МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №8**

**″ИССЛЕДОВАНИЕ АСИММЕТРИЧНЫХ ШИФРОВ RSA И ЭЛЬ-ГАМАЛЯ″**

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 RSA и Эль-Гамаля.

Задачи:

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

2. Разработать приложение для реализации асимметричного зашифрования/расшифрования на основе алгоритмов RSA и Эль-Гамаля.

3. Выполнить анализ криптостойкости асимметричных шифров RSA и Эль-Гамаля.

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 и формы.

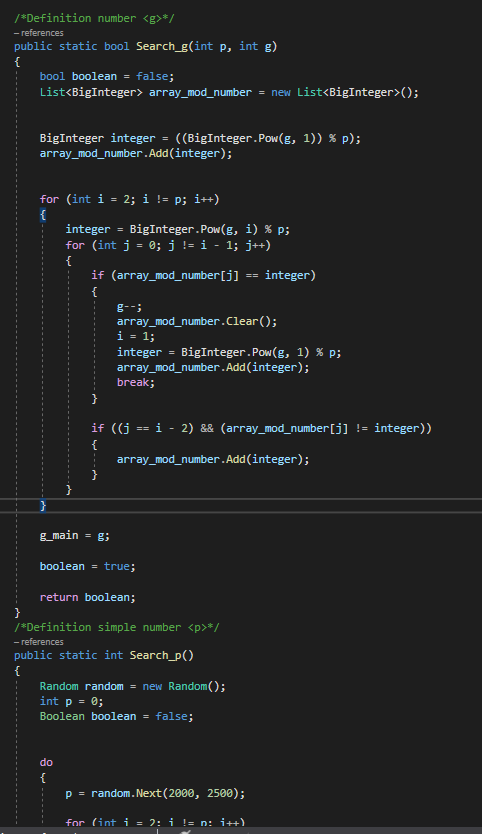


Рисунок 1 – Пример кода

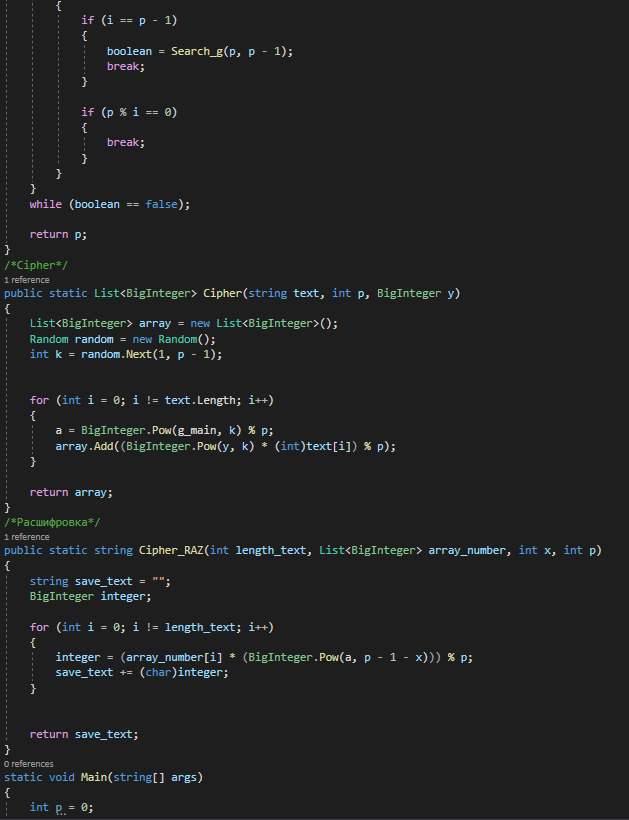


Рисунок 2 – Пример кода

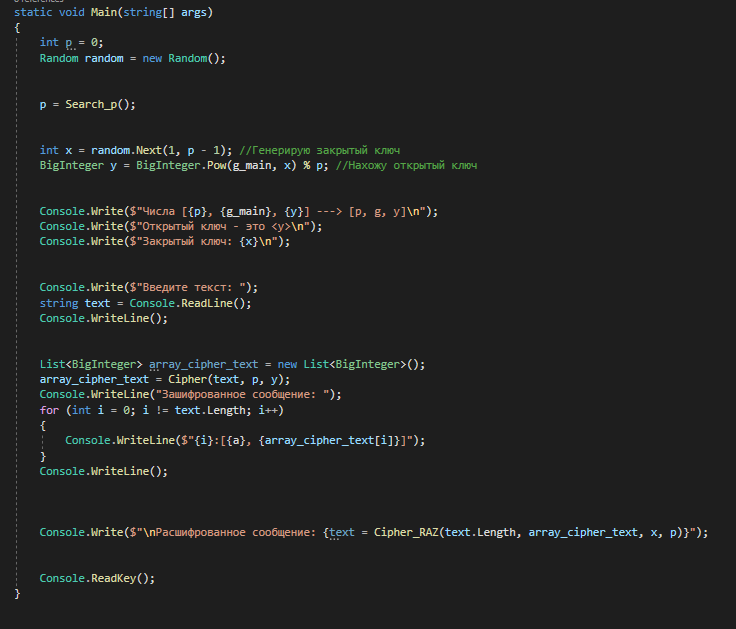


