Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра программного обеспечения информационных технологий

Дисциплина: ТИ (Теория информации)

ОТЧЕТ

по лабораторной работе № 3

Тема работы: Криптосистемы с открытым ключом

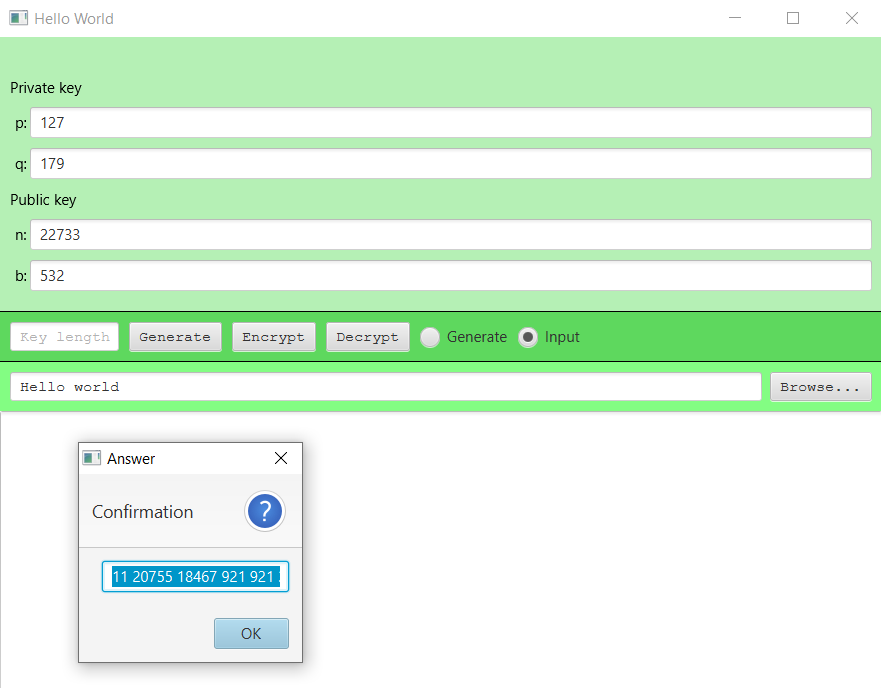
Выполнил: гр. 951007 Воривода М.А.

Проверила: Болтак С.В.

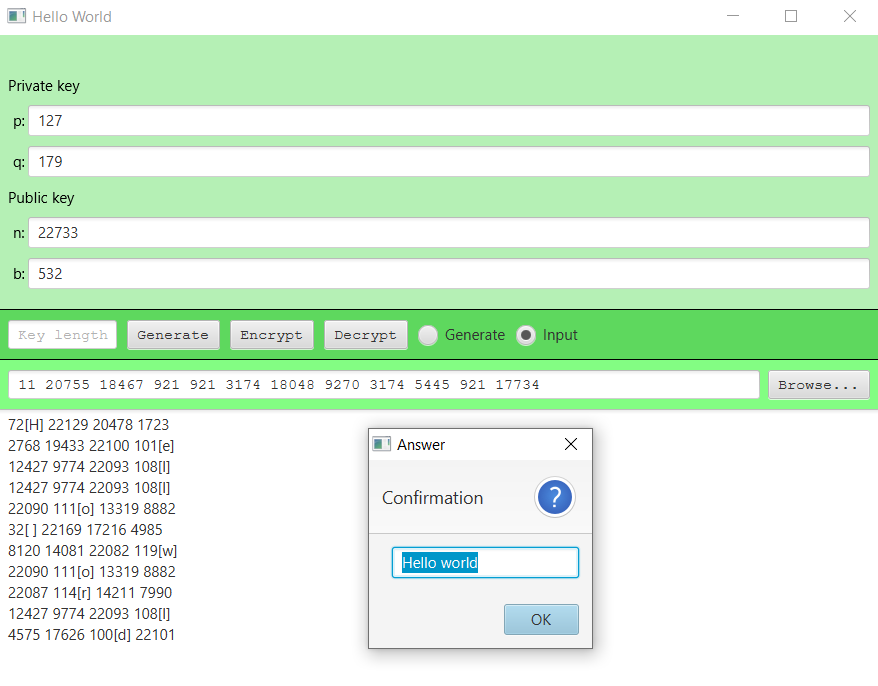
Минск 2021

**1 SMOKE TEST**

Шифрование маленького текстового сообщения маленькими ключами:



Расшифровка этого же сообщения:

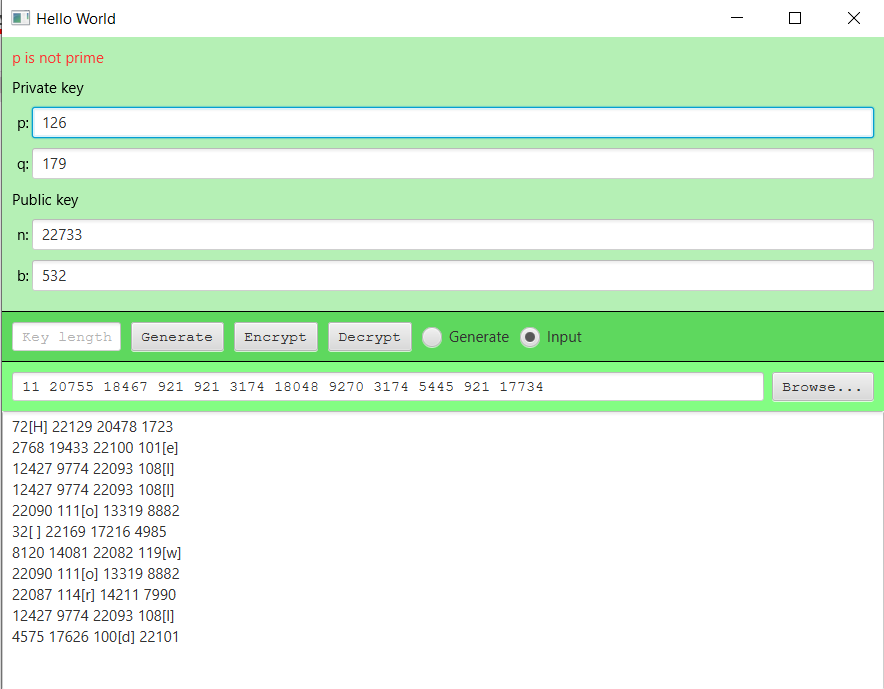


Генерация ключей:

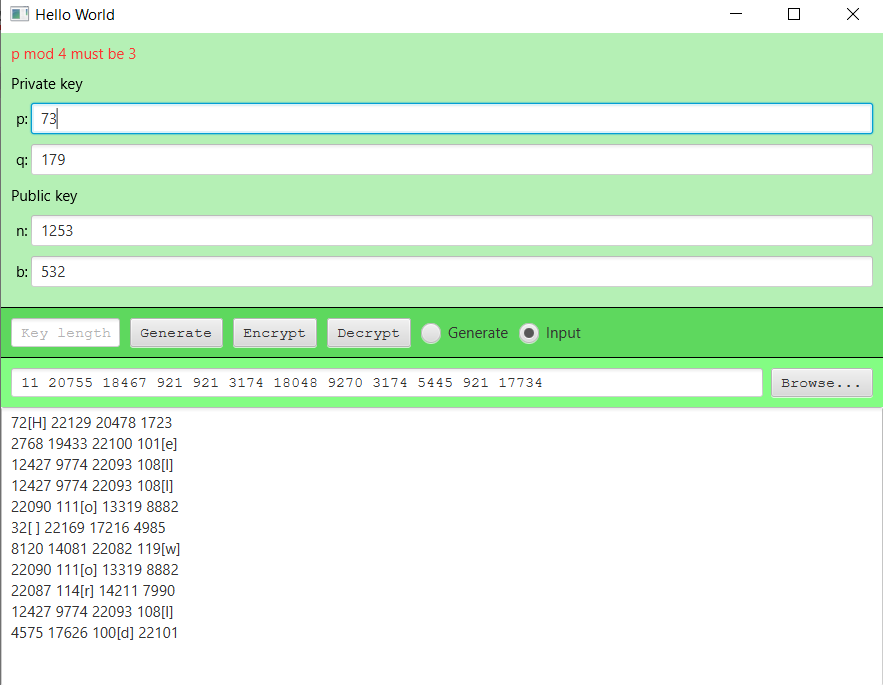


Проверка данных в программе:

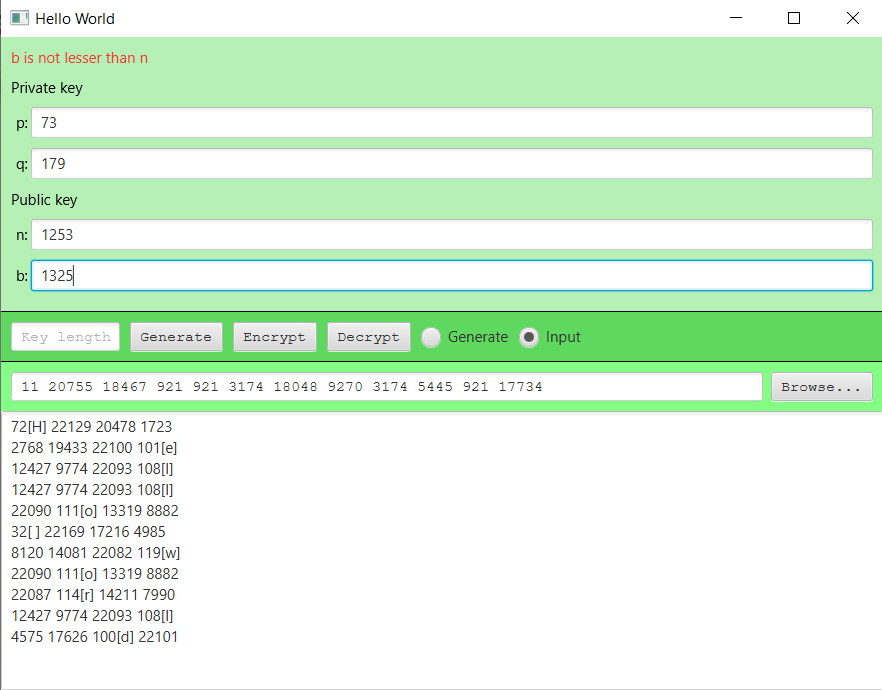
* Ввод не простого числа:



* Остаток от деления не 3:

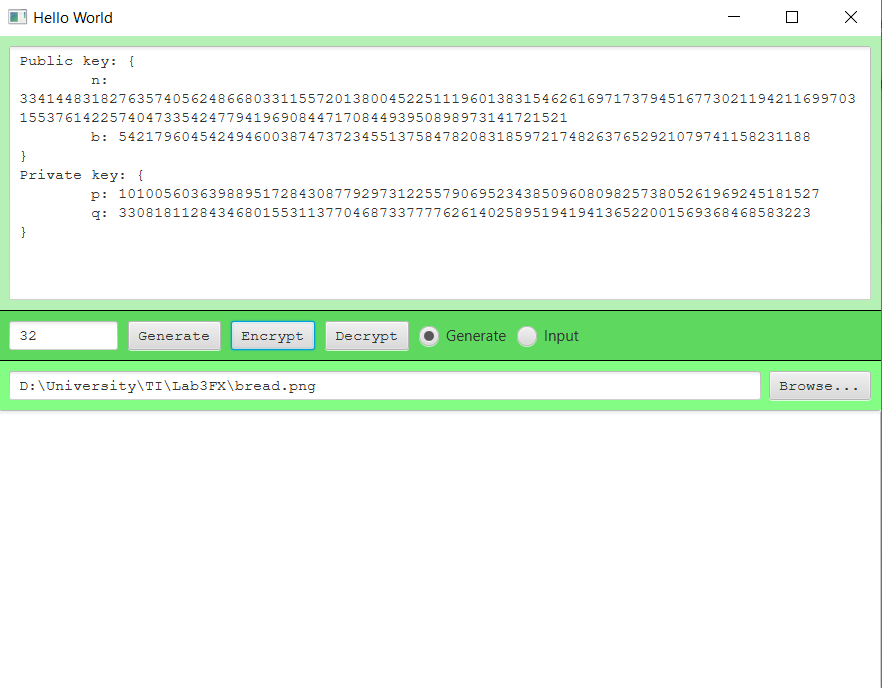


* b больше n:

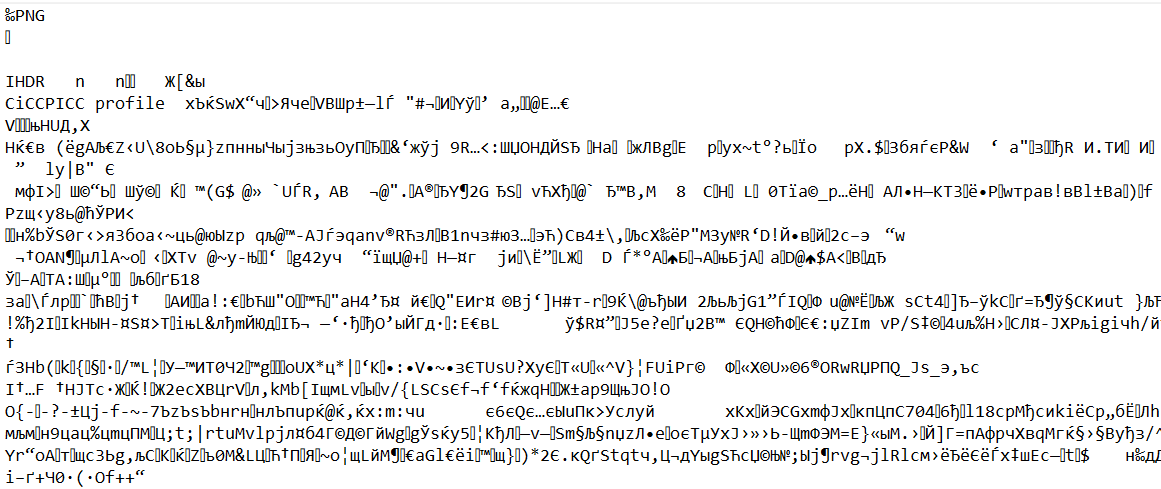


**2 ДЛИННАЯ АРИФМЕТИКА**

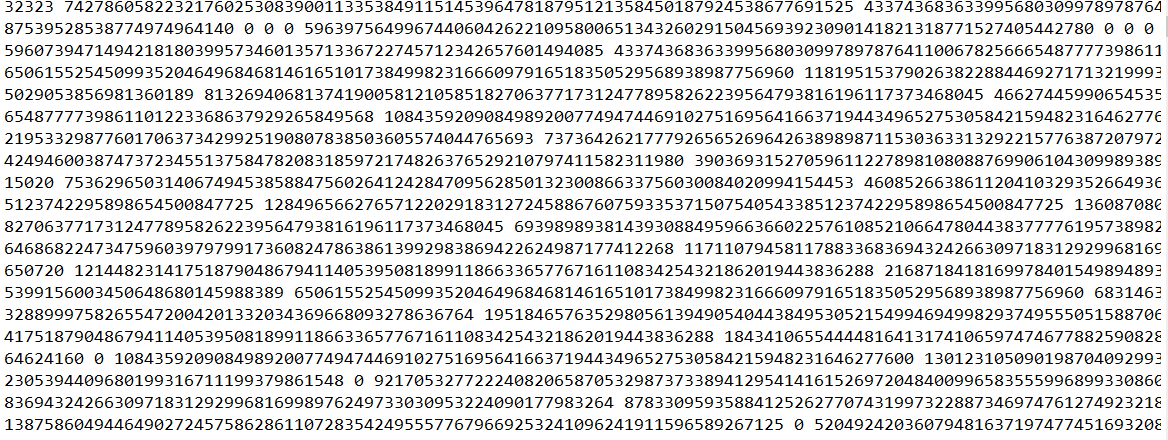
Генерация ключей длинной в 256 бит и зашифровка изображения и расшифровка:

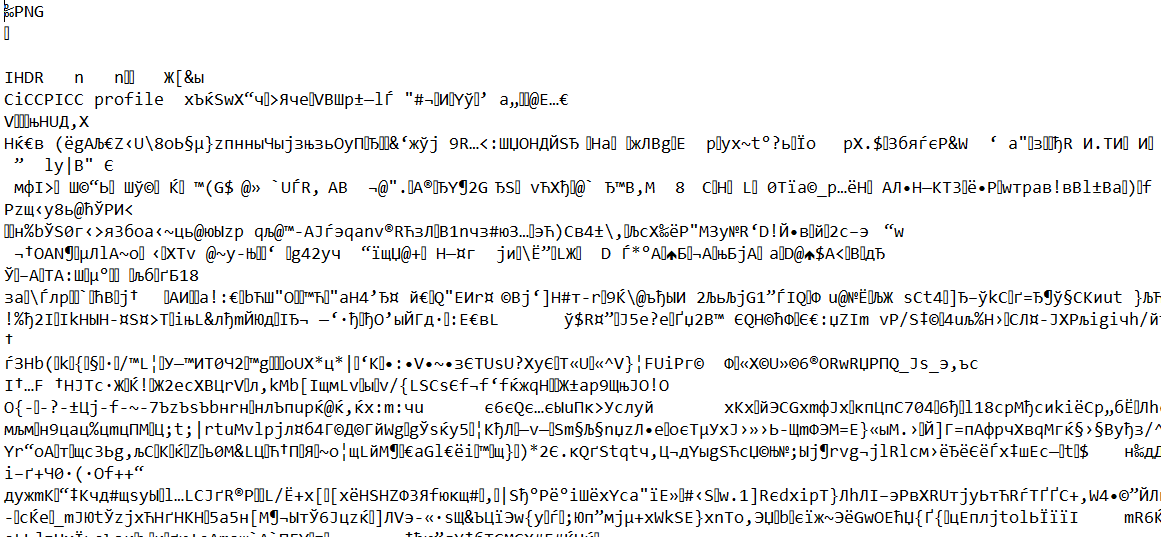


Изначальный файл:



Зашифрованный:

Расшифрованный:





**3 РАСЧЁТЫ**

**Быстрое возведение в степень**

Степень 0:

Степень 1:

Степень 2:

Степень 3:

Степень 4:

Степень 5:

**Первообразный корень по модулю**

Первообразный корень g по модулю m – это такое целое число, что

Нахождение первообразного корня по модулю 13.

**Расширенный алгоритм Евклида**

Расширенный алгоритм Евклида позволяет найти наибольший общий делитель и коэффициенты из леммы Безу. Лемма Безу гласит о том, что для любых целых чисел a и b есть такие целые числа x и y, для которых верно равенство 𝒂 ∗ 𝒙 + 𝒃 ∗ 𝒚 = (𝒂, 𝒃).

Пусть a = 36, b = 25. НОД(a, b) = 1

xn = xn – 2 – q \* xn - 1

yn = yn – 2 – q \* yn - 1

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **q** | **a** | **b** | **r** | **xn** | **yn** |
| - | 36 | 25 | - | 1 | 0 |
| - | 36 | 25 | - | 0 | 1 |
| 1 | 36 | 25 | 11 | 1 | -1 |
| 2 | 25 | 11 | 3 | -2 | 3 |
| 3 | 11 | 3 | 2 | 7 | -10 |
| 1 | 3 | 2 | **1** | **-9** | **13** |
| 2 | 2 | 1 | **0** | **-** | **-** |

-9 \* 36 + 13 \* 25 = -324 + 325 = 1