Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических хеш-функций

Студент: Голодок А. Ю.

ФИТ 3 курс 4 группа

Преподаватель: Сазонова Д. В.

Минск 2024

1. **Теоретическая часть**

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.

Основные задачи, решаемые с помощью хеш-функций:

• аутентификация (хранение паролей);

• проверка целостности данных;

• защита файлов;

• обнаружение зловредного ПО;

• криптовалютные технологии.

Хеш-функция должна обладать следующими свойствами: детерминированность, скорость вычисления хеша, сложность обратного вычисления, Н(M) ≠ Н(М'), коллизионная устойчивость.

MD5 состоит из четырех основных этапов:

1. Инициализация: задаются начальные значения для регистров, которые используются в процессе хеширования.
2. Предварительная обработка: сообщение дополняется битами таким образом, чтобы его длина была кратна 512 битам. Затем сообщение разбивается на блоки по 512 бит.
3. Основной цикл: каждый блок обрабатывается в цикле, состоящем из 64 итераций. В каждой итерации применяются различные преобразования к регистрам.
4. Финальная обработка: регистры объединяются в 128-битный хеш-код, который и является конечным результатом хеширования.

Алгоритм SHA-256 состоит из шести основных этапов:

1. Инициализация: задаются начальные значения для регистров, которые используются в процессе хеширования.
2. Предварительная обработка: сообщение дополняется битами таким образом, чтобы его длина была кратна 512 битам. Затем сообщение разбивается на блоки по 512 бит.
3. Инициализация переменных: переменные инициализируются значениями, используя начальные значения регистров и специальные константы.
4. Основной цикл: каждый блок обрабатывается в цикле, состоящем из 64 итераций. В каждой итерации применяются различные преобразования к переменным.
5. Формирование хеш-кода: после обработки всех блоков, значения переменных объединяются в 256-битный хеш-код.
6. Завершение: переменные и регистры очищаются.
7. **Практическая часть**

**2.1 SHA и MD5**

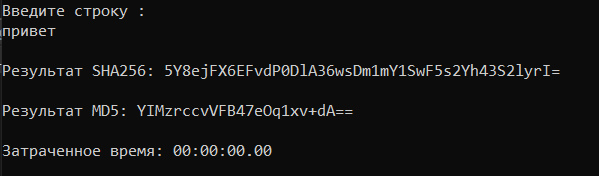


Рисунок 2.1 – Результат работы