Отчет к лабораторной работе №3

Лашкин Владислав Николаевич

Вариант 2

Алгоритм Эль-Гамаля

**Пример поиска всех первообразных корней**

Задано простое p = 271

Ищем простые делители p-1 = 270 = 2 \* 3 \* 3 \* 3 \* 5

Проверяем является ли каждое число из диапазона [2, 270] первообразным корнем по модулю 271:

2270/2 mod 271 = 1; 2270/3 mod 271 = 242; 2270/5 mod 271 = 244

Число 2 не является первообразным по модулю 271.

6270/2 mod 271 = 78; 6270/3 mod 271 = 227; 6270/5 mod 271 = 126

Число 6 является первообразным по модулю 271.

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

**y = gx mod p**

y = 611 mod 271 = 6 \* 610 mod 271 = 6 \* 365 mod 271 = 6 \* 36 \* 364 mod 271 = 6 \* 36 \* 12962 mod 271 = 6 \* 36 \* 1679616 mod 271 = 114

|  |  |  |  |
| --- | --- | --- | --- |
| a | z | x | Шаги выполнения |
| 6 | 11 | 1 | 0 |
| 6 | 10 | 1\*6 mod 271 = 6 | 1 |
| 36 | 5 | 6 | 2 |
| 36 | 4 | 6\*6 mod 271 = 36 | 3 |
| 1296 | 2 | 36 | 4 |
| 1679616 | 0 | 36\*1679616  mod 271 = 114 | 5 |

**Пример работы расширенного алгоритма Евклида**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **итерация** | **q** | **d0** | **d1** | **x0** | **x1** | **y0** | **y1** |
| 0 | - | 68 | 13 | 1 | 0 | 0 | 1 |
| 1 | 5 | 13 | 3 | 0 | 1 | 1 | -5 |
| 2 | 4 | 3 | 1 | 1 | -4 | -5 | 21 |

X1 = -4, y1 = 21

-4 \* 68 + 21 \* 13 =1

**Проверка работоспособности программы**

**Исходный текст:**

Этот сообщение записано в текстовый файл.

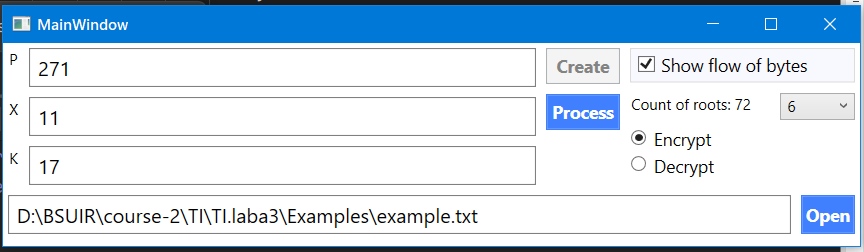
This message was written in the text file.

