Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование криптографических хеш-функций**

Студент: Чёрная Я. Р.

ФИТ 3 курс 4 группа

Минск 2025

**Теоретические сведения**

Хеш-функция – математическая или иная функ ция h = H(М), которая принимает на входе строку символов М, назы ваемую также прообразом, переменной длины n и преобразует ее в выходную строку фиксированной (обычно – меньшей) длины l.

Хеширование (или хэширование, англ. hashing) – это преобразование входного массива данных опреде ленного типа и произвольной длины (практически) в выходную би товую строку фиксированной длины.

Преобразования называются хеш-функциями, или функциями свертки, а их результаты называют хешем, хеш-кодом, хеш-табли цей или дайджестом сообщения (англ. message digest).

Криптографическая хеш-функция – это спе циальный класс хеш-функций, который имеет различные свойства, необходимые для решения задач в области криптографии. Основные задачи, решаемые с помощью хеш-функций: • аутентификация (хранение паролей); • проверка целостности данных; • защита файлов; • обнаружение зловредного ПО; • криптовалютные технологии.

К основным свойствам хеш-функций можно отнести следу ющие. Свойство 1. Детерминированность: независимо от того, сколько раз вычисляется H(M), M – const, при использовании оди накового алгоритма код хеш-преобразования h всегда должен быть одинаковым. Исследование криптографических хеш-функций 123 Свойство 2. Скорость вычисления хеша h: если процесс вы числения h недостаточно быстрый, система просто не будет эф фективной. Свойство 3. Сложность обратного вычисления: для извест ного H(М) невозможно (практически) определить М. Это важней шее свойство хеш-функции для криптографических применений – свойство односторонности преобразования.

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.

Особенности:

* Высокая скорость вычислений.
* Односторонность: невозможно восстановить исходное сообщение по хешу.
* Малейшее изменение входных данных приводит к совершенно иному результату (свойство лавины).

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

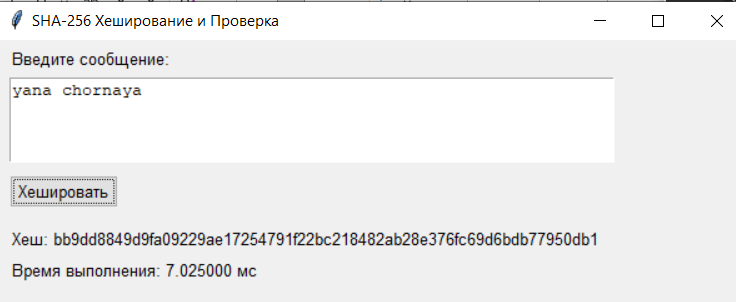


Рисунок 2.1 – Результат хеширования SHA256

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.

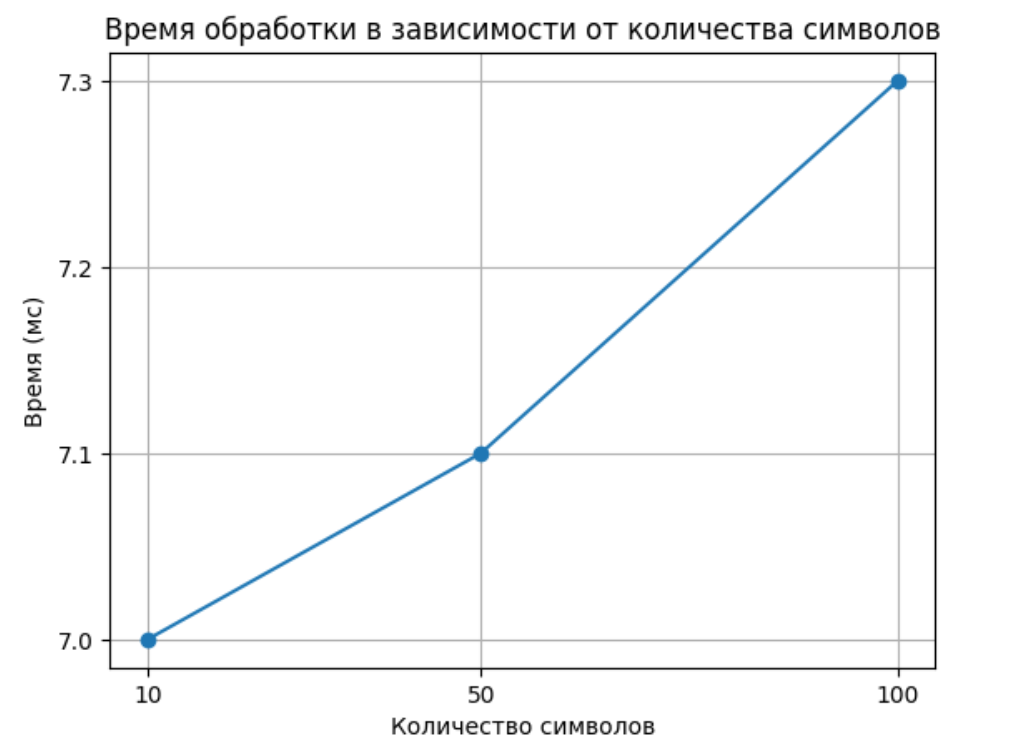


Рисунок 2.3 – звисимость количества символов от времени

График показывает линейную зависимость, что говорит о том, что увеличение количества символов приводит к незначительному увеличению времени обработки. Это может быть полезным для оценки производительности систем, работающих с текстовыми данными.

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.