Рисунок 3 – Пример кода

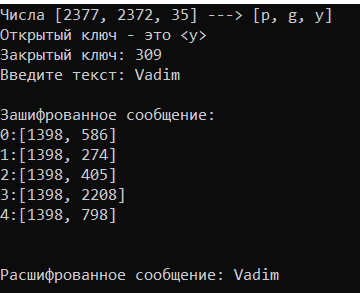


Рисунок 4 – Результат выполнения программы

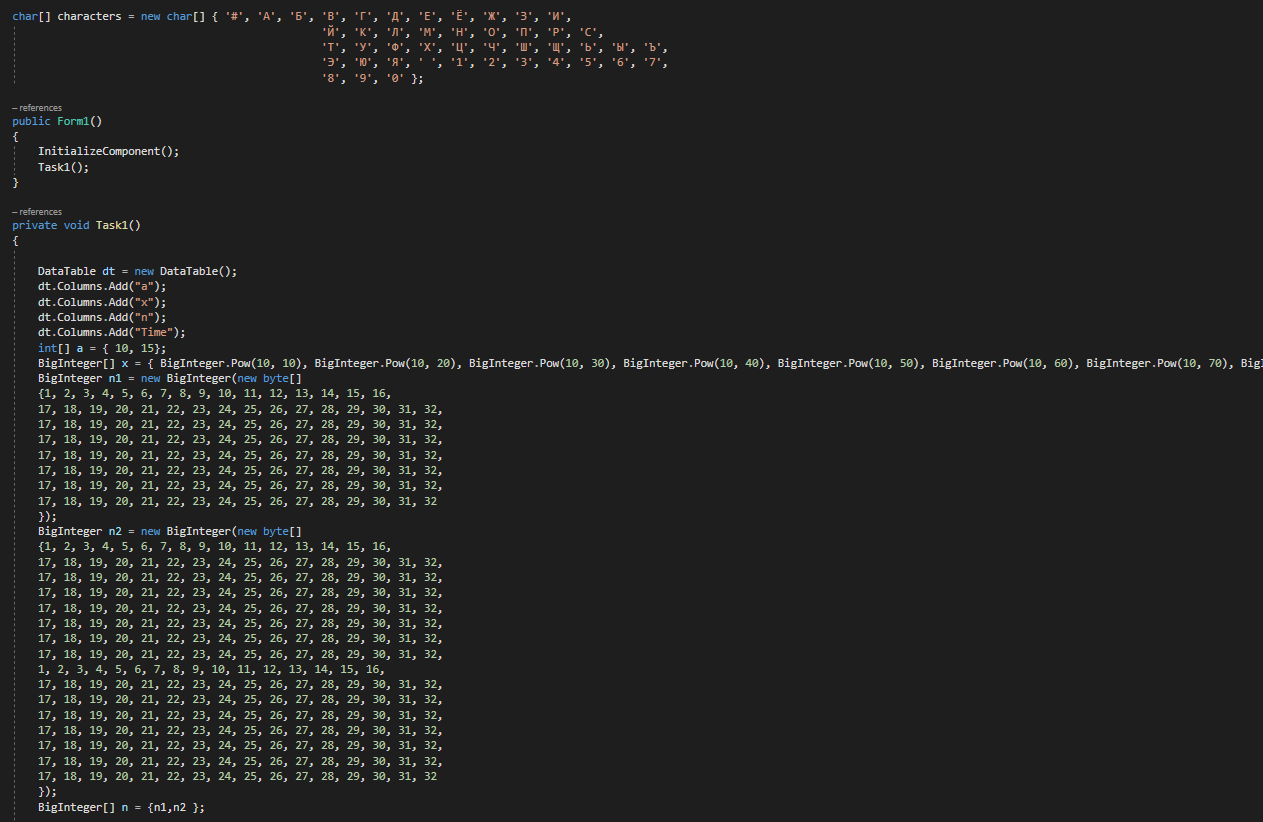


Рисунок 5 – Пример кода

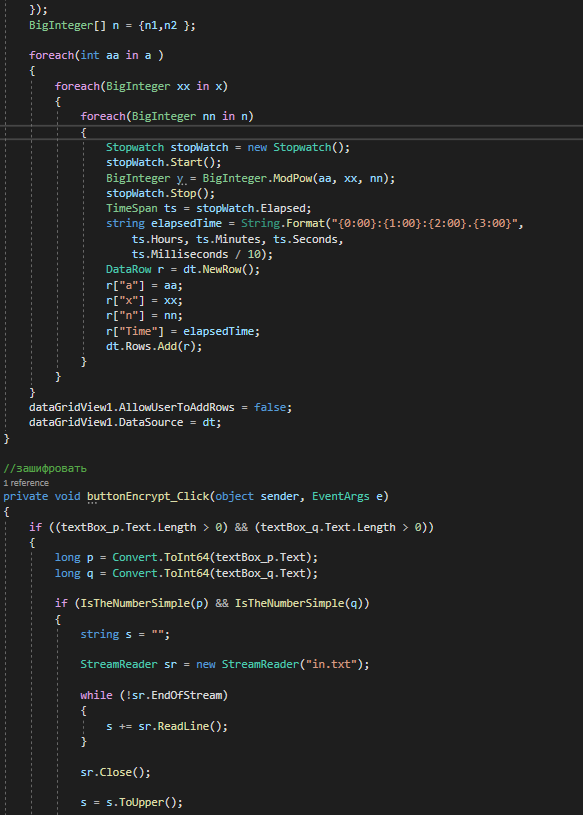


Рисунок 6 – Пример кода

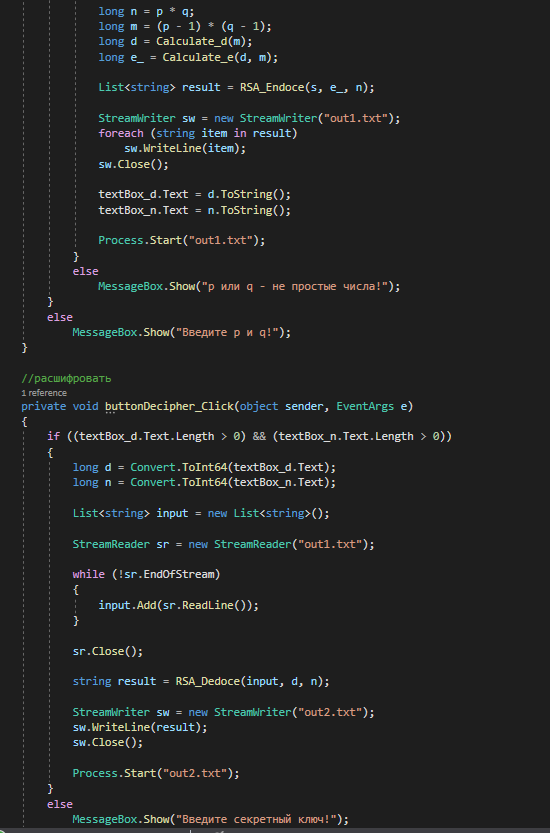


Рисунок 7 – Пример кода

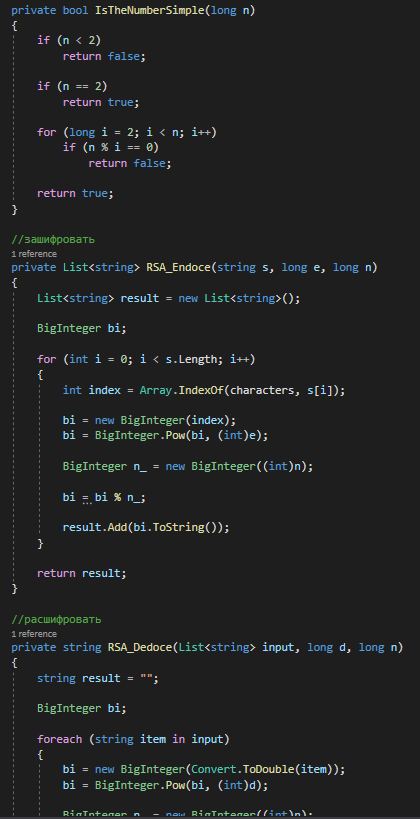


Рисунок 8 – Пример кода

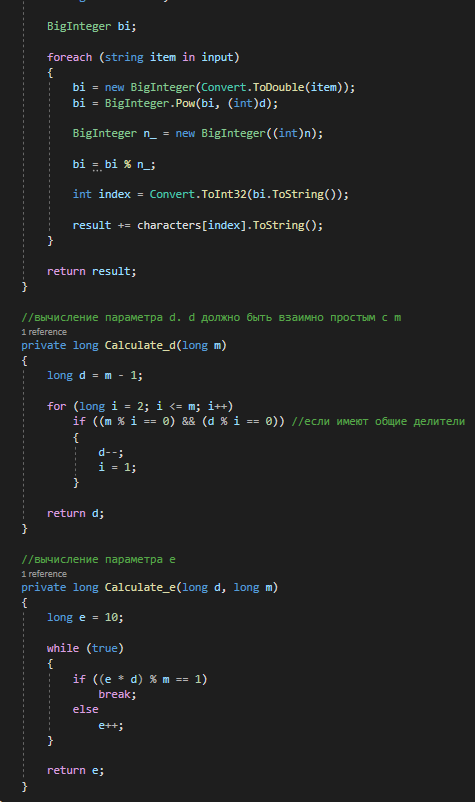


Рисунок 9 – Пример кода

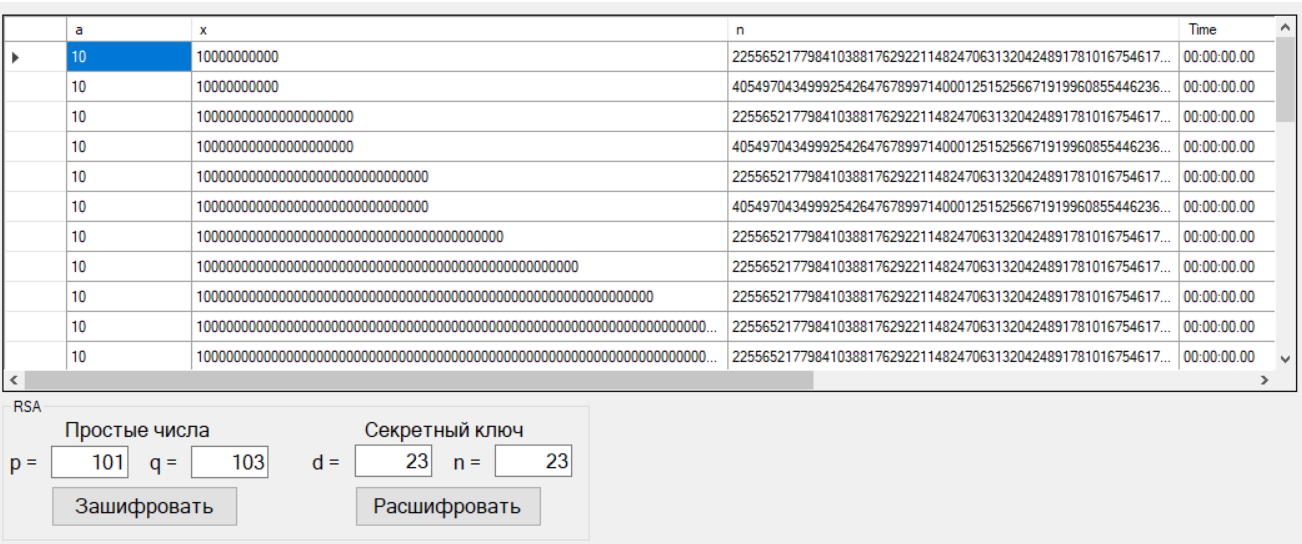


Рисунок 10 – Результат выполнения программы

Вывод: в результате данной лабораторной работы было разработано приложение для реализации асимметричного зашифрования/расшифрования на основе алгоритмов RSA и Эль-Гамаля.