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 2**

по Криптографические методы защиты информации

наименование дисциплины

Шифр Сцитала

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

Задачи:

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

**Реализация шифра**

1. **Описание шифра**

Для шифрования сообщения использовались пергаментная лента и палочка цилиндрической формы с фиксированными длиной и диаметром. Пергаментная лента наматывалась на палочку так, чтобы не было ни просветов, ни нахлёстов. Написание сообщения производилось по намотанной пергаментной ленте по длинной стороне цилиндра. После того, как достигался конец намотанной ленты, палочка поворачивалась на часть оборота и написание сообщения продолжалось. После разматывания ленты на ней оказывалось зашифрованное сообщение. Расшифрование выполнялась с использованием палочки таких же типоразмеров.

Сам процесс шифрования заключался в перестановке символов исходного текста в соответствии с длиной окружности палочки.

Получается таблица, у которой есть два параметра: n – количество столбцов, m – количество строк.  Обычно в качестве известного каждой стороне ключа выбирается один из них (часто это m), а второй вычисляется на основе известного и длины сообщения: n = [(k – 1)/m] + 1, где [x] – целая часть числа x, а k – длина сообщения.

Алгоритм шифрования:

1. первые n символов выписываются в первую строку слева направо;
2. следующие n символов выписываем во вторую строчку пока её не заполним и т.д.;
3. если все символы выписаны, а остались незаполненные ячейки, заполняем их пробелами или любыми другими символами по договоренности;
4. если выписаны не все символы, а таблица заполнена, значит, при выборе размеров допущена ошибка;
5. теперь разворачиваем текст по столбцам.

Алгоритм расшифрования:

1. разобьём наш зашифрованный текст по m букв, учитывая пробелы;
2. сначала восстановим первый столбец, для этого первую группу букв запишем в первый столбец сверху вниз;
3. по следующим m символам восстановим второй столбец;
4. после восстановления всех столбцов, можно будет прочитать текст.
5. **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**

**skitala.py**

**from** PyQt5 **import** QtWidgets  
  
**def** codingSkitala(text, m):  
 **if** text == **""**:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Введите текст!"**)  
 msgBox.exec\_()  
 **return** (**""**)  
 **for** i **in** text:  
 **if** i == **"\*"**:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Введите без звёздочек!"**)  
 msgBox.exec\_()  
 **return**(**""**)  
  
 **if** m > len(text):  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Должно быть меньше длины сообщения!"**)  
 msgBox.exec\_()  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Длина сообщения = "** + str(len(text)))  
 msgBox.exec\_()  
 **return** (**""**)  
  
 **if** m == 0:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Не может быть 0!"**)  
 msgBox.exec\_()  
 **return** (**""**)  
  
 n = (len(text) - 1) // m + 1  
 res = **""** m1 = m  
  
 **while** len(text) < m1\*n:  
 text+=**"\*"  
  
 if** n == 1 **or** m == 1:  
 **return** text  
  
 res+=text[0]  
 m = m - 1  
 i = j = 0  
 **while** len(res) != len(text):  
 i+=n  
 i = i % len(text)  
 res+=text[i]  
 m = m - 1  
 **if** m == 0 **and** len(res) != len(text):  
 m = m1  
 j += 1  
 i = j  
 res+=text[i]  
 m = m - 1  
  
 **return** res  
  
**def** decodingSkitala(text, m):  
 **if** text == **""**:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Введите текст!"**)  
 msgBox.exec\_()  
 **return** (**""**)  
 **if** m == 0:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Не может быть 0!"**)  
 msgBox.exec\_()  
 **return** (**""**)  
  
 n = m  
 m = (len(text) - 1) // m + 1  
 res = **""** m1 = m  
  
 **if** m > len(text):  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Должно быть меньше длины сообщения!"**)  
 msgBox.exec\_()  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Длина сообщения = "** + str(len(text)))  
 msgBox.exec\_()  
 **return** (**""**)  
  
