Федеральное государственное автономное

образовательное учреждение

высшего профессионального образования

«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт космических и информационных технологий

институт

Прикладная математика и компьютерная безопасность

кафедра

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ 6**

по Криптографические методы защиты информации

наименование дисциплины

Шифр Ришелье

тема

Преподаватель В.И. Вайнштейн

подпись**,** дата инициалы, фамилия

Студент КИ17-01, 031722011 К.А. Василенко

номер группы, зачетной книжки подпись**,** дата инициалы, фамилия

Красноярск 2021

# ВВЕДЕНИЕ

Цель работы: реализовать шифр Ришелье (шифрование и расшифрование) на любом языке программирования. Предусмотреть графический интерфейс.

Задачи:

1. реализовать программно шифр Ришелье, предусматривая графический интерфейс;
2. провести тесты на работоспособность программы;
3. сделать отчёт о проделанной работе.

**Реализация шифра**

1. **Описание шифра**

Шифр Ришелье, как метод защиты информации основан на применении решётки Кардано. Это металлический лист, с прорезанными в нём в случайном порядке прямоугольными окнами высотой, равной величине строки и длиной в произвольное количество символов.

Для написания сообщения лист с решёткой Кардано накладывался на лист бумаги, и в окна вписывался текст, содержащий закодированную информацию. Далее сетка убиралась и в промежутки между текстом документа вписывались произвольные слова или набор букв, имеющие цель запутать того, для кого сообщения не было предназначено.

Дополнительное кодирование

Основной текст тоже кодировался следующим образом:

* Составлялся некий код, например (4213) (32514) (312) (132);
* Буквы в сообщении разбивались на группы по количеству символов в группах кода;
* В каждой группе буквы переставлялись в порядке, указанном цифрами.

1. **Программная реализация**

Программа написана на языке Python с использованием библиотеки PyQt5 и Qt designer для отрисовки графического интерфейса.

1. **Листинг с описанием основного алгоритма программы**

**richelieu.py**

**from** PyQt5 **import** QtWidgets  
*#text = "Криптография"  
#key = "(3, 1, 2)(1, 2, 1)"***def** codingRichelieu(text, key, flag):  
 **if not** text **or not** key:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Введите текст!"**)  
 msgBox.exec\_()  
 **return** (**""**)  
 **for** i **in** key:  
 **for** j **in** range(len(i)):  
 **if** int(i[j]) < 1 **or** int(i[j]) > len(i) **or** len(i) != len(set(i)):  
 print(**'len'**, len(i))  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Ошибка в ключе!!"**)  
 msgBox.exec\_()  
 **return** (**""**)  
 lenText = len(text)  
 **if** flag == 1:  
 res = **""  
 for** i **in** range(len(key)):  
 text1 = text[:len(key[i])]  
 print(**'text1'**, text1)  
 **for** j **in** range(len(key[i])):  
 res+=text1[int(key[i][j]) - 1]  
 text = text[len(key[i]):]  
 print(**'text'**, text)  
 **if** len(res) != lenText:  
 res+=text  
 print(**'res'**, res)  
 **else**:  
 print(**'key'**, key)  
 print(**'text'**, text)  
 resArray = []  
 **for** i **in** range(len(key)):  
 res1 = []  
 **for** k **in** range(len(key[i])):  
 res1.append(**""**)  
 text1 = text[:len(key[i])]  
 **for** j **in** range(len(key[i])):  
 res1[(int(key[i][j])) - 1] = text1[j]  
 text = text[len(key[i]):]  
 resArray.append(res1)  
 **if** len(resArray) != lenText:  
 resArray.append(text)  
 res = **""  
 for** i **in** range(len(resArray)):  
 **for** j **in** range(len(resArray[i])):  
 res+=resArray[i][j]  
  
 *# except Exception:  
 # print('Error!')  
 # return None* **return** res

1. **Примеры работы программы**

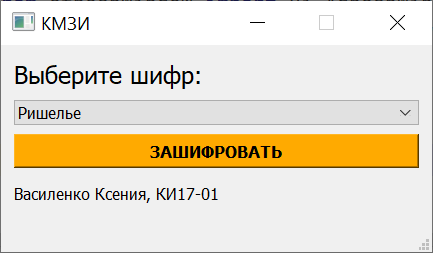


Рисунок 1 – Главное окно.

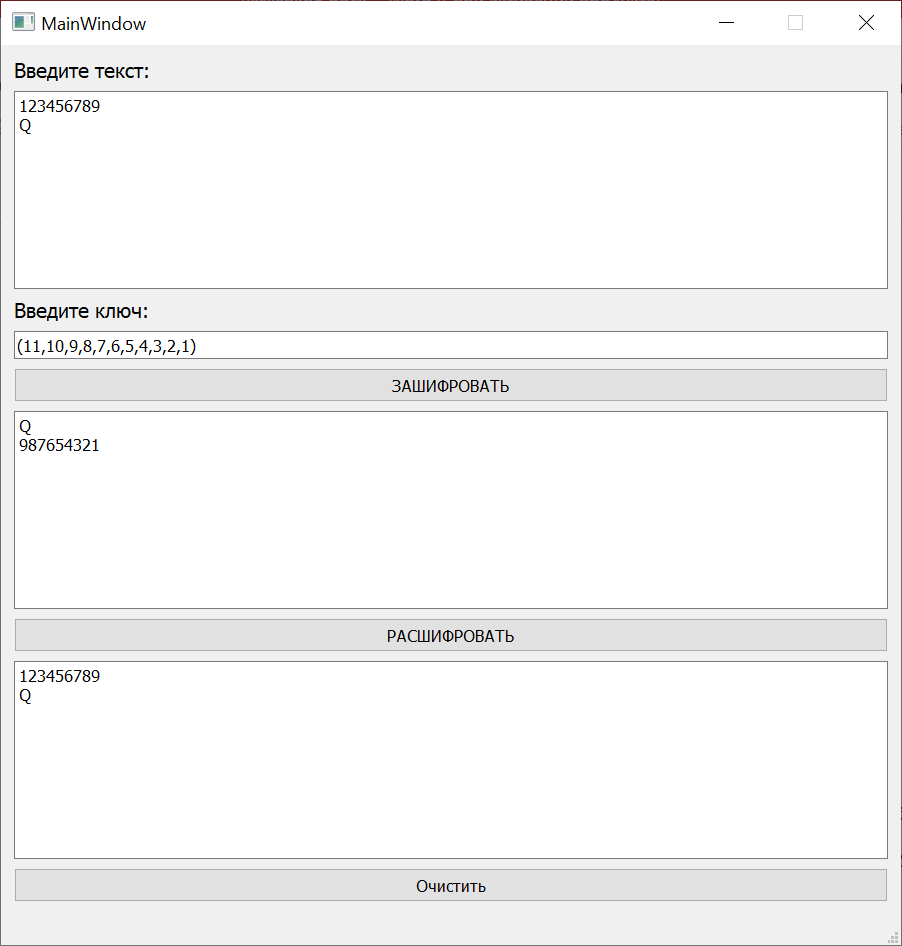


Рисунок 2 – Шифр Ришелье.

# ЗАКЛЮЧЕНИЕ

Во время выполнения лабораторной работы №6 мною был изучен и реализован программно шифр Ришелье, а также предусмотрен графический интерфейс с помощью PyQt5 и Qt designer.