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 7**

по Криптографические методы защиты информации

наименование дисциплины

Диск Альберти

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 «диск Альберти» (шифрование и расшифрование) на любом языке программирования. Предусмотреть графический интерфейс.

Задачи:

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

**Реализация шифра**

1. **Описание шифра**

«Диск Альберти» состоял из двух дисков — внешнего неподвижного (на нём были нанесены латинские буквы в алфавитном порядке и цифры 1, 2, 3, 4) и подвижного внутреннего диска, на котором буквы были переставлены. Диски крепились на одной оси так, чтобы внутренний мог вращаться. Окружность каждого диска разделена на 24 равные клетки. Скольжение алфавитов находится под контролем ключевых букв, включённых в тело криптограммы. Для того, чтобы расшифровать сообщение, написанное с использованием дисков Альберти вы должны были иметь соответствующий алфавит на ваш внутренний диск.

Принцип построения этого шифра заключается в следующем: для шифрования используются не один как в простой замене, а несколько шифралфавитов. Процесс шифрования заключался в нахождении буквы открытого текста на внешнем диске и замене её на букву с внутреннего диска, стоящую под ней. После этого внутренний диск сдвигался на одну позицию и шифрование второй буквы производилось уже по новому шифралфавиту.

Ключом данного шифра являлся порядок расположения букв на внутреннем диске и его начальное положение относительно внешнего диска.

Одно ключевое слово используется для формирования перестановки алфавита, другое ключевое слово используется, чтобы определить последовательность для нескольких алфавитов. Это техника, которая была названа «двойной шифр» была более точно описана как многоалфавитная.

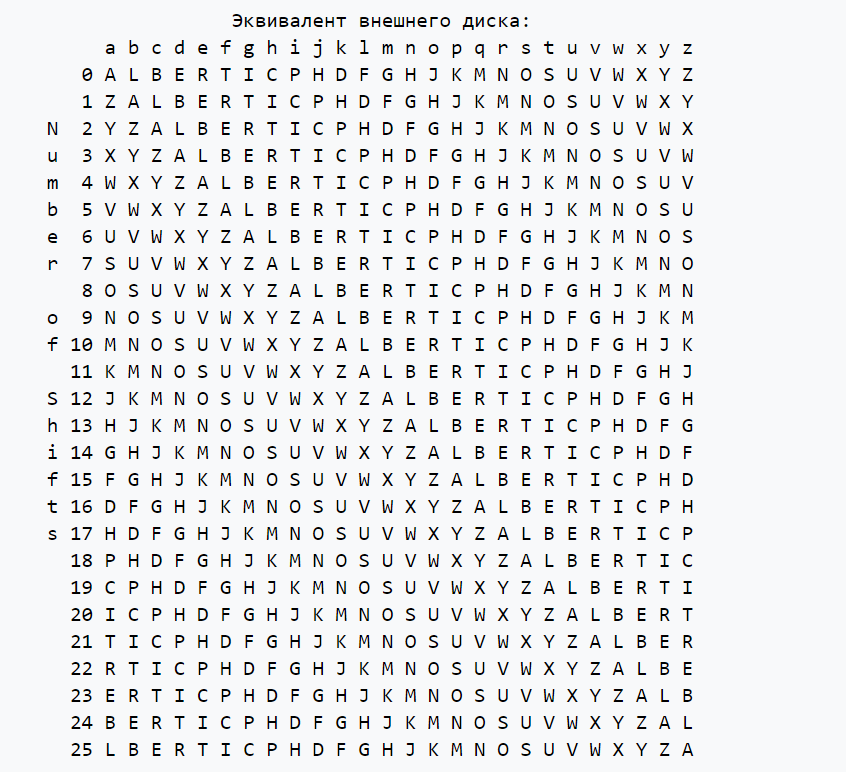


Рисунок 1 – Эквивалент внешнего диска.

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**

**alberti.py**

**from** PyQt5 **import** QtWidgets  
  
**def** codingAlberti(text, key, keyToShifr, flag):  
 *#на пустоту* **if not** text **or not** key **or not** keyToShifr:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Введите текст!"**)  
 msgBox.exec\_()  
 **return** (**""**)  
 *#dictSymb = " `~!@#№$;%^:?\*&()-+=\_,./1234567890"  
 #keyToShifr = "ALBERTICIPHER"* dict = **"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyzабвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"** tabl = **"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyzабвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ"** keyToShifr = keyToShifr[::-1]  
 **for** i **in** keyToShifr:  
 **if** i **not in** dict:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Введите текст!"**)  
 msgBox.exec\_()  
 **return** (**""**)  
 **else**:  
 tabl = tabl[:tabl.rfind(i)] + tabl[tabl.rfind(i)+1:]  
 tabl = i + tabl  
 *#print(tabl)* key1 = **""  
  
 for** i **in** key:  
 **if** i **not in** dict:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Введите текст из алфавита!"**)  
 msgBox.exec\_()  
 **return** (**""**)  
  
 *#догоняем ключ до длины текста и оставляем символы не из словаря* j = 0  
 **for** i **in** text:  
 **if** i **not in** dict **or** (ord(i) <= 13 **and** ord(i) >= 0):  
 key1 += i  
 **else**:  
 key1 += key[j]  
 j+=1  
 **if** j == len(key):  
 j = 0  
 *#print(key1)* s = []  
 **for** i **in** key1:  
 *#if dict.rfind(i) != -1:* s.append(dict.rfind(i))  
 *#print(s)* res = **""  
 for** i **in** range(len(text)):  
 **if** text[i] **in** dict:  
 **if** flag == 1:  
 res += tabl[(dict.rfind(text[i]) - s[i] - 1)% len(dict)]  
 **else**:  
 res += dict[(tabl.rfind(text[i]) + s[i] + 1)% len(dict)]  
 **else**:  
 res += text[i]  
  
 *# j = 0  
 # for i in text:  
 # if i in dict:  
 # res+=tabl[(dict.index(i) - int(s[j])-1) % len(dict)]  
 # j+=1  
 # else:  
 # res+=i* **return** res

1. **Примеры работы программы**

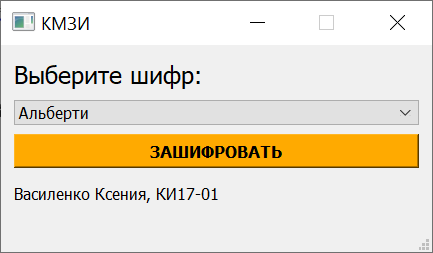


Рисунок 2 – Главное окно.

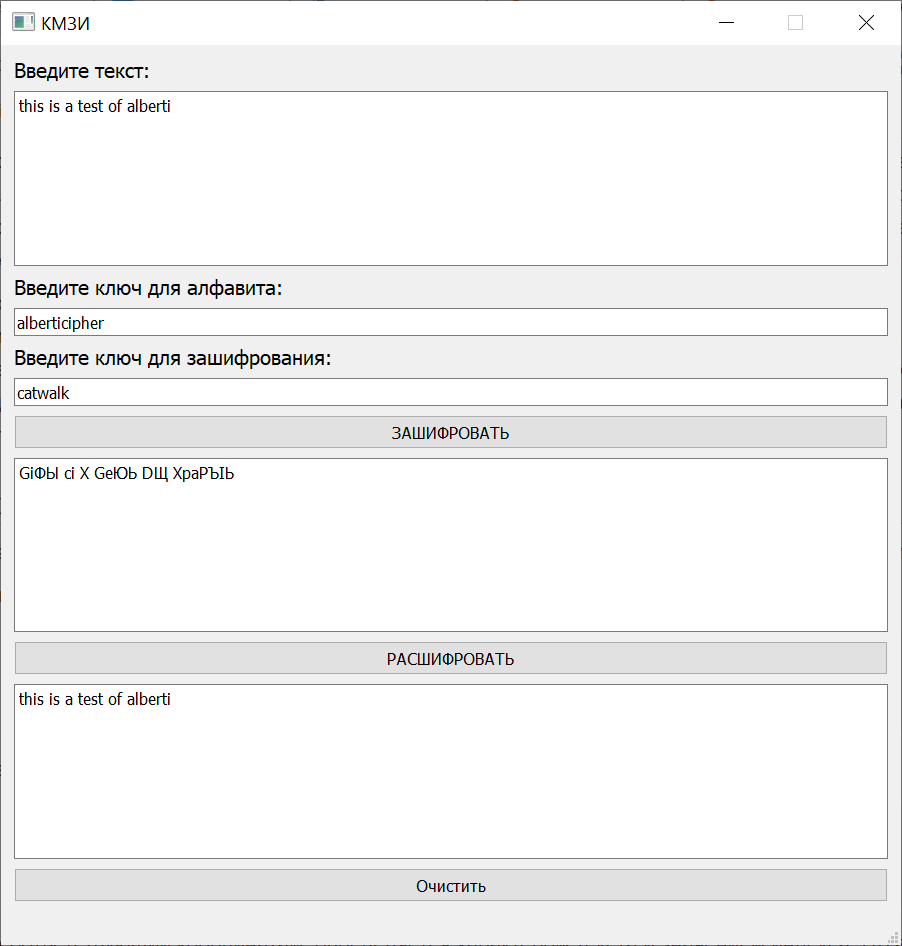


Рисунок 3 – Шифр «диск Альберти».

# ЗАКЛЮЧЕНИЕ

Во время выполнения лабораторной работы №7 мною был изучен и реализован программно шифр «диск Альберти», а также предусмотрен графический интерфейс с помощью PyQt5 и Qt designer.