УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе №3

по предмету «Теория информации»

Выполнил:

Бетеня К.С.

гр. 351004

Проверил:

Болтак С.В.

Минск 2025

1. **Быстрое возведение в степень по модулю:**

a = 5, z = 9 (1001), n = 21

59 mod 21 = 5\*58 mod 21 = 5 \* (54)2 mod 21 = 5 \* ( (52)2) 2 mod 20 = 20

|  |  |  |  |
| --- | --- | --- | --- |
| **а(основание степени)** | **z(степень)** | **х(результат)** | **Шаги выполнения** |
| 5 | 9 | 1 | 0 |
| 5 | 8 | (1 \* 5) mod 21 = 5 | 1 |
| (5 \* 5) mod 21 = 4 | 4 | 5 | 2 |
| (4 \* 4) mod 21 = 16 | 2 | 5 | 3 |
| (16 \* 16) mod 21 = 4 | 1 | 5 | 4 |
| 4 | 0 | (4 \* 5) mod 21 = 20 | 5 |

59 mod 21 = 20

1. **Поиск всех первообразных корней числа по модулю**

p = 11, =p – 1 = 10 (т.к. p простое)

|  |  |  |
| --- | --- | --- |
| **g** | **g^10 mod 11** | **Первообразный** |
| 2 | 1 | + |
| 3 | 1 | - |
| 4 | 1 | - |
| 5 | 1 | - |
| 6 | 1 | + |
| 7 | 1 | + |
| 8 | 1 | + |
| 9 | 1 | - |
| 10 | 1 | + |

2, 3, 4, 5, 6, 7, 8, 9, 10 – первообразные корни

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

**x1\*a + y1\*b = нод(a,b), a =67, b =17, нод(a,b) = 1**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 67 | 17 | 1 | 0 | 0 | 1 |
| 1 | 3 | 17 | 16 | 0 | 1 | 1 | -3 |
| 2 | 1 | 16 | 1 | 1 | -1 | -3 | 4 |
| 3 | 16 | 1 | 0 | -1 | 17 | 4 | -67 |

