Федеральное государственное автономное

образовательное учреждение

высшего образования

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт Космических и информационных технологий

институт

Кафедра «Информатика»

кафедра

**ОТЧЕТ О ПРАКТИЧЕСКОЙ РАБОТЕ №2**

«Основы криптографии с открытым ключом. Алгоритм RSA»

тема

Преподаватель \_\_\_\_\_\_\_\_\_ А.А. Сидарас

подпись, дата инициалы, фамилия

Студент КИ18-17/1б 031830504 \_\_\_\_\_\_\_\_\_ Е.В. Железкин

номер группы, зачетной книжки подпись, дата инициалы, фамилия

Красноярск 2020

Содержание

[Содержание 2](#_Toc18956750)

[1 Цель работы 3](#_Toc18956751)

[2 Задача работы 3](#_Toc18956752)

[3 Ход работы 3](#_Toc18956753)

[4 Вывод 10](#_Toc18956754)

# Цель работы

* ознакомиться с основами ассиметричной криптографии;
* ознакомиться с элементами теории чисел, используемых в криптографии с открытым ключом;
* изучить особенности алгоритма с открытым ключом RSA;
* получить навыки разработки криптосистем с открытым ключом с использованием языка программирования высокого уровня;

# Задача работы

Согласно Вашему персональному варианту (см. табл. 1) разработайте алгоритм шифрования/расшифровывания RSA, со следующими особенностями:

• объём исходного текста – любой (в разумных пределах);

• исходный текст может состоять из русских и английских букв, цифр, а также знаков препинания;

• исходный текст находится в кодировке ASCII (или Unicode);

• выступающее в качестве модуля число – N, которое выбирается автоматически и состоит из количества ДЕСЯТИЧНЫХ знаков, указанных в табл. 1. Числа P и Q выбираются случайным образом, так, что PQ N ⋅ = , где P и Q – простые числа.

• исходный текст разбивается на K блоков, где K выбирается исходя из значения модуля N;

Убедитесь в правильности составления алгоритмов, а затем на языке программирования составьте программу, которая реализует данный алгоритм.

На ряде контрольных примеров (не менее 10) открытого текста проверьте правильность работы алгоритмов шифрования и дешифрования (в качестве контрольного примера понимается текстовый файл в кодировке ASCII).

Оцените криптостойкость вашего варианта алгоритма RSA, а также сделайте оценку производительности, разработанной Вами программы.

**Вариант 7** – N = 28.

# Краткие теоретические сведения

Асимметричные алгоритмы шифрования называются также алгоритмами с открытым ключом. В отличие от алгоритмов симметричного шифрования (алгоритмов шифрования с закрытым ключом), в которых для шифрования и расшифрования используется один и тот же ключ, в ассиметричных алгоритмах один ключ используется для шифрования, а другой, отличный от первого, – для расшифрования. Алгоритмы называются асимметричными, так как ключи шифрования и расшифрования разные, следовательно, отсутствует симметрия основных криптографических процессов (см. рис .1). Один из двух ключей является открытым (public key) и может быть объявлен всем, а второй – закрытым (private key) и должен держаться в секрете. Какой из ключей, открытый или закрытый, используется для шифрования, а какой для расшифрования, определяется назначением криптографической системы.

В настоящее время асимметричные алгоритмы широко применяются на практике, например, в протоколах выработки общего секретного ключа, в протоколах электронной подписи, в протоколах безопасной передачи информации в сети интернет и др. Алгоритмы шифрования с открытым ключом можно использовать для решения, как минимум, трех задач:

• для шифрования передаваемых и хранимых данных в целях их защиты от несанкционированного доступа;

• для формирования цифровой подписи электронных документов;

• в задачах распределения секретных ключей, используемых в дальнейшем при симметричном шифровании.

# Ход работы

Листинг 1 – файл main.py

*# -\*- coding: utf-8 -\*-  
  
# Form implementation generated from reading ui file 'form.ui'  
#  
# Created by: PyQt5 UI code generator 5.13.2  
#  
# WARNING! All changes made in this file will be lost!*from PyQt5 import QtCore, QtGui, QtWidgets  
from PyQt5.QtWidgets import QMainWindow  
import funcs  
  
