МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №7**

**″ИССЛЕДОВАНИЕ АСИММЕТРИЧНЫХ ШИФРОВ″**

Выполнил:

Cтудент 3 курса 2 группы

Говоронок В.А.

Проверил:

Преподаватель-стажер

Копыток Д.В.

Минск 2021

Цель: изучение и приобретение практических навыков разработки и использования приложений для реализации асимметричных шифров.

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости асимметричных шифров.

2. Разработать приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для асимметричного зашифрования/расшифрования.

3. Выполнить анализ криптостойкости асимметричных шифров.

4. Оценить скорость зашифрования/расшифрования реализованных шифров.

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.

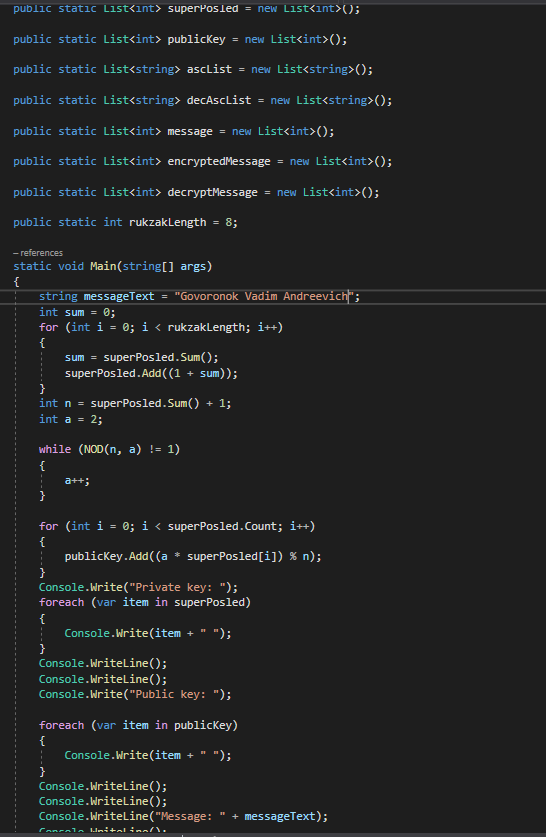


Рисунок 1 – Пример кода

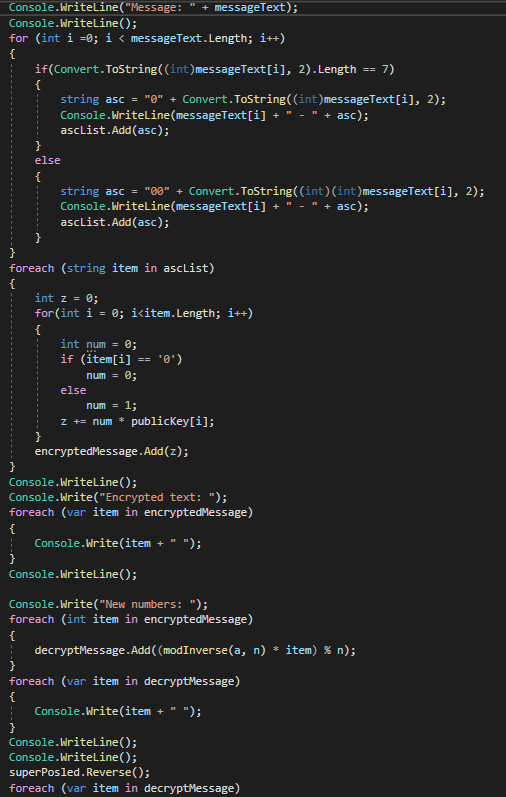


Рисунок 2 – Пример кода

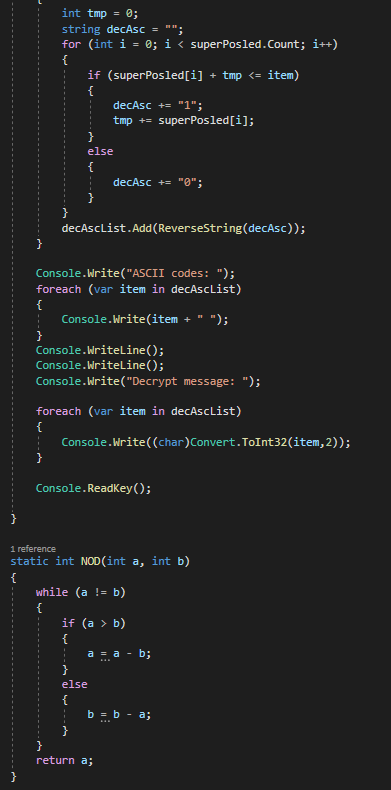


Рисунок 3 – Пример кода

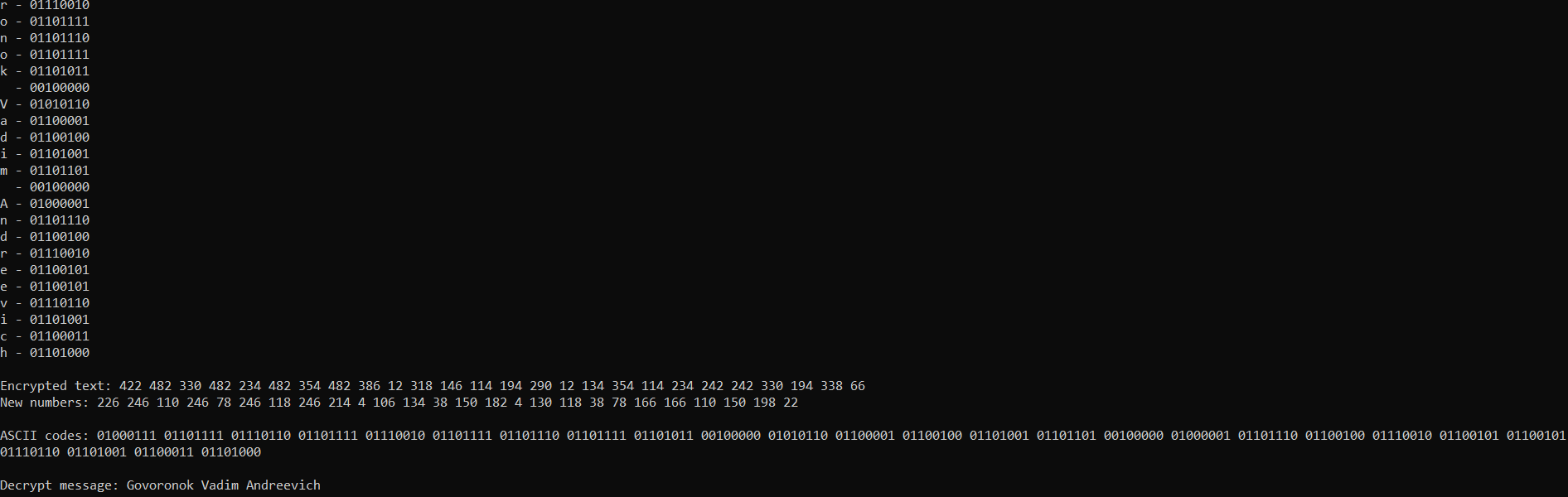


Рисунок 4 – Результат выполнения программы

Вывод: в результате данной лабораторной работы было разработано приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для асимметричного зашифрования/расшифрования.