Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование криптографических хеш-функций**

Выполнил:

студент 3 курса 4 группы

специальности ПОИТ

Сивак М.Н.

Минск 2021

**Цель**: изучение алгоритмов хеширования и приобретение практических навыков их реализации и использования в криптографии

**Задачи**:

1.Закрепить теоретические знания по алгебраическому описанию

и алгоритмам реализации операций вычисления однонаправленных

хеш-функций.

2. Освоить методику оценки криптостойкости хеш-преобразований на основе «парадокса дня рождения».

3. Разработать приложение для реализации заданного алгоритма

хеширования (из семейств MD и SHA).

4. Оценить скорость вычисления кодов хеш-функций.

5. Результаты выполнения лабораторной работы оформить в виде

описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента

**Практическое задание:**

1. Разработать оконное приложение, реализующее один из алгоритмов хеширования из указанного преподавателем семейства (MD или SHA; или иного). При этом можно воспользоваться доступными

готовыми библиотеками. Язык программирования – на свой выбор.

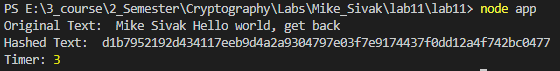
Приложение должно обрабатывать входные сообщения, длина которых определяется спецификацией на реализуемый алгоритм.

2. Оценить быстродействие выбранного алгоритма хеширования.

3. Результаты оформить в виде отчета по установленным правилам.

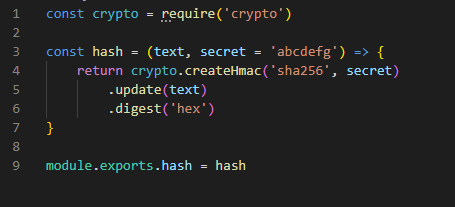
**Результат выполнения работы приложения**:

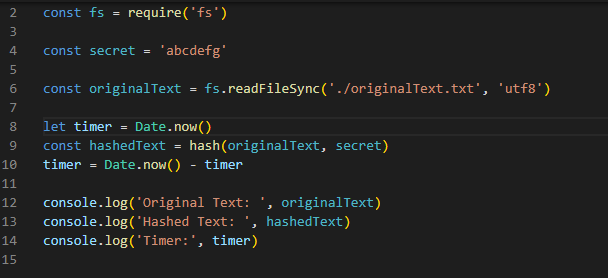
SHA-256



Ниже приведены несколько листингов исходного кода программы, написанной на языке javascript на платформе node.js.

Листинги





**Вывод**

В ходе выполнения лабораторной работы я получил опыт в написании приложения, использующего алгоритм шифрования SHA-256, которое реализует одностороннее шифрование текстового файла, результат которого называется хэшем.