**x1 = -1 y1 = 4**

**-1 \* 67 + 4 \* 17 = 1**

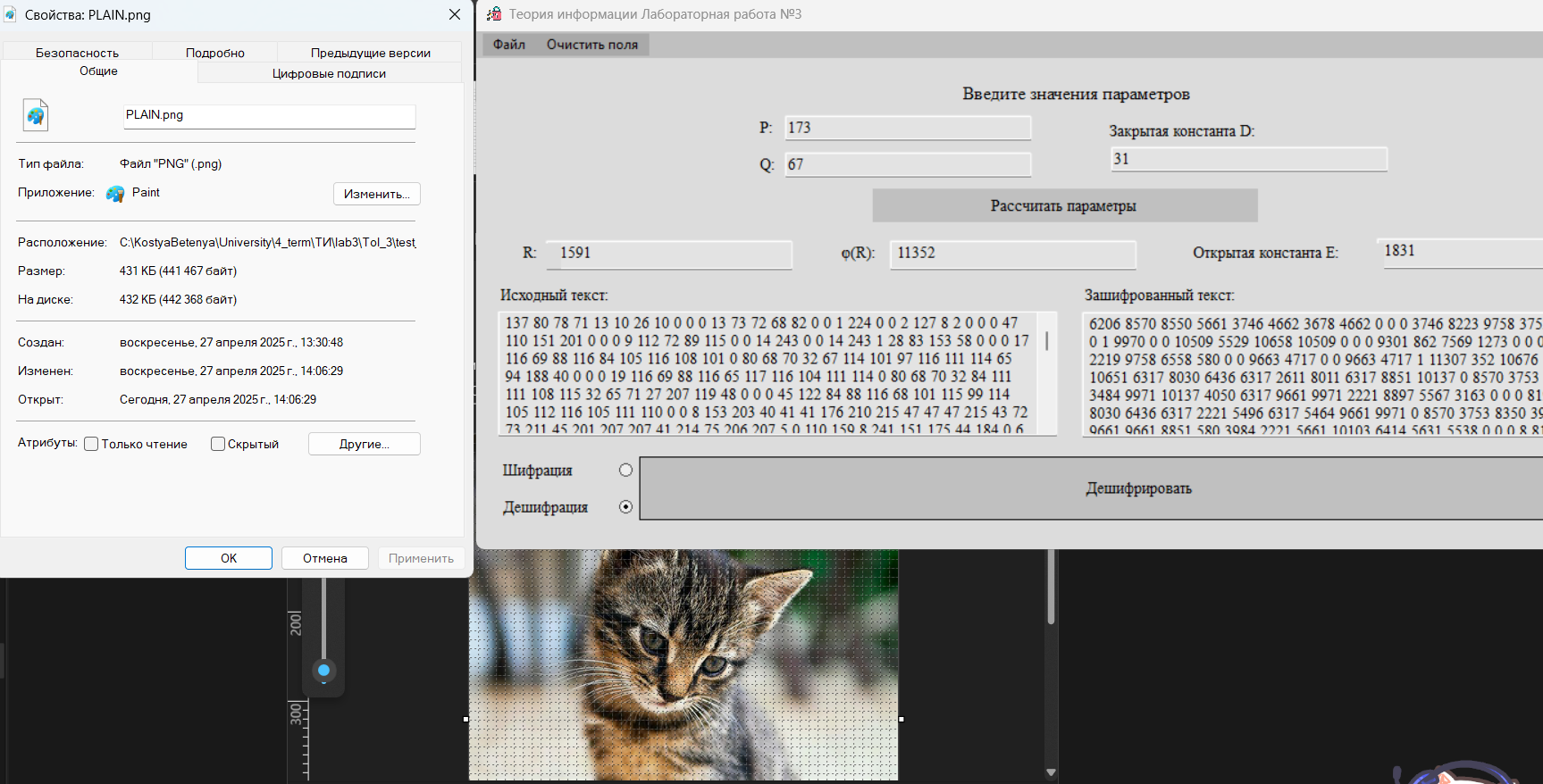
