



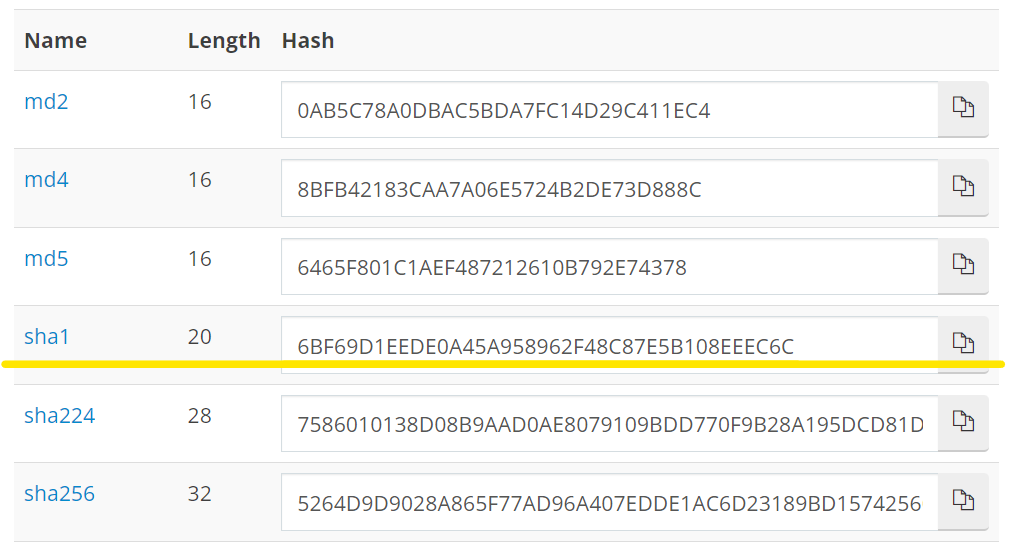
1. —Восстановление паролей SHA1



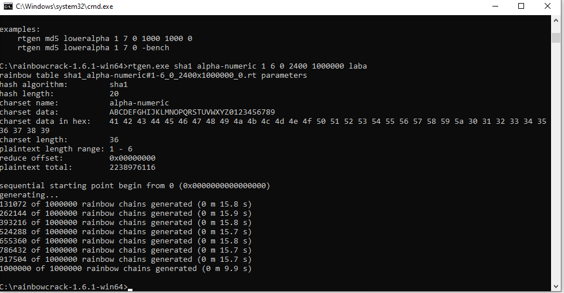
1. — Восстановление паролей MD5

## Формирование паролей, их sha1-хэшей и радужной таблицы

В онлайн хэш-калькуляторе зашифровали 5 шести символьных паролей (рисунок 5), которые состояли из прописных латинских букв и цифр (alpha-numeric). Далее сгенерировали соответствующую радужную таблицу (рисунок 6).



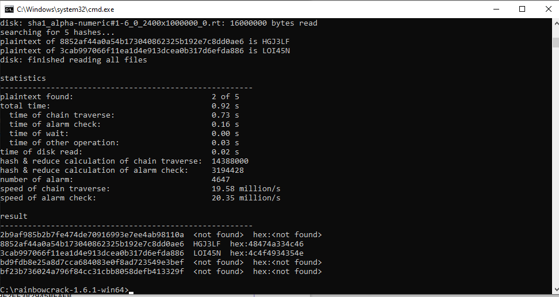
1. — Генерация ключей



1. — Формирование радужной таблицы

## Демонстрация восстановления созданных паролей

После генерации паролей, создания радужной таблицы и ее сортировки, используя команду rcrack начали восстановление паролей. В итоге удалось восстановить только 40% паролей (рисунок 7).



1. — Восстановление паролей

Заключение

В ходе лабораторной работы я закрепил навыки создания и проверки устойчивости паролей, сравнив эффективность восстановления паролей с различными параметрами. Было продемонстрировано, как даже использование стойких криптографических алгоритмов может привести к недостаточной защите данных при неправильной реализации. Практика восстановления паролей с помощью методов перебора и техники радужных таблиц на примере инструмента RainbowCrack позволила оценить их различия по скорости и эффективности.

Полученные знания будут полезны при создании защищённых систем аутентификации и при работе с криптографическими алгоритмами. Лабораторная работа показала значимость грамотного формирования и хранения паролей, а также безопасного использования криптографических технологий для защиты информации.