УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе № 3

по предмету «Теория информации»

Вариант 3

Выполнила:

Лисунова М.Д.

гр. 351003

Проверила:

Болтак С.В.

Минск 2025

**1. Пример работы алгоритма быстрого возведения в степень**

Пусть a1 = 4, Z = 23, n = 9.

423 mod 9 = 7

|  |  |  |  |
| --- | --- | --- | --- |
| Шаги выполнения | а1 (основание степени) | Z (степень) | х (результат) |
| 0 | 4 | 23 | 1 |
| 1 | 4 | 23 - 1 = 22 | (1 \* 4) mod 9 = 4 |
| 2 | (4 \* 4) mod 9 = 7 | 22 / 2 = 11 | 4 |
| 3 | 7 | 11 - 1 = 10 | (4 \* 7) mod 9 = 1 |
| 4 | (7 \* 7) mod 9 = 4 | 10 / 2 = 5 | 1 |
| 5 | 4 | 5 - 1 = 4 | (1 \* 4) mod 9 = 4 |
| 6 | (4 \* 4) mod 9 = 7 | 4 / 2 = 2 | 4 |
| 7 | (7 \* 7) mod 9 = 4 | 2 / 2 = 1 | 4 |
| 8 | 4 | 1 - 1 = 0 | (4 \* 4) mod 9 = 7 |

**2. Пример поиска случайного первообразного корня**

Пусть p = 29

Простые делители p – 1 = 28 = 2 \* 2 \* 7

|  |  |  |  |
| --- | --- | --- | --- |
| g | g28/2 mod 29 | g28/7 mod 29 | Первообразный |
| 2 | 28 | 16 | да |
| 3 | 28 | 23 | да |
| 4 | 1 | 24 | нет |
| 5 | 1 | 16 | нет |
| 6 | 1 | 20 | нет |
| 7 | 1 | 23 | нет |
| 8 | 28 | 7 | да |
| 9 | 1 | 7 | нет |
| 10 | 28 | 24 | да |
| 11 | 28 | 25 | да |
| 12 | 28 | 1 | нет |
| 13 | 1 | 25 | нет |
| 14 | 28 | 20 | да |
| 15 | 28 | 20 | да |
| 16 | 1 | 25 | нет |
| 17 | 28 | 1 | нет |
| 18 | 28 | 25 | да |
| 19 | 28 | 24 | да |
| 20 | 1 | 7 | нет |
| 21 | 28 | 7 | да |
| 22 | 1 | 23 | нет |
| 23 | 1 | 20 | нет |
| 24 | 1 | 16 | нет |
| 25 | 1 | 24 | нет |
| 26 | 28 | 23 | да |
| 27 | 28 | 16 | да |
| 28 | 1 | 1 | нет |

**3. Пример работы расширенного алгоритма Евклида**

x1\* a + y1\* b = НОД(a, b), a = 571, b = 727, (a, b) = 1

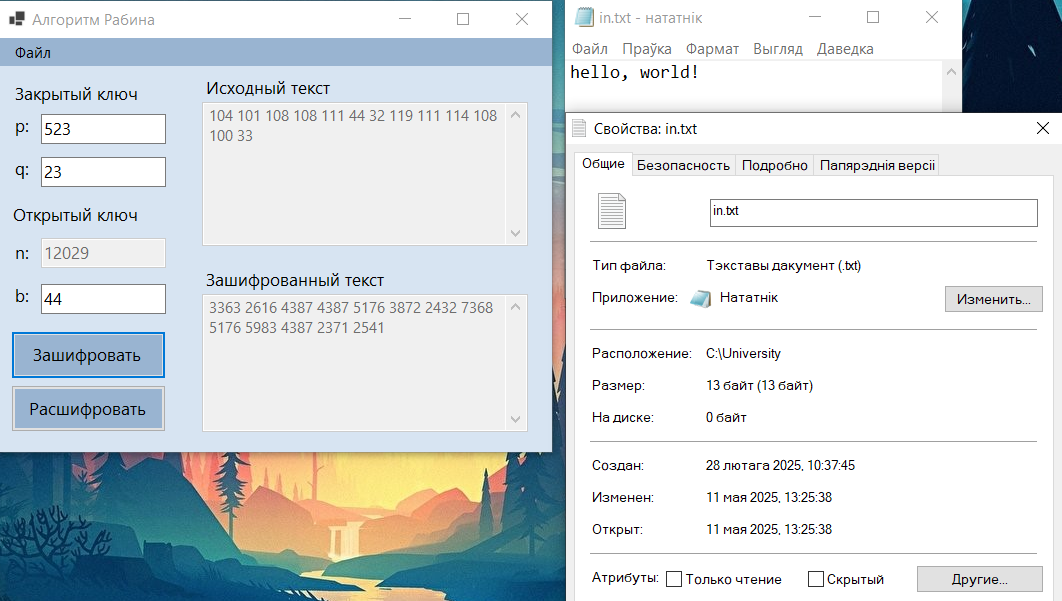
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0  d0** | **a1 d1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 571 | 727 | 1 | 0 | 0 | 1 |
| 1 | 0 | 727 | 571 | 0 | 1 | 1 | 0 |
| 2 | 1 | 571 | 156 | 1 | -1 | 0 | 1 |
| 3 | 3 | 156 | 103 | -1 | 4 | 1 | -3 |
| 4 | 1 | 103 | 53 | 4 | -5 | -3 | 4 |
| 5 | 1 | 53 | 50 | -5 | 9 | 4 | -7 |
| 6 | 1 | 50 | 3 | 9 | -14 | -7 | 11 |
| 7 | 16 | 3 | 2 | -14 | 233 | 11 | -183 |
| 8 | 1 | 2 | 1 | 233 | -247 | -183 | 194 |
| 9 | 2 | 1 | 0 | -247 | 480 | 194 | -377 |