 **if** n == 1 **or** m == 1:  
 **return** text  
  
 res+=text[0]  
 m = m - 1  
 i = j = 0  
 **while** len(res) != len(text):  
 i+=n  
 i = i % len(text)  
 res+=text[i]  
 m = m - 1  
 **if** m == 0 **and** len(res) != len(text):  
 m = m1  
 j += 1  
 i = j  
 res+=text[i]  
 m = m - 1  
  
 **return** res

1. **Примеры работы программы**

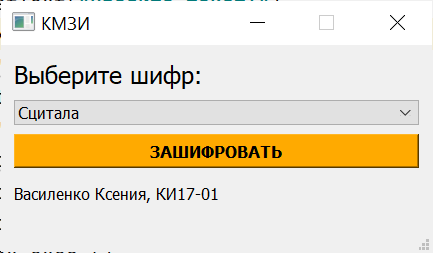


Рисунок 1 – Главное окно.

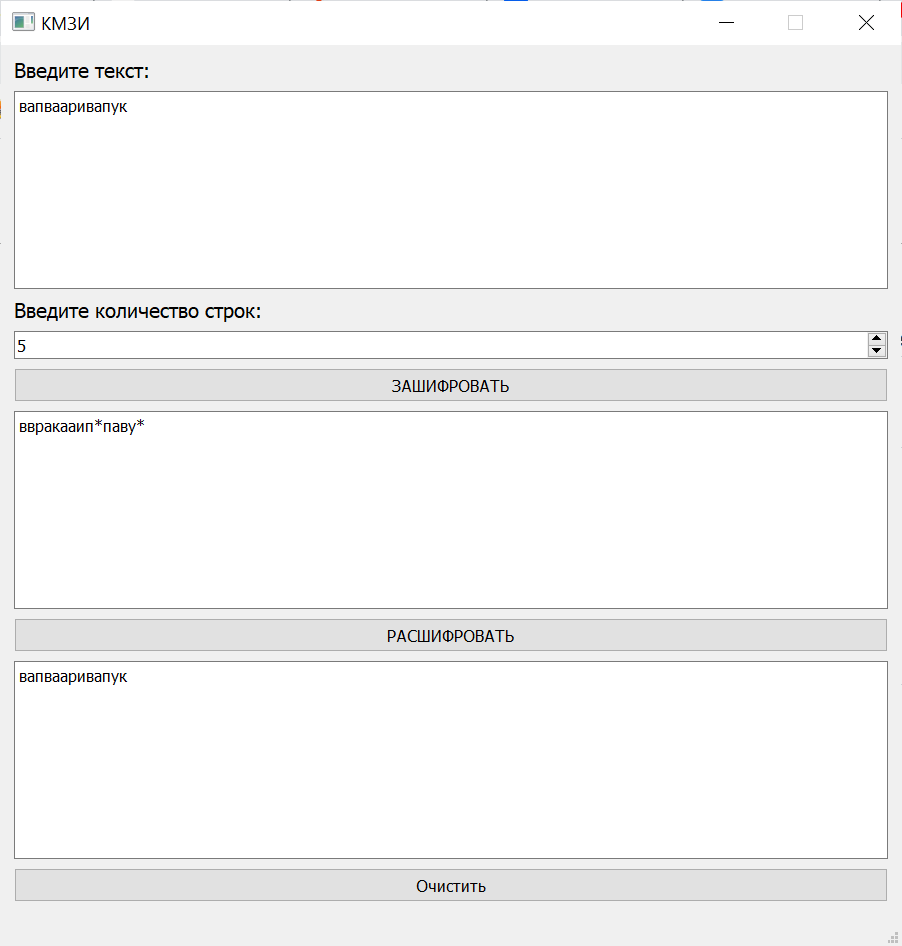


Рисунок 2 – Шифр Сцитала.

# ЗАКЛЮЧЕНИЕ

Во время выполнения лабораторной работы №2 мною был изучен и реализован программно шифр Сцитала, а также предусмотрен графический интерфейс с помощью PyQt5 и Qt designer.