  
class Ui\_form(object):  
 def setupUi(self, form):  
 form.setObjectName(**"form"**)  
 form.resize(916, 801)  
 self.centralwidget = QtWidgets.QWidget(form)  
 self.centralwidget.setObjectName(**"centralwidget"**)  
 self.gridLayout\_11 = QtWidgets.QGridLayout(self.centralwidget)  
 self.gridLayout\_11.setObjectName(**"gridLayout\_11"**)  
 self.pushButton\_3 = QtWidgets.QPushButton(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.pushButton\_3.setFont(font)  
 self.pushButton\_3.setObjectName(**"pushButton\_3"**)  
 self.gridLayout\_11.addWidget(self.pushButton\_3, 17, 2, 1, 1)  
 self.label = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(25)  
 self.label.setFont(font)  
 self.label.setAutoFillBackground(False)  
 self.label.setObjectName(**"label"**)  
 self.gridLayout\_11.addWidget(self.label, 0, 1, 1, 5)  
 self.gridLayout\_5 = QtWidgets.QGridLayout()  
 self.gridLayout\_5.setObjectName(**"gridLayout\_5"**)  
 self.label\_2 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_2.setFont(font)  
 self.label\_2.setAutoFillBackground(False)  
 self.label\_2.setObjectName(**"label\_2"**)  
 self.gridLayout\_5.addWidget(self.label\_2, 0, 0, 1, 1)  
 self.lineEdit\_p = QtWidgets.QLineEdit(self.centralwidget)  
 self.lineEdit\_p.setEnabled(True)  
 font = QtGui.QFont()  
 font.setPointSize(12)  
 self.lineEdit\_p.setFont(font)  
 self.lineEdit\_p.setAutoFillBackground(False)  
 self.lineEdit\_p.setText(**""**)  
 self.lineEdit\_p.setReadOnly(True)  
 self.lineEdit\_p.setPlaceholderText(**""**)  
 self.lineEdit\_p.setObjectName(**"lineEdit\_p"**)  
 self.gridLayout\_5.addWidget(self.lineEdit\_p, 0, 1, 1, 1)  
 self.gridLayout\_11.addLayout(self.gridLayout\_5, 1, 1, 1, 4)  
 self.gridLayout\_3 = QtWidgets.QGridLayout()  
 self.gridLayout\_3.setObjectName(**"gridLayout\_3"**)  
 self.label\_5 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_5.setFont(font)  
 self.label\_5.setObjectName(**"label\_5"**)  
 self.gridLayout\_3.addWidget(self.label\_5, 0, 0, 1, 1)  
 self.lineEdit\_s = QtWidgets.QLineEdit(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(12)  
 self.lineEdit\_s.setFont(font)  
 self.lineEdit\_s.setReadOnly(True)  
 self.lineEdit\_s.setObjectName(**"lineEdit\_s"**)  
 self.gridLayout\_3.addWidget(self.lineEdit\_s, 0, 1, 1, 1)  
 self.gridLayout\_11.addLayout(self.gridLayout\_3, 6, 1, 1, 4)  
 self.gridLayout\_8 = QtWidgets.QGridLayout()  
 self.gridLayout\_8.setObjectName(**"gridLayout\_8"**)  
 self.label\_10 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_10.setFont(font)  
 self.label\_10.setAutoFillBackground(False)  
 self.label\_10.setObjectName(**"label\_10"**)  
 self.gridLayout\_8.addWidget(self.label\_10, 0, 0, 1, 1)  
 self.lineEdit\_pq\_A = QtWidgets.QLineEdit(self.centralwidget)  
 self.lineEdit\_pq\_A.setEnabled(True)  
 font = QtGui.QFont()  
 font.setPointSize(12)  
 self.lineEdit\_pq\_A.setFont(font)  
 self.lineEdit\_pq\_A.setAutoFillBackground(False)  
 self.lineEdit\_pq\_A.setText(**""**)  
 self.lineEdit\_pq\_A.setReadOnly(True)  
 self.lineEdit\_pq\_A.setPlaceholderText(**""**)  
 self.lineEdit\_pq\_A.setObjectName(**"lineEdit\_pq\_A"**)  
 self.gridLayout\_8.addWidget(self.lineEdit\_pq\_A, 0, 1, 1, 1)  
 self.gridLayout\_11.addLayout(self.gridLayout\_8, 12, 1, 1, 2)  
 self.pushButton = QtWidgets.QPushButton(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.pushButton.setFont(font)  
 self.pushButton.setObjectName(**"pushButton"**)  
 self.gridLayout\_11.addWidget(self.pushButton, 1, 5, 3, 1)  
 self.pushButton\_2 = QtWidgets.QPushButton(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.pushButton\_2.setFont(font)  
 self.pushButton\_2.setObjectName(**"pushButton\_2"**)  
 self.gridLayout\_11.addWidget(self.pushButton\_2, 4, 5, 3, 1)  
 self.line = QtWidgets.QFrame(self.centralwidget)  
 self.line.setFrameShape(QtWidgets.QFrame.HLine)  
 self.line.setFrameShadow(QtWidgets.QFrame.Sunken)  
 self.line.setObjectName(**"line"**)  
 self.gridLayout\_11.addWidget(self.line, 8, 1, 2, 5)  
 self.gridLayout\_4 = QtWidgets.QGridLayout()  
 self.gridLayout\_4.setObjectName(**"gridLayout\_4"**)  
 self.label\_9 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_9.setFont(font)  
 self.label\_9.setObjectName(**"label\_9"**)  
 self.gridLayout\_4.addWidget(self.label\_9, 1, 0, 1, 1)  
 self.lineEdit\_d = QtWidgets.QLineEdit(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(12)  
 self.lineEdit\_d.setFont(font)  
 self.lineEdit\_d.setText(**""**)  
 self.lineEdit\_d.setReadOnly(True)  
 self.lineEdit\_d.setPlaceholderText(**""**)  
 self.lineEdit\_d.setObjectName(**"lineEdit\_d"**)  
 self.gridLayout\_4.addWidget(self.lineEdit\_d, 1, 1, 1, 1)  
 self.gridLayout\_11.addLayout(self.gridLayout\_4, 5, 1, 1, 4)  
 self.label\_12 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_12.setFont(font)  
 self.label\_12.setObjectName(**"label\_12"**)  
 self.gridLayout\_11.addWidget(self.label\_12, 10, 4, 1, 2)  
 self.gridLayout\_10 = QtWidgets.QGridLayout()  
 self.gridLayout\_10.setObjectName(**"gridLayout\_10"**)  
 self.label\_15 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_15.setFont(font)  
 self.label\_15.setAutoFillBackground(False)  
 self.label\_15.setObjectName(**"label\_15"**)  
 self.gridLayout\_10.addWidget(self.label\_15, 0, 0, 1, 1)  
 self.lineEdit\_pq\_B = QtWidgets.QLineEdit(self.centralwidget)  
 self.lineEdit\_pq\_B.setEnabled(True)  
 font = QtGui.QFont()  
 font.setPointSize(12)  
 self.lineEdit\_pq\_B.setFont(font)  
 self.lineEdit\_pq\_B.setAutoFillBackground(False)  
 self.lineEdit\_pq\_B.setText(**""**)  
 self.lineEdit\_pq\_B.setReadOnly(True)  
 self.lineEdit\_pq\_B.setPlaceholderText(**""**)  
 self.lineEdit\_pq\_B.setObjectName(**"lineEdit\_pq\_B"**)  
 self.gridLayout\_10.addWidget(self.lineEdit\_pq\_B, 1, 0, 1, 1)  
 self.gridLayout\_11.addLayout(self.gridLayout\_10, 13, 4, 1, 2)  
 self.gridLayout\_9 = QtWidgets.QGridLayout()  
 self.gridLayout\_9.setObjectName(**"gridLayout\_9"**)  
 self.label\_13 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_13.setFont(font)  
 self.label\_13.setObjectName(**"label\_13"**)  
 self.gridLayout\_9.addWidget(self.label\_13, 0, 0, 1, 1)  
 self.lineEdit\_e\_B = QtWidgets.QLineEdit(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(12)  
 self.lineEdit\_e\_B.setFont(font)  
 self.lineEdit\_e\_B.setReadOnly(True)  
 self.lineEdit\_e\_B.setObjectName(**"lineEdit\_e\_B"**)  
 self.gridLayout\_9.addWidget(self.lineEdit\_e\_B, 1, 0, 1, 1)  
 self.gridLayout\_11.addLayout(self.gridLayout\_9, 11, 4, 2, 2)  
 self.gridLayout\_2 = QtWidgets.QGridLayout()  
 self.gridLayout\_2.setObjectName(**"gridLayout\_2"**)  
 self.label\_4 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_4.setFont(font)  
 self.label\_4.setObjectName(**"label\_4"**)  
 self.gridLayout\_2.addWidget(self.label\_4, 0, 0, 1, 1)  
 self.lineEdit\_e = QtWidgets.QLineEdit(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(12)  
 self.lineEdit\_e.setFont(font)  
 self.lineEdit\_e.setReadOnly(True)  
 self.lineEdit\_e.setObjectName(**"lineEdit\_e"**)  
 self.gridLayout\_2.addWidget(self.lineEdit\_e, 0, 1, 1, 1)  
 self.gridLayout\_11.addLayout(self.gridLayout\_2, 7, 1, 1, 4)  
 self.line\_3 = QtWidgets.QFrame(self.centralwidget)  
 self.line\_3.setFrameShape(QtWidgets.QFrame.VLine)  
 self.line\_3.setFrameShadow(QtWidgets.QFrame.Sunken)  
 self.line\_3.setObjectName(**"line\_3"**)  
 self.gridLayout\_11.addWidget(self.line\_3, 9, 3, 10, 1)  
 self.gridLayout\_6 = QtWidgets.QGridLayout()  
 self.gridLayout\_6.setObjectName(**"gridLayout\_6"**)  
 self.label\_3 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_3.setFont(font)  
 self.label\_3.setAutoFillBackground(False)  
 self.label\_3.setObjectName(**"label\_3"**)  
 self.gridLayout\_6.addWidget(self.label\_3, 0, 0, 1, 1)  
 self.lineEdit\_q = QtWidgets.QLineEdit(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(12)  
 self.lineEdit\_q.setFont(font)  
 self.lineEdit\_q.setAutoFillBackground(False)  
 self.lineEdit\_q.setText(**""**)  
 self.lineEdit\_q.setReadOnly(True)  
 self.lineEdit\_q.setPlaceholderText(**""**)  
 self.lineEdit\_q.setObjectName(**"lineEdit\_q"**)  
 self.gridLayout\_6.addWidget(self.lineEdit\_q, 0, 1, 1, 1)  
 self.gridLayout\_11.addLayout(self.gridLayout\_6, 2, 1, 1, 4)  
 self.label\_14 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_14.setFont(font)  
 self.label\_14.setObjectName(**"label\_14"**)  
 self.gridLayout\_11.addWidget(self.label\_14, 13, 1, 1, 2)  
 self.gridLayout\_7 = QtWidgets.QGridLayout()  
 self.gridLayout\_7.setObjectName(**"gridLayout\_7"**)  
 self.label\_6 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_6.setFont(font)  
 self.label\_6.setAutoFillBackground(False)  
 self.label\_6.setObjectName(**"label\_6"**)  
 self.gridLayout\_7.addWidget(self.label\_6, 0, 0, 1, 1)  
 self.lineEdit\_s\_A = QtWidgets.QLineEdit(self.centralwidget)  
 self.lineEdit\_s\_A.setEnabled(True)  
 font = QtGui.QFont()  
 font.setPointSize(12)  
 self.lineEdit\_s\_A.setFont(font)  
 self.lineEdit\_s\_A.setAutoFillBackground(False)  
 self.lineEdit\_s\_A.setText(**""**)  
 self.lineEdit\_s\_A.setReadOnly(True)  
 self.lineEdit\_s\_A.setPlaceholderText(**""**)  
 self.lineEdit\_s\_A.setObjectName(**"lineEdit\_s\_A"**)  
 self.gridLayout\_7.addWidget(self.lineEdit\_s\_A, 0, 1, 1, 1)  
 self.gridLayout\_11.addLayout(self.gridLayout\_7, 11, 1, 1, 2)  
 self.label\_7 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_7.setFont(font)  
 self.label\_7.setAutoFillBackground(False)  
 self.label\_7.setObjectName(**"label\_7"**)  
 self.gridLayout\_11.addWidget(self.label\_7, 7, 5, 1, 1)  
 self.label\_11 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_11.setFont(font)  
 self.label\_11.setObjectName(**"label\_11"**)  
 self.gridLayout\_11.addWidget(self.label\_11, 10, 2, 1, 1)  
 self.label\_16 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_16.setFont(font)  
 self.label\_16.setObjectName(**"label\_16"**)  
 self.gridLayout\_11.addWidget(self.label\_16, 14, 4, 1, 2)  
 self.gridLayout = QtWidgets.QGridLayout()  
 self.gridLayout.setObjectName(**"gridLayout"**)  
 self.lineEdit\_pq = QtWidgets.QLineEdit(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(12)  
 self.lineEdit\_pq.setFont(font)  
 self.lineEdit\_pq.setAutoFillBackground(False)  
 self.lineEdit\_pq.setText(**""**)  
 self.lineEdit\_pq.setReadOnly(True)  
 self.lineEdit\_pq.setPlaceholderText(**""**)  
 self.lineEdit\_pq.setObjectName(**"lineEdit\_pq"**)  
 self.gridLayout.addWidget(self.lineEdit\_pq, 0, 1, 1, 1)  
 self.label\_8 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_8.setFont(font)  
 self.label\_8.setAutoFillBackground(False)  
 self.label\_8.setObjectName(**"label\_8"**)  
 self.gridLayout.addWidget(self.label\_8, 0, 0, 1, 1)  
 self.gridLayout\_11.addLayout(self.gridLayout, 3, 1, 2, 4)  
 self.textForRSA = QtWidgets.QTextEdit(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(12)  
 self.textForRSA.setFont(font)  
 self.textForRSA.setObjectName(**"textForRSA"**)  
 self.gridLayout\_11.addWidget(self.textForRSA, 14, 1, 2, 2)  
 self.textEdit = QtWidgets.QTextEdit(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(12)  
 self.textEdit.setFont(font)  
 self.textEdit.setReadOnly(True)  
 self.textEdit.setObjectName(**"textEdit"**)  
 self.gridLayout\_11.addWidget(self.textEdit, 18, 1, 1, 2)  
 self.textEdit\_2 = QtWidgets.QTextEdit(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(12)  
 self.textEdit\_2.setFont(font)  
 self.textEdit\_2.setObjectName(**"textEdit\_2"**)  
 self.gridLayout\_11.addWidget(self.textEdit\_2, 15, 4, 4, 2)  
 self.label\_17 = QtWidgets.QLabel(self.centralwidget)  
 font = QtGui.QFont()  
 font.setPointSize(15)  
 self.label\_17.setFont(font)  
 self.label\_17.setObjectName(**"label\_17"**)  
 self.gridLayout\_11.addWidget(self.label\_17, 16, 1, 2, 1)  
 form.setCentralWidget(self.centralwidget)  
 self.statusbar = QtWidgets.QStatusBar(form)  
 self.statusbar.setObjectName(**"statusbar"**)  
 form.setStatusBar(self.statusbar)  
  
 self.retranslateUi(form)  
 QtCore.QMetaObject.connectSlotsByName(form)  
  
 self.pushButton.clicked.connect(lambda: funcs.pqse\_gen(self))  
  
 \_\_open\_number\_s = 0  
 \_\_secret\_number\_e = 0  
  
 @property  
 def open\_number\_s(self):  
 return self.\_\_open\_number\_s  
  
 @open\_number\_s.setter  
 def open\_number\_s(self, value):  
 self.\_\_open\_number\_s = value  
  
 @property  
 def open\_number\_e(self):  
 return self.\_\_open\_number\_e  
  
 @open\_number\_e.setter  
 def open\_number\_e(self, value):  
 self.\_\_open\_number\_e = value  
  
 def retranslateUi(self, form):  
 \_translate = QtCore.QCoreApplication.translate  
 form.setWindowTitle(\_translate(**"form"**, **"MainWindow"**))  
 self.pushButton\_3.setText(\_translate(**"form"**, **"Зашифровать и отправить пользотелю Б"**))  
 self.label.setText(\_translate(**"form"**, **"ЛР\_№2. Алгоритм RSA. Вариант 7; N = 28"**))  
 self.label\_2.setText(\_translate(**"form"**, **"1)P:"**))  
 self.label\_5.setText(\_translate(**"form"**, **"3)s(public):"**))  
 self.label\_10.setText(\_translate(**"form"**, **"P\*Q(public):"**))  
 self.pushButton.setText(\_translate(**"form"**, **"Сгенерировать P и Q**\n**"  
 "Вычислить s и e"**))  
 self.pushButton\_2.setText(\_translate(**"form"**, **"Сохранить e(private) и**\n**"  
 "отправить (d, P\*Q)(public)"**))  
 self.label\_9.setText(\_translate(**"form"**, **"2)d = (P-1)\*(Q-1):"**))  
 self.label\_12.setText(\_translate(**"form"**, **"Владелец(Пользователь Б)"**))  
 self.label\_15.setText(\_translate(**"form"**, **"P\*Q(public):"**))  
 self.label\_13.setText(\_translate(**"form"**, **"e (private):"**))  
 self.label\_4.setText(\_translate(**"form"**, **"4)e (private):"**))  
 self.label\_3.setText(\_translate(**"form"**, **"1)Q:"**))  
 self.label\_14.setText(\_translate(**"form"**, **"Текст для шифрования и передачи:"**))  
 self.label\_6.setText(\_translate(**"form"**, **"s(public):"**))  
 self.label\_7.setText(\_translate(**"form"**, **"(вывод для наглядности)"**))  
 self.label\_11.setText(\_translate(**"form"**, **"Получатель(Пользователь А)"**))  
 self.label\_16.setText(\_translate(**"form"**, **"Расшифрованный текст:"**))  
 self.label\_8.setText(\_translate(**"form"**, **"2)P\*Q:"**))  
 self.label\_17.setText(\_translate(**"form"**, **"Шифротекст:"**))  
  
  
class MyWidget(QMainWindow, Ui\_form):  
 def \_\_init\_\_(self):  
 super(MyWidget, self).\_\_init\_\_()  
  
 self.setupUi(self)  
 self.setWindowTitle(**'FirstWindow'**)  
  
 self.pushButton\_2.clicked.connect(self.show\_window\_2)  
 self.pushButton\_3.clicked.connect(self.show\_window\_3)  
  
 def show\_window\_2(self):  
 if MyWidget.check\_const\_flag(self):  
 msg = QtWidgets.QMessageBox()  
 msg.setIcon(QtWidgets.QMessageBox.Critical)  
 msg.setText(**"Сначала необходимо сгенерировать P и Q!"**)  
 msg.setWindowTitle(**"Error"**)  
 msg.exec\_()  
 else:  
 funcs.prepare\_encryption(self)  
  
 def show\_window\_3(self):  
 if MyWidget.check\_const\_flag\_2(self) or self.textForRSA.toPlainText() == **""**:  
 msg = QtWidgets.QMessageBox()  
 msg.setIcon(QtWidgets.QMessageBox.Critical)  
 if MyWidget.check\_const\_flag(self):  
 msg.setText(**"Сначала необходимо сгенерировать P и Q!"**)  
 else:  
 msg.setText(**"Сначала необходимо отправить данные!"**)  
 if self.textForRSA.toPlainText() == **""**:  
 msg.setText(**"Сначала необходимо ввести текст!"**)  
 msg.setWindowTitle(**"Error"**)  
 msg.exec\_()  
 else:  
 funcs.encryption\_decryption(self)  
  
 def check\_const\_flag(self):  
 if self.const\_flag == 0:  
 return 1  
 else:  
 return 0  
  
 def check\_const\_flag\_2(self):  
 if self.const\_flag\_2 == 0:  
 return 1  
 else:  
 return 0  
  
 \_\_const\_flag = 0  
 \_\_const\_flag\_2 = 0  
  
 @property  
 def const\_flag(self):  
 return self.\_\_const\_flag  
  
 @const\_flag.setter  
 def const\_flag(self, value):  
 self.\_\_const\_flag = value  
  
 @property  
 def const\_flag\_2(self):  
 return self.\_\_const\_flag\_2  
  
 @const\_flag\_2.setter  
 def const\_flag\_2(self, value):  
 self.\_\_const\_flag\_2 = value  
  
  
if \_\_name\_\_ == **"\_\_main\_\_"**:  
 import sys  
  
 app = QtWidgets.QApplication(sys.argv)  
 ex = MyWidget()  
 ex.show()  
 sys.exit(app.exec\_())

Листинг 2 –файл funcs.py

import sympy  
import math  
import random  
  
  
def pqse\_gen(self):  
 i = sympy.randprime(40000000000000, 90000000000000)  
 self.lineEdit\_p.setText(str(i))  
  
 i = sympy.randprime(40000000000000, 90000000000000)  
 self.lineEdit\_q.setText(str(i))  
  
 self.lineEdit\_pq.setText(str(int(self.lineEdit\_p.text()) \* int(self.lineEdit\_q.text())))  
 self.lineEdit\_d.setText(str((int(self.lineEdit\_p.text()) - 1) \* (int(self.lineEdit\_q.text()) - 1)))  
  
 self.open\_number\_s = sympy.randprime(40000000000000, int(self.lineEdit\_d.text()))  
 self.lineEdit\_s.setText(str(self.open\_number\_s))  
  
 e = ex\_gcd\_recursive(int(self.lineEdit\_s.text()), int(self.lineEdit\_d.text()))[0]  
 if e < 0:  
 e = -e  
 self.lineEdit\_e.setPlaceholderText(str(e))  
  
 self.const\_flag = 1  
  
  
def prepare\_encryption(self):  
 self.lineEdit\_s\_A.setText(self.lineEdit\_s.text())  
 self.lineEdit\_pq\_A.setText(self.lineEdit\_pq.text())  
 self.lineEdit\_e\_B.setPlaceholderText(self.lineEdit\_e.placeholderText())  
 self.lineEdit\_pq\_B.setText(self.lineEdit\_pq.text())  
  
