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 8**

по Криптографические методы защиты информации

наименование дисциплины

Шифр Гронсфельда

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 Гронсфельда (шифрование и расшифрование) на любом языке программирования. Предусмотреть графический интерфейс.

Задачи:

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

**Реализация шифра**

1. **Описание шифра**

Шифр Гронсфельда — полиалфавитный подстановочный шифр создан графом Гронсвельдом (руководителем первой дешифровальной службы Германии) в XVII веке. Шифр можно считать усовершенствованием шифра Цезаря (надежность) и Виженера / Бофора (скорость).

Ключ:

Длина ключа (*K*) должна быть равной длине исходного текста. Для этого циклически записывают ключ до тех пор, пока его длина не будет соответствовать длине исходного текста.

Шифрование:

Каждый символ *Mi* открытого текста *M* нужно на *Ki* (соответствующий символ ключа *K*) шагов сдвинуть вправо.  
Или пользуясь таблицей Гронсфельда (*Tx y*, где *x* — номер строки, а *y* — номер столбца и отсчет ведется с нуля):  
каждый символ *Ci* шифротекста *C* находится на пересечении столбца *y*, первый (заголовочный) символ которого равен соответствующему символу открытого текста *Mi*, и *Ki*-й (соответствующей цифры ключа) строки — (*TKi y*).

Расшифрование:

Каждый символ (*Ci*) зашифрованного текста *C* нужно на *Ki* (соответствующий символ ключа *K*) шагов сдвинуть влево.  
Или пользуясь таблицей Гронсфельда (*Tx y*, где *x* — номер строки, а *y* — номер столбца и отсчет ведется с нуля):  
нужно в *Ki* (*i*-ая цифра ключа *K*) строке найти символ, который равен соответствующему символу шифротекста (*TKi y = Ci*), и первый (заголовочный) элемент столбца будет *i*-ый символ открытого текста.



Рисунок 1 – Таблица Гронсфельда.

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**

**gronsfeld.py**

**from** PyQt5 **import** QtWidgets  
**def** codingGronsfeld(text, key, flag):  
 **if not** text **or not** key:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Введите текст!"**)  
 msgBox.exec\_()  
 **return** (**""**)  
  
 dict = **"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZабвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"** key1 = **""** dictNum = **"0123456789"  
  
 for** i **in** key:  
 **if** i **not in** dictNum:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Введите цифры!"**)  
 msgBox.exec\_()  
 **return** (**""**)  
  
 **while** len(key1) != len(text):  
 key1 += key  
 **if** len(key1) > len(text):  
 key1 = key1[:len(text)]  
  
 s = **""** j = 0  
 **for** i **in** text:  
 **if** i **in** dict:  
 s+=dict[(dict.index(i) + flag\*int(key1[j])) % len(dict)]  
 **else**:  
 s+=i  
 j+=1  
 **return** s

1. **Примеры работы программы**

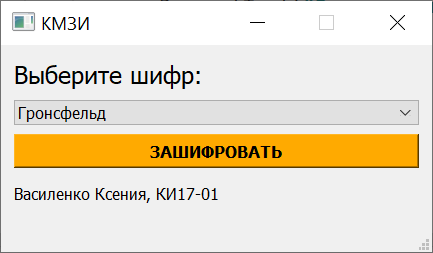


Рисунок 2 – Главное окно.

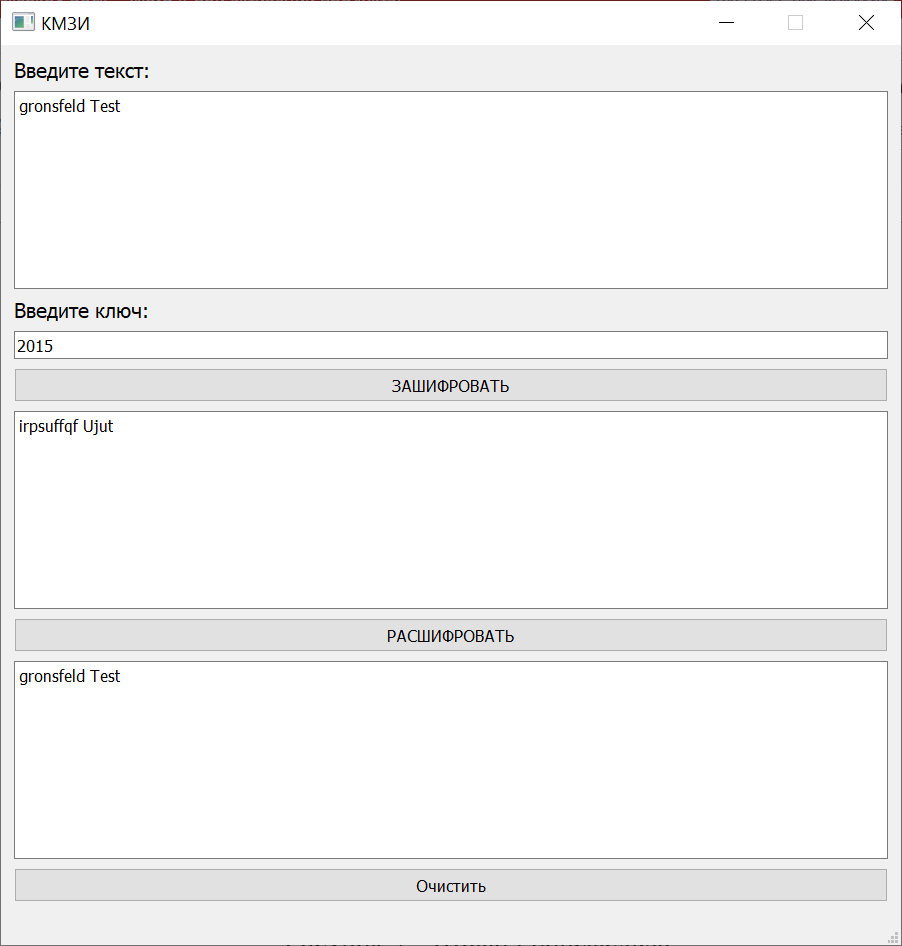


Рисунок 3 – Шифр Гронсфельда.

# ЗАКЛЮЧЕНИЕ

Во время выполнения лабораторной работы №8 мною был изучен и реализован программно шифр Гронсфельда, а также предусмотрен графический интерфейс с помощью PyQt5 и Qt designer.