**РАБОТА ПРОГРАММЫ:**

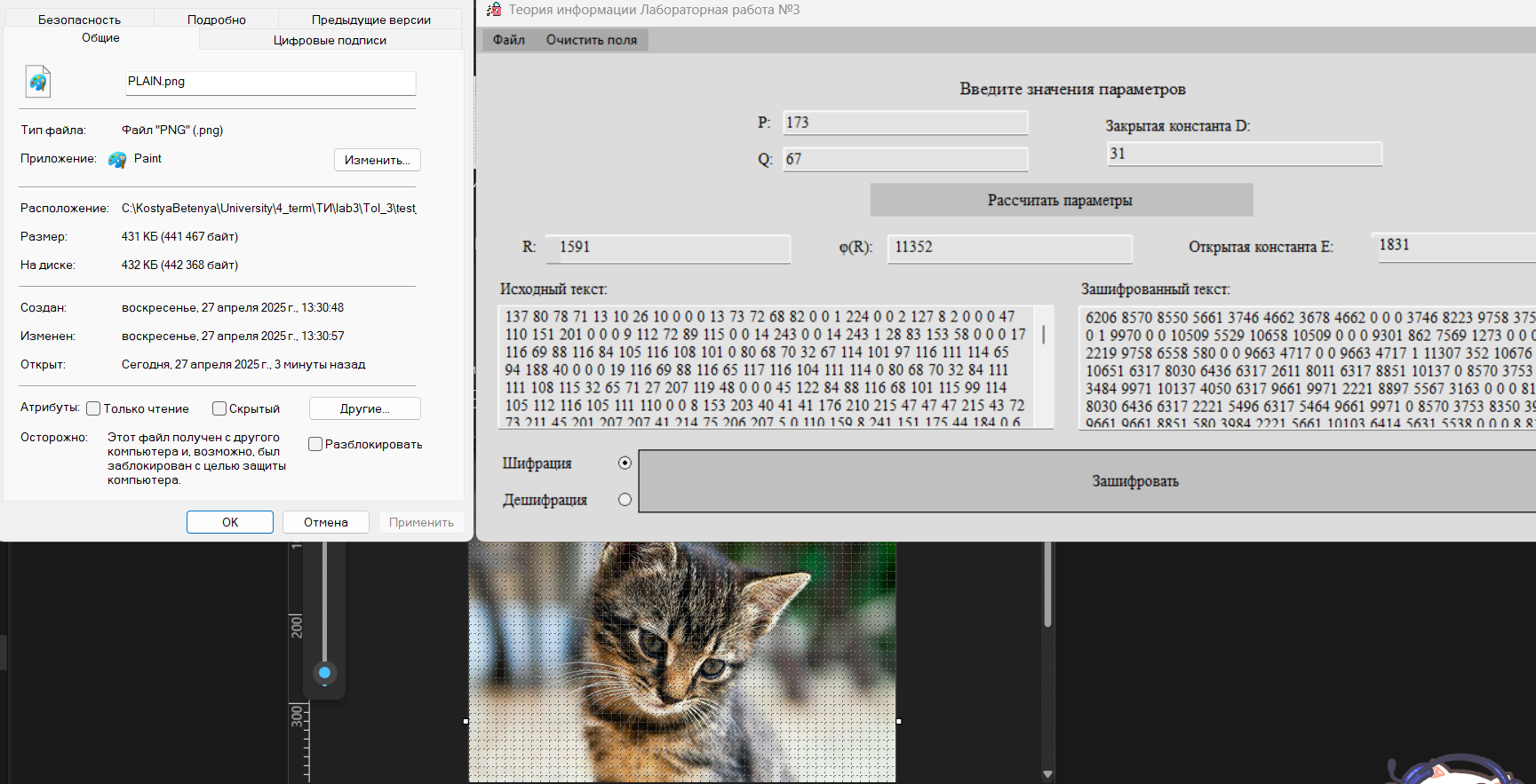
**Тест 1 (\*.png):**

P = 173;

Q = 67;

D = 31;



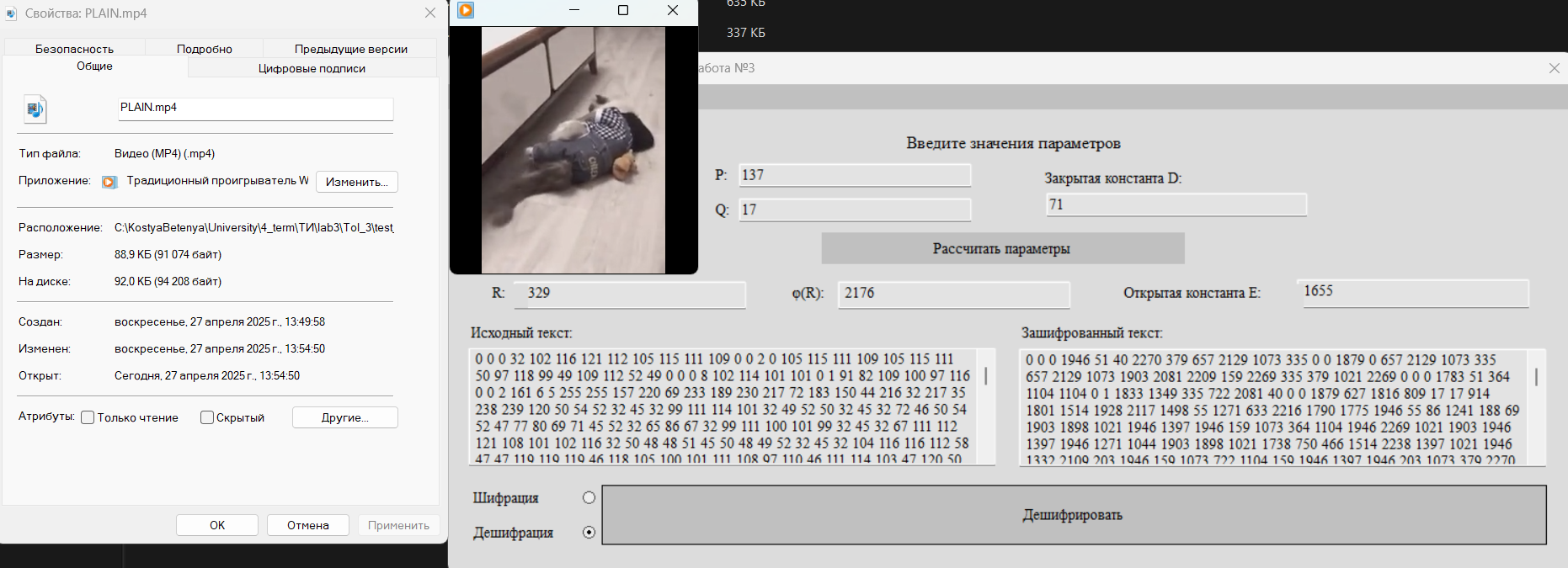
****

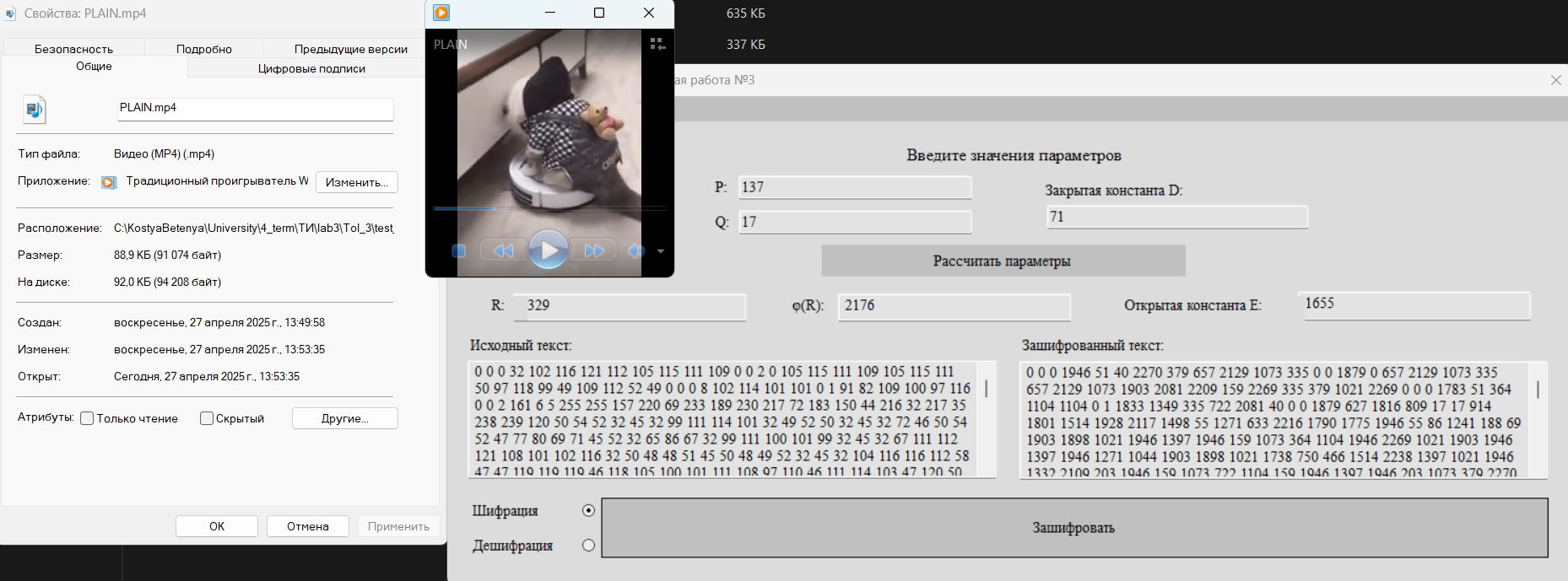
**Тест 2 (\*.mp4):**

P = 137;

Q = 17;

D = 71;



****

**Тест 3 (\*.txt):**

P = 17;

Q = 137;

D = 3;

