МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа № 11**

**ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ХЕШ-ФУНКЦИЙ**

Разработала: Некрасова А.П.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2023

**Цель**: изучение 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.

**Практическая часть**

В данной лабораторной работе необходимо разработать оконное приложение, реализующее алгоритм хеширования MD5. При этом можно воспользоваться доступными готовыми библиотеками.

Так, для реализации этого алгоритма была использована библиотека System.Security.Cryptography, реализующая алгоритм хеширования MD5. Для этого была написана следующая функция, представленная на рисунке 1.

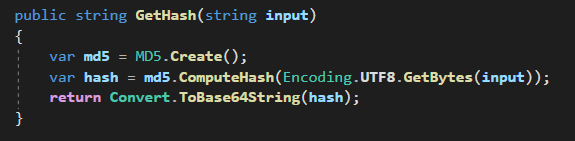


Рисунок 1 – Реализация функции хеширования

Функция принимает в себя один параметр – исходный текст, хэш которого необходимо получить. Затем создается экземпляр встроенного класса MD5, который содержит в себе метод ComputeHash, позволяющий получить хэш сообщения. В метод необходимо передать сообщение в двоичном виде.

Также программа позволяет узнавать время выполнения работы алгоритма Работа программы продемонстрирована на рисунке 2.

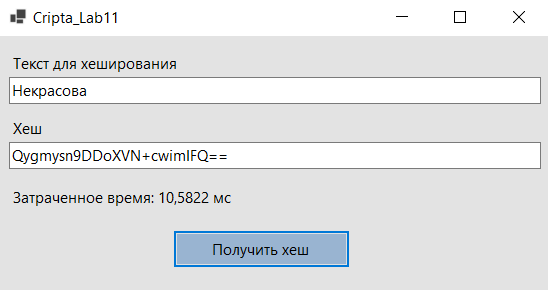


Рисунок 2 – Работа программы с входной строкой «Некрасова»

Основное правило хеширования гласит, что разные строки должны образовывать разный хеш, результат работы приложения, подтверждающий это правило представлен на рисунке 3:

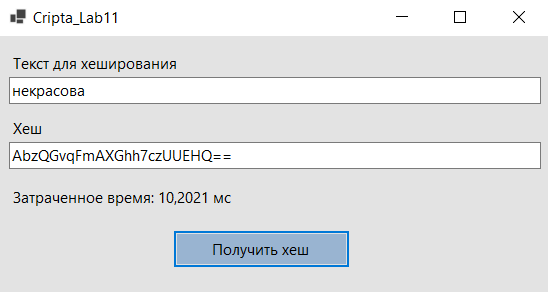


Рисунок 3 – Работа программы с входной строкой «некрасова»

Тем самым мы опытным путём подтверждаем это правило т.к. строки «Некрасова» и «некрасова» между собой схожи, но по факту разные.

На рис. 4 представлен график зависимости времени от кол-ва символов шифруемого сообщения.

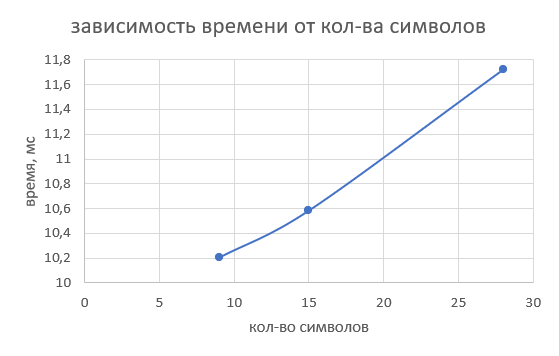


Рисунок 3 – Зависимости времени от кол-ва символов

**Вывод:** таким образом, в данной лабораторной работе я закрепила теоретические знания по алгебраическому описанию, алгоритмам реализации операций вычисления однонаправленных хэш-функций, разработала приложение для реализации алгоритма хеширования MD5, а также оценила скорость вычисления кодов хеш-функций.