# МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

# федеральное государственное автономное образовательное учреждение высшего образования

# «САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

# АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 34

ОТЧЕТ   
ЗАЩИЩЕН С ОЦЕНКОЙ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

ПРЕПОДАВАТЕЛЬ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| доцент, кандидат технических наук |  |  |  | Мыльников В.А. |
| должность, уч. степень, звание |  | подпись, дата |  | инициалы, фамилия |

|  |
| --- |
| ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ |
| **Хеширование по алгоритмам MD5, SHA-1, SHA-256, SHA-512.**  **Оценка криптостойкости.** |
| по курсу: ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ |
|  |

РАБОТУ ВЫПОЛНИЛ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| СТУДЕНТ ГР. № | 3143 |  |  |  | Казаков И.А. |
|  |  |  | подпись, дата |  | инициалы, фамилия |

Санкт-Петербург 2022 г.

Оглавление

[**Цель работы.** 2](#_Toc104740621)

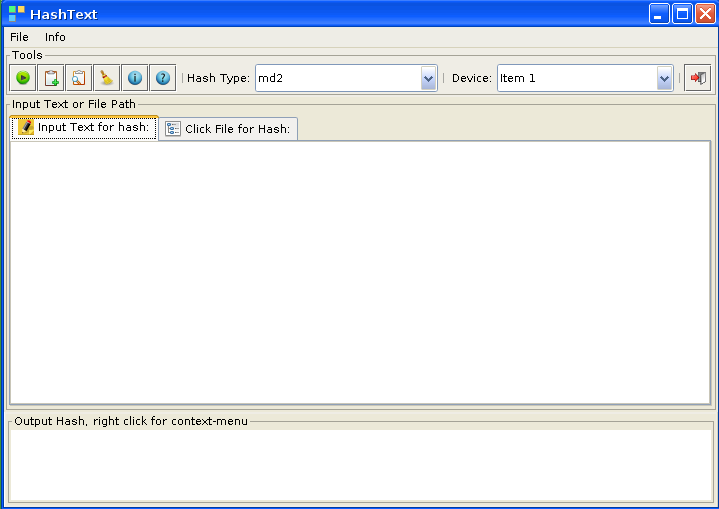
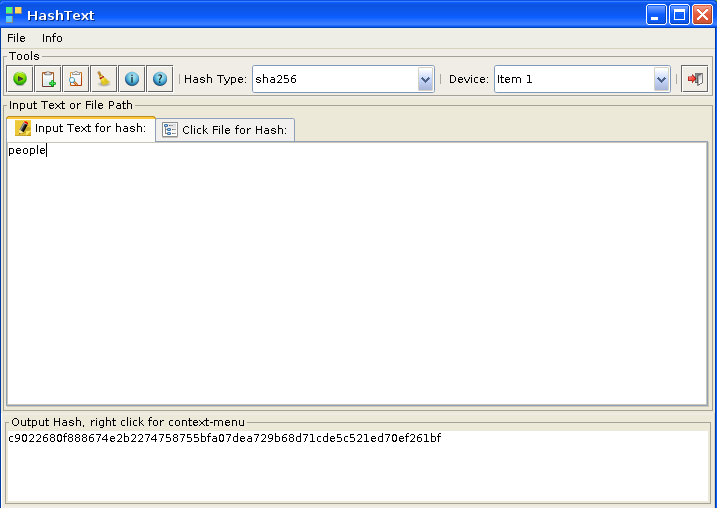
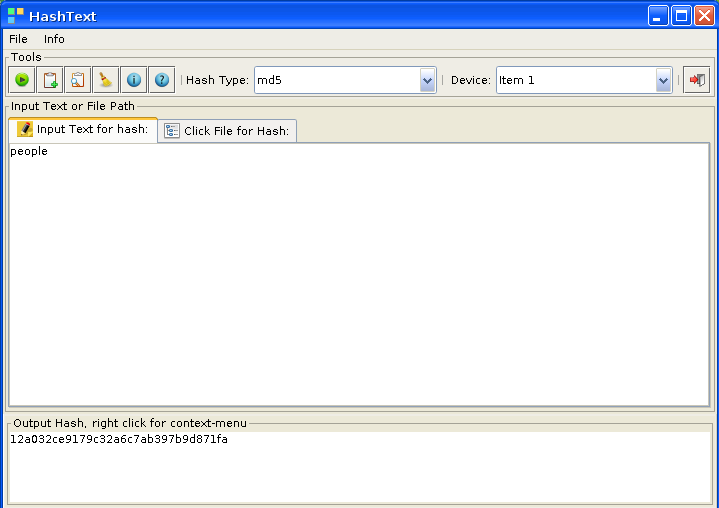
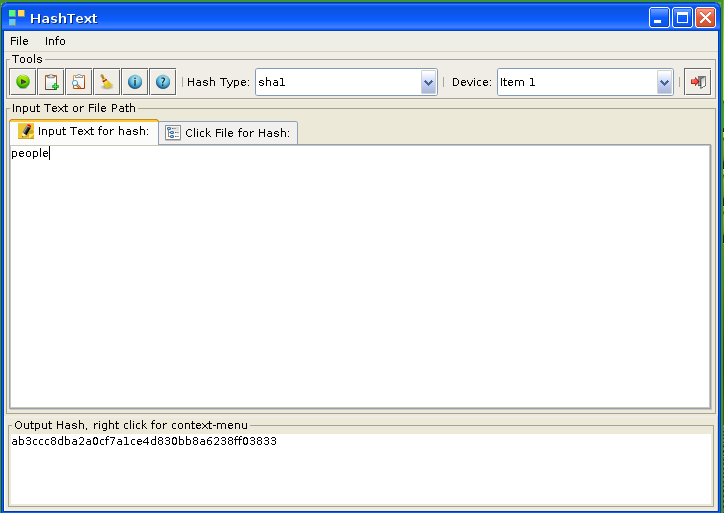
[**Ход работы.** 3](#_Toc104740622)

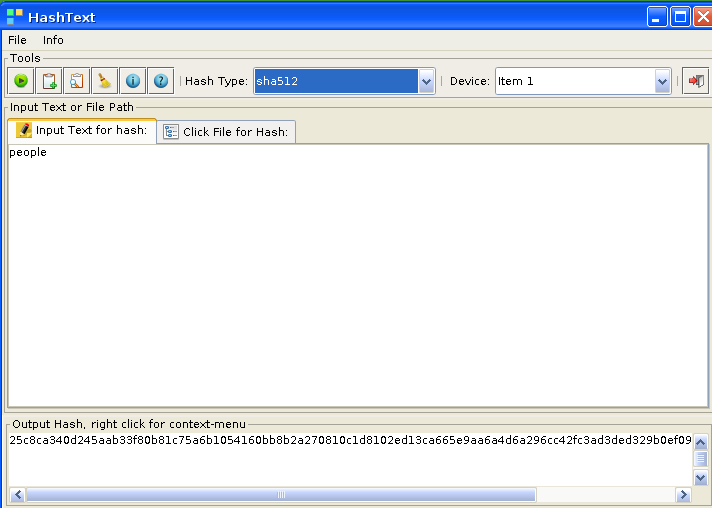
[**Результаты лабораторной работы и выводы.** 7](#_Toc104740623)

## **Цель работы.**

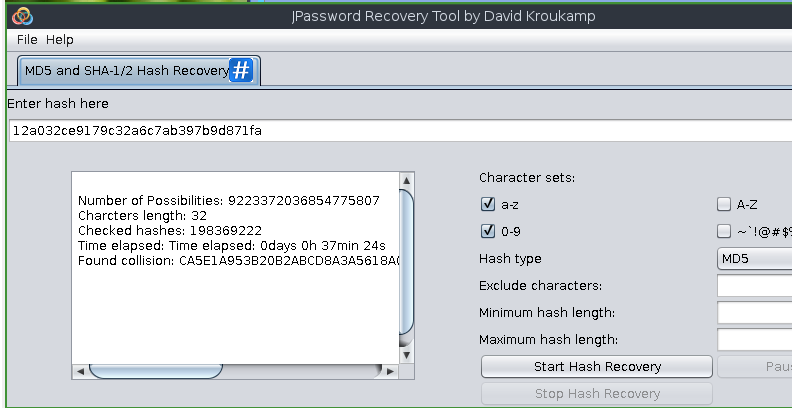
Получить навыки создания хеш ключей.

## **Ход работы.**

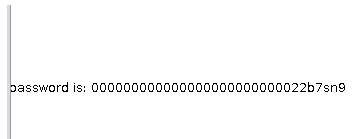
1. Запустим утилиты для генерации хешей (Hofat):
2. ****Сгенерируем хеши по алгоритмам MD5, SHA-1, SHA-256, SHA-512 для слова «people»:



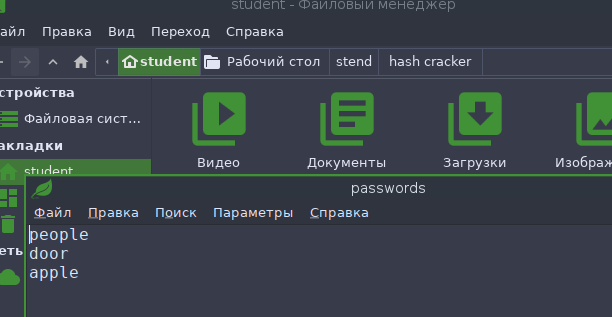
1. Из-за разных методов хеширования и стандартов полученный хеш у MD5, SHA-1, SHA-256, SHA-512 является разным по длине.
2. Запустим JPassword Recovery Tool и зададим параметры данного слова. Дадим примерную оценку времени перебора всех возможных вариантов с учетом заданных ограничений (длина, тип символов):



Перебор хеша всех возможных вариантов по времени больше 37 минут.

Результат перебора в течение 37 минут:

1. Создадим текстовый документ с паролями в одном, из которых будет заданный (people), запустим Hash Code Cracke, укажем путь к файлу, выберем нужный алгоритм согласно признакам хеша, запустим подбор:



Подбор прошел успешно, пароль найден.

## **Результаты лабораторной работы и выводы.**

Получил навык создания хеш ключей.