Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических хеш-функций

Студент: Чистякова Ю.А.

ФИТ 3 курс 5 группа

Преподаватель: Берников В.О.

Минск 2020

## 1. Описание приложения

Приложение написано на языке программирования C# и реализиует алгоритм хеширования SHA256, SHA1, MD5. Приложение обрабатывает входное сообщение, длина которого определена спецификацией

## 2. Методика выполнения поставленных задач

## Алгоритм SHA256 имеет 64 итерации в одном цикле, принимает на вход сообщения предельно допустимого размера до 264 бит, и выдает на выходе дайджест размером 32 байт.

Во-первых, необходимо сгенерировать так называемую «соль» указанной длины – строка данных, которая позже будет передана хэш-функции вместе с входным массивом данных (прообразом) для вычисления хэша. Программная реализация генерации соли продемонстрирована на рисунке 2.1.

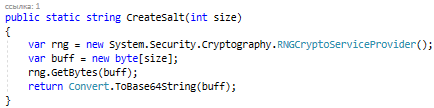


Рис. 2.1 – Генерация соли

Далее вызывается функция генерации хэша с помощью алгоритма SHA256, встроенная в библиотеку. Входными параметрами данной функции являются вычисленная на предыдущем шаге «соль» и входное сообщение. Программная реализация данной функции продемонстрирована на рисунке 2.2.

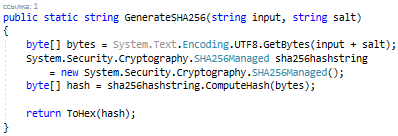


Рис. 2.2 – Реализация функции хэширования

Дайджест в алгоритме SHA1 – 160 бит. При этом дайджест – результат хеш-функции. Алгоритмы семейства MD входные сообщения максимальной длины преобразуют в хеш длиной l = 128 бит. Исключением является последняя – 6 – из версий алгоритма, где длина результирующего хеша может изменяться от 1 до 512 бит.

Реализация алгоритма MD5 представлена на рисунке 2.3.

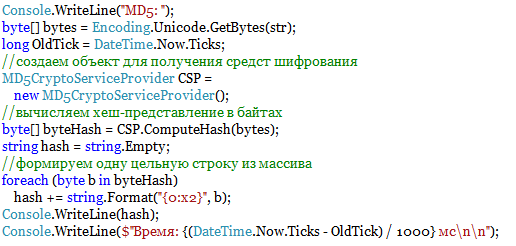


Рис. 2.3 – Реализация MD5

Реализация алгоритма SHA1 представлена на рисунке 2.4.

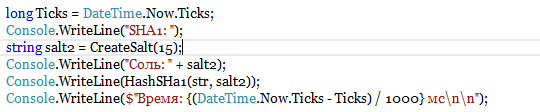


Рис. 2.4 – Реализация SHA1

Результат работы приложения представлен на рисунке 2.5.

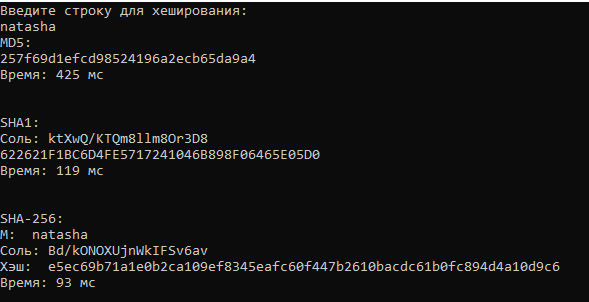


Рис. 2.5 – Результат работы приложения

Таким образом, были реализованы все поставленные задачи, а также оценено время выполнения разных алгоритмов шифрования

## Вывод

В ходе лабораторной работы были изучены алгоритмы хеширования и приобретены практические навыки их реализации и использования в криптографии.