Учреждение образования

«Белорусский Государственный Технологический Университет»

**Лабораторная работа №8**

**«**Исследование асимметричных шифров RSA и Эль-Гамаля»

Выполнил:

Студент 3 курса 1 группы ФИТ

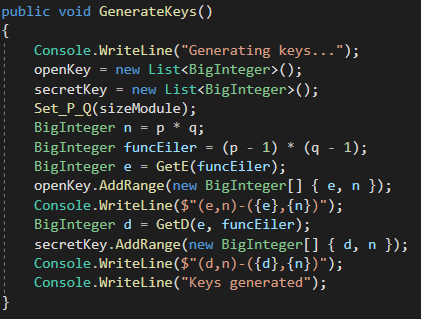
Дырда Дмитрий Геннадьевич

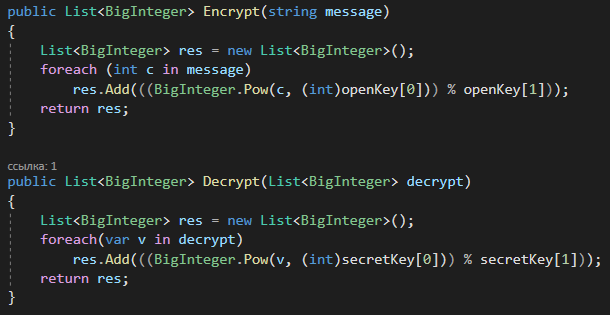
Минск 2020

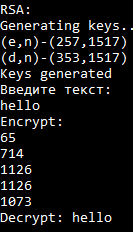
**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации асимметричных шифров RSA и Эль-Гамаля.

Разработать авторское приложение в соответствии с целью лабораторной работы. При этом можно воспользоваться доступными библиотеками либо программными кодами. В основе вычислений – кодировочные таблицы Base64 и ASCII. Приложение должно реализовывать следующие операции: • зашифрование и расшифрование текстовых документов на основе алгоритмов RSA и Эль-Гамаля; • определение времени выполнения операций. Исходный текст для зашифрования – собственные фамилия, имя, отчество. Для численного представления блоков текста можно, в том числе, пользоваться указанными выше кодировочными таблицами.

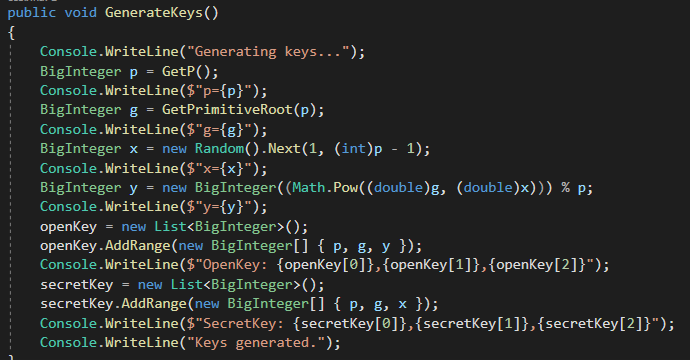
RSA:

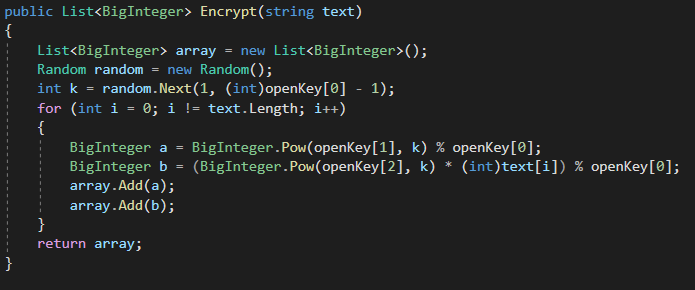


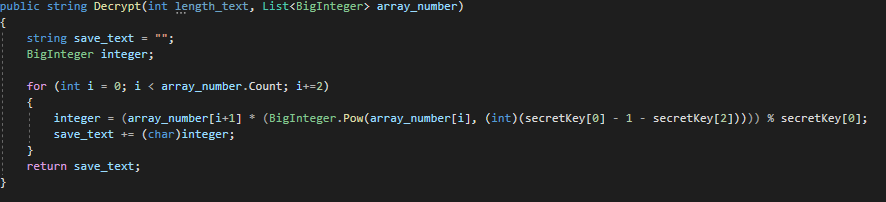


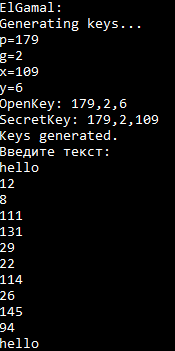


Эль-Гамаль:









**Вывод:** я изучил и приобрел практические навыки разработки и использования приложений для реализации асимметричных шифров RSA и Эль-Гамаля.