Отчет к лабораторной работе №3

Гатальский Дмитрий Витальевич 251001

Вариант 3

Реализовать шифратор и дешифратор *алгоритма* ***Рабина***

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

**y = g^x mod p**

**y = 210 mod 199 = 45 mod 199 = 4\*44 mod 199 = 4 \* 162 mod 131 = 4 \* 2561 mod 199 = 4 \* 57 mod 199 = 228 mod 199 = 29**

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | Z(степень) | х(результат) | Шаги выполнения |
| 2 | 10 | 2 mod 199 = 2 | 0 |
| 4 | 5 | 1 | 1 |
| 4 | 4 | 4 | 2 |
| 16 | 2 | 4 | 3 |
| 256 | 1 | 4 | 4 |
| 256 | 0 | 4\*256 mod 199 = 4 \* 57 mod 199 | 5 |
| 57 | 0 | 1. \* 57 mod 199 = 29 | 6 |

**2 Пример работы расширенного алгоритма Евклида**

**x1\*a + y1\*b = нод(a,b), a = 23, b = 17, (a,b) = 1**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **a0** | **a1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 23 | 17 | 1 | 0 | 0 | 1 |
| 1 | 0 | 17 | 6 | 0 | 1 | 1 | -1 |
| 2 | 2 | 6 | 5 | 1 | -2 | -1 | 3 |
| 3 | 1 | 5 | 1 | -2 | 3 | 3 | -4 |
| 4 | 5 | 1 | 0 | 3 | -17 | -4 | 23 |

**x1 = 3 y1 = -4**

**3 \* 23 + (-4) \* 17 = 1**

Проверка работоспособности программы, на текстовых данных

P = 3 Q = 523 b = 21

Вводный текст:

Текст для тестирования на русском

Интересный текст на русском языке

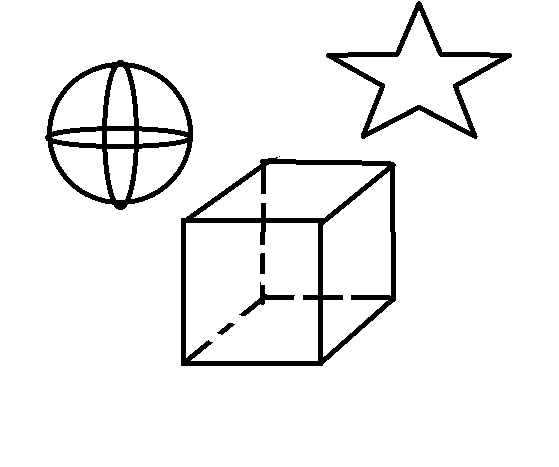
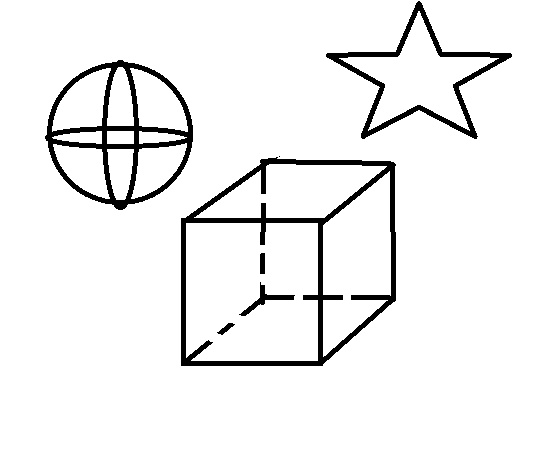
Зашифрованный текст в числах:

562,1192,562,465,1000,802,562,475,1000,244,562,475,1000,522,562,465,1000,274,562,454,127,1000,802,562,475,562,846,1000,522,1000,802,127,562,465,562,154,127,1000,244,1000,1084,1000,522,1000,522,562,846,562,865,562,67,127,1000,1486,562,1245,1000,274,562,846,562,475

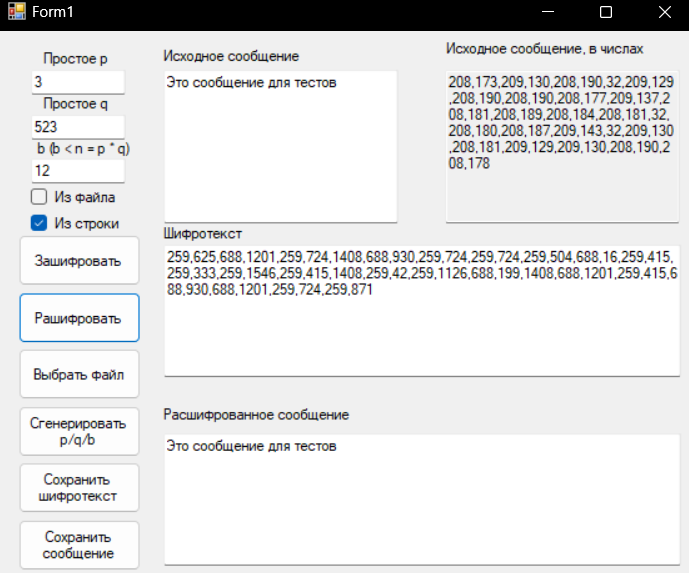
После расшифровки получился исходный текст

Тест 2: проверка на изображении

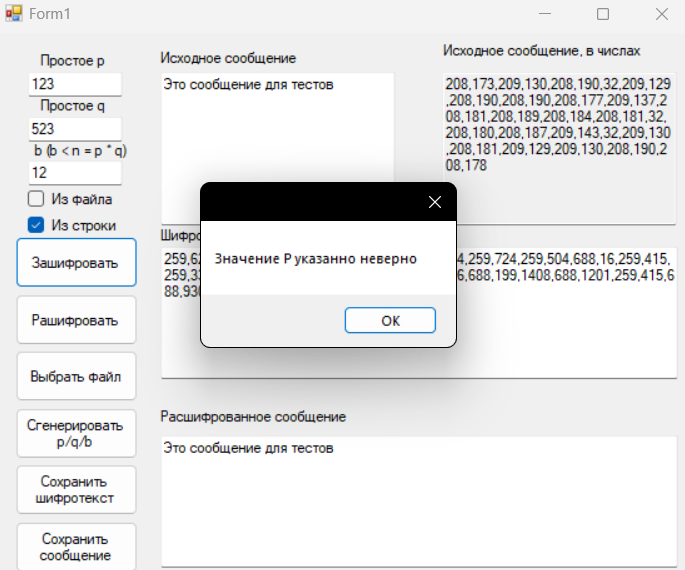
Входное изображение: Выходное изображение после расшифровки:



Видно что после расшифровки изображение осталось прежним, следовательно на больших объемах данных программа работает корректно.



Попытка ввести p, которое будет являться не простым числом:



Попытка ввести не валидные данные:

