# 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 |
| **Использование алгоритмов хеширования для подтверждения неизменности файла с применением OpenSSL** |
| 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](#_Toc101175785)

[**Ход работы.** 3](#_Toc101175786)

[**Результат лабораторной работы.** 4](#_Toc101175787)

## **Цель работы.**

Получить навыки применения программного продукта OpenSSL для применения алгоритмов хеширования.

## **Ход работы.**

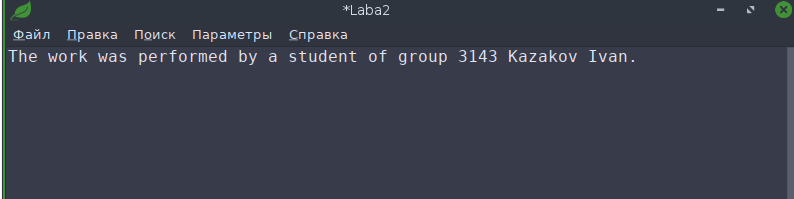
1. Создадим файл с семантически понятным текстом:

Рисунок : исходный файл.

2. Вычислим значение хеш-функции MD5 для этого файла:



Рисунок : хеш-сумма файла Laba2 по алгоритму MD5.

3. Вычислим значение хеш-функции SHA-1 для этого файла:



Рисунок : хеш-сумма файла Laba2 по алгоритму SHA-1.

4. Время выполнения:

MD5=0,002 c.

SHA-1= 0,002 c.

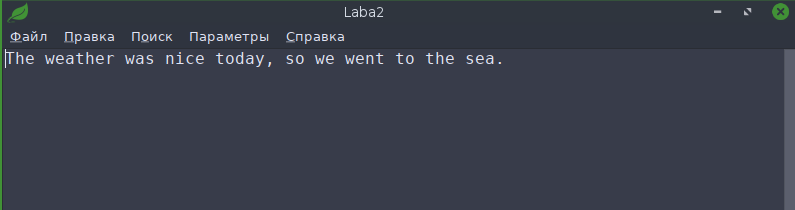
5. Изменим содержимое исходного файла:

Рисунок : изменённый исходный файл.

6. Вычислим значение хеш-функции MD5 для этого файла:

Рисунок : хеш-сумма файла Laba2 (изменённый) по алгоритму MD5.

7. Вычислим значение хеш-функции SHA-1 для этого файла:



Рисунок : хеш-сумма файла Laba2 (изменённый) по алгоритму SHA-1.

Сравнивая рисунки 2,6 и 3,7, можно убедиться, что хеш-сумма изменилась с изменением содержания файла.

8. Получим аутентификатор выбранного файла с применением алгоритма DES-CBC

с помощью OpenSSL:

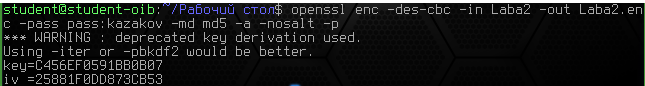


Рисунок 7: аутентификатор.

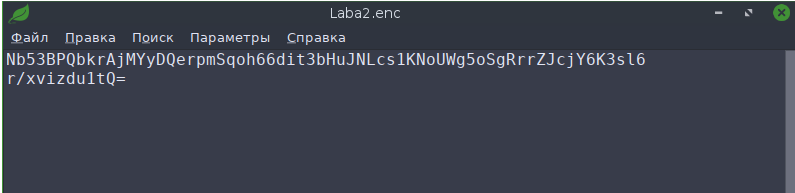


Рисунок 8: содержание файла.

## **Результат лабораторной работы.**

Получил навыки применения программного продукта OpenSSL для применения алгоритмов хеширования.