 *# self.lineEdit\_p.setText("")  
 # self.lineEdit\_q.setText("")  
 # self.lineEdit\_s.setText("")  
 # self.lineEdit\_d.setText("")  
 # self.lineEdit\_e.setPlaceholderText("")  
 # self.lineEdit\_pq.setText("")* self.const\_flag = 0  
 self.const\_flag\_2 = 1  
  
  
def encryption\_decryption(self):  
 *# Зашифровывание текста открытым ключом* encoded\_ascii\_message = **""** for char in self.textForRSA.toPlainText().encode(**"unicode-escape"**):  
 encoded\_ascii\_message += str(char)  
  
 print(**"Сообщение в ascii-формате: {0}"**.format(encoded\_ascii\_message))  
  
 encoded\_message = []  
  
 while len(encoded\_ascii\_message) > 0:  
  
 if len(encoded\_ascii\_message) > 20:  
 block\_size = random.randint(1, 20)  
 else:  
 block\_size = len(encoded\_ascii\_message)  
  
 temp\_str = encoded\_ascii\_message[0:block\_size]  
 encoded\_ascii\_message = encoded\_ascii\_message[block\_size:len(encoded\_ascii\_message)]  
  
 i = 0  
 while len(encoded\_ascii\_message) - i:  
 if encoded\_ascii\_message[i] != **'0'**:  
 break  
 else:  
 temp\_str = temp\_str + encoded\_ascii\_message[i]  
 i += 1  
  
 encoded\_message.append(pow(int(temp\_str), int(self.lineEdit\_s\_A.text()), int(self.lineEdit\_pq\_A.text())))  
  
 self.textEdit.setText(str(encoded\_message).replace(**"["**, **""**).replace(**"]"**, **""**).replace(**","**, **""**).replace(**" "**, **""**))  
 print(**"Зашифрованное ascii-сообщение(Шифр RSA): {0}; len - {1}"**.format(encoded\_message, len(self.textEdit.toPlainText())))  
  
 *# Расшифровывание текста закрытым ключом* decoded\_ascii\_message = **""** for i in range(0, len(encoded\_message)):  
 decoded\_ascii\_message += str(pow(encoded\_message[i], int(self.lineEdit\_e\_B.placeholderText()),  
 int(self.lineEdit\_pq\_B.text())))  
  
 print(**"Расшифрованное ascii-сообщение(Шифр RSA): {0}; len - {1}"**.format(decoded\_ascii\_message, len(decoded\_ascii\_message)))  
  
 decoded\_message = ascii\_to\_string(decoded\_ascii\_message)  
 self.textEdit\_2.setText(decoded\_message)  
 print(decoded\_message.encode().decode(**"unicode-escape"**) + **"**\n\n**"**)  
  
 self.const\_flag = 0  
  
  
def ex\_gcd\_recursive(a, b):  
 if not b:  
 return 1, 0, a  
 y, x, g = ex\_gcd\_recursive(b, a % b)  
 return x, y - (a // b) \* x, g  
  
  
def ascii\_to\_string(ascii\_text):  
 text = **u""** i = 0  
 while i < len(ascii\_text):  
 if ascii\_text[i] == **'1'**:  
 chars = ascii\_text[i:i+3]  
 text += chr(int(chars))  
 i += 3  
 else:  
 chars = ascii\_text[i:i+2]  
 text += chr(int(chars))  
 i += 2  
  
 return text

1. Примеры выполнения алгоритма и работы с интерфейсом:

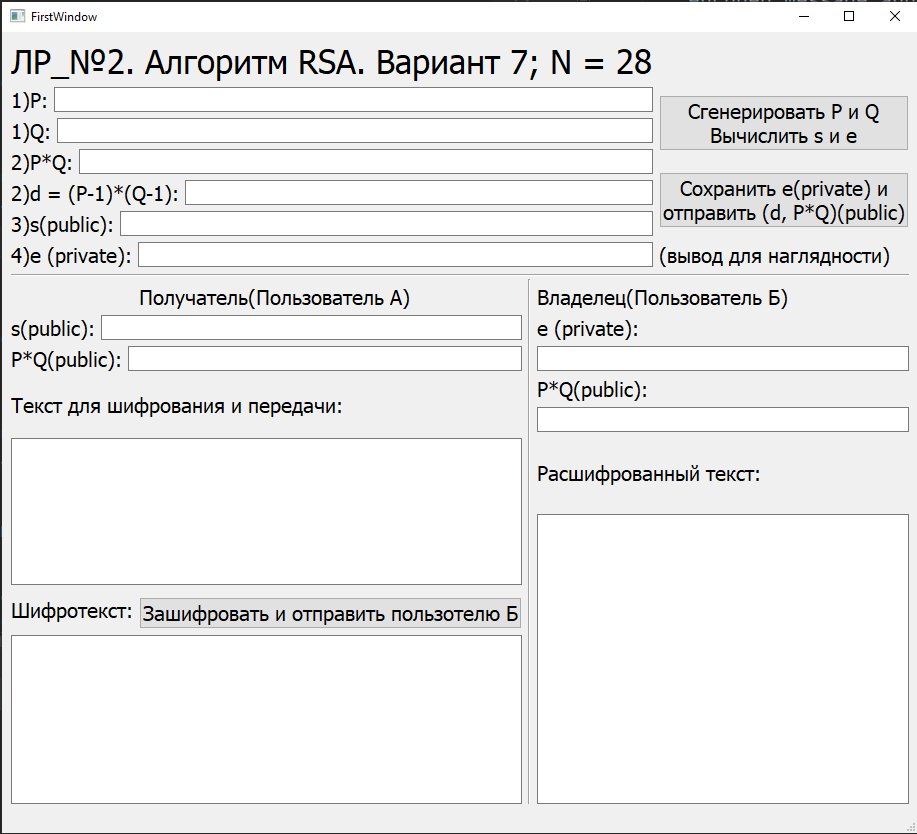


Рисунок 1 – Внешний вид окна интерфейса

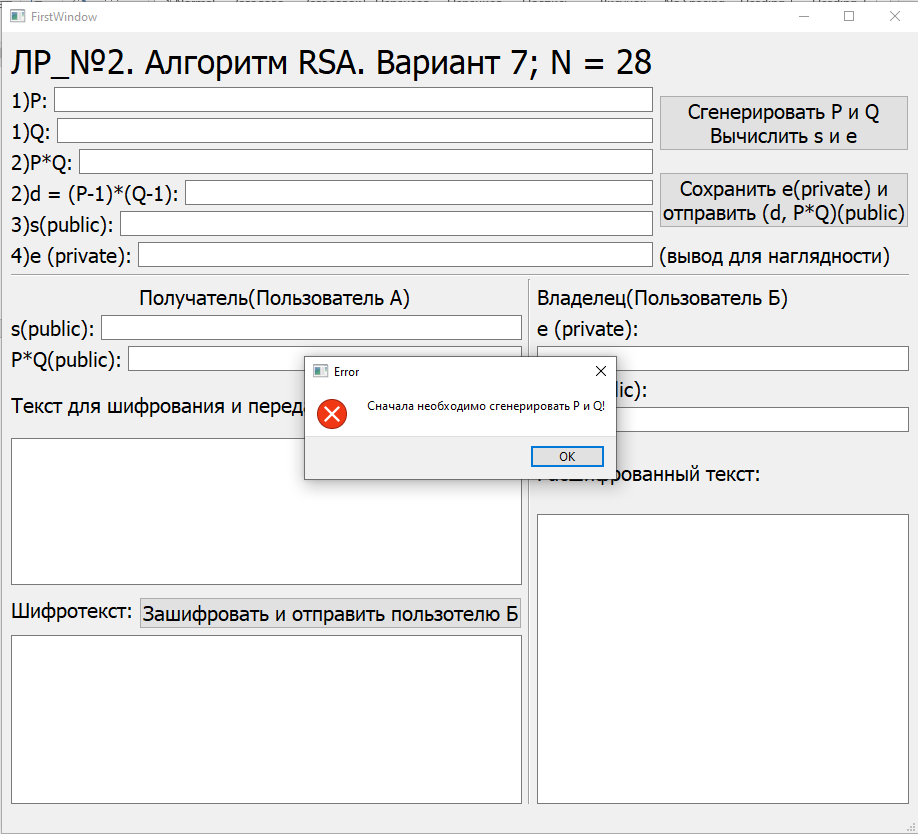


Рисунок 2 – ошибка 1

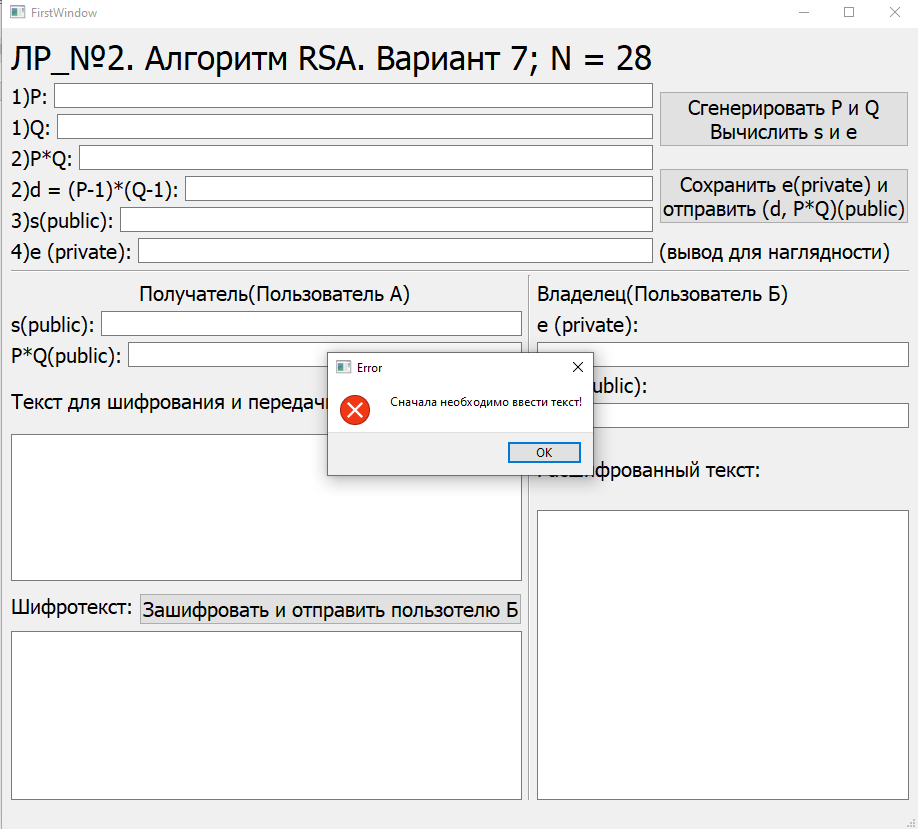


Рисунок 3 – ошибка 2

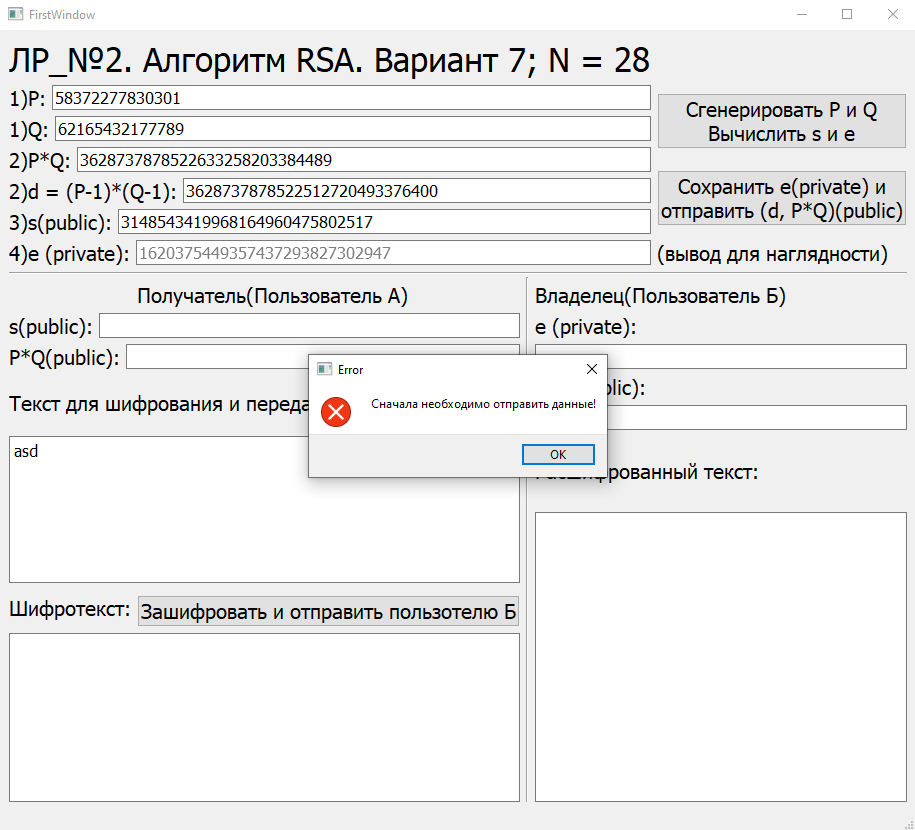


Рисунок 4 – ошибка 3

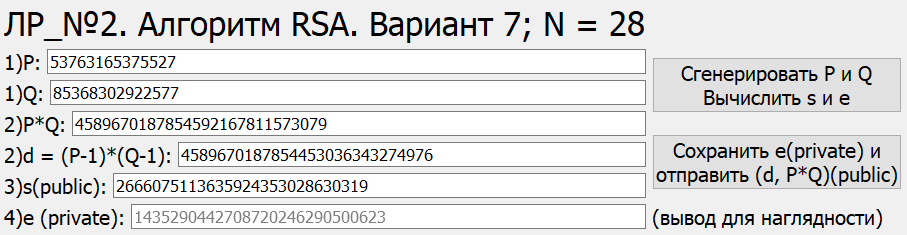


Рисунок 5 – пример генерации чисел P и Q

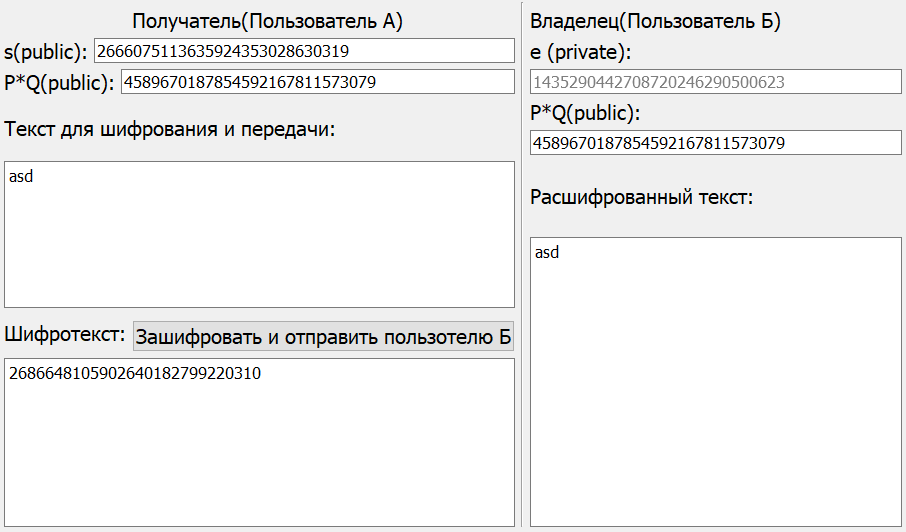


Рисунок 6 – просто пример работы программы

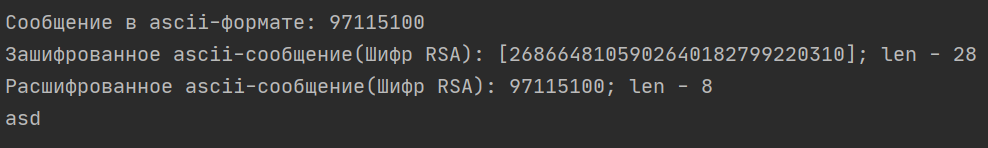


Рисунок 7 – более подробный вывод в консоль

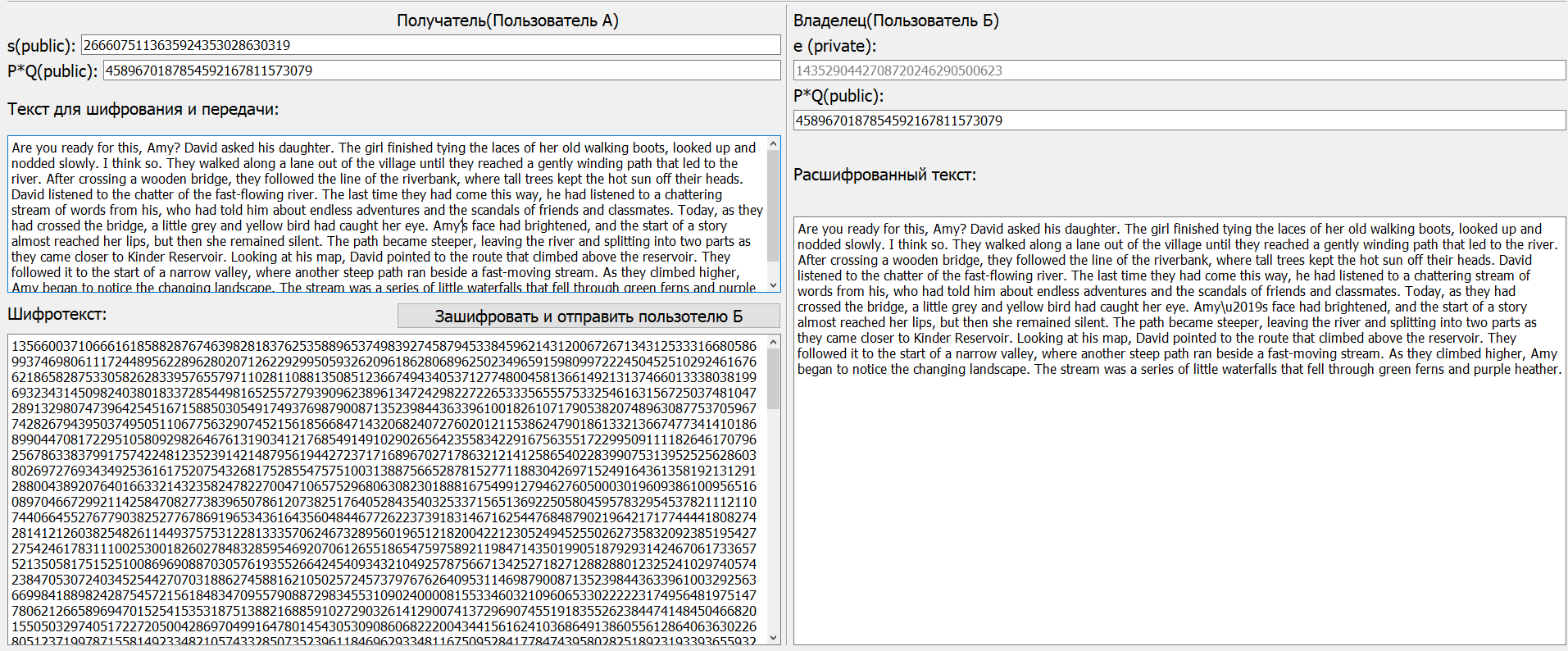


