Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Криптографические методы защиты информации

Студент: Сенченя В.И.

ФИТ 3 курс 5 группа

Преподаватель: Савельева М. Г.

Минск 2023

**Лабораторная работа №3**

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

Цель: приобретение практических навыков расчета и анализа

параметров и информативных характеристик дискретных ИС.

Задачи:

1. Закрепить теоретические знания по основам теории информации.

2. Научиться практически решать задачи с использованием простых и взаимно простых чисел, вычислений по правилам модулярной арифметики и нахождению обратных чисел по модулю.

3. Разработать приложение для реализации указанных преподавателем операций с числами.

4. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения эксперимента с использованием приложения и результатов эксперимента.

**Вычисление НОД двух чисел**

**НОД –** Наибольшеецелоечисло, которое делить без остатка числа *a* и *b*

Для вычисления НОД двух чисел мною был реализован алгоритм Евклида, в котором используется цепочка вычислений двумя исходными числами.

Реализация алгоритма приведена на рисунке на рисунке 1.1

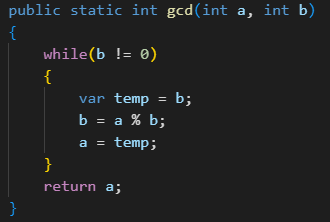
****

Рисунок 1.1 – Реализация алгоритма Евклида

А также на рисунке 1.2 приведен результат выполнения

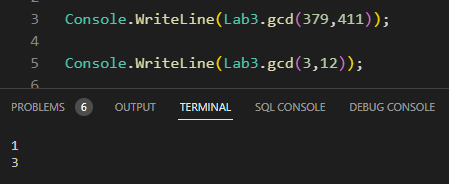


Рисунок 1.2 – Результат работы функции

**Поиск простых чисел**

Для поиска простых была разработана функция, которая заключается в том, чтобы проверить, делиться ли число на какое-либо другое число, кроме как на себя и на единицу.

Для этого создаём цикл, который проходит от 3 до с прибавлением к индексу 2 на каждом шаге, таким образом можно сократить количество итераций используя **свойство собственного делителя**.

Код программы и результат работы предоставлены соответственно на рисунках 1.3 и 1.4.

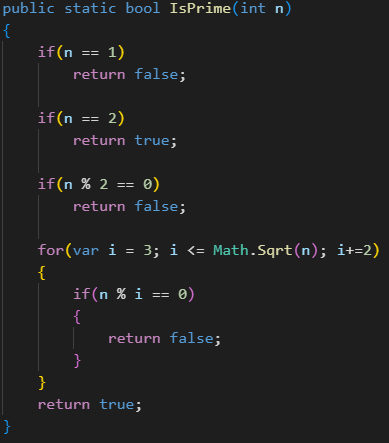


Рисунок 1.3 – Код программы по поиску простых чисел

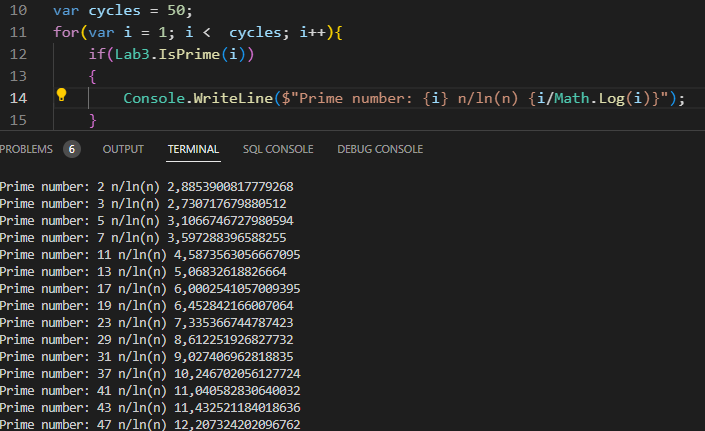


Рисунок 1.4 Результат работы программы

И вручную посчитанное решето Эратосфена представлена в Таблице 1.1

Таблица 1.1 – решето Эратосфена

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| - | 2 | 3 | 4 | 5 | 6 | 7 | 9 | 10 | 11 |
| 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 |

**Каноническая запись числа**

Каноническая запись числа – разложение числа на простые множители, перемножив которые можно получить исходное число.

Код программы и результат выполнения представлен на рисунках 1.5 и 1.6 соответственно.



Рисунок 1.5 – Код программы разложения числа



Рисунок 1.6 – Результат работы программы по разложению числа

**Заключение**

В ходе выполнения лабораторной работы я приобрёл практические навыки выполнения операций с числами для решения задач в области криптографии и работки приложений для автоматизации этих операций.