МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №9**

**″Исследование криптографических хеш-функций″**

Выполнил:

Cтудент 3 курса 2 группы

Говоронок В.А.

Проверил:

Преподаватель-стажер

Копыток Д.В.

Минск 2021

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.

Выполнение работы:

Программная реализация выполнена на языке C# с использованием консольного приложения и формы.

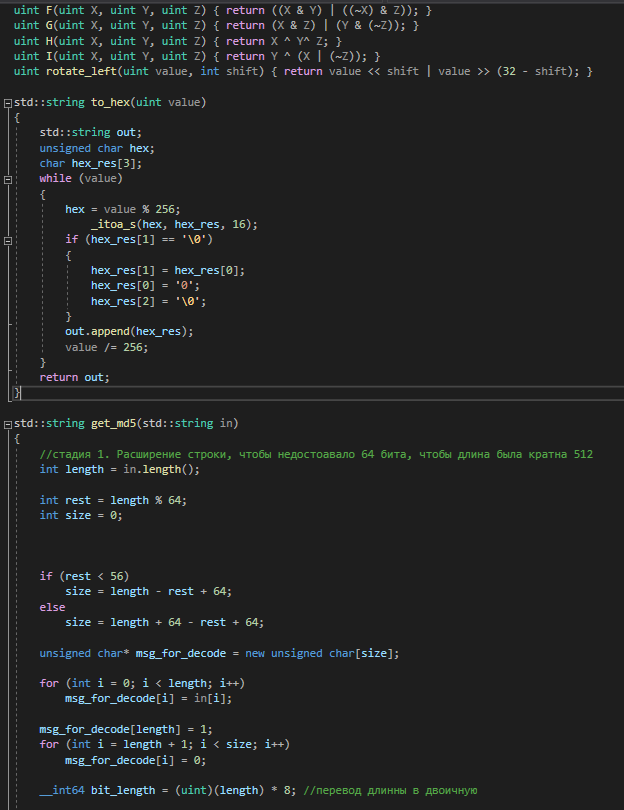


Рисунок 1 – Пример кода

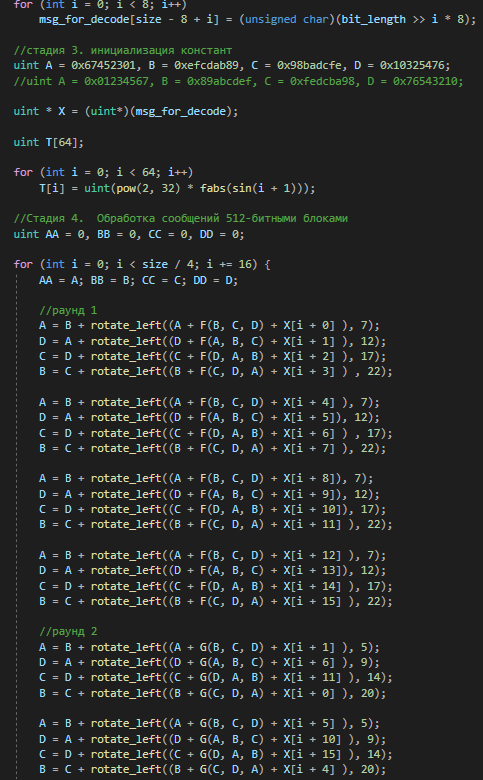


Рисунок 2 – Пример кода

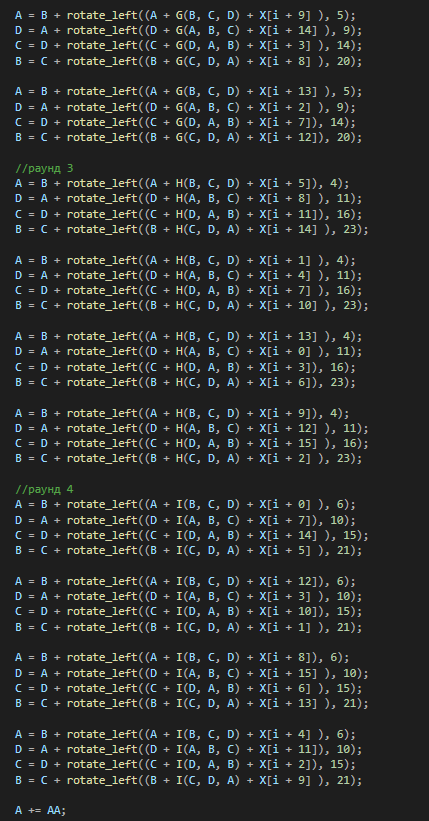
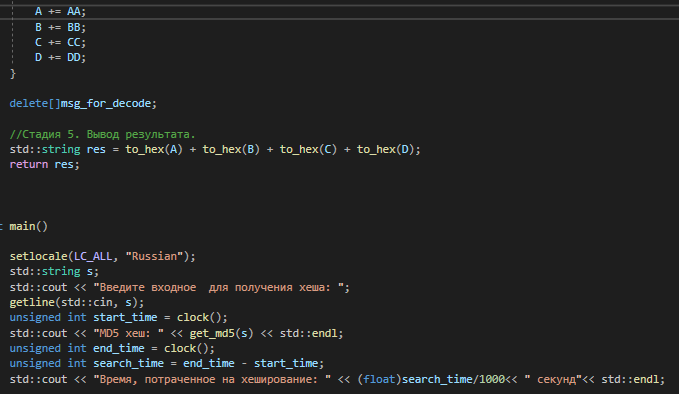


Рисунок 3 – Пример кода

Рисунок 4 – Пример кода

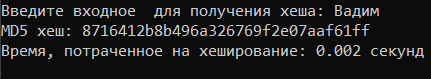


Рисунок 5 – Результат выполнения программы

Вывод: в результате данной лабораторной работы было разработано приложение для реализации заданного алгоритма хеширования – MD5.