УО «Белорусский государственный университет информатики и радиоэлектроники»

Кафедра ПОИТ

Отчет по лабораторной работе № 4

по предмету «Теория информации»

Вариант 1

Выполнила:

Сологуб Е. М.

гр. 351003

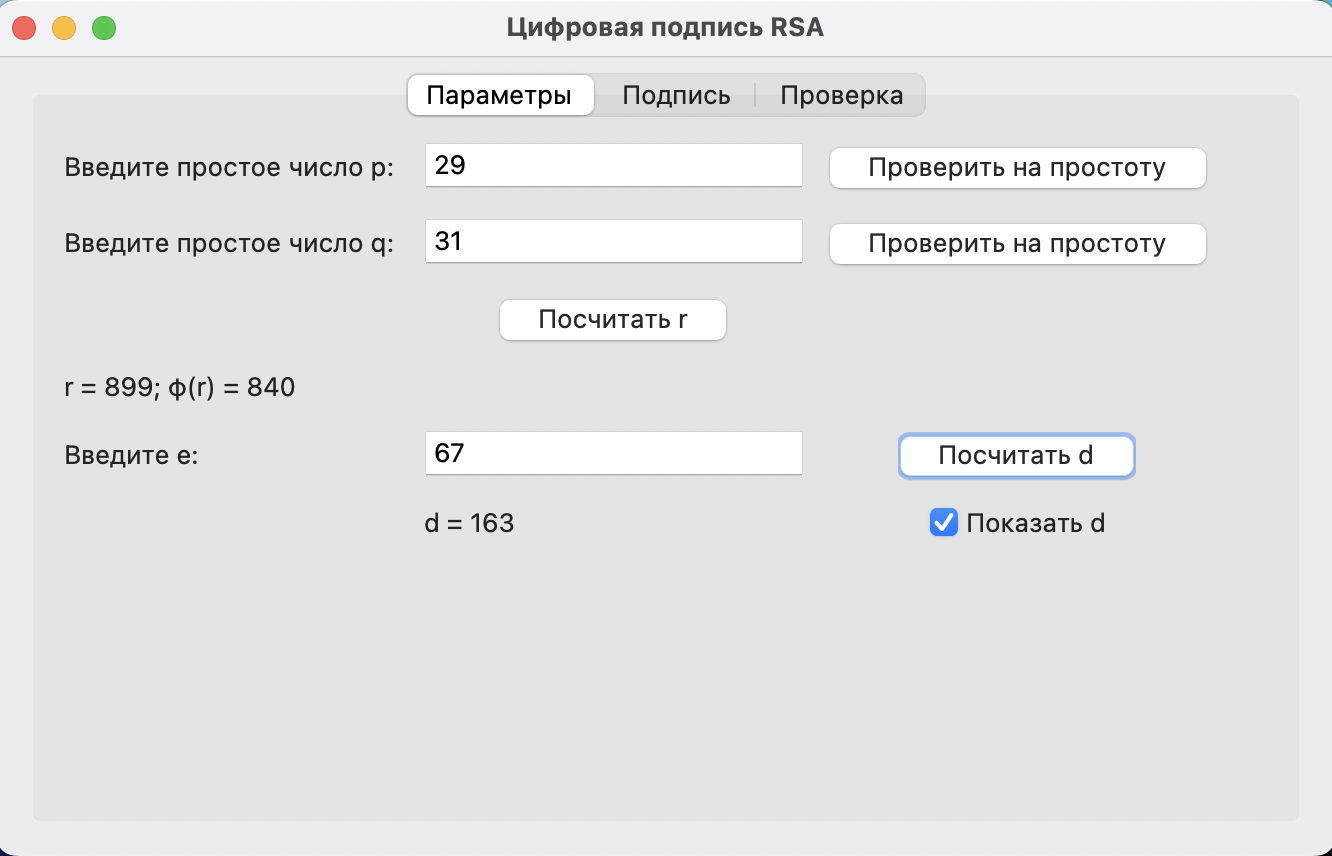
Проверила:

Болтак С. В.

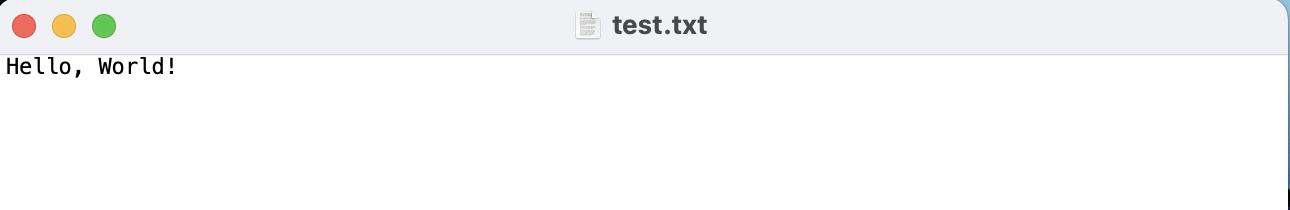
Минск 2025

**Цифровая подпись RSA**

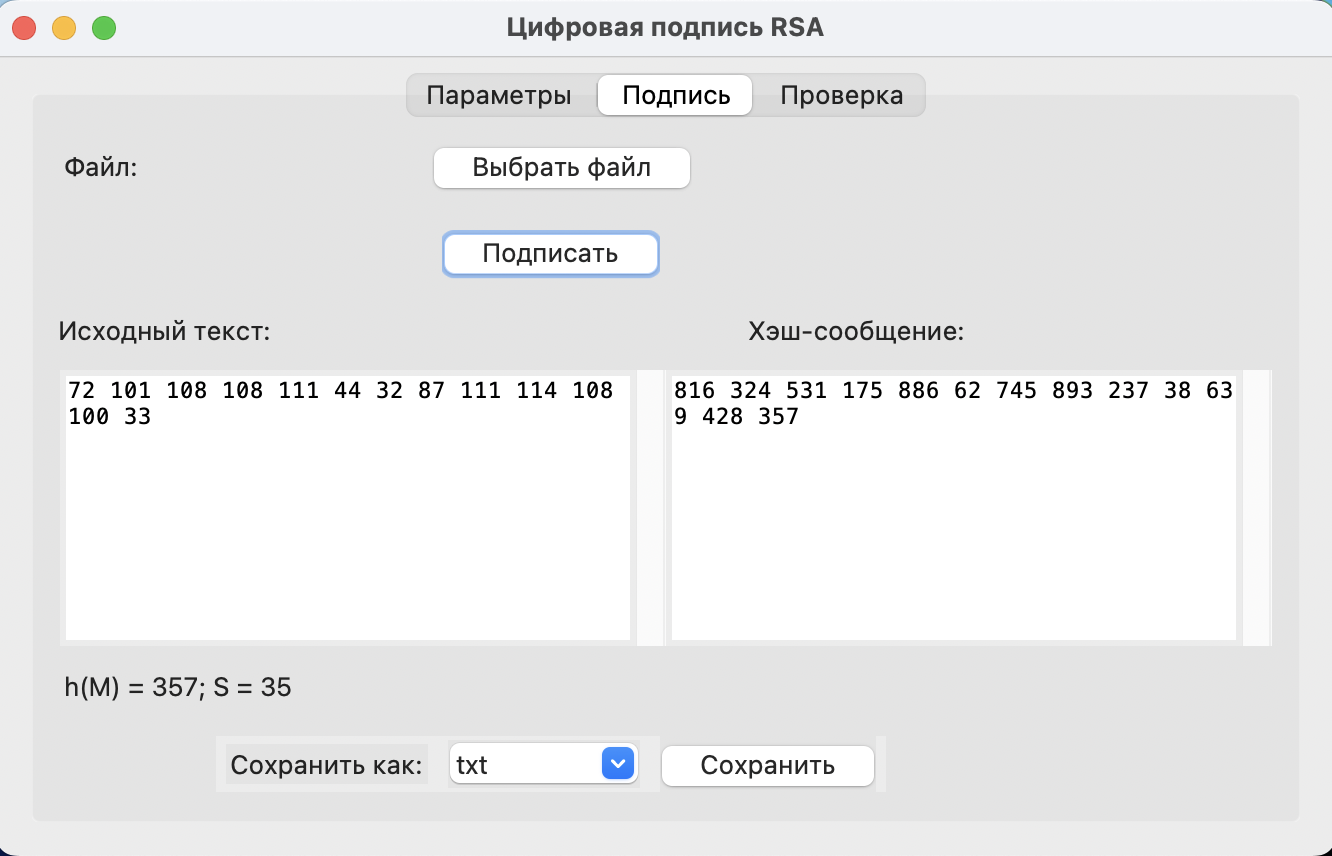
Ввод параметров:



Исходный файл:



Подпись:

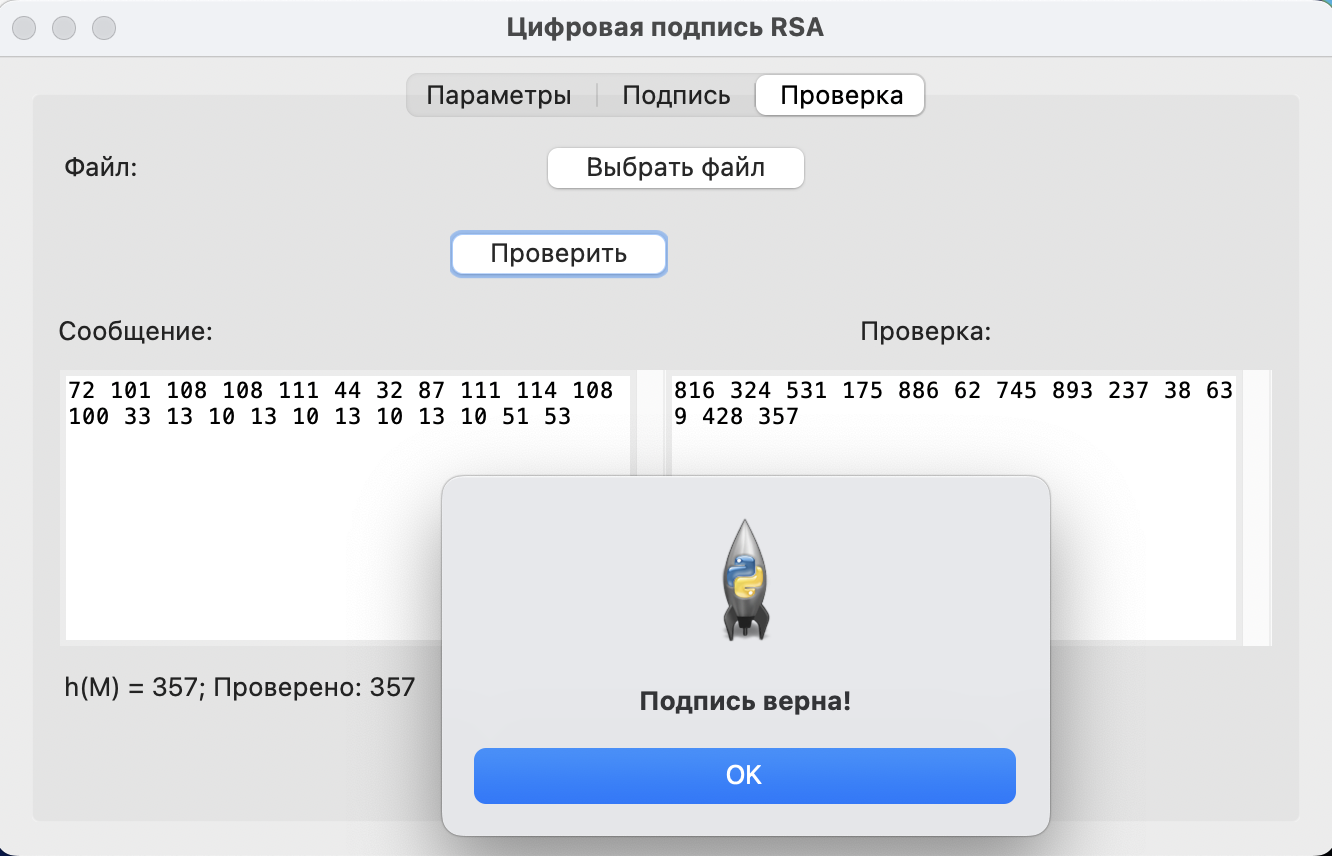


Подписанный файл:

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Проверка:

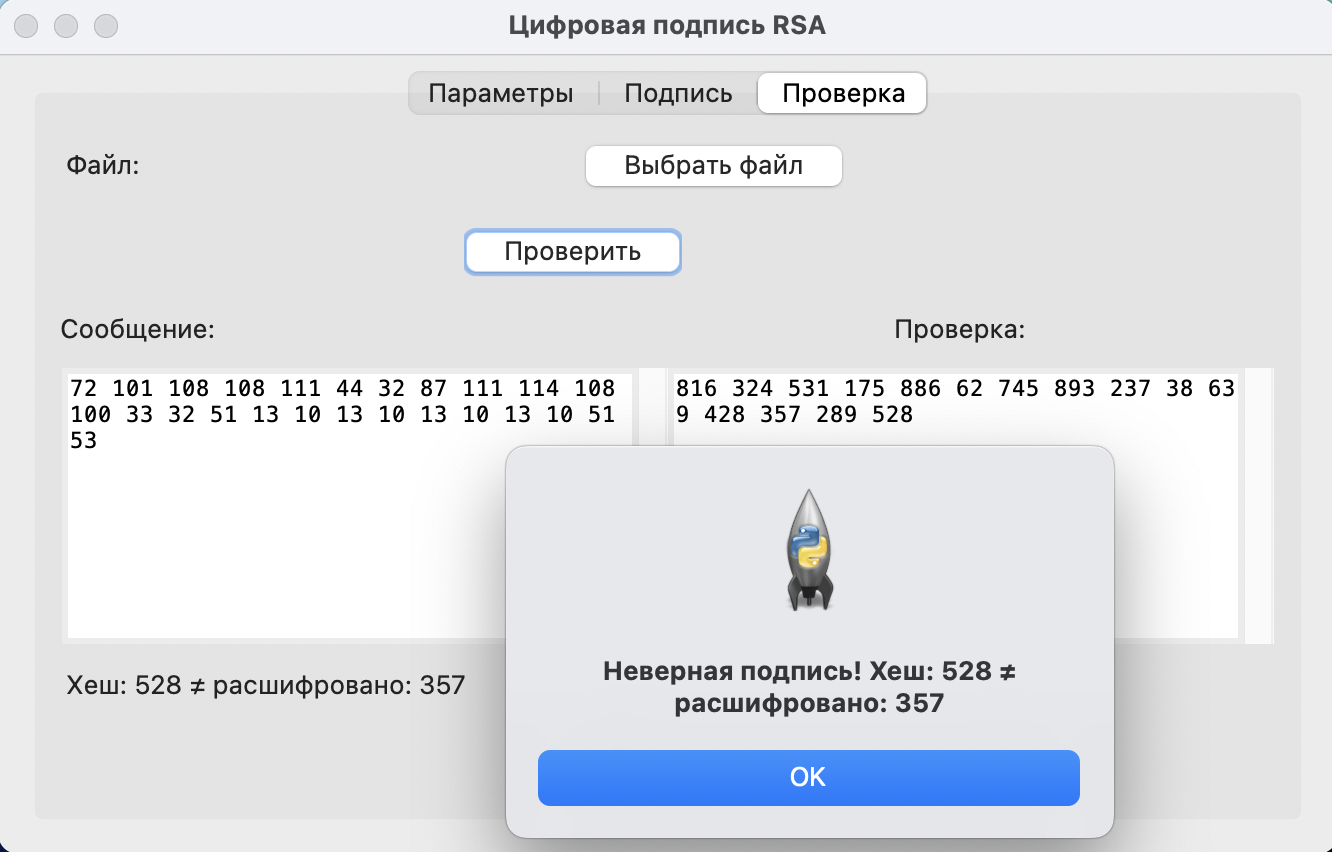


Изменим содержимое подписанного файла.

Изображение выглядит как текст, снимок экрана

Автоматически созданное описание

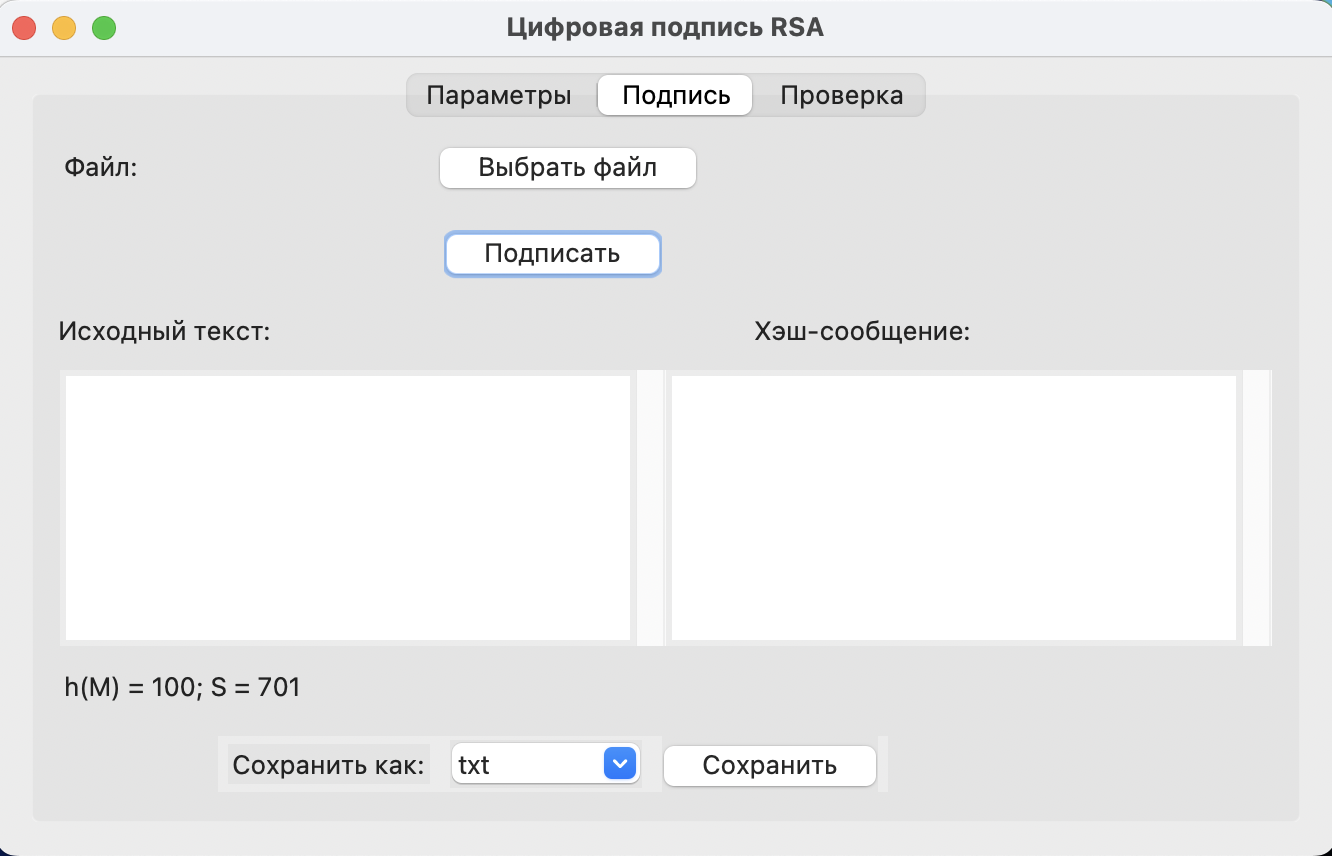
Проверим:



**Подпишем пустой файл:**

Изображение выглядит как снимок экрана

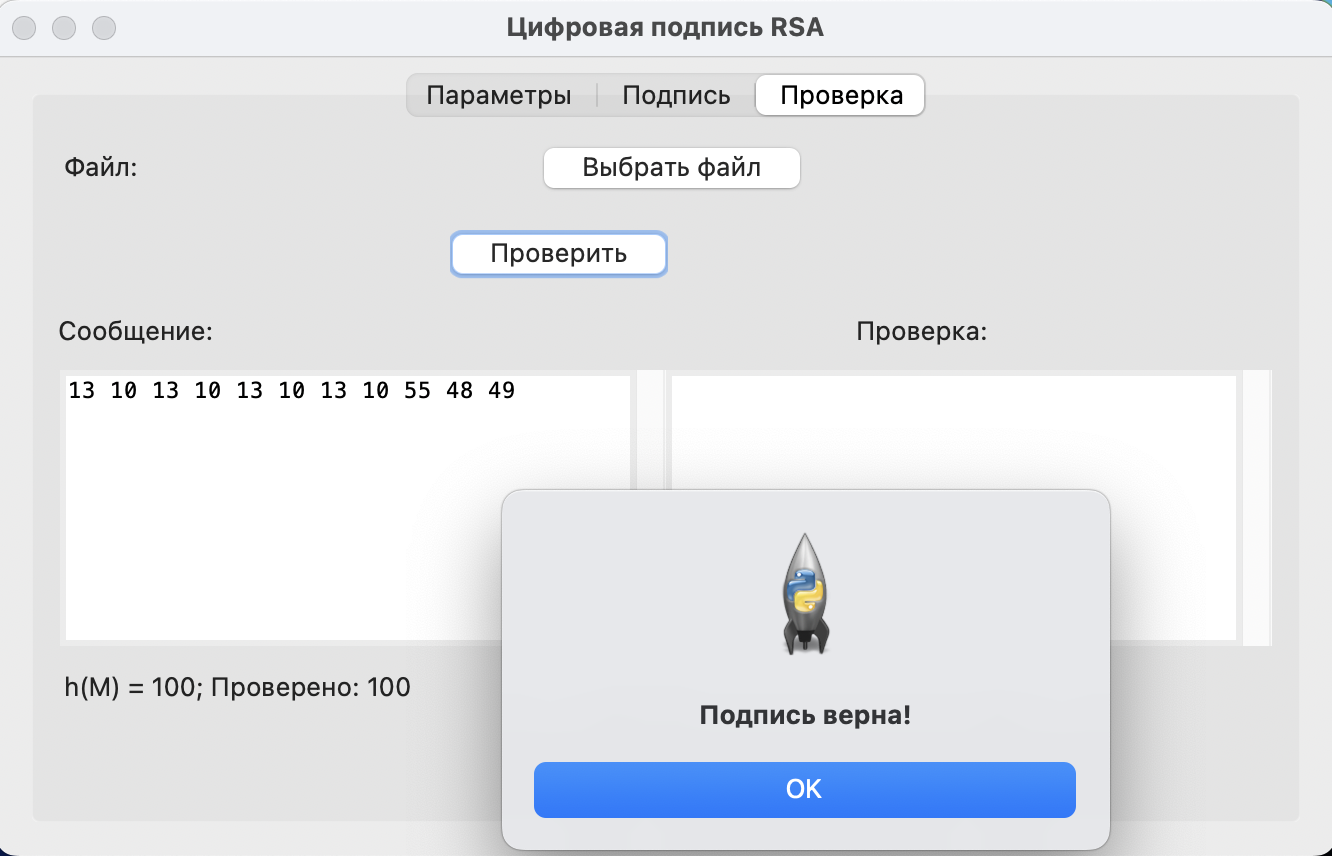
Автоматически созданное описание



