Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра информационных систем и технологий

Отчет

по дисциплине «Защита информации и надежность информационных систем»

Студент: Шумова Е.И.

ФИТ 3 курс, 1 группа, 1 подгруппа

Преподаватель: Савельева М.Г.

Минск 2022

Лабораторная работа №1

**Тема «Основы теории чисел и их использование в криптографии»**

**Цель:** приобретение практических навыков выполнения операций с числами для решения задач в области криптографии и разработка приложений для автоматизации этих операций.

**Задачи:**

* Закрепить теоретические знания по высшей арифметике.
* Научиться практически решать задачи с использованием простых и взаимно простых чисел, вычислений по правилам модулярной арифметики и нахождению обратных чисел по модулю.
* Ознакомиться с особенностями реализации готового программного средства L\_PROST и особенностями выполнения с его помощью операций над простыми числами.
* Разработать приложение для реализации указанных преподавателем операций с числами.
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения эксперимента с использованием приложения и результатов эксперимента.

**Теоретические сведения**

Теория чисел, или высшая арифметика, – раздел математики, изучающий натуральные числа и иные похожие величины.

Множество всех целых чисел (обозначим буквой *Z*) есть набор всех действительных чисел без дробной части: *{..., –3, –2, –1, 0, 1, 2, 3, ...}.*

Натуральные числа являются подмножеством целых чисел и образуют множество *N*: *{1, 2, 3, ...}.*

Всякое целое число а можно представить с помощью положительного целого числа *b* равенством вида *а = bq + r*, 0 ≤ *r* ≤ *b*. Число *q* называется неполным частным, а число *r* – остатком от деления *а* на *b*.

Если число не имеет делителей, кроме самого себя и единицы, то оно называется простым, а если у числа есть еще делители, то составным.

Основная теорема арифметики. Всякое натуральное число *n*, кроме 1, можно представить как произведение простых множителей: *n = p1p2p3...pz, z >* 1.

Если два простых числа отличаются на 2, то их называют числами-близнецами.

Наибольшее целое число, которое делит без остатка числа *a* и *b*, называется наибольшим общим делителем этих чисел – НОД (*a, b*).

Взаимно простыми являются целые числа, наибольший общий делитель которых равен 1.

Свойства простых чисел.

*Свойство 1*. Любое составное число представляется уникальным образом в виде произведения простых чисел; иначе еще говорят, что разложение числа на простые множители однозначно.

*Свойство 2.* Простых чисел бесконечно много, причем существует примерно *n / ln(n)* простых чисел, меньших числа *n*.

*Свойство 3.* Наименьший простой делитель составного числа n не превышает *√n*, поэтому для проверки простоты числа достаточно проверить его делимость на 2 и на все нечетные (а еще лучше простые) числа, не превосходящие *√n*; как видим, данное свойство коррелирует со свойством 1 собственного делителя.

*Свойство 4*. Любое четное число, большее 2, представимо в виде суммы двух простых чисел, а любое нечетное, большее 5, представимо в виде суммы трех простых чисел.

*Свойство 5*. Для любого натурального *n*, большего 1, существует хотя бы одно простое число на интервале от *n* до *2n*.

**Результат выполнения программы**

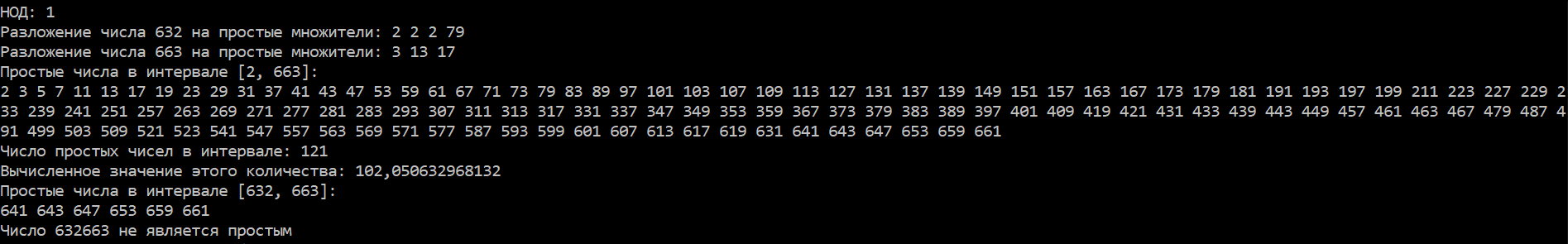


Рисунок 1 – Результат выполнения программы

*n/ln(n)* = 102. Вычисленное программой количество простых чисел = 121. Программа высчитывает логарифм неверно из-за особенностей языка.

Число 632663 является составным.

**Вывод:** в данной лабораторной работе были изучены основные задачи криптографии, а также были приобретены практические навыки выполнения операций с числами, а именно нахождение простых и взаимно простых чисел, вычисления по правилам модулярной арифметики и нахождение обратных чисел по модулю. Было разработано приложение для автоматизации обозначенных выше операций, которое было проверено при помощи тестовых данных для моего варианта.