Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Лабораторная работа № 3**

« Основы теории чисел и их использование в криптографии»

Выполнил:

Студент: Белицкий В.Д.

ФИТ 2 курс 5 группа

Преподаватель: Савельева М.Г.

Минск 2022

1. **Описание приложения**

Приложение написано на языке программирования C# и позволяет провести расчет НОД двух либо трех чисел, найти все простые числа в заданном промежутке и разложить число на множители.

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 наибольшегообщего делителя (НОД).

1. **Методика выполнения расчетов**

В данной лабораторной работе была поставлена цель создания приложения, позволяющее произвести расчёт НОД двух либо трёх чисел, а также выполнить поиск простых чисел из диапазона. На листинге 2.1 представлен класс, реализующий данную функциональность.

static class NOD

{

public static int Compute(int x, int y)

{

while (x != 0 && y != 0)

{

if (x > y)

{

x -= y;

}

else

{

y -= x;

}

}

return Math.Max(x, y);

}

private static bool IsSimple(int x)

{

for (int i = 2; Math.Pow(i, 2) <= x; i++)

{

if (x % i == 0)

{

return false;

}

}

return true;

}

public static void FindSimple(int m, int n)

{

int counter = 0;

if (n < m)

{

Console.WriteLine("Неверный промежуток");

}

Console.Write($"Простые числа интервала [{m},{n}]: ");

for (int i = m; i <= n; i++)

{

if (IsSimple(i))

{

Console.Write(i.ToString() + " ");

counter++;

}

}

Console.WriteLine();

Console.WriteLine($"Количество простых чисел: {counter}");

}

}

Листинг 2.1 – класс, реализующий необходимый функционал

Метод Compute используется для получения НОД двух чисел путём исполнения алгоритма Евклида. Метод IsSimple осуществляет проверку на то, является ли переданное в него в качестве параметра число простым. Метод FindSimple находит все простые числа в диапазоне, границы которого переданы в него в качестве двух параметров.

**3. Результаты работы приложения**

Для выполнения расчетов достаточно необходимо запустить приложение, выбрать необходимый пункт задания и ввести числа. Рисунки 3.1, 3.2, 3.3 показывают необходимые расчеты и вызовы методов, требуемые в данной лабораторной работе.

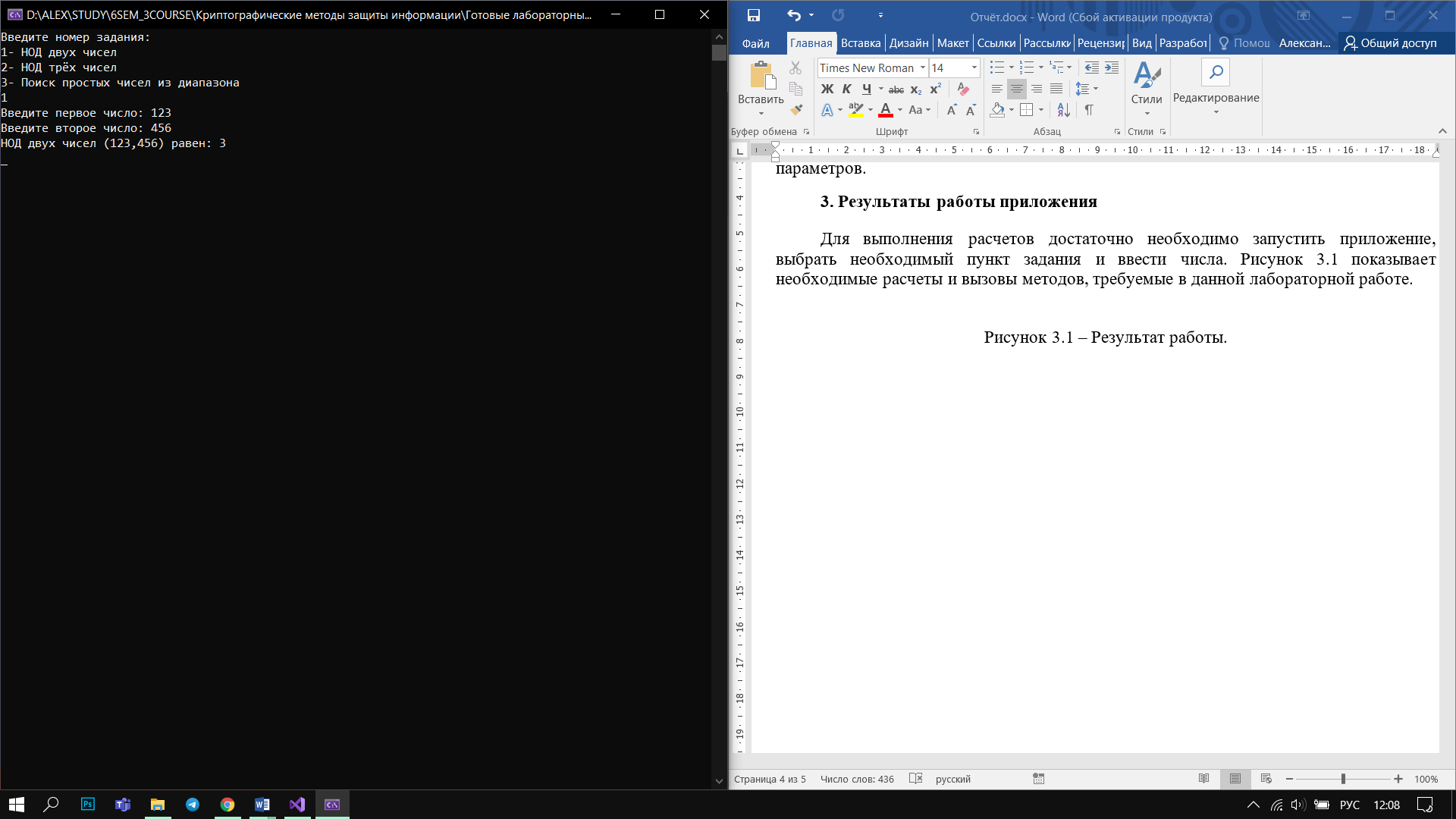


Рисунок 3.1 – Результат работы методе Compute с двумя числами

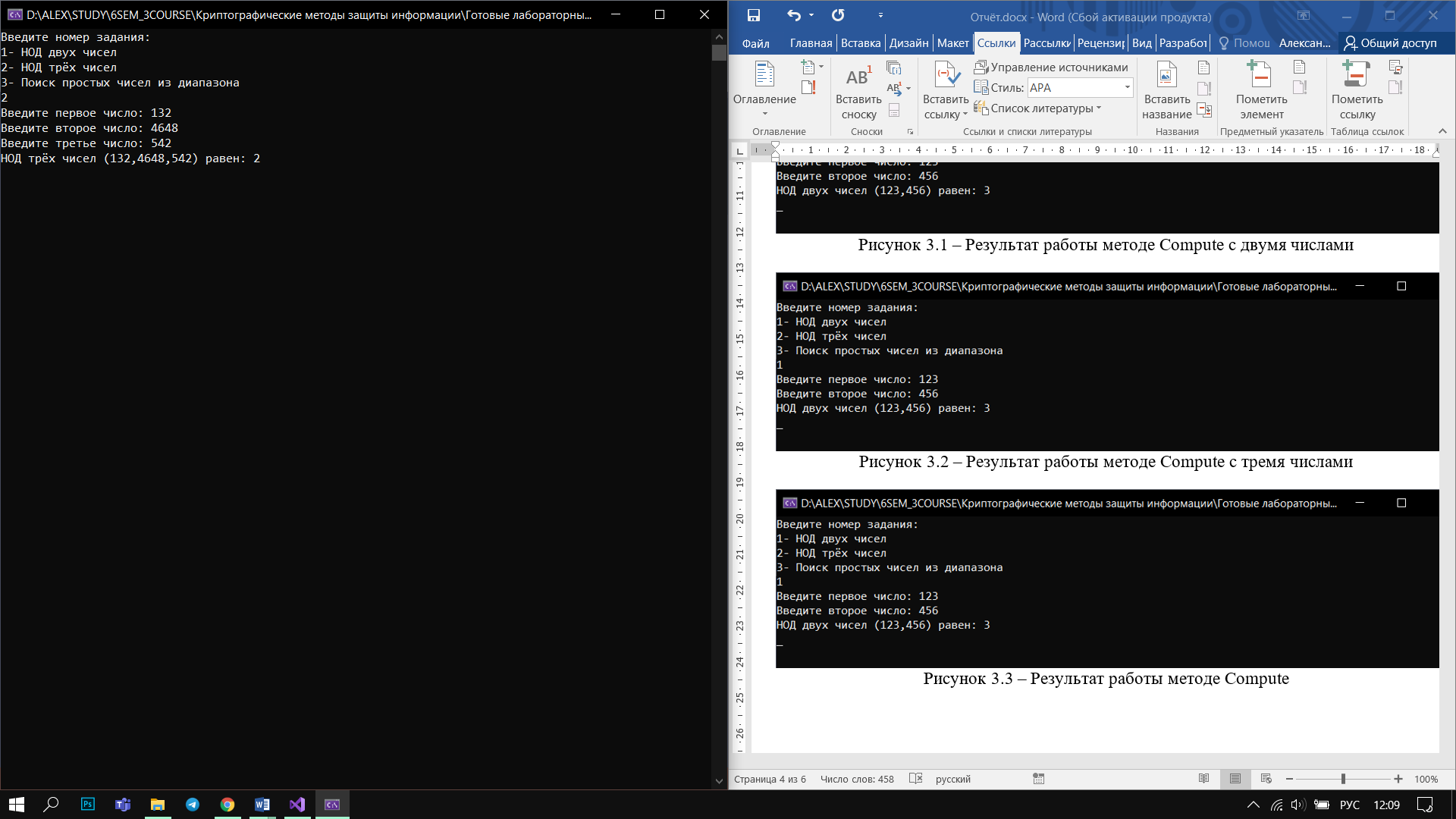


Рисунок 3.2 – Результат работы методе Compute с тремя числами

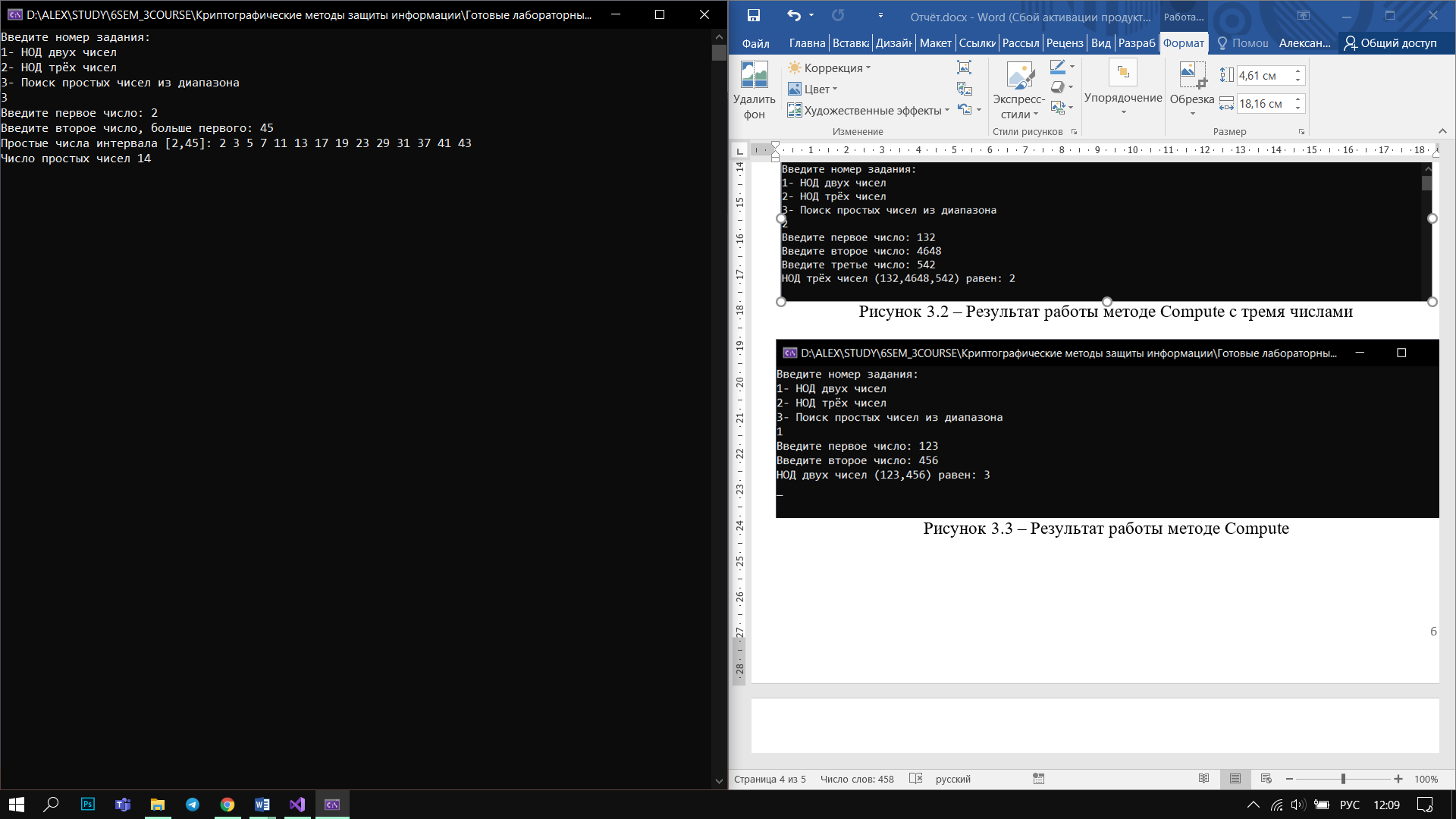


Рисунок 3.3 – Результат работы методе FindSimple

**Вывод**

В ходе изучения теоретических материалов лабораторной работы и выполнения её практической части были изучены основы теории чисел, используемые в криптографии. Изучены основные свойства простых и составных чисел, взаимно простых чисел, а также признаки делимости чисел. На практике полученные знания были закреплены через создание собственного приложения, реализующего функционал вычисления НОД двух и трёх чисел и получения списка простых чисел в заданном диапазоне.