МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №3**

по дисциплине «Криптографические методы защиты информации»

на тему: ОСНОВЫ ТЕОРИИ ЧИСЕЛ И ИХ ИСПОЛЬЗОВАНИЕ В КРИПТОГРАФИИ

Выполнил студентка 3 курса 5 группы специальность ПОИТ Буранко В.Д.

(Ф.И.О.)

Преподаватель ассистент Савельева Маргарита Геннадьевна

(Ф.И.О.)

Оглавление

[**Теоретические сведения** 3](#_Toc130160227)

[**Практические задания** 5](#_Toc130160228)

[Задание 1 5](#_Toc130160229)

[Задание 2 5](#_Toc130160230)

[Задание 3 6](#_Toc130160231)

[Задание 4 6](#_Toc130160232)

[Задание 5 6](#_Toc130160234)

**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;
* 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. В зависимости от используемых методов в теории чисел рассматривают несколько направлений. Нас будут интересовать вопросы делимости целых чисел, вычисления наибольшего общего делителя (НОД), разложение числа на простые множители, малая теорема Ферма́, теорема Эйлера, элементы теории вычетов.

Множество всех целых чисел (обозначим буквой *Z*) есть набор всех ***действительных чисел*** без дробной части: {..., –3, –2, –1, 0, 1, 2, 3, ...}. Основы теории чисел и их использование в криптографии

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

***Делимость*** – одно из основных понятий теории чисел. Если для некоторого целого числа a и натурального числа *b* существует целое число *q*, при котором *bq = a*, то говорят, что число a делится на *b*. В этом случае *b* называется делителем числа *a*, а a называется кратным числу *b*.

Натуральное число n называется ***простым***, если *n* > *1* и не имеет положительных делителей, отличных от 1 и *n*.

Для нахождения всех простых чисел не больше заданного числа n в соответствии с ***«решетом Эратосфена»*** нужно выполнить следующие шаги:

1) выписать подряд все целые числа от двух (либо от *m*) до n (2, 3, 4, …, *n*). Пусть некоторая переменная (например, *s*) изначально равна 2 – первому простому числу;

2) удалить из списка числа от 2*s* до *n*, считая шагами по *s* (это будут числа, кратные *s*: 2*s*, 3*s*, 4*s*, …);

3) найти первое из оставшихся чисел в списке, большее чем *s*, и присвоить значению переменной *s* это число;

4) повторять шаги 2 и 3, пока возможно.

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

# **Практические задания**

Задание 1:

Найти все простые числа в интервале [2, *n*]. Подсчитать количество простых чисел в указанном интервале. Сравнить это число с *n*/ln(*n*) (по варианту: *n*=553).

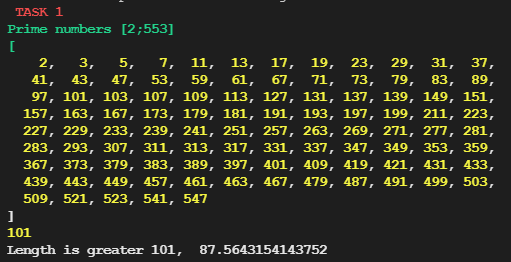


Рисунок 1 — Простые числа в интервале [2, *n*]

Задание 2:

Повторить задание 1 для интервала [*m*, *n*]. Сравнить полученные результаты с «ручными» вычислениями, используя «решето Эратосфена» (по варианту: *m*=521).

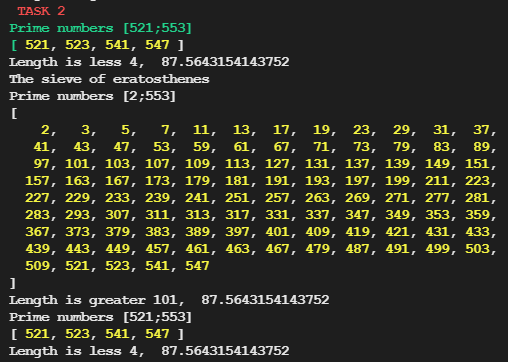


Рисунок 2 — Простые числа в интервале [*m*, *n*]. Простые числа в интервалах [2, *n*] и [*m*, *n*], используя «решето Эратосфена»

Задание 3:

Записать числа *m* и *n* в виде произведения простых множителей (форма записи – каноническая).

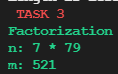


Рисунок 3 — Числа *m* и *n* в виде произведения простых множителей

Задание 4:

Проверить, является ли число, состоящее из конкатенации цифр *m* ǀǀ *n*, простым.



Рисунок 4 — Проверка, является ли число, состоящее из конкатенации цифр *m* ǀǀ *n*, простым

Задание 5:

Найти НОД (*m*, *n*). Вычислить НОД трех чисел.



Рисунок 5 — НОД (*m*, *n*). НОД трех чисел

# **Выводы**

В ходе выполнения лабораторной работы ознакомилась с основами теории чисел и их использованием в криптографии. Было разработано приложение, предназначенное для автоматизации операций с числами для решения задач в области криптографии. Так же были закреплены теоретические знания по высшей арифметике.