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 10**

по Криптографические методы защиты информации

наименование дисциплины

Шифр Плейфера

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

Задачи:

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

**Реализация шифра**

1. **Описание шифра**

Шифр Плейфера или квадрат Плейфера — ручная симметричная техника шифрования, в которой впервые использована замена биграмм.

Для того чтобы зашифровать сообщение, необходимо разбить его на биграммы (группы из двух символов), например «Hello World» становится «HE LL OW OR LD», и отыскать эти биграммы в таблице. Два символа биграммы соответствуют углам прямоугольника в ключевой матрице. Определяем положения углов этого прямоугольника относительно друг друга. Затем, руководствуясь следующими 4 правилами, зашифровываем пары символов исходного текста:

1. Если два символа биграммы совпадают (или если остался один символ), добавляем после первого символа «Х», зашифровываем новую пару символов и продолжаем. В некоторых вариантах шифра Плейфера вместо «Х» используется «Q».
2. Если символы биграммы исходного текста встречаются в одной строке, то эти символы замещаются на символы, расположенные в ближайших столбцах справа от соответствующих символов. Если символ является последним в строке, то он заменяется на первый символ этой же строки.
3. Если символы биграммы исходного текста встречаются в одном столбце, то они преобразуются в символы того же столбца, находящиеся непосредственно под ними. Если символ является нижним в столбце, то он заменяется на первый символ этого же столбца.
4. Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются на символы, находящиеся в тех же строках, но соответствующие другим углам прямоугольника.

Для расшифровки необходимо использовать инверсию этих четырёх правил, откидывая символы «Х» (или «Q»), если они не несут смысла в исходном сообщении.

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

**playfair.py**

**from** PyQt5 **import** QtWidgets  
**from** math **import** sqrt  
  
#text = "Првиетю каук вп"  
#keyToShifr = "WHEATSON"  
  
**def** find(mtx, symb):  
 **for** i **in** range(len(mtx)):  
 **for** j **in** range(len(mtx[i])):  
 **if** mtx[i][j] == symb:  
 **return** i, j  
  
**def** codingPlayfair(text, keyToShifr):  
 **if not** text **or not** keyToShifr:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle("Ошибка")  
 msgBox.setText("Введите текст!")  
 msgBox.exec\_()  
 **return** ("")  
  
 tabl = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyzабвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ1234567890 \*.,!?();:**\n**+=-\_%"  
  
 **for** i **in** text:  
 **if** i == '\*':  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle("Ошибка")  
 msgBox.setText("Без звёздочки!")  
 msgBox.exec\_()  
 **return** ("")  
  
 # for i in keyToShifr:  
 # if i == '\*':  
 # msgBox = QtWidgets.QMessageBox()  
 # msgBox.setWindowTitle("Ошибка")  
 # msgBox.setText("Без звёздочки!")  
 # msgBox.exec\_()  
 # return ("")  
  
 **for** i **in** text:  
 **if** i **not in** tabl:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle("Ошибка")  
 msgBox.setText("Введите текст!")  
 msgBox.exec\_()  
 **return** ("")  
  
 keyToShifr = keyToShifr[::-1]  
 **for** i **in** keyToShifr:  
 **if** i **not in** tabl:  
 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  
  
 num = int(sqrt(len(tabl)))  
 tablMtx = []  
 **for** j **in** range(len(tabl)//num):  
 tablMtx.append(list(tabl[0:num]))  
 tabl = tabl[num:]  
  
 **for** i **in** range(len(tablMtx)):  
 print(tablMtx[i])  
  
 arrBigr1 = list(text)  
 arrBigr = []  
 **for** i **in** range(1, len(arrBigr1)):  
 **if** arrBigr1[i] == arrBigr1[i - 1]:  
 arrBigr.append(text[i-1])  
 arrBigr.append('\*')  
 **else**:  
 arrBigr.append(text[i-1])  
 arrBigr.append(arrBigr1[len(arrBigr1)-1])  
 print(arrBigr)  
  
 **if** len(arrBigr) % 2 != 0:  
 arrBigr.append("\*")  
  
 arrBigr1 = []  
 tmp = ""  
 **for** i **in** arrBigr:  
 tmp+=i  
 **if** len(tmp) == 2:  
 arrBigr1.append(tmp)  
 tmp = ""  
 print(arrBigr1)  
  
 res = []  
 **for** i **in** range(len(arrBigr1)):  
 tmp = []  
 **for** j **in** range(len(arrBigr1[i])):  
 tmp.append('')  
 res.append(tmp)  
 print(res)  
  
 **for** i **in** range(len(arrBigr1)):  
 indI0, indJ0 = find(tablMtx, arrBigr1[i][0])  
 indI1, indJ1 = find(tablMtx, arrBigr1[i][1])  
 #Если символы биграммы исходного текста встречаются в одной строке,  
 # то эти символы замещаются на символы, расположенные в ближайших столбцах  
 # справа от соответствующих символов. Если символ является последним в строке,  
 # то он заменяется на первый символ этой же строки.  
 **if** indI0 == indI1:  
 **if** indI0 == indI1 **and** indJ0 == num-1:  
 res[i][0] = tablMtx[indI0][0]  
 res[i][1] = tablMtx[indI1][indJ1 + 1]  
 **elif** indI0 == indI1 **and** indJ1 == num-1:  
 res[i][0] = tablMtx[indI0][indJ0 + 1]  
 res[i][1] = tablMtx[indI1][0]  
 **elif** indI0 == indI1 **and** indJ1 == num-1 **and** indJ0 == num-1:  
 res[i][0] = tablMtx[indI0][0]  
 res[i][1] = tablMtx[indI1][0]  
 **else**:  
 res[i][0] = tablMtx[indI0][indJ0+1]  
 res[i][1] = tablMtx[indI1][indJ1+1]  
 #Если символы биграммы исходного текста встречаются в одном столбце,  
 # то они преобразуются в символы того же столбца, находящиеся непосредственно  
 # под ними. Если символ является нижним в столбце, то он заменяется  
 # на первый символ этого же столбца.  
 **if** indJ0 == indJ1:  
 **if** indJ0 == indJ1 **and** indI0 == num-1:  
 res[i][0] = tablMtx[0][indJ0]  
 res[i][1] = tablMtx[indI1 + 1][indJ1]  
 **if** indJ0 == indJ1 **and** indI1 == num-1:  
 res[i][0] = tablMtx[indI0 + 1][indJ0]  
 res[i][1] = tablMtx[0][indJ1]  
 **if** indJ0 == indJ1 **and** indI0 == num-1 **and** indI1 == num-1:  
 res[i][0] = tablMtx[0][indJ0]  
 res[i][1] = tablMtx[0][indJ1]  
 **else**:  
 res[i][0] = tablMtx[indI0 + 1][indJ0]  
 res[i][1] = tablMtx[indI1 + 1][indJ1]  
 #Если символы биграммы исходного текста находятся в разных столбцах и разных  
 # строках, то они заменяются на символы, находящиеся в тех же строках,  
 # но соответствующие другим углам прямоугольника.  
 **if** indI0 != indI1 **and** indJ0 != indJ1:  
 res[i][1] = tablMtx[indI1][indJ0]  
 res[i][0] = tablMtx[indI0][indJ1]  
  
 restext = ""  
 **for** i **in** range(len(res)):  
 **for** j **in** range(len(res[i])):  
 restext+=res[i][j]  
 **return** restext  
  
**def** decodingPlayfair(text, keyToShifr):  
 **if not** text **or not** keyToShifr:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle("Ошибка")  
 msgBox.setText("Введите текст!")  
 msgBox.exec\_()  
 **return** ("")  
  
 tabl = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyzабвгдеёжзийклмнопрстуфхцчшщъыьэюяАБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ1234567890 \*.,!?();:**\n**+=-\_%"  
  
 # for i in keyToShifr:  
 # if i == '\*':  
 # msgBox = QtWidgets.QMessageBox()  
 # msgBox.setWindowTitle("Ошибка")  
 # msgBox.setText("Без звёздочки!")  
 # msgBox.exec\_()  
 # return ("")  
  
 **for** i **in** text:  
 **if** i **not in** tabl:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle("Ошибка")  
 msgBox.setText("Введите текст!")  
 msgBox.exec\_()  
 **return** ("")  
  
 keyToShifr = keyToShifr[::-1]  
 **for** i **in** keyToShifr:  
 **if** i **not in** tabl:  
 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  
  
 num = int(sqrt(len(tabl)))  
 tablMtx = []  
 **for** j **in** range(len(tabl)//num):  
 tablMtx.append(list(tabl[0:num]))  
 tabl = tabl[num:]  
  
 **for** i **in** tablMtx:  
 print(i)  
  
 res = []  
 **for** i **in** range(len(text)//2):  
 tmp = []  
 **for** j **in** range(2):  
 tmp.append(text[j])  
 text = text[2:]  
 res.append(tmp)  
  
 arrBigr = []  
 **for** i **in** range(len(res)):  
 tmp = []  
 **for** j **in** range(len(res[i])):  
 tmp.append('')  
 arrBigr.append(tmp)  
  
 **for** i **in** range(len(res)):  
 indI0, indJ0 = find(tablMtx, res[i][0])  
 indI1, indJ1 = find(tablMtx, res[i][1])  
 #Если символы биграммы исходного текста встречаются в одной строке,  
 # то эти символы замещаются на символы, расположенные в ближайших столбцах  
 # справа от соответствующих символов. Если символ является последним в строке,  
 # то он заменяется на первый символ этой же строки.  
 **if** indI0 == indI1:  
 **if** indI0 == indI1 **and** indJ0 == 0:  
 arrBigr[i][0] = tablMtx[indI0][num-1]  
 arrBigr[i][1] = tablMtx[indI1][indJ1 - 1]  
 **elif** indI0 == indI1 **and** indJ1 == 0:  
 arrBigr[i][0] = tablMtx[indI0][indJ0 - 1]  
 arrBigr[i][1] = tablMtx[indI1][num-1]  
 **elif** indI0 == indI1 **and** indJ1 == 0 **and** indJ0 == 0:  
 arrBigr[i][0] = tablMtx[indI0][num-1]  
 arrBigr[i][1] = tablMtx[indI1][num-1]  
 **else**:  
 arrBigr[i][0] = tablMtx[indI0][indJ0 - 1]  
 arrBigr[i][1] = tablMtx[indI1][indJ1 - 1]  
 #Если символы биграммы исходного текста встречаются в одном столбце,  
 # то они преобразуются в символы того же столбца, находящиеся непосредственно  
 # под ними. Если символ является нижним в столбце, то он заменяется  
 # на первый символ этого же столбца.  
 **if** indJ0 == indJ1:  
 **if** indJ0 == indJ1 **and** indI0 == 0:  
 arrBigr[i][0] = tablMtx[0][indJ0]  
 arrBigr[i][1] = tablMtx[indI1 - 1][indJ1]  
 **if** indJ0 == indJ1 **and** indI1 == 0:  
 arrBigr[i][0] = tablMtx[indI0 - 1][indJ0]  
 arrBigr[i][1] = tablMtx[num-1][indJ1]  
 **if** indJ0 == indJ1 **and** indI0 == 0 **and** indI1 == 0:  
 arrBigr[i][0] = tablMtx[num-1][indJ0]  
 arrBigr[i][1] = tablMtx[num-1][indJ1]  
 **else**:  
 arrBigr[i][0] = tablMtx[indI0 - 1][indJ0]  
 arrBigr[i][1] = tablMtx[indI1 - 1][indJ1]  
 #Если символы биграммы исходного текста находятся в разных столбцах и разных  
 # строках, то они заменяются на символы, находящиеся в тех же строках,  
 # но соответствующие другим углам прямоугольника.  
 **if** indI0 != indI1 **and** indJ0 != indJ1:  
 arrBigr[i][1] = tablMtx[indI1][indJ0]  
 arrBigr[i][0] = tablMtx[indI0][indJ1]  
  
 restext = ""  
 **for** i **in** range(len(arrBigr)):  
 **for** j **in** range(len(arrBigr[i])):  
 restext+=arrBigr[i][j]  
  
