Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерного проектирования

Кафедра ИПиЭ

Дисциплина: Криптографические технологии

Отчет

**по Лабораторной работе №4**

на тему «Исследование ассиметричных алгоритмов шифрования»

Студент гр. 910902 Шпак В.А.

Проверил Давыдович К.И.

Минск 2022

*Цель работы:* изучить ассиметричные алгоритмы шифрования, написать программу.

## *Ход работы:*

Листинг кода

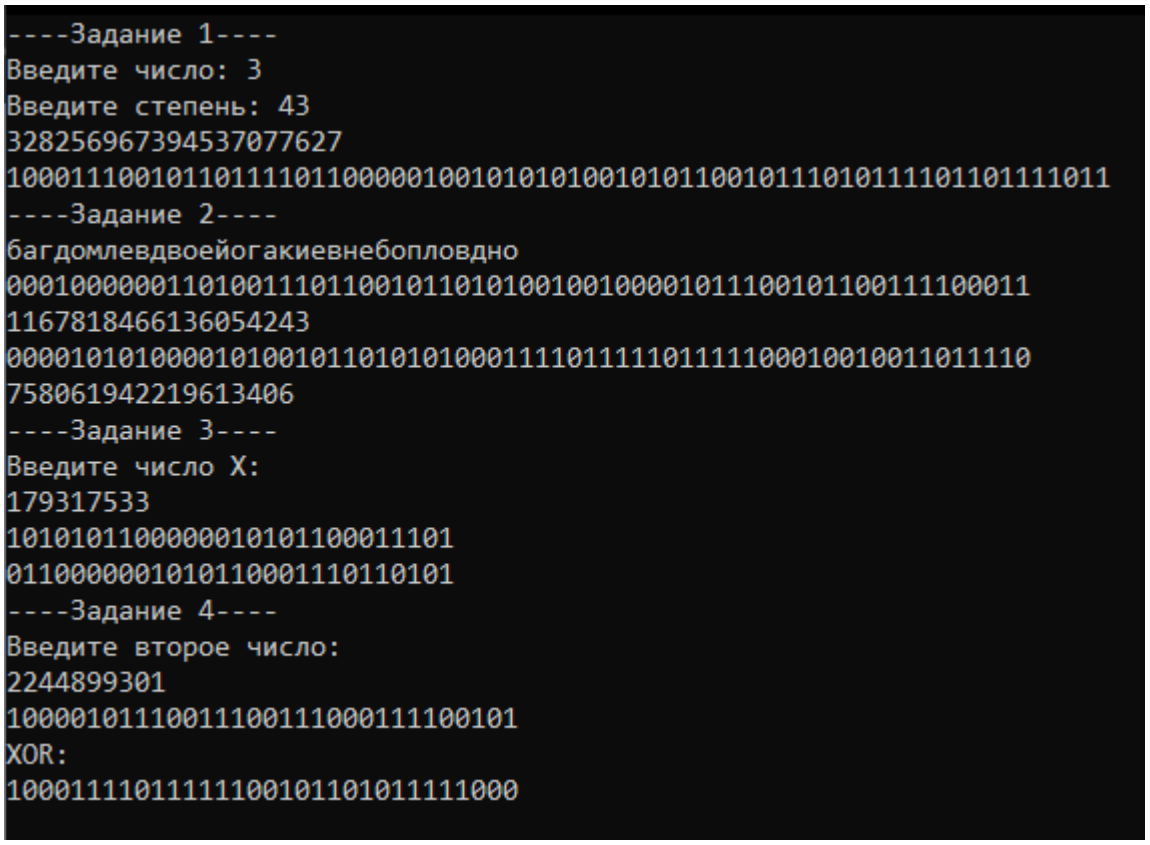
```
using System;
using System.Diagnostics;
using System.Numerics;
using System.Reflection;
using System.Text;
using static System.Console;

class Lama4 {
    public static void Main(string[] args)
    {
        Console.OutputEncoding = System.Text.Encoding.UTF8;
        Console.WriteLine("----Задание 1----");
        PowNum();
        Console.WriteLine("----Задание 2----");
        Alf();
        Console.WriteLine("----Задание 3----");
        LeftShift();
    }

    public static void PowNum()
    {
        Console.Write("Введите число: ");
        int num = int.Parse(Console.ReadLine());
        Console.Write("Введите степень: ");
        int powN = int.Parse(Console.ReadLine());
        var watch = Stopwatch.StartNew();
        BigInteger res = 1;
        for(int i = 0; i < powN; i++)
        {
            res *= num;
        }
        Console.WriteLine(res);
        var binNum = DecimalToBinary((BigInteger)res);
        Console.WriteLine(binNum);
    }
    static string DecimalToBinary(BigInteger decimalNumber)
    {
        var binaryNumber = string.Empty;
        while (decimalNumber > 0)
        {
            binaryNumber = (decimalNumber % 2) + binaryNumber;
            decimalNumber /= 2;
        }
        return binaryNumber;
    }

    static ulong BinaryToDecimal(string binaryNumber)
    {
        BigInteger bigNum = BigInteger.Parse(binaryNumber);
        ulong decimalNumber = 0;
        int i = 0, rem;
        while (bigNum != 0)
        {
            rem = (int)(bigNum % 10);
            bigNum /= 10;
            decimalNumber += (ulong)rem * (ulong)Math.Pow(2, i);
            ++i;
        }
```

```
        return decimalNumber;
    }
    public static void Alf()
    {
        string alf = "абвгдежзийклмноп";
        string text = "багдомлевдвоейогакиевнебопловдно";
        Console.WriteLine(text);
        for (int i = 0; i < 2; i++)
        {
            long number = 0;
            for (int j = 0; j < 16; j++)
            {
                number *= 16;
                number |= alf.IndexOf(text[i * 16 + j]);
            }
            string result = Convert.ToString(number, 2);
            int indx = 0;
            string binRes = "";
            for (int j = 0; j < 16; j++)
            {
                indx = alf.IndexOf(text[i * 16 + j]);
                string binIndx = Convert.ToString(indx, 2);
                string str = "0000"[binIndx.Length..]+ binIndx;
                binRes += str;
            }
            var num = BinaryToDecimal(binRes);
            Console.WriteLine(binRes);
            Console.WriteLine(num);
        }
    }
    public static void LeftShift()
    {
        Console.WriteLine("Введите число X: ");
        var num = uint.Parse(Console.ReadLine());
        var binNum = DecimalToBinary(num);
        Console.WriteLine(binNum);
        var binNumInt = Convert.ToInt32(binNum, 2);
        StringBuilder sb = new StringBuilder(binNum);
        for (int i = 0; i < 5; i++)
            sb.Remove(0, 1).Append(binNum[i]);
        var leftShift = sb.ToString();
        Console.WriteLine(leftShift);
        Console.WriteLine("----Задание 4----");
        Console.WriteLine("Введите второе число: ");
        var num2 = uint.Parse(Console.ReadLine());
        var binNum2 = DecimalToBinary(num2);
        Console.WriteLine(binNum2);
        var binNumInt2 = Convert.ToInt32(binNum2, 2);
        var res = binNumInt ^ binNumInt2;
        Console.WriteLine("XOR:");
        Console.WriteLine(DecimalToBinary((uint)res));
    }
}
```




**Вывод:** таким образом, в ходе лабораторной работы была изучены алгоритмы шифрования и написана программа.