Изображение выглядит как текст, Шрифт, снимок экрана

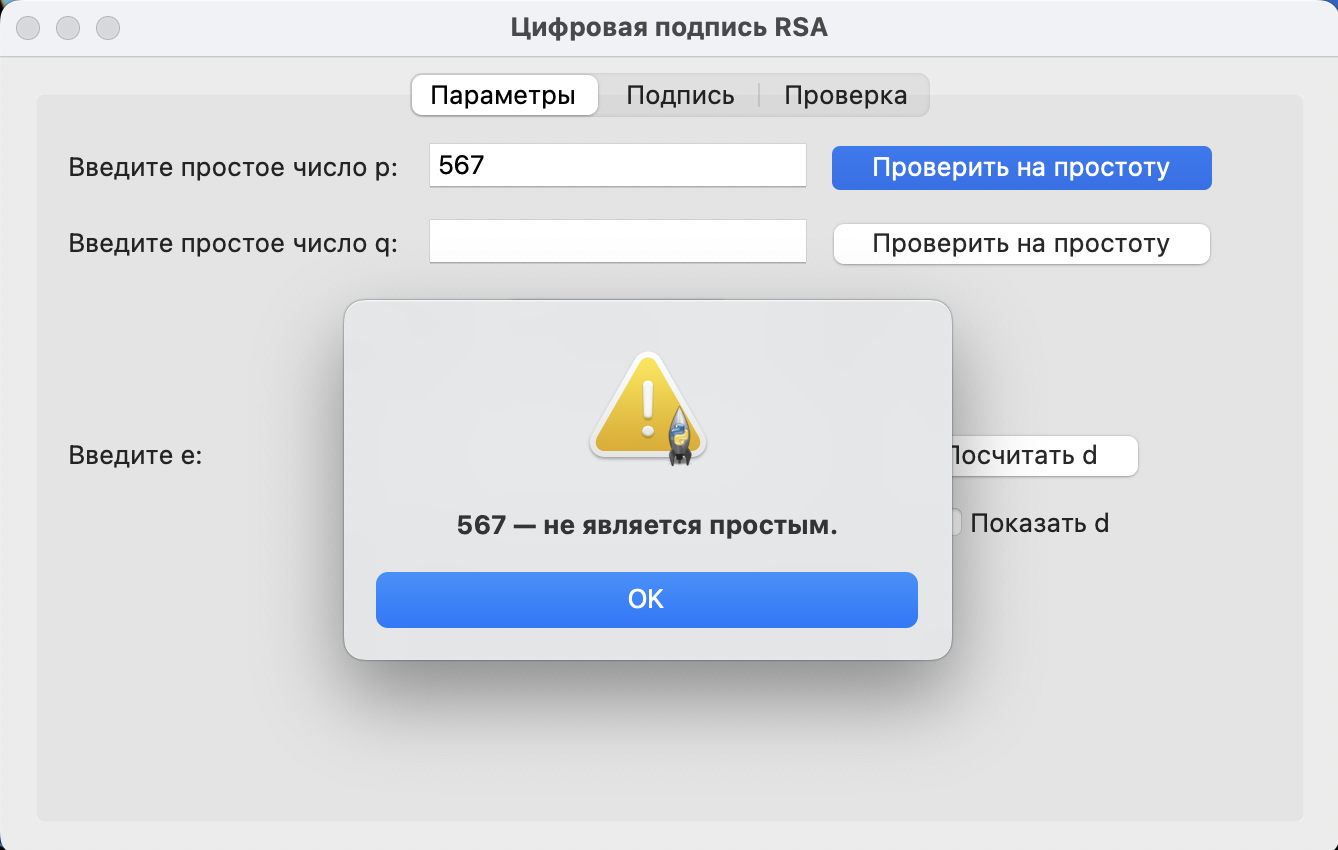
Автоматически созданное описание

Проверка:

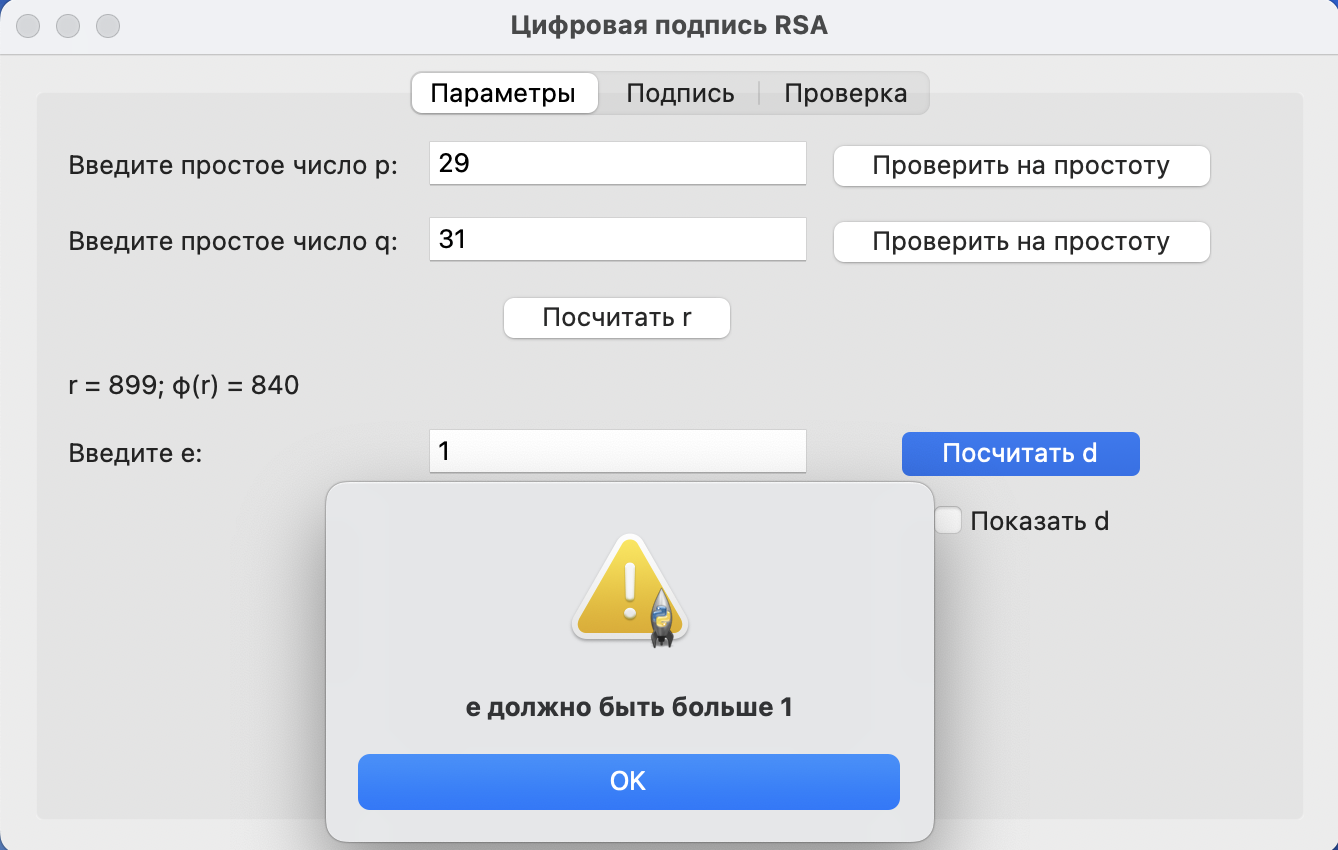


**Проверки на ввод**

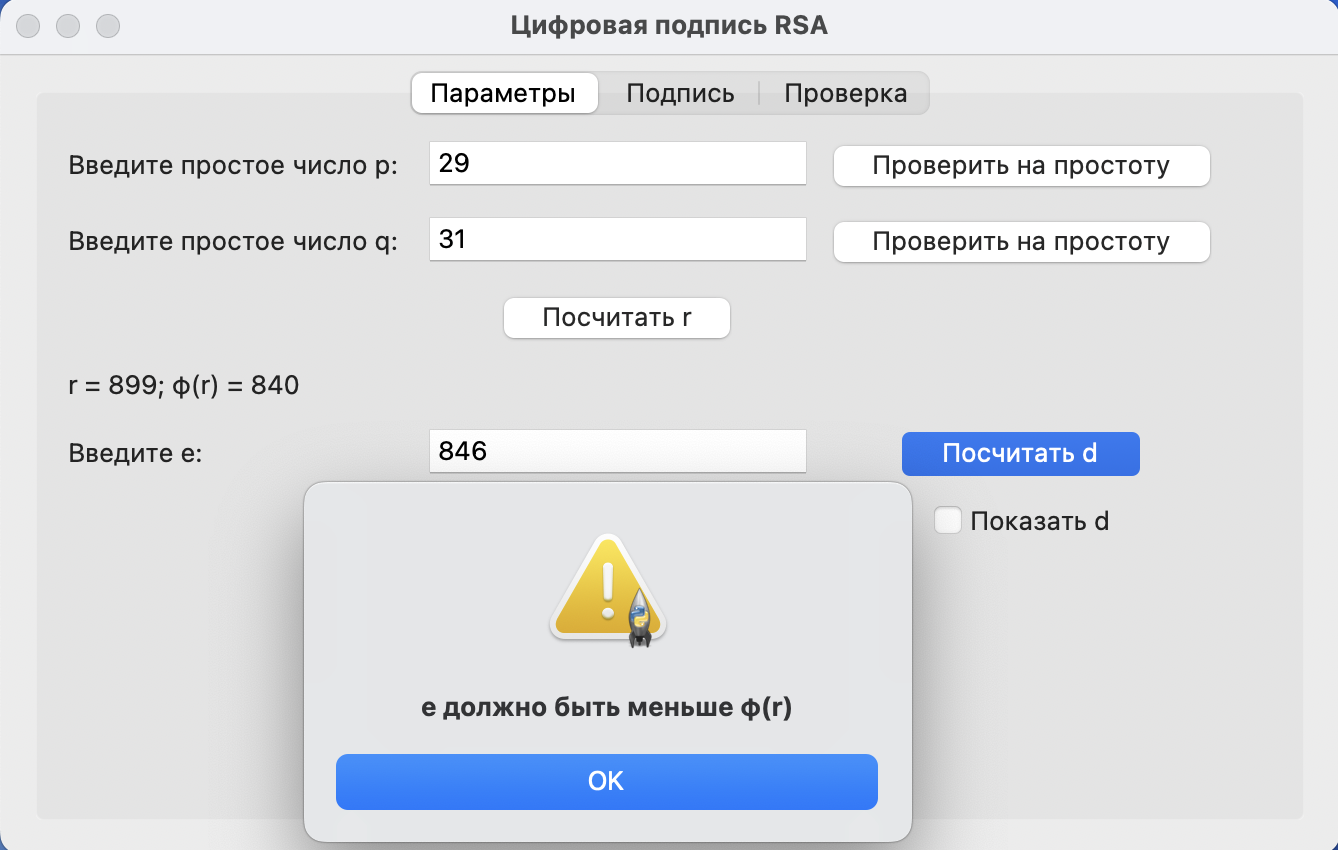
* Составное число



* Открытая экспонента e = 1



* Открытая экспонента e > φ(r)



* НОД(e, φ(r)) != 1

