МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

**«Исследование криптографических хэш-функций»**

Студент: Высоцкий Я.А.

ФИТ 3 курс 5 группа

Вариант 4

Преподаватель: Савельева М. Г.

Минск 2023

1. **Разработка приложения, реализующего алгоритм SHA-512**

Для разработки приложения использующее алгоритм для хэширования SHA-512 был выбран язык C#, а также встроенная библиотека System.Security.Cryptography которая в себе содержит множество семейств хэширования.

Приложение принимает текст произвольной длинны, а возвращает 512 бит захэшированного сообщения, или 128 символов.

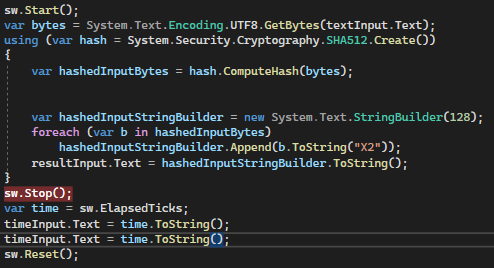
****

Рисунок 1.1 – Код хэширования входного сообщения

Так же помимо хэширования данный метод засекает время, затраченное на хэширование.

**2) Оценка времени выполнения**

Для оценки времени выполнения шифрования и расшифрования были взяты исходные текста с количеством символов 36, 72, 144.

Рисунок 2.1 – График времени выполненния хэширования текста алгоритмом SHA - 512

При увеличении количества символов в входном тексте время затраченное на хэширование уменьшается. Возможно это связано с накладными расходами на расширения изначального сообщения нулевыми битами.

**Вывод**

При выполнении лабораторной работы были изучены алгоритмы хэширования, а также были приобретены навыки по реализации и использовании их в криптографии.