Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное

учреждение высшего образования

«ПЕТРОЗАВОДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт Математики и Информационных технологий.

Криптографические средства защиты информации

Лабораторная работа №1

Выполнили

Студенты 3 курса Диков Е., Шамарин Р.

Группа: 22307

Преподаватель:

Воронов Роман Владимирович

Петрозаводск

2020

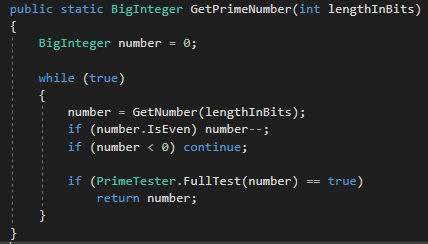
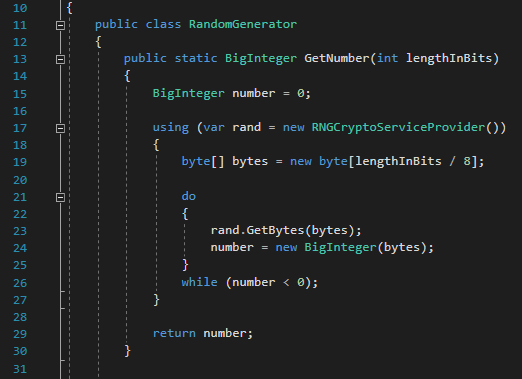
Язык программирования – C#

Библиотека для работы с большими числами – System.Numerics (BigInteger).

Генерация чисел

Класс RandomGenerator содержит 2 основных метода для генерации чисел:

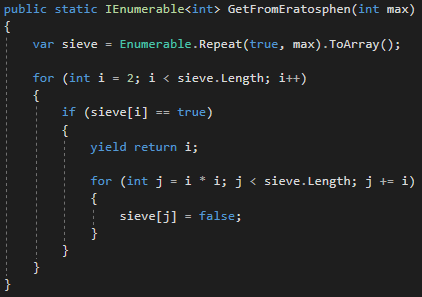
* Генерация произвольного числа
* Генерация простого числа



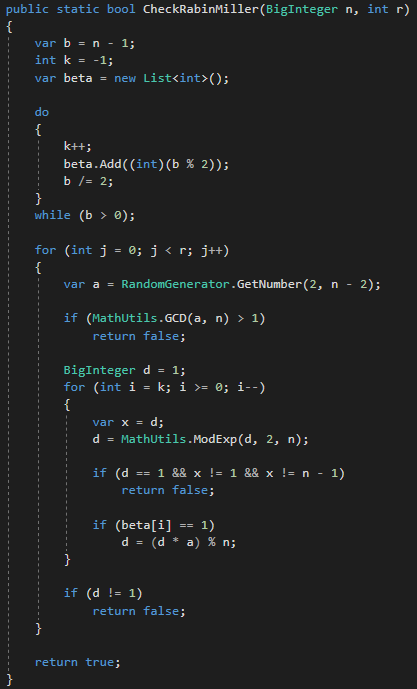
Проверка числа на простоту

Класс PrimeTester содержит методы для проверки числа на простоту:

Метод GetFromEratosphen(max) – возвращает список первых простых чисел, не превосходящих max (2, 3, 5, 7, 11, …):



Метод CheckRabinMiller(n, r) проверяет число на простоту:



Проверка an-1 mod n = 1

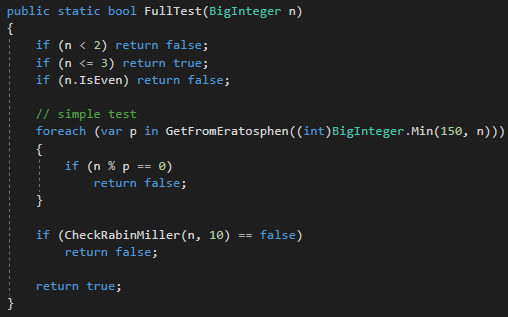
Находим (an-1 mod n). При возведении в квадрат проверяем на нетривиальный корень из 1

