УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Тесты к лабораторной работе №3

по предмету

Теория Информации

Вариант 1

Выполнила:

Писарчик. Е.А.

Проверила:

Болтак С.В.

Группа 351003

Минск 2025

**Задание**

Разработать программное средство, выполняющее вычисление открытого ключа Ko алгоритма RSA и побайтовое шифрование данным ключом по алгоритму RSA произвольного файла. Значения параметров p, q и закрытого ключа Kc, а также имя входного файла задаются пользователем и проходят проверку на корректность. Результат шифрования выводится на экран в виде чисел в 10 системе счисления.

Разработать программное средство, выполняющее расшифровку файла, каждый 16-битный блок которого представляет собой зашифрованное по алгоритму RSA 8-битное значение. Значения модуля r и закрытого ключа Kc задаются пользователем.

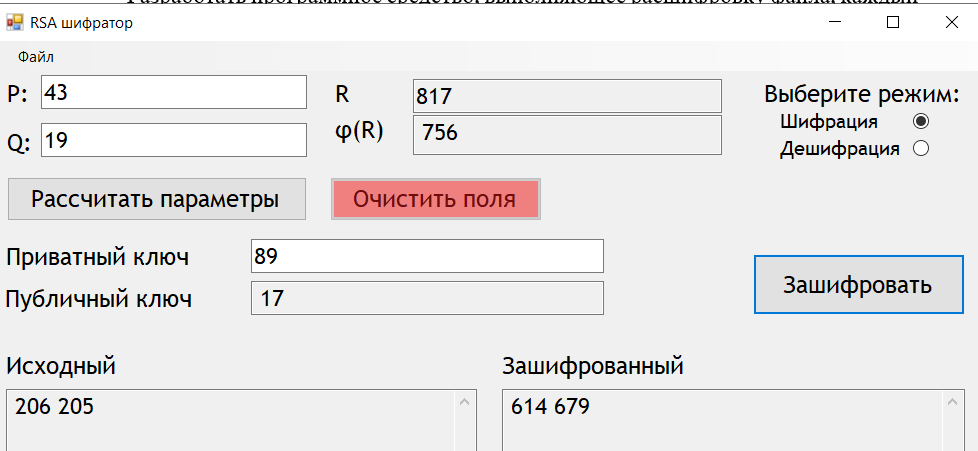
Использовать следующие алгоритмы:

* алгоритм быстрого возведения в степень,
* расширенный алгоритм Евклида,
* для определения простоты числа использовать один из вероятностных тестов: тест Ферма или тест Миллера-Рабина.

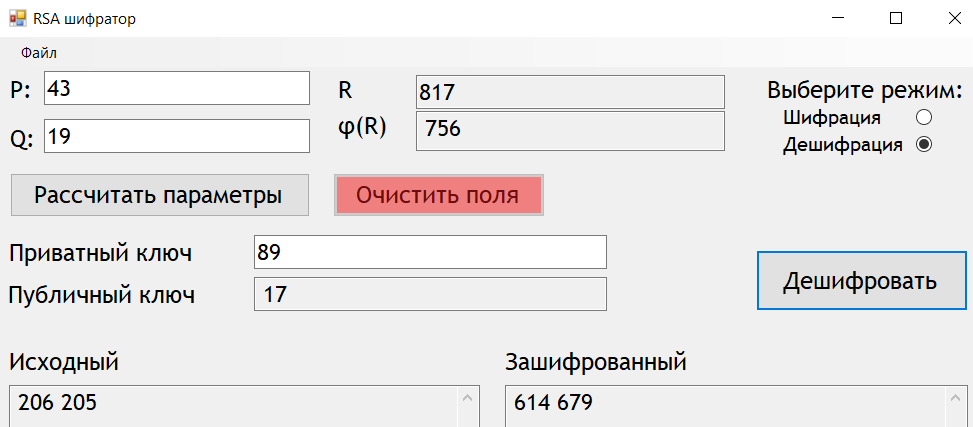
**Тесты**

1. **Простые данные**

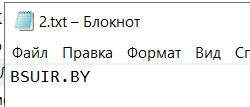
Шифрование:



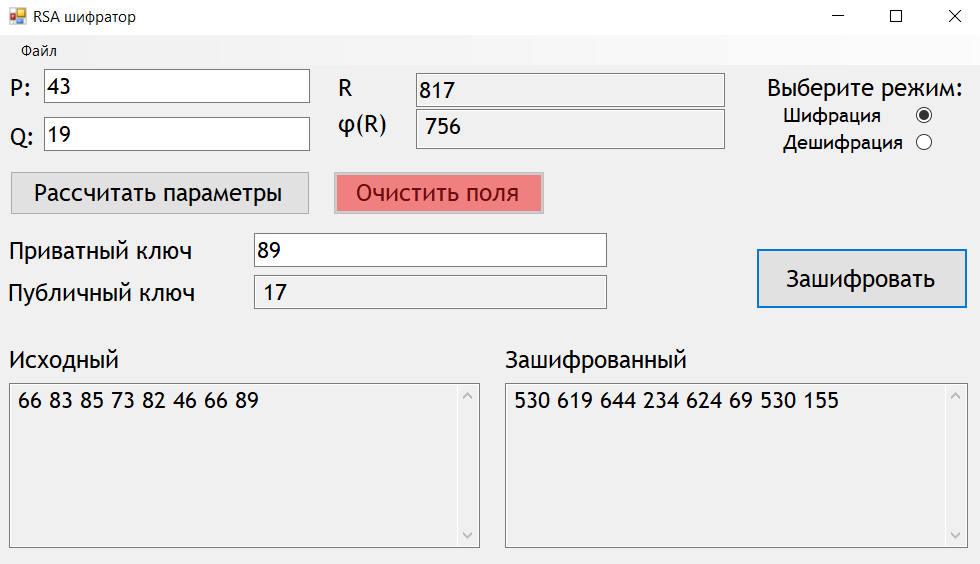
Дешифрование:

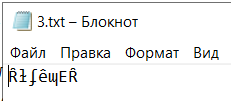


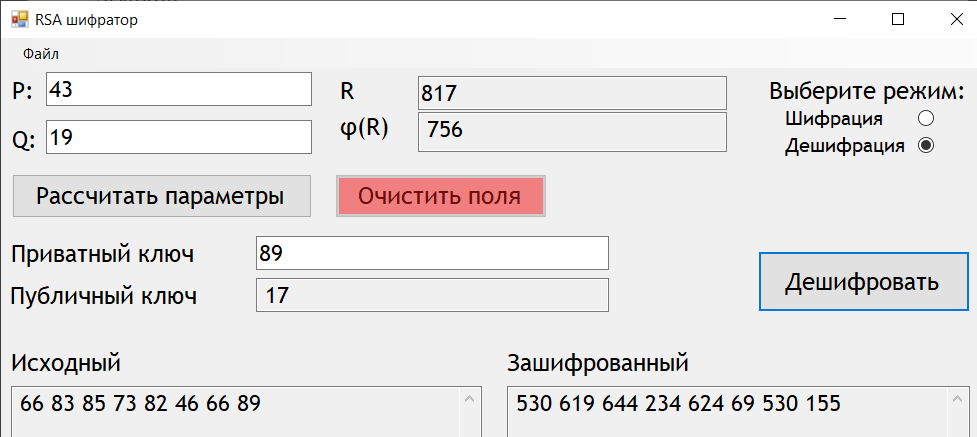
1. **Текстовый файл**

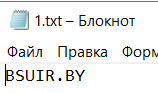
Исходный файл:  


Шифрование:



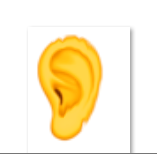
Зашифрованный файл:  


Дешифрование:  


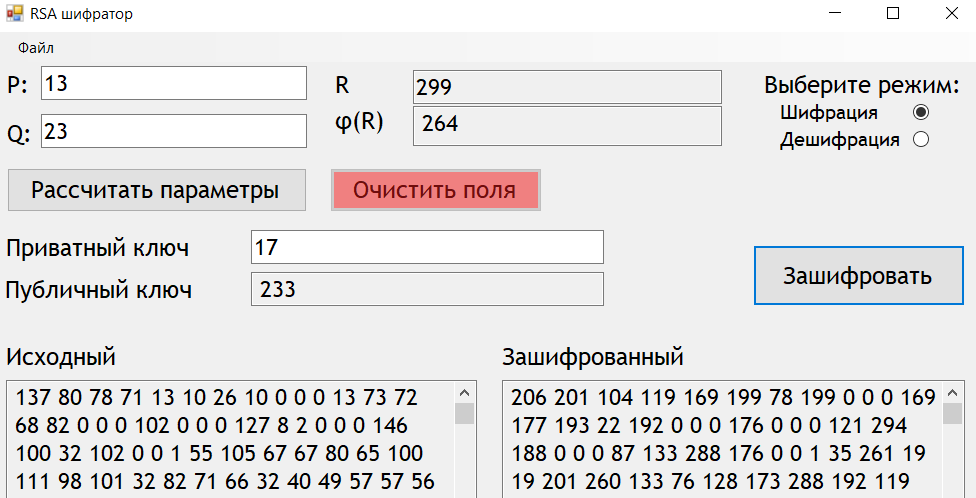
Результат расшифровки:  


1. **Файл с картинкой (.png)**

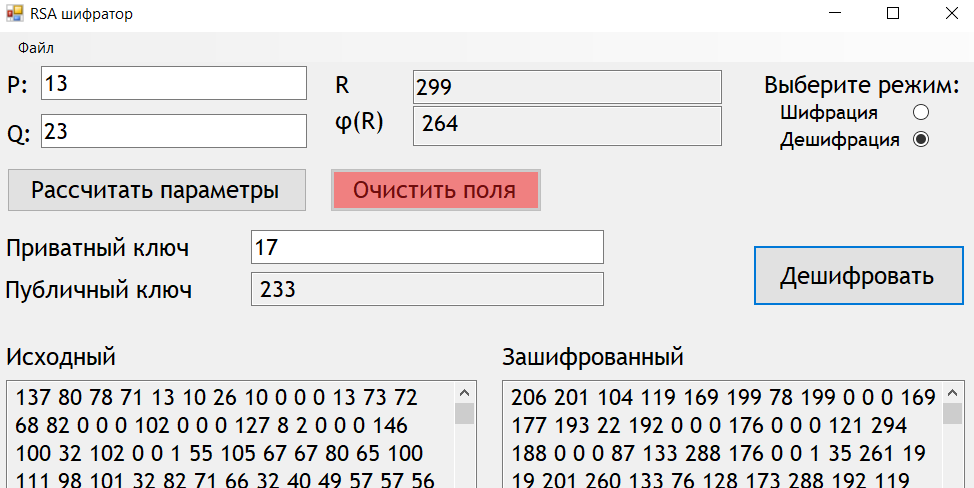
Исходная картинка:



Шифрование:



Расшифровка:



Сохраним в файл, и получим прежнюю картинку:



**Информация о тестовых файлах:**  
