БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

ОТЧЕТ ПО КРИПТОГРАФИЧЕСКИМ МЕТОДАМ

студента 2 курса 13 группы

Лабораторная работа №5

Вариант 11

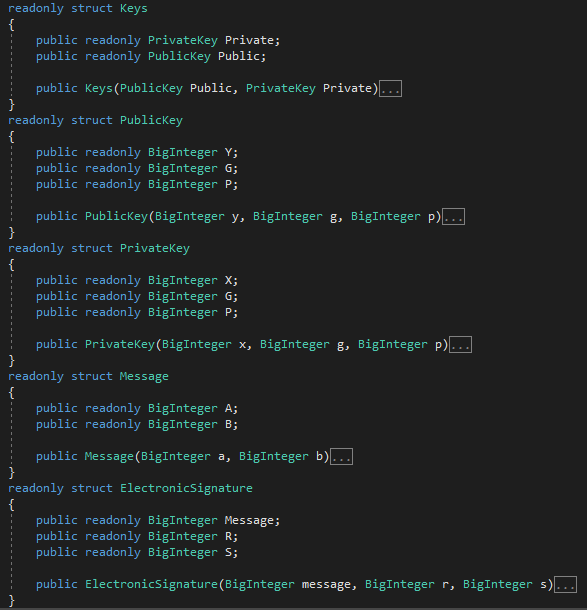
Преподаватель

Ярошеня Ю.С.

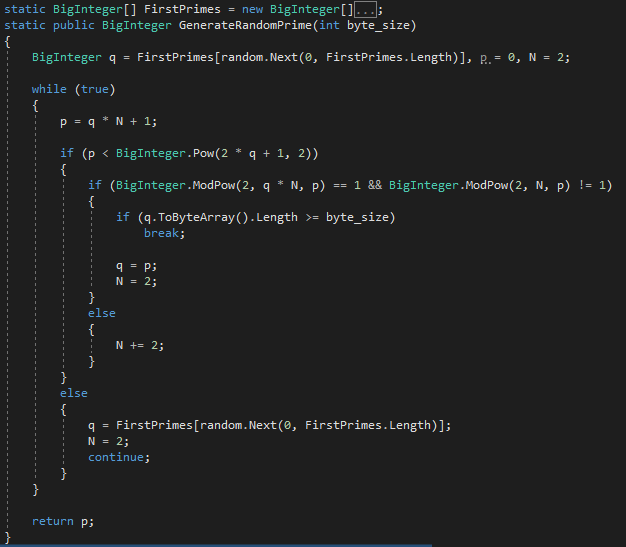
Минск 2020

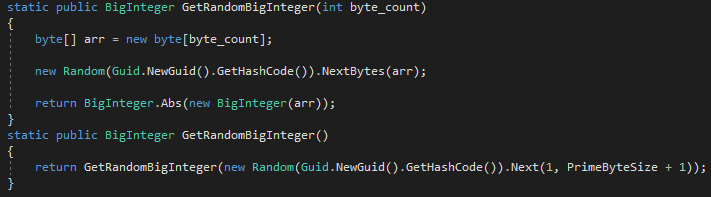
ElGamal

В алгоритме использованы следующие структуры:



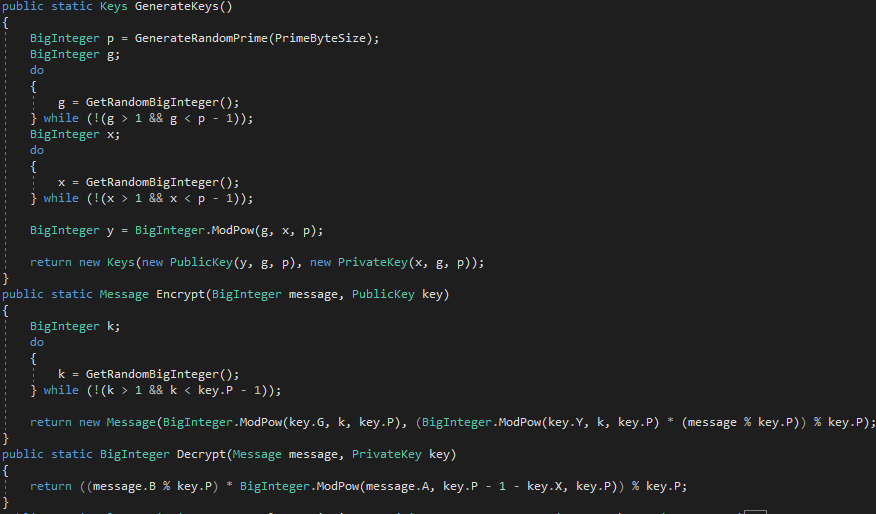
И методы генерации больших в т.ч. простых чисел из первой лабораторной:



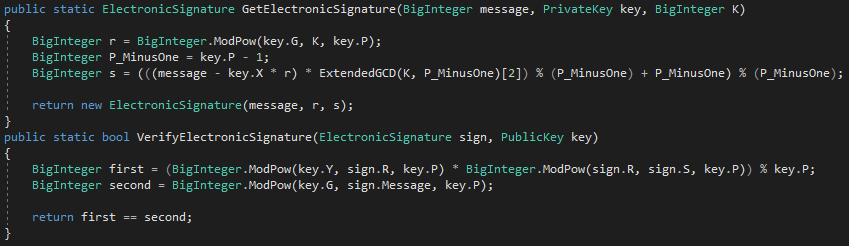


Алгоритм:

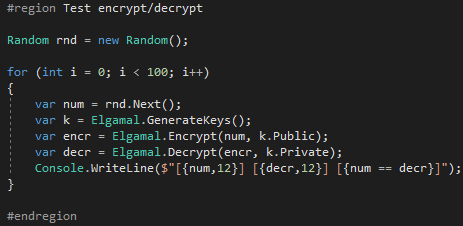
Я реализовал методы генерации ключей, а также шифровки-дешифровки, хотя для эцп они не нужны:

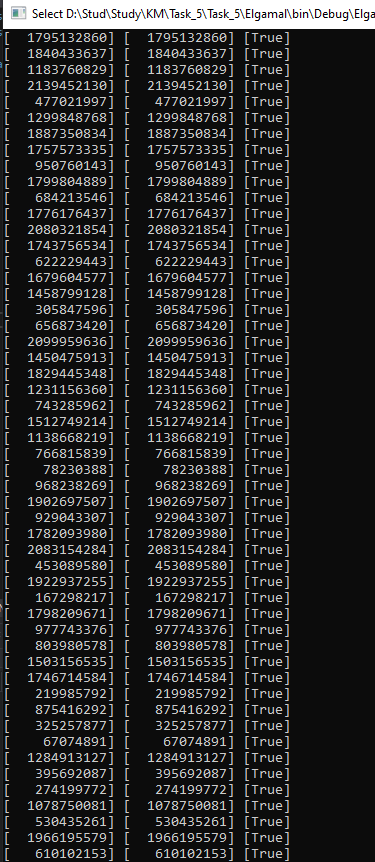


Создание и подтверждение подписи:



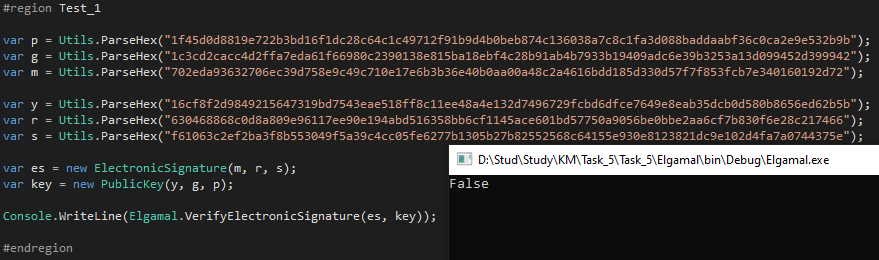
Проверка шифрования:



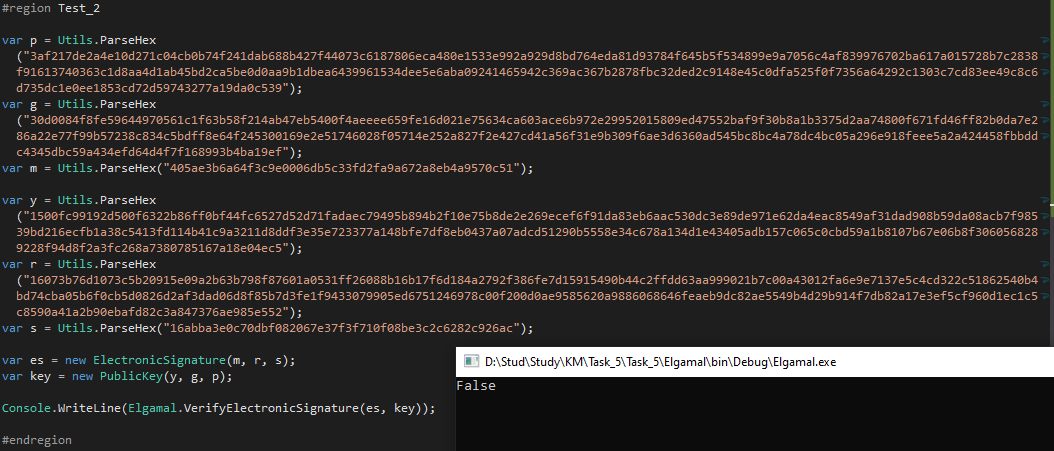


Подписи (вариант 11):

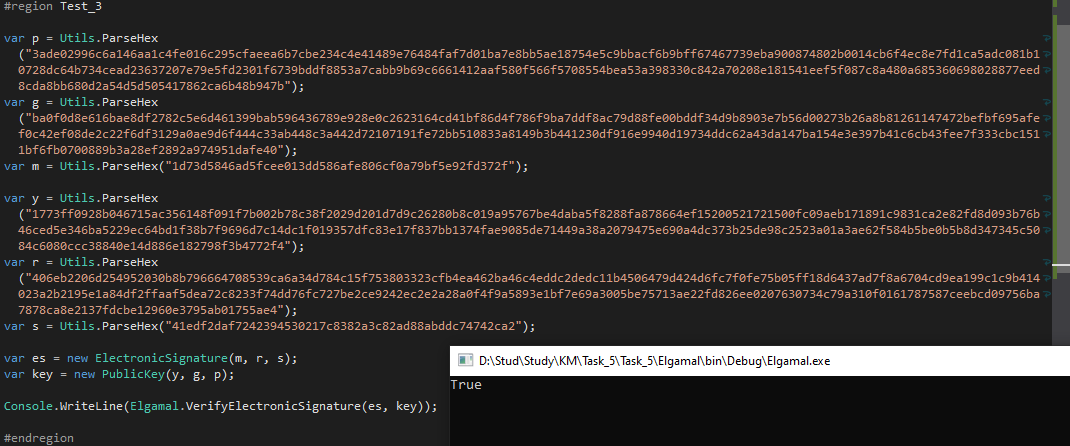
Первая подпись



Вторая подпись



Третья подпись



Четвертая подпись