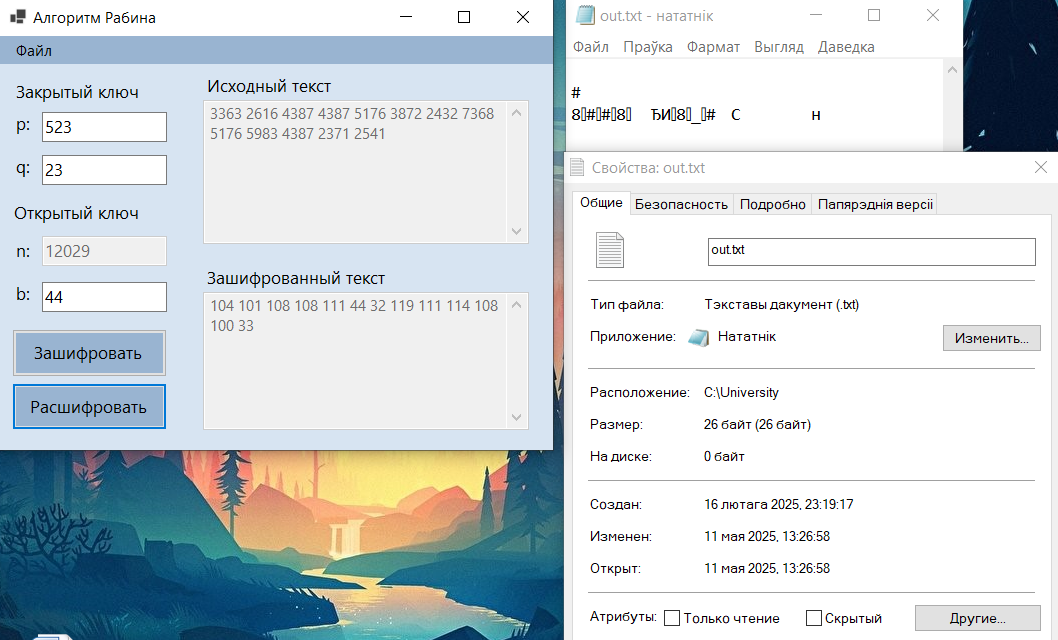
x1 = -247, y1 = 194

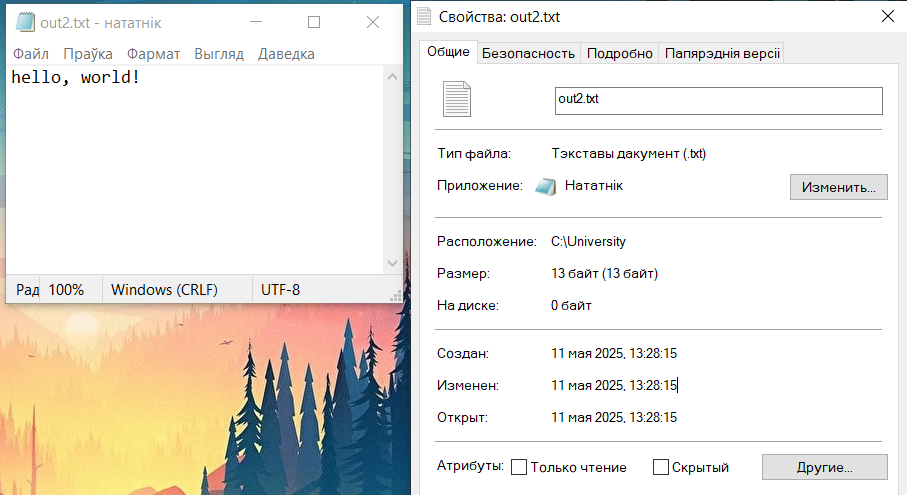
-247 \* 571 + 194 \* 727 = 1

Примеры шифрования файлов:

Текст







Картинка

