Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

**Отчёт по лабораторной работе №11**

**«Исследование криптографических хеш-функций»**

Исполнитель:

Студент 3 курса группы 4

Гурина К. С.

Руководитель:

Ассистент Сазонова Д. В.

1. **Цель и задачи работы**

**Цель:** исследование 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

**2. Теоретические сведения**

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.

Хеширование – это преобразование входного массива данных определенного типа и произвольной длины (практически) в выходную битовую строку фиксированной длины.

Преобразования называются хеш-функциями, или функциями свертки, а их результаты называют хешем, хеш-кодом, хеш-таблицей или дайджестом сообщения.

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.

К основным свойствам хеш-функций можно отнести следующие.

Свойство 1. Детерминированность: независимо от того, сколько раз вычисляется H(M), M – const, при использовании одинакового алгоритма код хеш-преобразования h всегда должен быть одинаковым.

Свойство 2. Скорость вычисления хеша h: если процесс вычисления h недостаточно быстрый, система просто не будет эффективной.

Свойство 3. Сложность обратного вычисления: для известного H(М) невозможно (практически) определить М. Это важнейшее свойство хеш-функции для криптографических применений – свойство односторонности преобразования.

Свойство 4. Даже минимальные изменения в хешируемых данных (М ≠ М') должны изменять хеш: Н(M) ≠ Н(М').

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').

Свойство 5. Коллизионная устойчивость (стойкость). Зная М, трудно найти такое М' (М ≠ М'), для которого H(М) = H(М'). Если последнее равенство выполняется, то говорят о коллизии 1-го рода. Если случайным образом выбраны два сообщения (М и М'), для которых H(М) = H(М'), говорят о коллизии 2-го рода.

Мерой криптостойкости хеш-функции считается вычислительная сложность нахождения коллизии. Для хеш-функций одним из основных средств поиска коллизий является метод, основанный на известной статистической задаче – «парадоксе дня рождения».

Основной постулат парадокса «дней рождения» гласит: в группе минимум из 23 человек с вероятностью более 0,5 день рождения одинаков хотя бы у двух членов группы. Парадоксом является высокая (как кажется на первый взгляд) вероятность наступления указанного события. При этом предполагается, что:

• в этой группе нет близнецов;

• люди рождаются независимо друг от друга, т. е. дата (день) рождения любого человека не влияет на дату рождения другого;

• люди рождаются равномерно и случайно, т. е. люди с равной вероятностью могут рождаться в любой день года; с формальной точки зрения это означает, что вероятность р1 рождения отдельно выбранного члена группы (как и любого человека) в любой выбранный день равна р1 = 1 / 365 (хотя известно, что в реальности рождение людей не совсем соответствует такому предположению).

Хеш-функция – это функция, выполняющая отображение из множества М в число, находящееся в интервале [0, m – 1]: h: M → [0, m – 1].

**3. Ход работы**

**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.

**Ход работы**

Для реализации алгоритмов семейства SHA и MD использовался модуль crypto.

Функция хеширования алгоритмом SHA-256 принимает на вход строку сообщения и возвращают хэш, его длину и время, затраченное на хэширование. Код функции представлен на рисунке 3.1.



Рисунок 3.1 – Код функции hashWithSHA256

Результат работы приложения представлен на рисунке 3.2.



Рисунок 3.2 – Результат работы функции hashWithSHA256

Длина хеша – 32 байта или 256 бит. Время хеширования сообщения – менее 1 мс, что отражает высокую временную эффективность алгоритма.

Функция хеширования алгоритмом MD5 принимает на вход строку сообщения и возвращают хэш, его длину и время, затраченное на хэширование. Код функции представлен на рисунке 3.3.



Рисунок 3.3 – Код функции hashWithMD5

Результат работы функции представлен на рисунке 3.4.

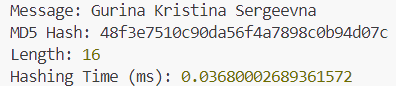


Рисунок 3.4 – Результат работы функции hashWithMD5

Длина хэша равна 16 байтами или 128 битам. Время зашифрования сообщения – менее 1 мс, что сравнимо с алгоритмом SHA-256.

**Вывод**

В ходе выполнения лабораторной работы был изучен принцип реализации алгоритмов хеширования SHA-256 и MD5. Также было разработано приложение, выполняющее хеширования на основе данных алгоритмов. Была оценена скорость хеширования различными алгоритмами.