100 р. 13% !"№;%:?\*()\_+

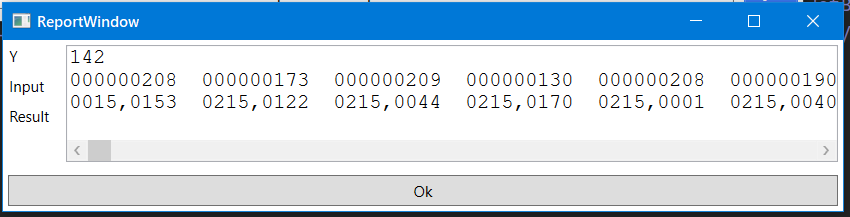
qwertyuiop

[];',./ 123456789

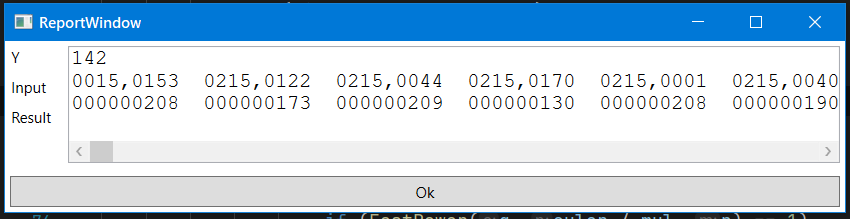
**Окно программы:**



**Результат шифрования:**

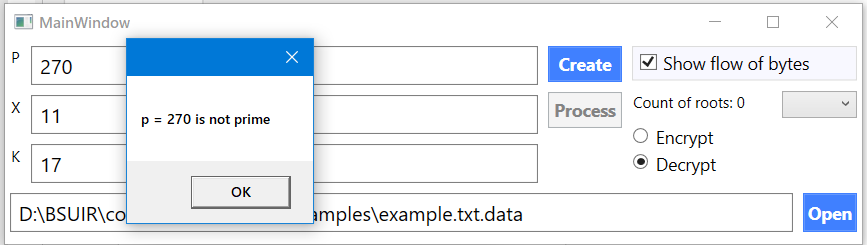


**Результат дешифрования:**



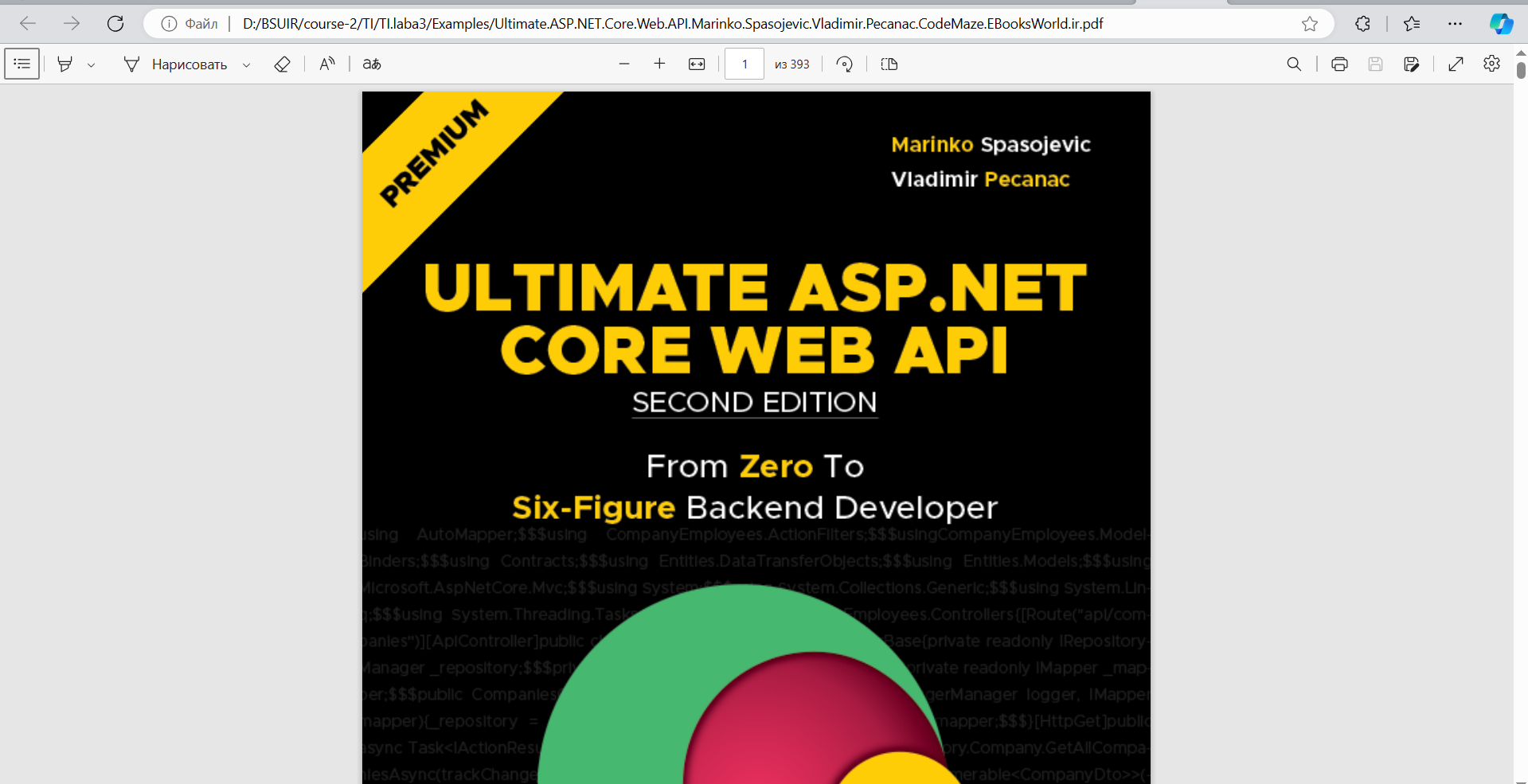
Получился исходный текст, который был до шифрования