Если найден нетривиальный корень из единицы, то число составное

k – длина списка beta

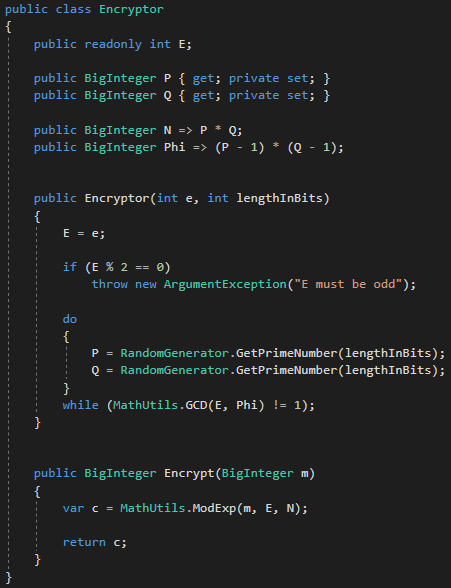
beta – список для двоичного представления числа n-1

Метод FullTest(n) использует вышеуказанные методы для проверки числа на простоту.



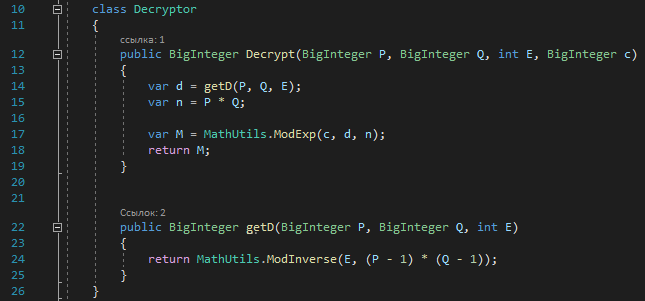
Шифрование

Для шифрования используется класс Encryptor:



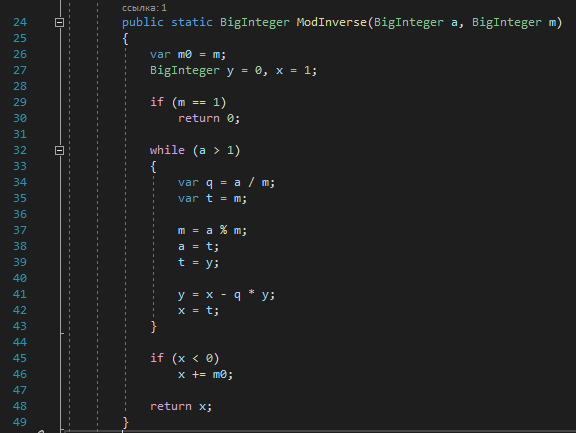
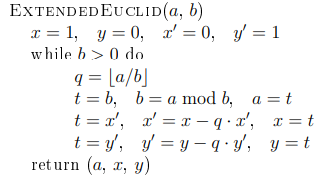
Расшифровка

Для расшифровки используется класс Decryptor:

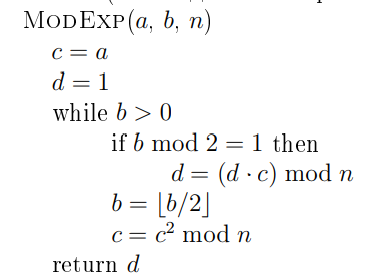


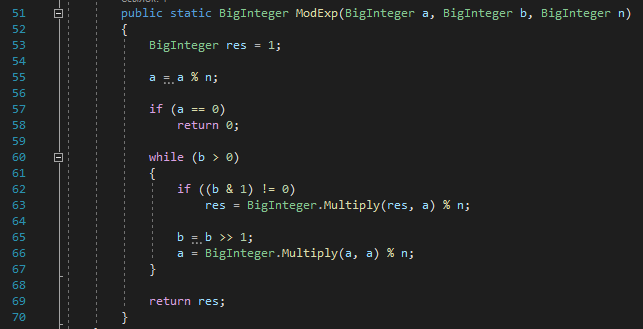
Функции для работы с большими числами

Вычисление обратного элемента по модулю:

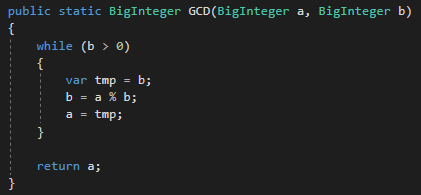


Метод повторного возведения в квадрат:



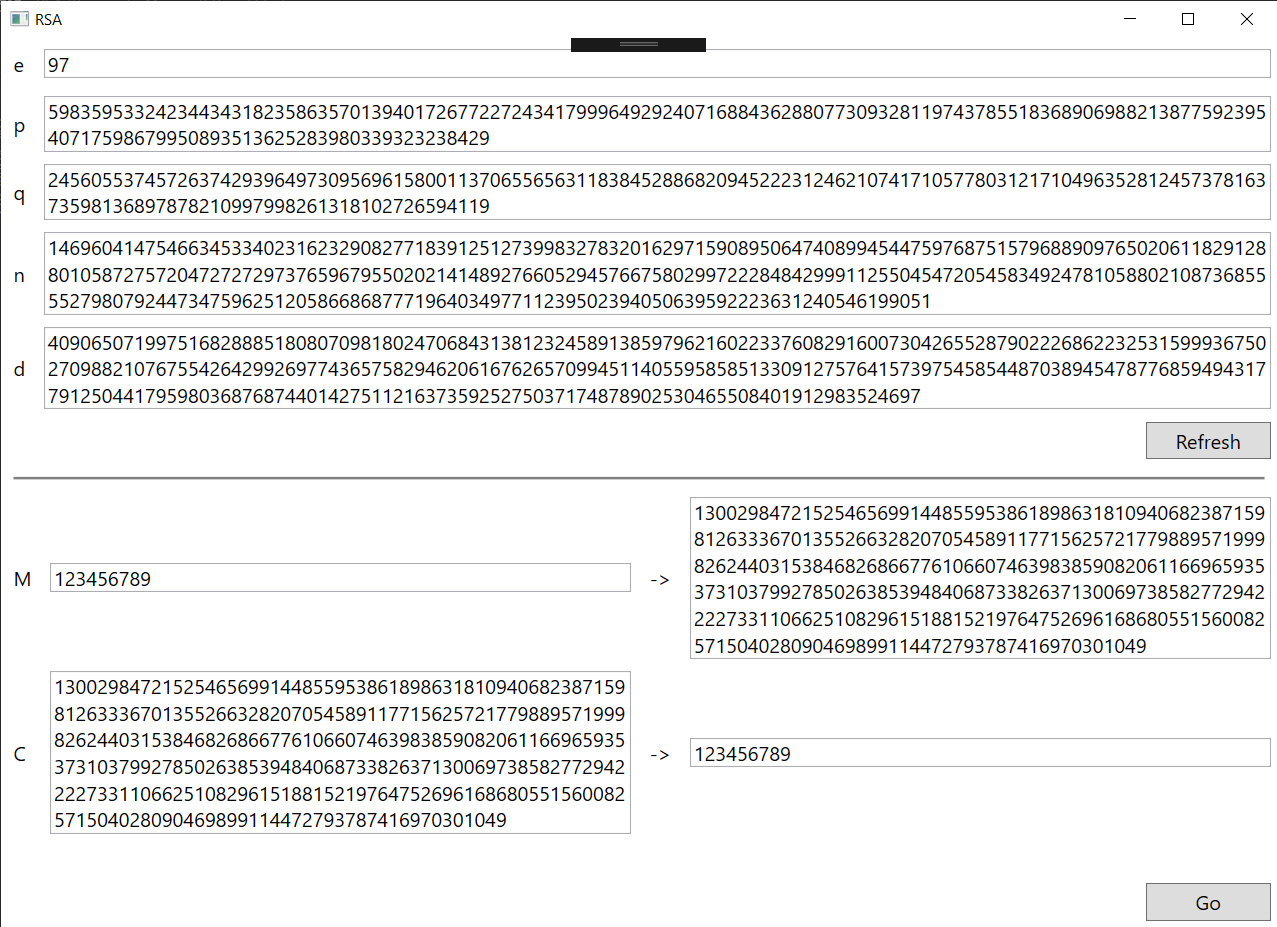


Нахождение НОД:



Пользовательский интерфейс и демонстрация работы

Генерация чисел длины не больше 512 бит:



Генерация чисел длины не больше 1024 бит:

