УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Тесты к лабораторной работе №3

по предмету

Теория Информации

Вариант 1

Выполнил:

Кужовник В.С.

Группа 351001

Проверила:

Болтак С.В.

Минск 2025

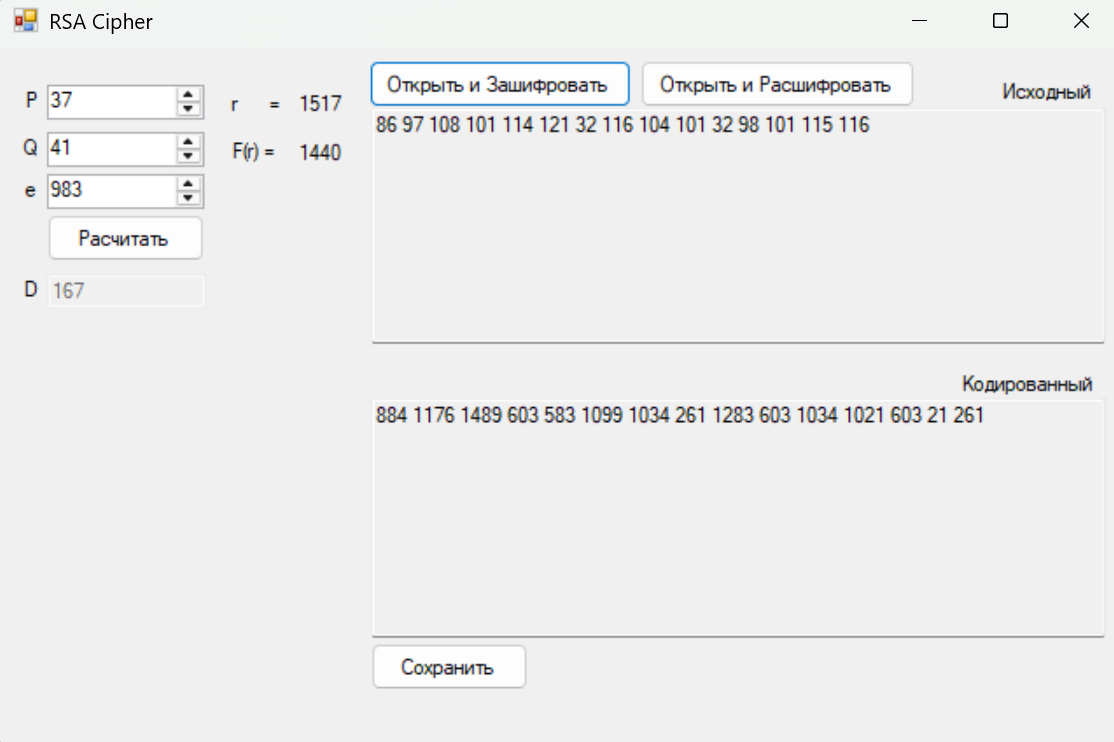
**Задание**

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.

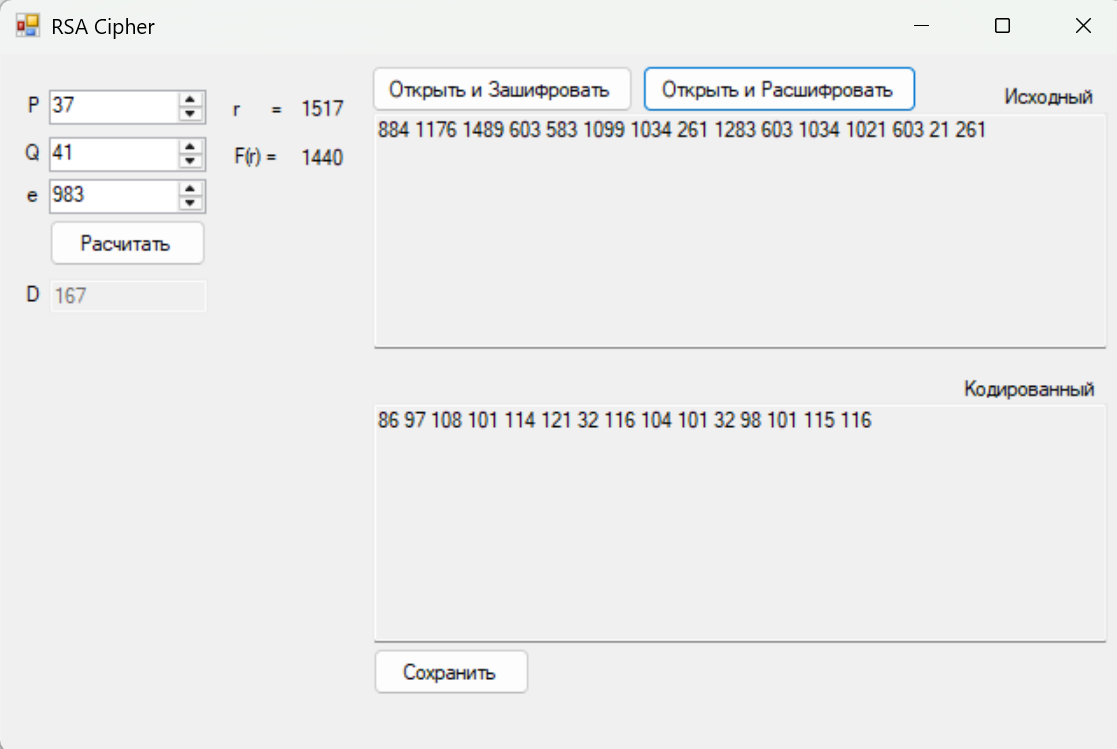
Разработать программное средство, выполняющее расшифровку файла, каждый 16-битный блок которого представляет собой зашифрованное по алгоритму RSA 8-битное значение. Значения модуля r и закрытого ключа Kc задаются пользователем.  
 **Тесты**

1. **Текстовый файл**

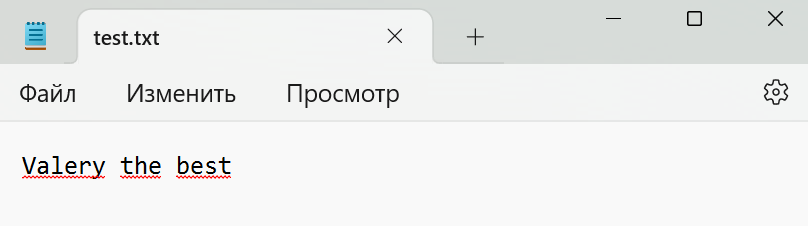
Шифрование:

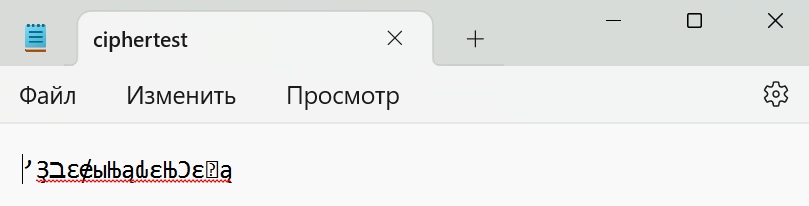


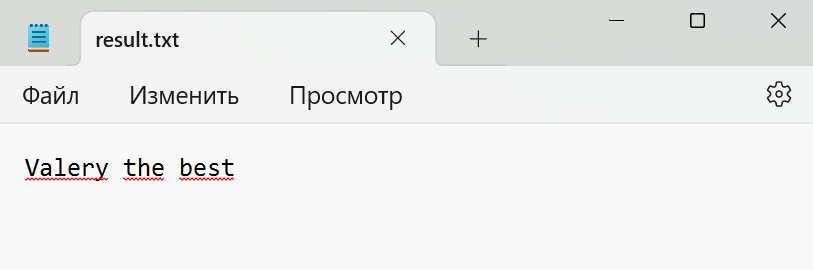
Дешифрование:



Результат:

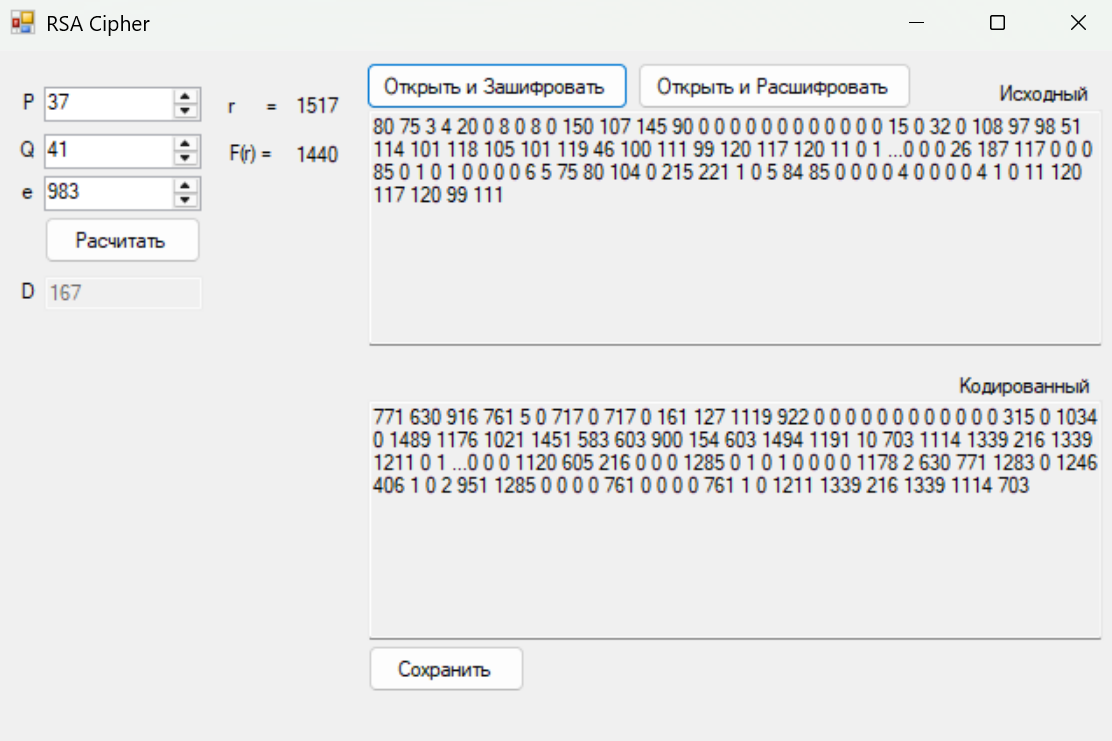
****

****

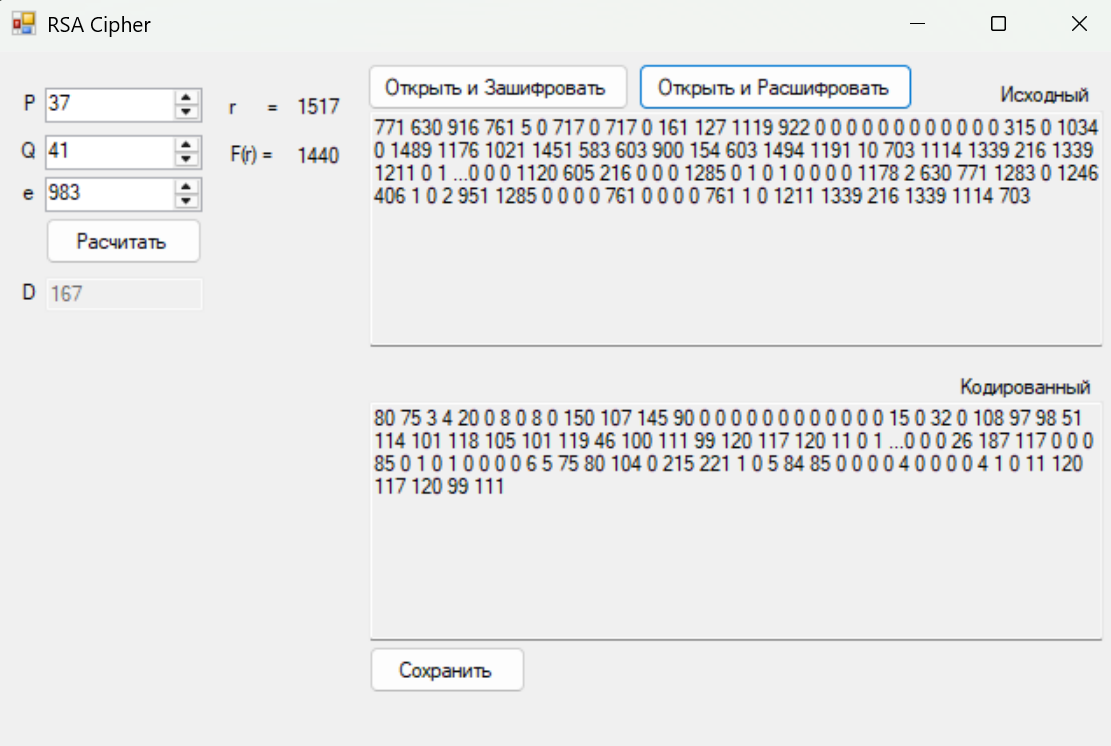
****

1. **ZIP-файл**

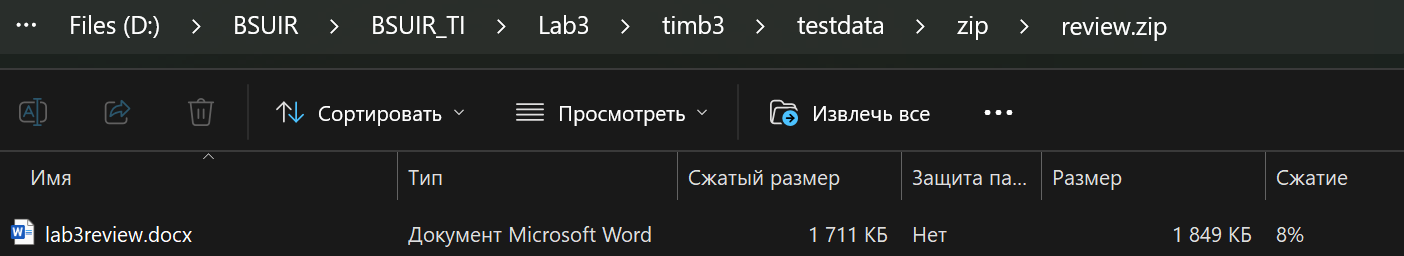
Шифрование:

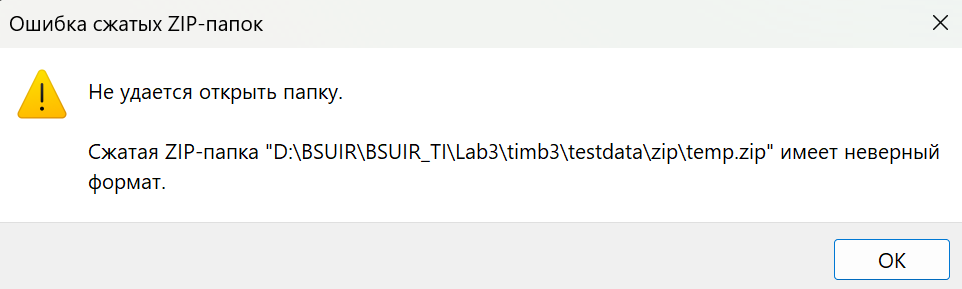


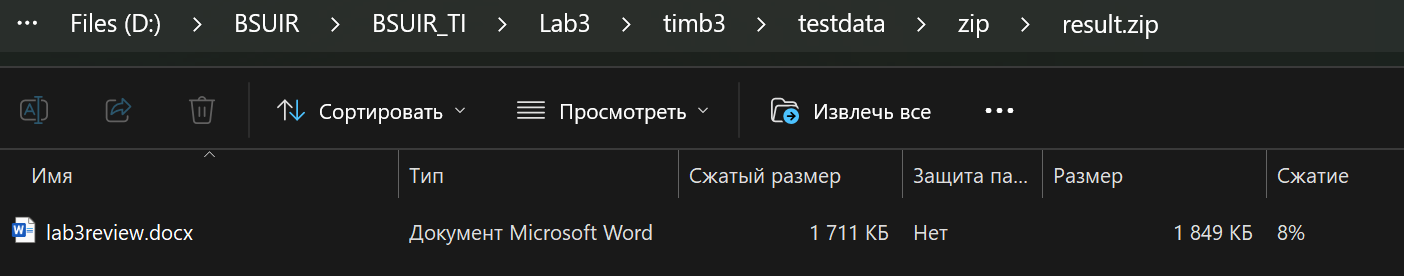
Дешифрование:



Результат:

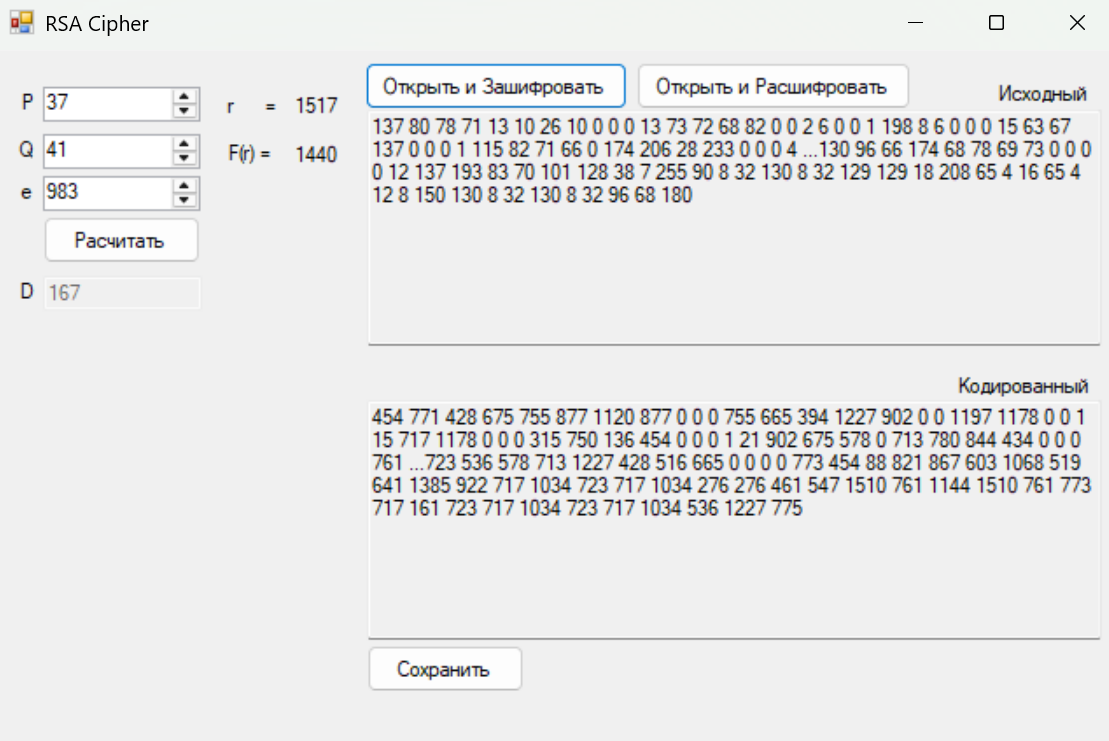






1. **PNG-файл**

Шифрование:



Дешифрование:



Результат:

