Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование криптографических хеш-функций**

Студент: Сятковская Е. Д.

ФИТ 3 курс 4 группа

Минск 2023

1. **Описание приложения**

Приложение написано на языке программирования Python и позволяет:

* хешировать входное сообщение;
* оценивать скорость выполнения алгоритма.

1. **Методика выполнения поставленных задач**

SHA256 – хеш-функция из семейства алгоритмов SHA-2, которая предназначена для создания дайджестов для сообщений произвольной длины. Длина дайджеста – 256 бит. Исходное сообщение дополняется до нужной длины, а затем разбивается на блоки. Каждый блок – на 16 слов. Каждый блок сообщения пропускается через 64 итерации. На каждой итерации 2 слова преобразуются, функцию преобразования задают остальные слова. Результаты обработки каждого блока складываются, сума – значение хеш-функции. Т.к. инициализация внутреннего состояния производится результатом обработки предыдущего блока, то нет возможности обрабатывать блоки параллельно.

Результат обработки строки с помощью алгоритма SHA256 представлен на рисунке 2.1.

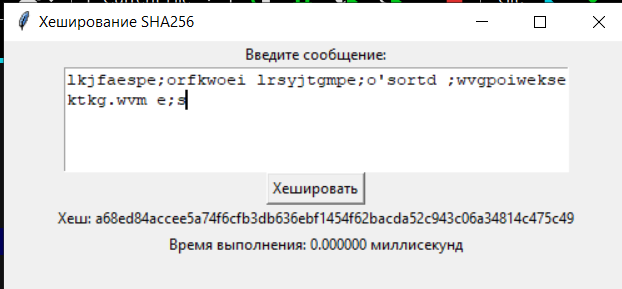


Рисунок 2.1 – Результат хеширования SHA256

Функция для хеширования строки с помощью алгоритма SHA256 представлена на рисунке 2.2.



Рисунок 2.2 – Функция для хеширования строки

В алгоритмах хеширования часто используется такое понятие как соль. Соль – строка данных, которая передается хеш-функции вместе с входными данными для вычисления хеша. Используется для усложнения определения прообраза хеш-функции методом перебора по словарю возможных значений, включая радужные атаки. Позволяет скрыть факт использования одинаковых прообразов при использовании разной соли.

Таким образом, были реализованы все поставленные задачи. Были исследованы асимметричные шифры.

**Вывод**

В ходе лабораторной работы были приобретены навыки хеширования используя алгоритм SHA256. Были изучены основные принципы работы хеширования.

Также было разработано приложение, на языке программирования Python, для реализации задач, связанных с хешированием данных.