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 9**

по Криптографические методы защиты информации

наименование дисциплины

Шифр Вижинера

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

Задачи:

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

**Реализация шифра**

1. **Описание шифра**

Шифр Виженера — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

В шифре Цезаря каждая буква алфавита сдвигается на несколько позиций; например в шифре Цезаря при сдвиге +3, A стало бы D, B стало бы E и так далее. Шифр Виженера состоит из последовательности нескольких шифров Цезаря с различными значениями сдвига. Для зашифровывания может использоваться таблица алфавитов, называемая tabula recta или квадрат (таблица) Виженера. Применительно к латинскому алфавиту таблица Виженера составляется из строк по 26 символов, причём каждая следующая строка сдвигается на несколько позиций. Таким образом, в таблице получается 26 различных шифров Цезаря. На каждом этапе шифрования используются различные алфавиты, выбираемые в зависимости от символа ключевого слова.

Расшифровывание производится следующим образом: находим в таблице Виженера строку, соответствующую первому символу ключевого слова; в данной строке находим первый символ зашифрованного текста. Столбец, в котором находится данный символ, соответствует первому символу исходного текста. Следующие символы зашифрованного текста расшифровываются подобным образом.

Если *n*{\displaystyle n} — количество букв в алфавите, {\displaystyle m\_{j}} *mj* — буквы открытого текста, *{\displaystyle k\_{j}}kj* — буквы ключа, то шифрование Виженера можно записать следующим образом:

*cj = (mj + kj) mod n{\displaystyle c\_{j}=(m\_{j}+k\_{j})\mod {n}}*

И расшифровывание:

*cj = (mj + n - kj) mod n*

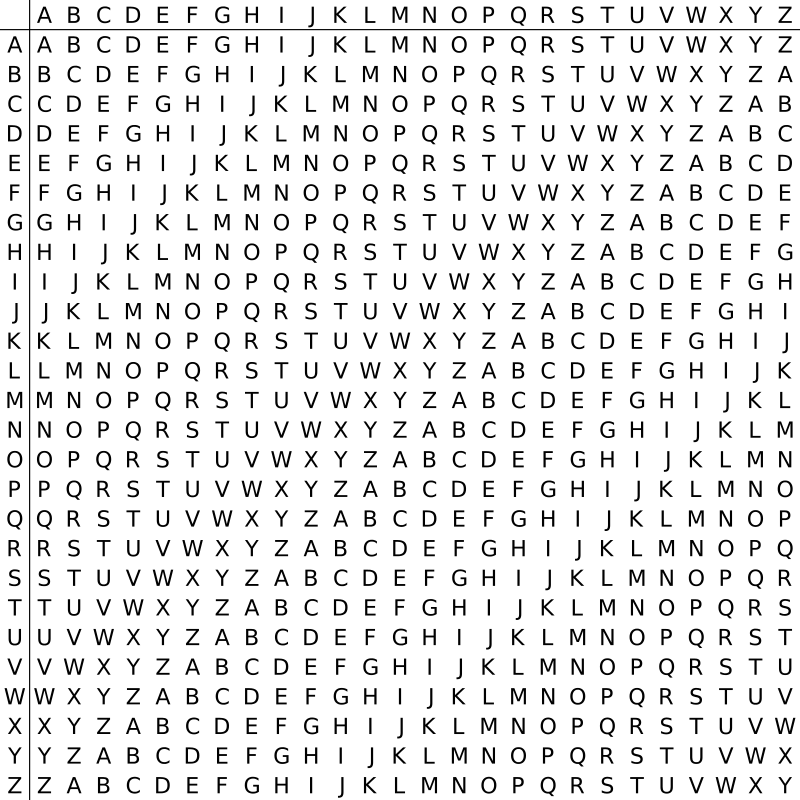
{\displaystyle c\_{j}=(m\_{j}+k\_{j})\mod {n}}{\displaystyle m\_{j}=(c\_{j}+n-k\_{j})\mod {n}}

Рисунок 1 – Таблица Вижинера.

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**

**viginer.py**

**from** PyQt5 **import** QtWidgets  
  
**def** codingViginer(text, key, flag):  
 **global** tmpDict  
 *#на пустоту ввода* **if not** text **or not** key:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Введите текст!"**)  
 msgBox.exec\_()  
 **return** (**""**)  
 dictEngUp = **"ABCDEFGHIJKLMNOPQRSTUVWXYZ"** dictEng = **"abcdefghijklmnopqrstuvwxyz"** dictRusUp = **"АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"** dictRus = **"абвгдеёжзийклмнопрстуфхцчшщъыьэюя"** key1 = **""** *#какой алфавит первый символ из алфавита* **for** i **in** text:  
 **if** i **in** dictEng:  
 tmpDict = dictEng  
 **break  
 elif** i **in** dictEngUp:  
 tmpDict = dictEngUp  
 **break  
 elif** i **in** dictRus:  
 tmpDict = dictRus  
 **break  
 elif** i **in** dictRusUp:  
 tmpDict = dictRusUp  
 **break  
 else**:  
 tmpDict = []  
  
 **for** i **in** text:  
 **if** (i **in** dictRus) **or** (i **in** dictRusUp) **or** (i **in** dictEng) **or** (i **in** dictEngUp):  
 **if** i **not in** tmpDict:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Текст должен быть из одного алфавита!"**)  
 msgBox.exec\_()  
 **return** (**""**)  
  
 **for** i **in** key:  
 **if** (i **in** dictRus) **or** (i **in** dictRusUp) **or** (i **in** dictEng) **or** (i **in** dictEngUp):  
 **if** i **not in** tmpDict:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Алфавит ключа и текста не совпадает!!"**)  
 msgBox.exec\_()  
 **return** (**""**)  
 **else**:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Ключ только из символов!"**)  
 msgBox.exec\_()  
 **return** (**""**)  
  
 *#догоняем ключ до длины текста* **while** len(key1) != len(text):  
 key1 += key  
 **if** len(key1) > len(text):  
 key1 = key1[:len(text)]  
 *#print(key1)* s = **""** j = 0  
 **for** i **in** text:  
 **if** i **in** dictEng:  
 s+=dictEng[(dictEng.index(i) + flag\*dictEng.index(key1[j]))% len(dictEng)]  
 **elif** i **in** dictEngUp:  
 s+=dictEngUp[(dictEngUp.index(i) + flag\*dictEngUp.index(key1[j])) % len(dictEngUp)]  
 **elif** i **in** dictRus:  
 s+=dictRus[(dictRus.index(i) +flag\*dictRus.index(key1[j])) % len(dictRus)]  
 **elif** i **in** dictRusUp:  
 s+=dictRusUp[(dictRusUp.index(i) + flag\*dictRusUp.index(key1[j])) % len(dictRusUp)]  
 **else**:  
 s+=i  
 j+=1  
 **return** s

1. **Примеры работы программы**

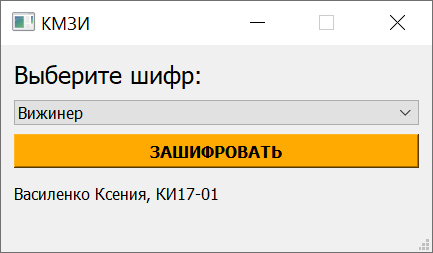


Рисунок 2 – Главное окно.

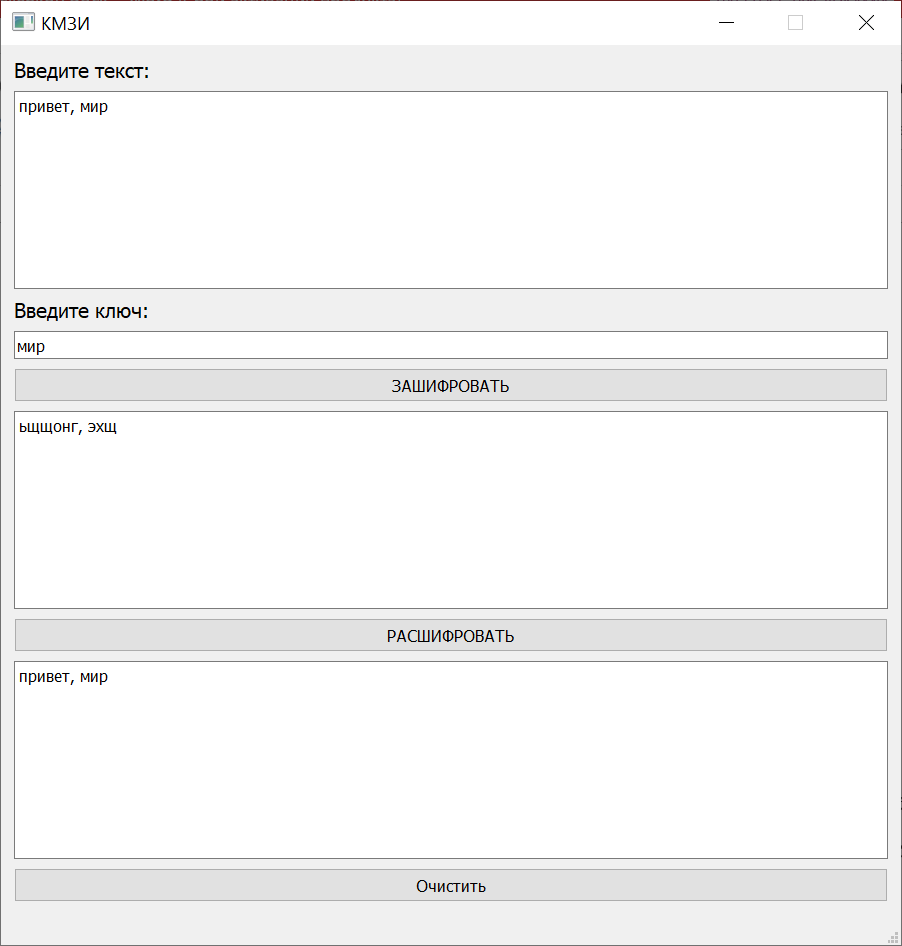


Рисунок 3 – Шифр Вижинера.

# ЗАКЛЮЧЕНИЕ

Во время выполнения лабораторной работы №9 мною был изучен и реализован программно шифр Вижинера, а также предусмотрен графический интерфейс с помощью PyQt5 и Qt designer.