Рисунок 8 – пример работы с текстом 1

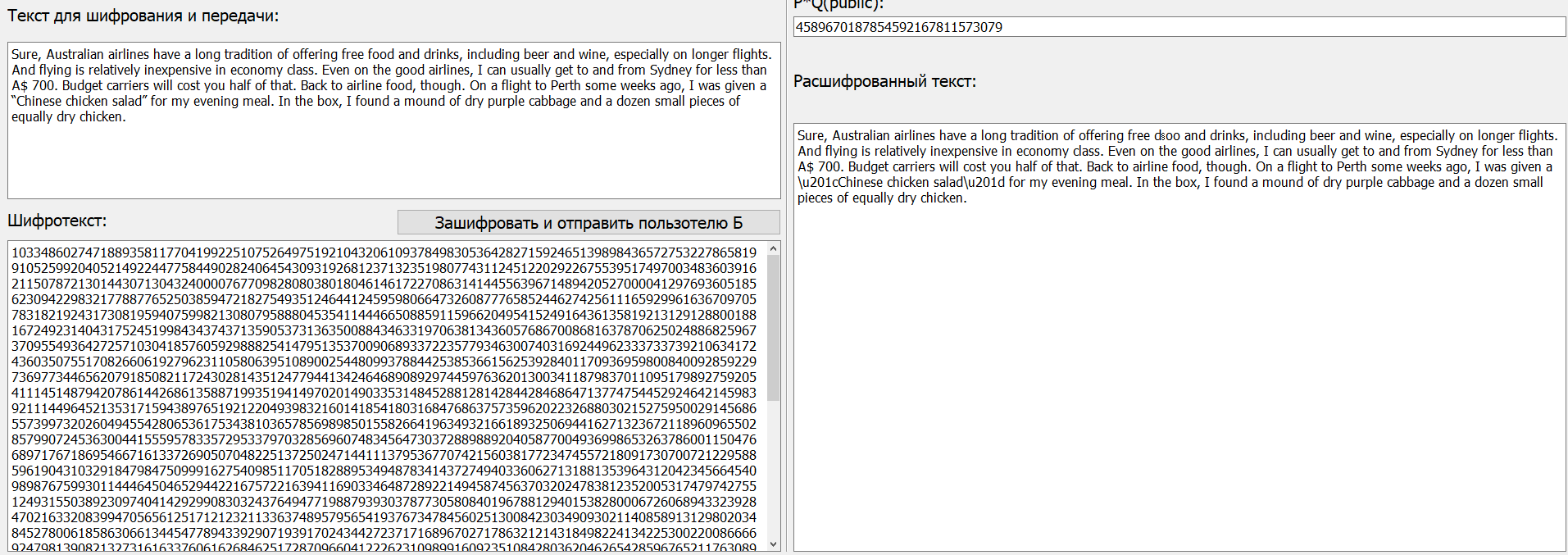


Рисунок 9 – пример работы с текстом 2

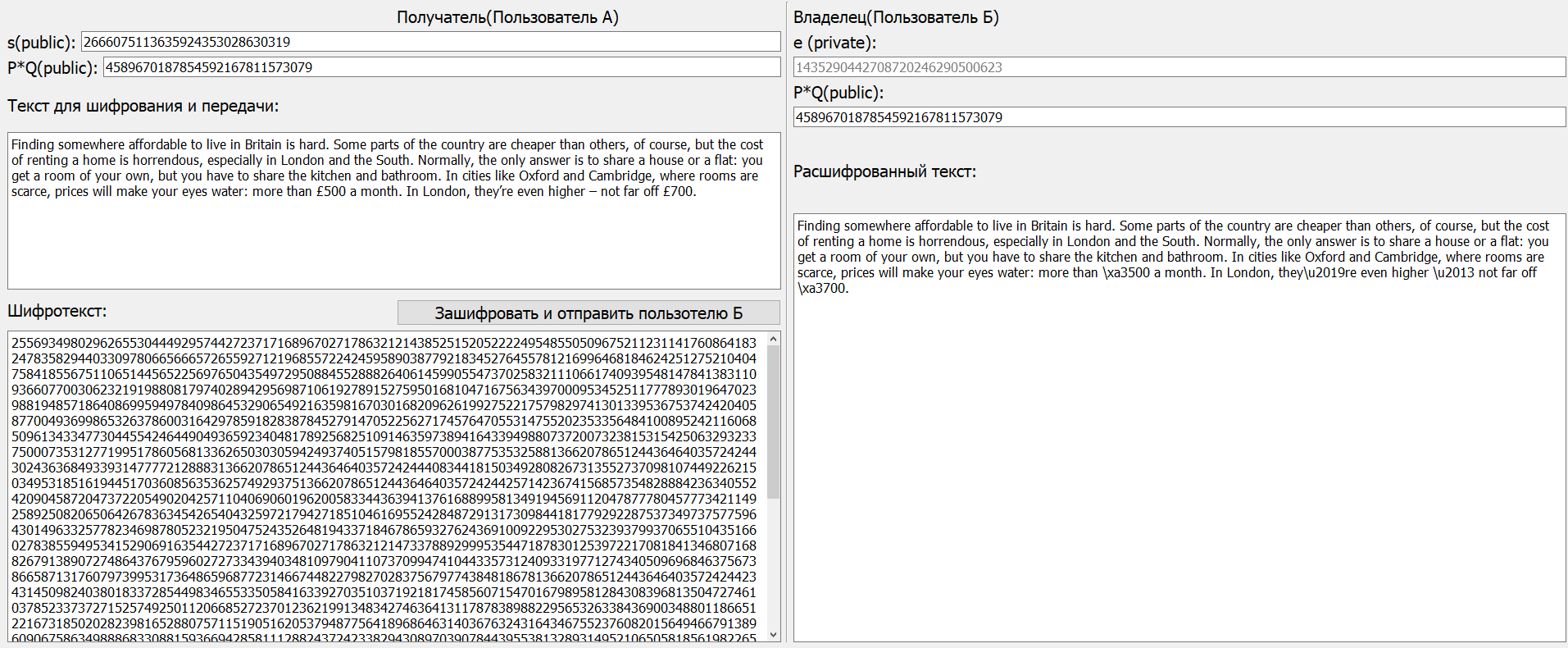


Рисунок 10 - пример работы с текстом 3

Так как алгоритмы разрабатывались на языке python, а графический интерфейс генерировался с помощью QT Designer и крепился к функциям шифрования с помощью библиотеки для python “pyqt5-tools”, то мне не удалось корректно вывести символы юникода на графический интерфейс, однако в консоль выводилось правильно.

# Вывод

Оценка криптостойкости: как было сказано ранее, для гарантирования криптостойкости алгоритма RSA необходимо как минимум 1024 значащих двоичных знака в записи числа N, однако в моем случае N имеет только 28 значащих десятичных знаков или 90 - 94 значащих двоичных знаков, так что моя реализация не гарантирует криптостойкости.

Оценка производительности: так как числа относительно не большие и благодаря использованию уместных функций python, удалось реализовать алгоритм, который работает менее чем за секунду даже для объёма информации в 10000 символов.

В ходе выполнения данной практической работы были изучены основы ассиметричного шифрования, в частности реализован алгоритм RSA.