МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №11**

**″Исследование криптографических хеш-функций″**

Выполнила студентка 3 курса 5 группы Максимчикова Ю. С.

Проверила: Блинова Е. А.

Минск 2020

**Цель**: изучение алгоритмов хеширования и приобретение практических навыков их реализации и использования в криптографии.

**Задачи**:

* Закрепить теоретические знания по алгебраическому описанию и алгоритмам реализации операций вычисления однонаправленных хеш-функций.
* Освоить методику оценки криптостойкости хеш-преобразований на основе «парадокса дня рождения».
* Разработать приложение для реализации заданного алгоритма хеширования (из семейств MD и SHA).
* Оценить скорость вычисления кодов хеш-функций.
* Оценить скорость зашифрования/расшифрования реализованных способов шифров.
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Теория.** 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 (или хэширование, англ. hashing ) – 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 (анг. message digest).

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 не достаточно 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 – односторонности преобразования. Это означает, что по хеш-коду должно быть практически невозможным восстановление входной строки 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'). Мерой криптостойкости хеш-функции считается вычислительная сложность нахождения коллизии. В более общем случае: для того, чтобы хеш-функция H (M) считалась криптографически стойкой, она должна удовлетворять трем основным требованиям: необратимостью вычислений (свойство 3), устойчивостью к коллизиям первого рода и устойчивостью к коллизиям второго рода (свойство 5).

Основной постулат парадокса «дней рождения» гласит: в группе минимум из 23 человек с вероятностью более 0,5 день рождения у 2-х лиц одинаков. 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).

Синхронные потоковые шифры (СПШ) характеризуются тем поток ключей генерируется независимо от открытого текста и шифртекста. Главное свойство СПШ – нераспространение ошибок. Ошибки отсутствуют, пока работают синхронно шифровальное и дешифровальное устройства отправителя и получателя информации. Один из методов борьбы с рассинхронизацией – разбить отрытый текст на отрезки, начало и конец которых выделить вставкой контрольных меток (специальных маркеров). Иначе говоря, стоит задача отыскания наименьшего n, при котором хеши двух значений m будут «одним днём рождения».

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, SHA256, SHA-384 и SHA-512. SHA-224 и SHA-384 являются, по сути, аналогами SHA-256 и SHA-512 соответственно.

**Задание.** В данной лабораторной работе необходимо было разработать авторское приложение, реализующее один из алгоритмов хеширования из 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. Приложение было реализовано с помощью уже готовой реализации алгоритма MD5, находящейся в пространстве имён System.Security.Cryptography.

Функция получения хеша представлена на рисунке 1.

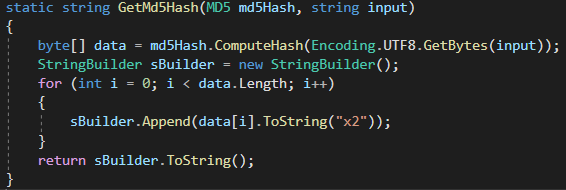


Рис. 1 – Функция для получения хеша с помощью MD5

Реализация функции проверки хешей представлена на рисунке 2.

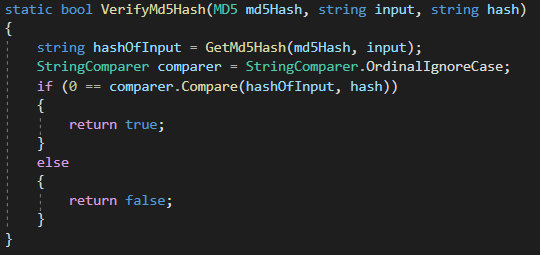


Рис. 2 – Функция проверки хеша с помощью RSA

Результат работы алгоритма и замеры времени выполнения операций вычисления и проверки хеша сообщения, введённого с консоли представлены на рисунке 3.

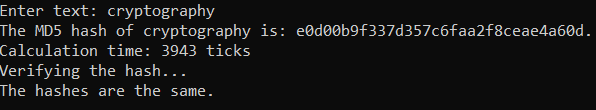


Рис. 3 – Результат работы приложения

Вывод: в результате данной лабораторной работы было разработано приложение для выполнения операций вычисления и проверки хеша сообщения. Также был проведен анализ его криптостойкости и замеры времени работы данных операций с помощью этого алгоритма.