МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**Лабораторная работа №11**

**«Исследование криптографических хеш-функций»**

Студент:

Храмых Владислав Олегович

Преподаватель:

Блинова Евгения Александровна

2020 г.

**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.

1. Освоить методику оценки криптостойкости хеш-преобразований на основе «парадокса дня рождения».
2. Разработать приложение для реализации заданного алгоритма

хеширования (из семейств MD и SHA).

1. Оценить скорость вычисления кодов хеш-функций.
2. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.
3. **Теоретические сведения**

**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.

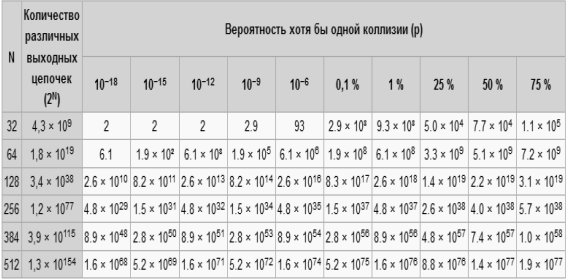
Преобразования называются **хеш-функциями или функциями свертки**, а их результаты называют **хешем, хеш-кодом, хеш-таблицей или дайджестом сообщения** (анг. message digest).

**Криптографическая хеш-функция** – это специальный класс хеш-функций, который имеет различные свойства, необходимые для решения задач в области криптографии.

Основные задачи, решаемые с помощью хеш-функций:

* аутентификация (хранение паролей),
* проверка целостности данных;
* защита файлов;
* обнаружение зловредного ПО;
* криптовалютные технологии.

На рисунке ниже приведены вероятностные оценки появления коллизии для хеш-функций различной длины:



1. **Практическая часть**

Для реализации хеширования был выбран алгоритм SHA256 и использовалась встроенная библиотека System.Security.Cryptography среды CLR (используемый язык разработки С#)

Исходный код программы представлен на рисунке 2:

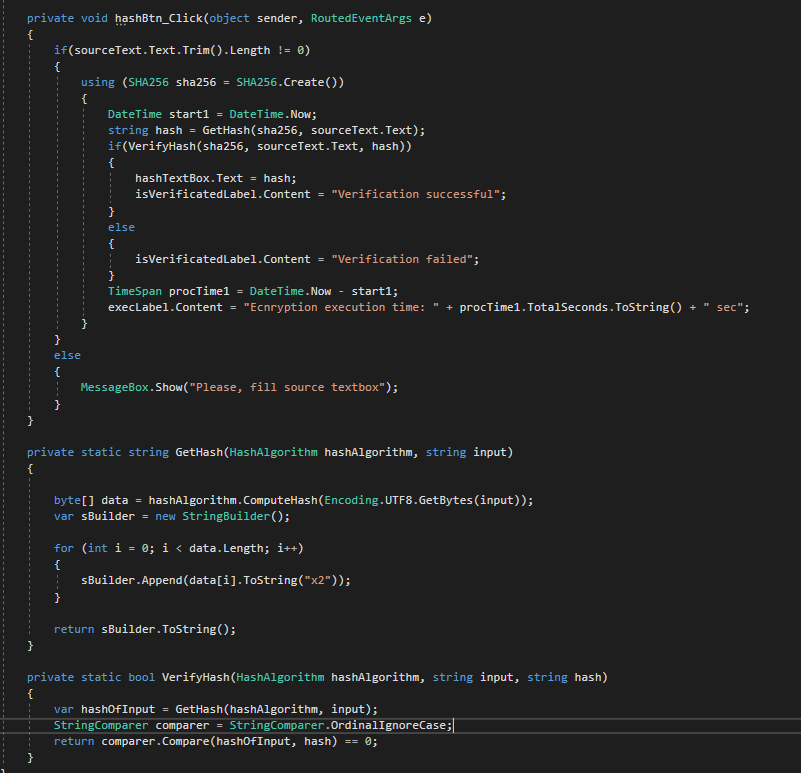


Рисунок 2 – программный код

**Вывод:** в ходе лабораторной работы были разобраны принципы работы хеш-функций, их свойства и некоторые парадоксы. Также была разработана программа, которая хеширует сообщение и проверяет его на одно из свойств хеш-функций (детерминированность). Также была проведена оценка работы функций.