Сообщение при вводе недопустимого p

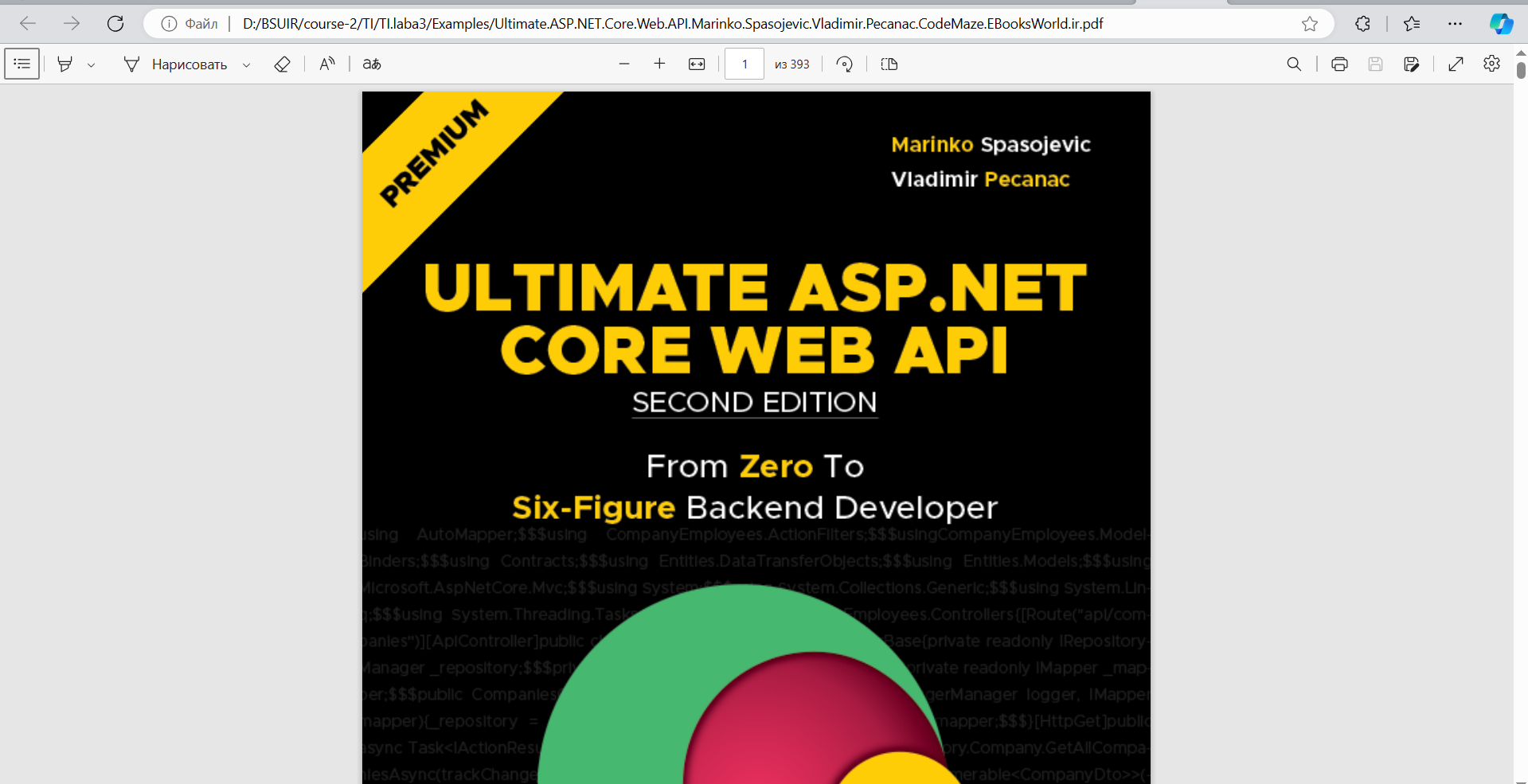


**Проверка работоспособности программы на больших данный на примере книги в формате PDF**

Книга до шифрования:



Книга после дешифрования:



Примерное время работы программы 4 секунды. Следовательно, шифратор работает за приемлемое время