УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе № 3

по предмету «Теория информации»

Вариант 2

Выполнил:

Калинкович А.Д

Гр. 351003

Проверил:

Болтак С. В.

Минск 2025

1. **Пример работы алгоритма быстрого возведения в степень с модульной арифметикой**:

**753 mod 23 = (732 mod 23 \* 716 mod 23 \* 74 mod 23 \* 7 mod 23) mod 23**

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | Z(степень) | х(результат) | Шаги выполнения |
| 7 | 1 | 7 mod 23 = 7 | 0 |
| 7 mod 23 | 2 | (7 \* 7) mod 23 = 26;  72 mod 23 = 26 | 1 |
| 72 mod 23 | 2 | (26 \* 26) mod 23 = 9;  74 mod 23 = 9; | 2 |
| 74 mod 23 | 2 | (9 \* 9) mod 23 = 12;  78 mod 23 = 12; | 3 |
| 78 mod 23 | 2 | (12 \* 12) mod 23 = 6;  716 mod 23 = 6; | 4 |
| 716 mod 23 | 2 | (6 \* 6) mod 23 = 13;  732 mod 23 = 13; | 5 |

7 mod 23 = 7;

74 mod 23 = 9;

716 mod 23 = 6;

732 mod 23 = 13;

(13 \* 6 \* 9 \* 7) mod 23 = 753 mod 23**;**

((13 \* 6) mod 23 \* (9 \* 7) mod 23) mod 23 = (78 mod 23 \* 63 mod 23) mod 23 = (9 \* 17) mod 23 = 15;

1. **Пример поиска всех первообразных корней по заданному модулю**

1) Задано простое p = 11

2) Ищем простые делители p - 1 = phi = 10 = 2 \* 5

3) Итерируем от 1 до p – 1 = 10, проверяя все значения в соответствии с условием

for g = 1 to p – 1 do:

3.1) Итерируем по простым делителями и проверяем условие,

foreach factor in (2,5):

g (phi / factor) mod p != 1

Если результат возведения в степень будет равен 1 по модулю p – значит порядок числа **g** меньше **p – 1** и он не является первообразным корнем.

Пример:

3(10 / 2) mod 11 = 1 (3 не является первообразным корнем)

2(10 / 2) mod 11 = 10

2(10 / 5) mod 11 = 4 (т.к оба делителя по mod p не дали 1, то это означает, что 2 – первообразный корень)

Результатом алгоритма является полный список всех первообразных корней в диапазоне [1,p – 1];

1. **Пример работы расширенного алгоритма Евклида с взаимно простыми числами**

**x1\*a + y1\*b = нод(a,b), a = 43, b = 13**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 43 | 13 | 1 | 0 | 0 | 1 |
| 1 | 3 | 13 | 4 | 0 | 1 | 1 | -3 |
| 2 | 3 | 4 | 1 | 1 | -3 | -3 | 10 |
| 3 | 4 | 1 | 0 | -3 | 13 | 10 | -43 |

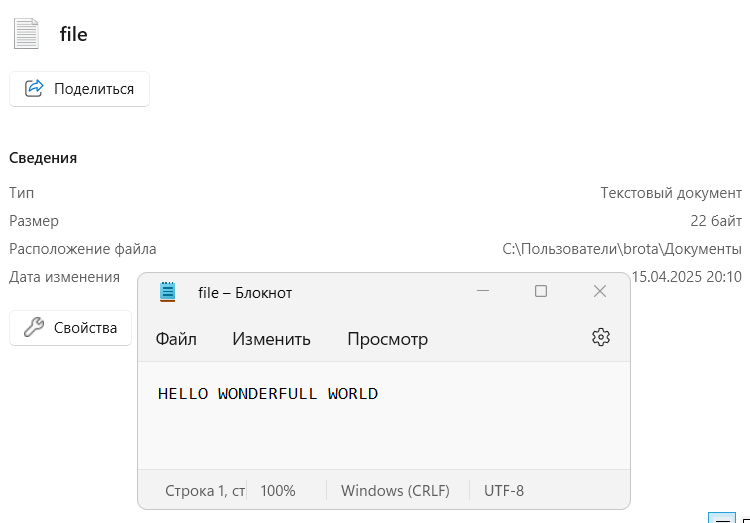
**x1 = -3**

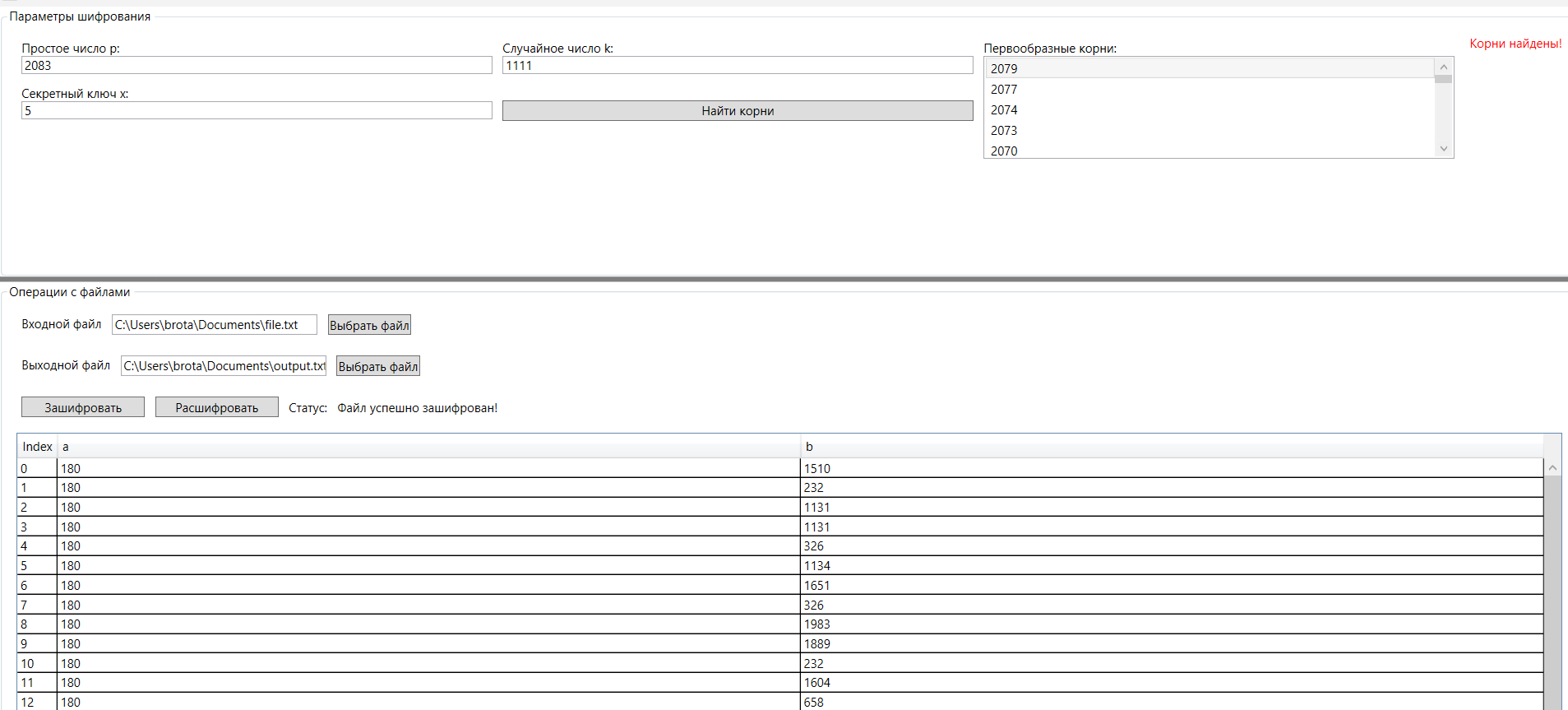
**y1 = 10**

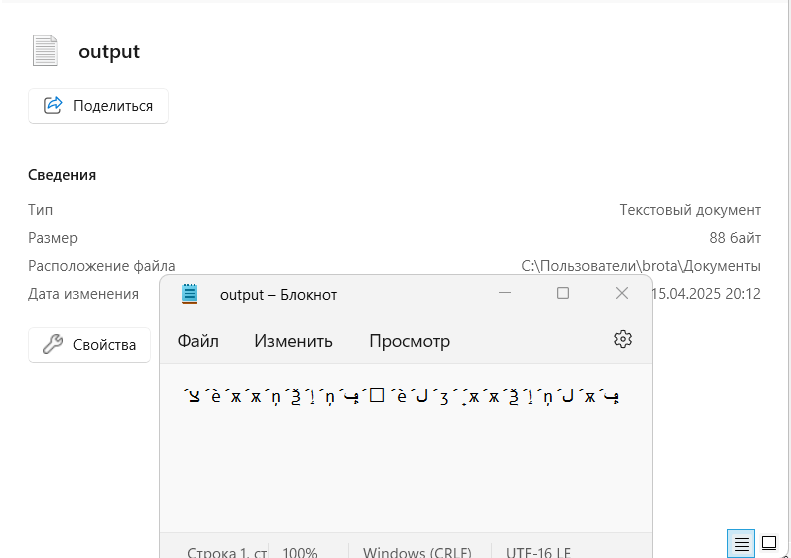
**-3 \* 43 + 13 \* 10 = 1**

Пример работы программы:

1. Текстовый документ:







Пример расшифровки:

