Учреждение образования

«Белорусский государственный технологический университет»

**Лабораторная работа №11**

Исследование криптографических хеш-функций

Выполнил:

Студент 3 курса 5 группы ФИТ

Коршун Никита Игоревич

2024

В данной лабораторной работе было разработано приложение используя язык программирования Python.

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

Криптографическая хеш-функция – это специальный 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.

Коллизией хеш-функции *Н* называют ситуацию, при которой различным входам (в общем случае – *х* и *у* или *М ≠ М'*) соответствует одинаковый хеш-код: *H(x) = H(y)* или *H(М) = = H(М').*

Алгоритмы семейства MD-x (2/4/5/6) являются творениями Р. Ривеста; MD – Message Digest. Алгоритм MD6, в отличие от предыдущих версий алгоритма этого семейства, не стандартизован. Алгоритмы семейства SHA (SHA – Secure Hash Algorithm) являются в настоящее время широко распространенными. По существу, во многих случаях завершился переход от SHA-1 к стандартам версии SHA-2. SHA-2 – собирательное название алгоритмов SHA-224, SHA-256, SHA-384 и SHA-512. SHA-224 и SHA-384 являются, по сути, аналогами SHA-256 и SHA-512 соответственно.

Максимальный объем хешируемых сообщений для алгоритмов SHA-1, SHA-256, SHA-224 такой же, как и для алгоритмов MD. Однако длина хешей разная: в SHA-1 – 160 битов; в алгоритмах, относящихся к семейству SHA-2, – соответствует числу, дополняющему через дефис название алгоритма. Максимальная же длина входных сообщений в алгоритмах SHA-512, SHA-384, SHA-512/256, SHA-512/224 составляет 2128 – 1 битов.

Базовые алгоритмы обоих рассматриваемых семейств (MD и SHA) условно можно разделить на 5 стадий:

• расширение входного сообщения;

• разбивка расширенного сообщения на блоки;

• инициализация начальных констант;

• обработка сообщения поблочно (основная процедура алгоритма хеширования);

• вывод результата.

В MD4 входное сообщение «дополняется» (расширяется) так, чтобы его длина (в битах) была конгруэнтной к 448 по модулю 512. Это значит, что сообщение начальной длиной *L* битов расширяется так, что остаются незаполненными всего лишь 64 бита, чтобы итоговая длина *L'* была кратной 512. В указанные 64 бита записывается двоичная длина. Расширение происходит всегда, даже если длина сообщения уже соответствует 448, по модулю 512. Эта операция выполняется следующим образом: один бит «1» добавляется к сообщению, а затем добавляются биты «0», так что длина в битах дополненного сообщения стала конгруэнтной 448 по модулю 512. Добавляется не менее одного бита, но не более 448 битов.

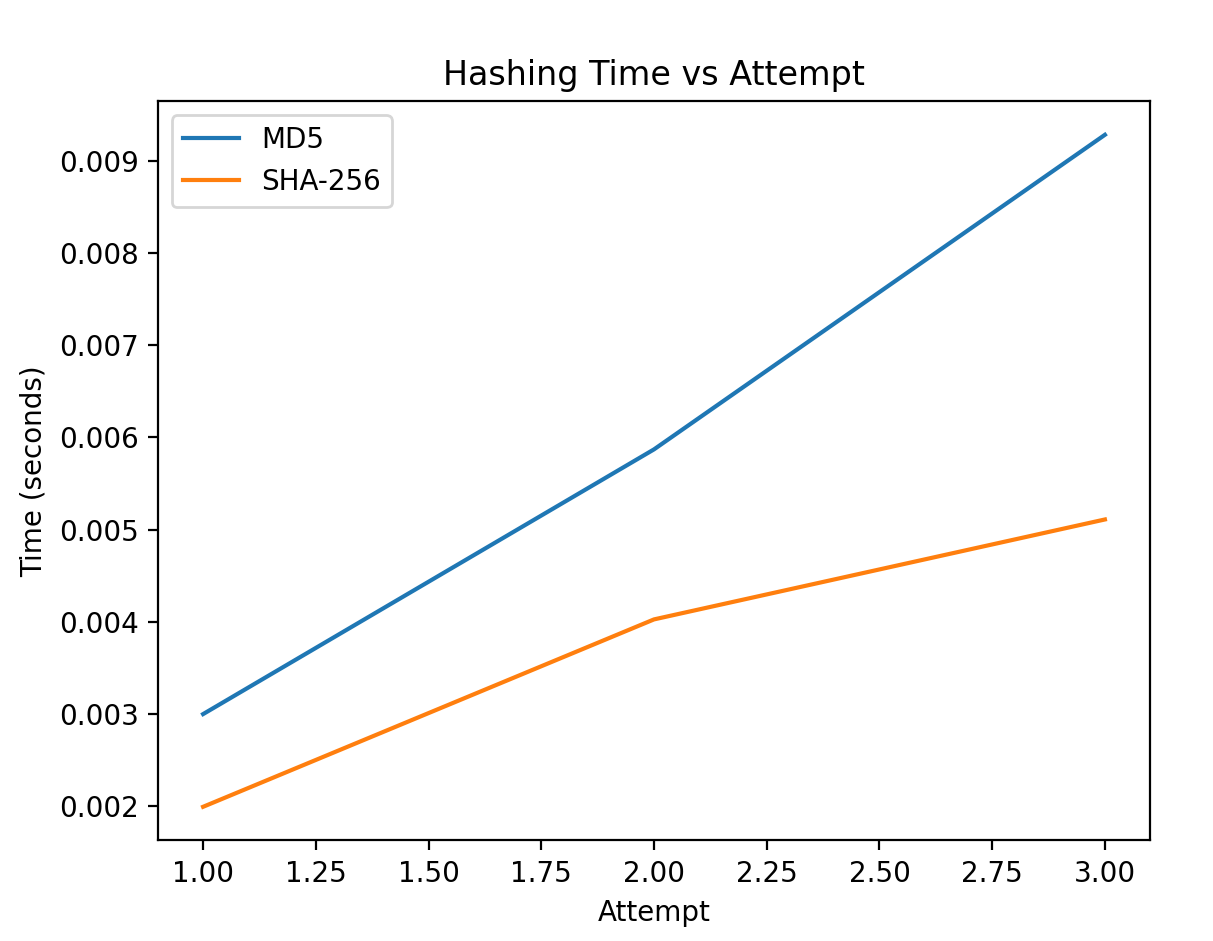


Рисунок 1 – Время вычисления хеша

Как можно заметить время вычисления при помощи SHA-256 немного быстрее чем при помощи MD5. Также видно что при увеличении размера входящего сообщения увеличивается время хэширования.

**Вывод.** В данной лабораторной работе были изучены алгоритмы хеширования SHA-256 и MD5. Было оценено время выполнения хеширования.