Отчет к лабораторной работе №3

Бруцкая Анастасия Сергеевна 251001

Вариант 2

Реализовать шифратор и дешифратор *алгоритма* ***Эль-Гамаля***

1. **Пример поиска всех первообразных корней**

Задано простое p = 131

Ищем простые делители p-1 = 130 = 2\*5\*13

Проверяем является ли каждое число из диапазона [2, 130] первообразным корнем по модулю 131:

*2130/2 mod 131 = 130; 2130/5 mod 131 = 53; 2130/13 mod 131 = 107 Число 2 является первообразным по модулю 131.*

*3130/2 mod 131 = 1; 3130/5 mod 131 = 58; 3130/13 mod 131 = 99 Число 3 не является первообразным по модулю 131.*

*и т. д.*

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

**y = g^x mod p**

**y = 210 mod 131 = 45 mod 131 = 4\*44 mod 131 = 4 \* 162 mod 131 = 4 \* 2561 mod 131 = 1024 mod 131 = 107**

|  |  |  |  |
| --- | --- | --- | --- |
| а1(основание степени) | Z(степень) | х(результат) | Шаги выполнения |
| 2 | 10 | 1 | 0 |
| 4 | 5 | 1 | 1 |
| 4 | 4 | 1\*4 mod 131 = 4 | 2 |
| 16 | 2 | 4 | 3 |
| 256 | 1 | 4 | 4 |
| 256 | 0 | 4\*256 mod 131 = 107 | 5 |

Проверка работоспособности программы, на текстовых данных

Вводный текст:

Текст для тестирования на русском

Tekst for testing in english

Зашифрованный текст:

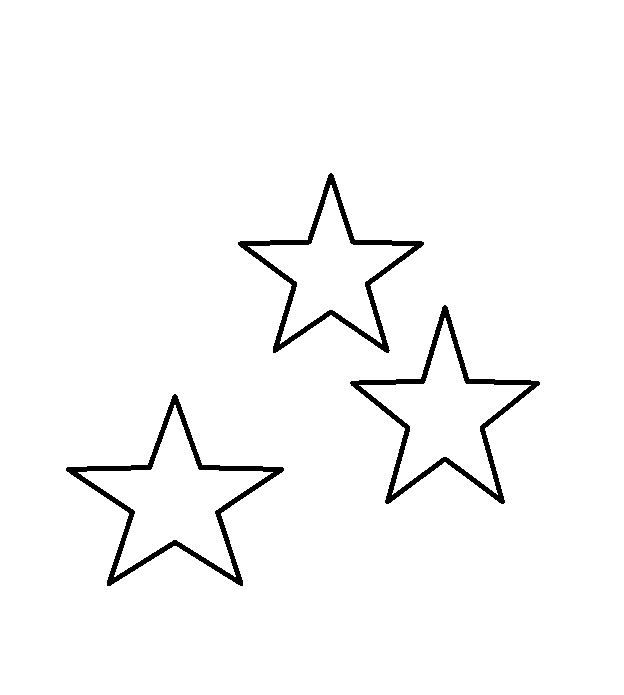
�)#��#|��/V�/�##

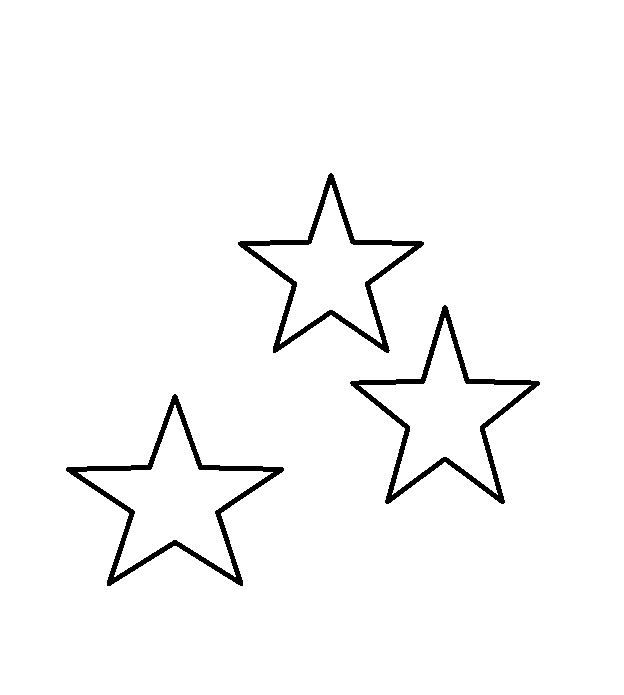
��Q�� ϊ�#�B�^�׮���/�$�b��#h#/�U�b##�o?b$#n��#$\T9�bV��b�#:T(

� �x�$/�#�j��#T(#��#U#�#/#+�C\*�$ 4��

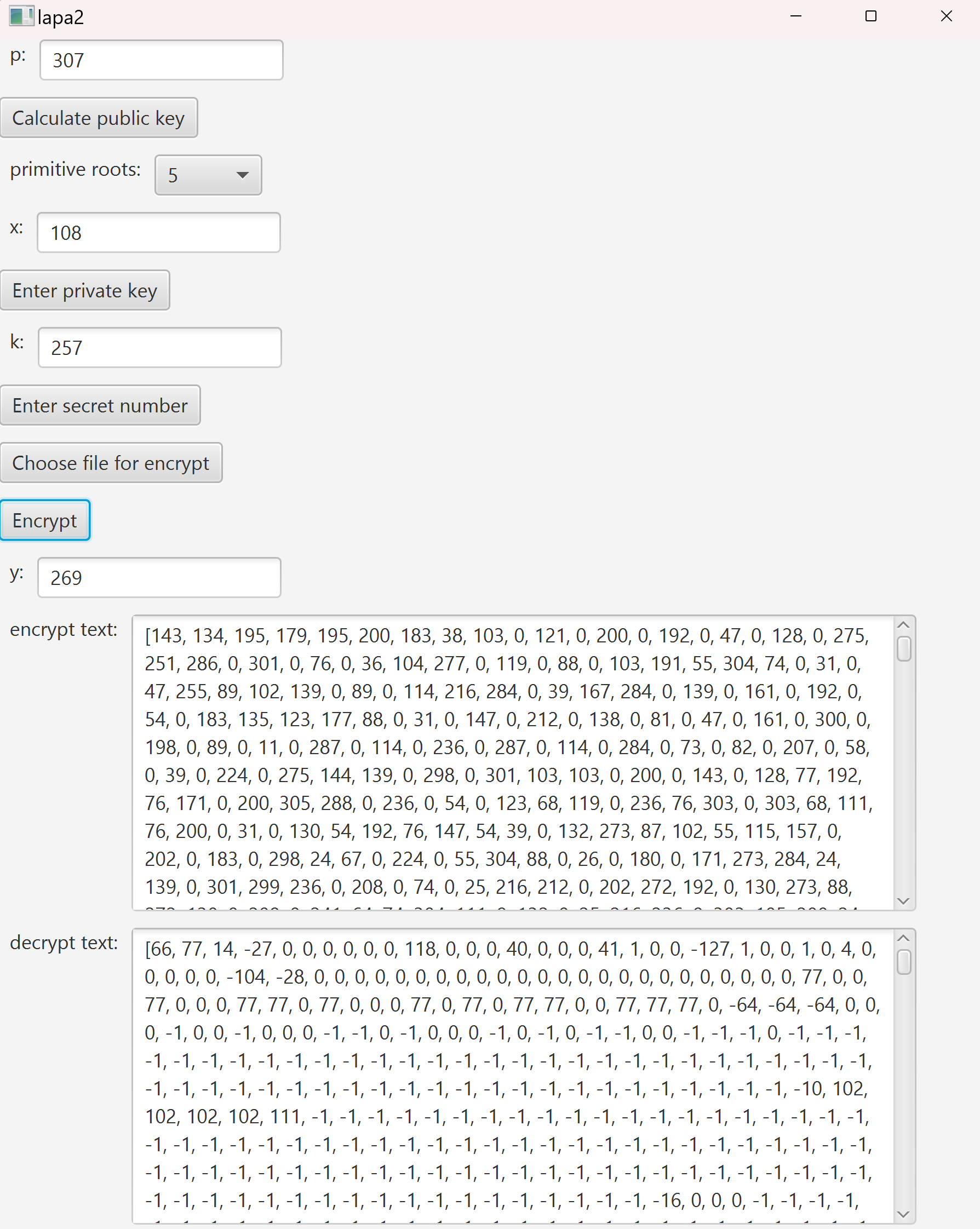
После расшифровки получился исходный текст

Тест 2: проверка на изображении

Входное изображение: Выходное изображение после расшифровки:



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



Попытка ввести p, которое будет являться не простым числом:

