Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Исследование криптографических**

**хеш-функций**

Студент: Буданова К. А.

ФИТ 3 курс 5 группа

Преподаватель:

Савельева Маргарита Геннадьевна

1. **Цель работы**

Изучение алгоритмов хеширования и приобретение практических навыков их реализации и использования в криптографии.

1. **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.

1. **Ход работы**

В качестве используемого алгоритма был выбран алгоритм MD5.

Алгоритм MD5 (Message Digest Algorithm 5) — это криптографическая хеш-функция, которая принимает на вход произвольное сообщение фиксированной длины и вычисляет 128-битный хеш-код (MD5-хеш) для этого сообщения. Алгоритм MD5 был разработан Рональдом Ривестом в 1991 году. Вот шаги, описывающие работу алгоритма MD5:

1. Исходное сообщение делится на блоки фиксированного размера (512 бит).
2. Каждый блок обрабатывается независимо. Для начала обработки блока выполняется инициализация четырех 32-битных переменных, известных как A, B, C и D.
3. Блок разбивается на 16 слов по 32 бита каждое. Каждое из этих слов обрабатывается внутри цикла.
4. Инициализируются четыре вспомогательные переменные, известные как F, G, H и I.
5. Выполняются четыре раунда, в каждом из которых слово блока преобразуется с использованием функций F, G, H и I, а также текущих значений переменных A, B, C и D.
6. После завершения всех раундов, значения переменных A, B, C и D объединяются в одно 128-битное значение, которое и представляет собой MD5-хеш исходного сообщения.
7. В конечном итоге, MD5-хеш является уникальным идентификатором исходного сообщения. Любое изменение в сообщении, даже незначительное, приводит к значительным изменениям в хеш-коде.

Для реализации данного алгоритма в приложении было использовано пространство имён System.Security.Cryptography, которое содержит поддержку наиболее распространенных симметричных (DES, 3DES, RC2, Rijndael), асимметричных (RSA, DSA) и хеш-(MD5, SHA-1, SHA-256, SHA-384, SHA- 512) алгоритмов криптографии.

Класс, представленный на рисунке 3.1 использует функции из данного пространства имён для хэширования сообщения.



Рисунок 3.1 – Класс MD5Hash, реализующий алгоритм MD5

На следующих рисунках 3.2 – 3.3 можно увидеть пример использования класса MD5Hash и результат его работы.

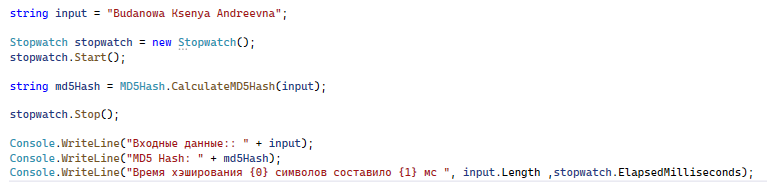


Рисунок 3.2 – Пример использования класса MD5Hash

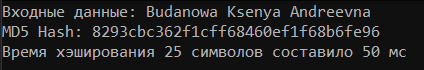


Рисунок 3.3 – Результат хэширования

Теперь увеличим длину сообщения и оценим время работы алгоритма. Результаты можно увидеть на рисунке 3.4.

Рисунок 3.4 – Скорость хэширования сообщений различной длины

**Вывод**

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

Также было разработано авторское приложение в соответствии с целью лабораторной работы.