 # for i in range(len(restext) - 1):  
 # if restext[i] == "\*":  
 # if restext[i] != restext[-1]:  
 # if restext[i - 1] == restext[i + 1]:  
 # restext.remove(restext[i])  
 # #restext = restext[:i] + restext[i + 1:]  
 # else:  
 # restext.remove(restext[i])  
 #  
 # restext1 = ""  
 # for i in range(len(restext)):  
 # restext1+=restext[i]  
  
 restext = restext.replace("\*", "")  
 **return** restext  
  
#text1 = codingPlayfair(text, keyToShifr)  
#print(text1)  
#print(decodingPlayfair(text1, keyToShifr))

1. **Примеры работы программы**

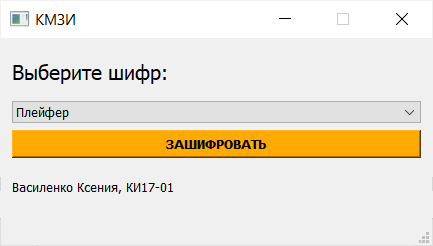


Рисунок 1 – Главное окно.

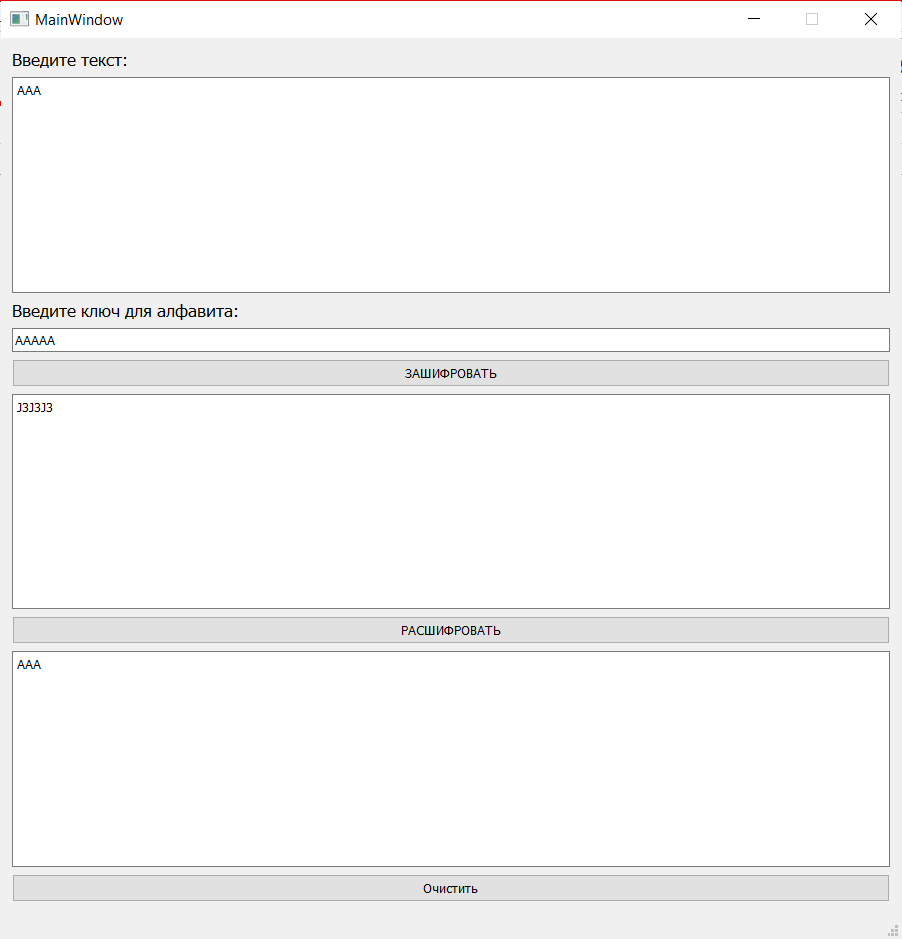


Рисунок 2 – Шифр Плейфера.

# ЗАКЛЮЧЕНИЕ

Во время выполнения лабораторной работы №10 мною был изучен и реализован программно шифр Плейфера, а также предусмотрен графический интерфейс с помощью PyQt5 и Qt designer.