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 3**

по Криптографические методы защиты информации

наименование дисциплины

Квадрат Полибия

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

Задачи:

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

**Реализация шифра**

1. **Описание шифра**

К каждому языку отдельно составляется таблица шифрования с одинаковым (не обязательно) количеством пронумерованных строк и столбцов, параметры которой зависят от его мощности (количества букв в алфавите). Берутся два целых числа, произведение которых ближе всего к количеству букв в языке — получаем нужное число строк и столбцов. Затем вписываем в таблицу все буквы алфавита подряд — по одной в каждую клетку. При нехватке клеток можно вписать в одну две буквы (редко употребляющиеся или схожие по употреблению).

Алгоритм шифрования первого метода заключался в том, что на квадрате находили букву текста и вставляли в шифровку нижнюю от неё в том же столбце. Если буква была в нижней строке, то брали верхнюю из того же столбца.

Алгоритм шифрования второго метода заключался в том, что:

1. сообщение преобразуется в координаты по квадрату Полибия, координаты записываются вертикально;
2. затем координаты считывают по строкам;
3. далее координаты преобразуются в буквы по этому же квадрату.

Алгоритм шифрования третьего метода:

1. полученный первичный шифротекст шифруется вторично. При этом он выписывается без разбиения на пары;
2. полученная последовательность цифр сдвигается циклически влево на один шаг (нечётное количество шагов);
3. эта последовательность вновь разбивается в группы по два;
4. и по таблице заменяется на окончательный шифротекст.
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**

**polybius.py**

**from** PyQt5 **import** QtWidgets  
  
**def** codingPolybius(text):  
 dictSymb = **" `~!@#№$;%^:?\*&()-+=\_,./1234567890"** dictRusUp = {**"А"**:**"11"**, **"Б"**:**"12"**, **"В"**:**"13"**, **"Г"**:**"14"**, **"Д"**:**"15"**, **"Е"**:**"16"**,  
 **"Ё"**:**"21"**, **"Ж"**:**"22"**, **"З"**:**"23"**, **"И"**:**"24"**,**"Й"**:**"25"**, **"К"**:**"26"**,  
 **"Л"**:**"31"**, **"М"**:**"32"**, **"Н"**:**"33"**, **"О"**:**"34"**, **"П"**:**"35"**, **"Р"**:**"36"**,  
 **"С"**:**"41"**, **"Т"**:**"42"**, **"У"**:**"43"**, **"Ф"**:**"44"**, **"Х"**:**"45"**, **"Ц"**:**"46"**,  
 **"Ч"**:**"51"**, **"Ш"**:**"52"**, **"Щ"**:**"53"**, **"Ъ"**:**"54"**, **"Ы"**:**"55"**, **"Ь"**:**"56"**,  
 **"Э"**:**"61"**, **"Ю"**:**"62"**, **"Я"**:**"63"**}  
  
 dictRus = {**"а"**:**"11"**, **"б"**:**"12"**, **"в"**:**"13"**,  
 **"г"**:**"14"**, **"д"**:**"15"**, **"е"**:**"16"**, **"ё"**:**"21"**,  
 **"ж"**:**"22"**, **"з"**:**"23"**, **"и"**:**"24"**,**"й"**:**"25"**,  
 **"к"**:**"26"**, **"л"**:**"31"**, **"м"**:**"32"**, **"н"**:**"33"**,  
 **"о"**:**"34"**, **"п"**:**"35"**, **"р"**:**"36"**, **"с"**:**"41"**,  
 **"т"**:**"42"**, **"у"**:**"43"**, **"ф"**:**"44"**, **"х"**:**"45"**,  
 **"ц"**:**"46"**, **"ч"**:**"51"**, **"ш"**:**"52"**, **"щ"**:**"53"**,  
 **"ъ"**:**"54"**, **"ы"**:**"55"**, **"ь"**:**"56"**, **"э"**:**"61"**,  
 **"ю"**:**"62"**, **"я"**:**"63"**}  
  
 dictEngUp = {**"A"**:**"11"**, **"B"**:**"12"**, **"C"**:**"13"**, **"D"**:**"14"**, **"E"**:**"15"**, **"F"**:**"16"**,  
 **"G"**:**"21"**, **"H"**:**"22"**, **"I"**:**"23"**, **"J"**:**"24"**, **"K"**:**"25"**, **"L"**:**"26"**,  
 **"M"**:**"31"**, **"N"**:**"32"**, **"O"**:**"33"**, **"P"**:**"34"**, **"Q"**:**"35"**, **"R"**:**"36"**,  
 **"S"**:**"41"**, **"T"**:**"42"**, **"U"**:**"43"**, **"V"**:**"44"**, **"W"**:**"45"**, **"X"**:**"46"**,  
 **"Y"**:**"51"**, **"Z"**:**"52"**}  
  
 dictEng = {**"a"**:**"11"**, **"b"**:**"12"**, **"c"**:**"13"**, **"d"**:**"14"**, **"e"**:**"15"**, **"f"**:**"16"**,  
 **"g"**:**"21"**, **"h"**:**"22"**, **"i"**:**"23"**, **"j"**:**"24"**, **"k"**:**"25"**, **"l"**:**"26"**,  
 **"m"**:**"31"**, **"n"**:**"32"**, **"o"**:**"33"**, **"p"**:**"34"**, **"q"**:**"35"**, **"r"**:**"36"**,  
 **"s"**:**"41"**, **"t"**:**"42"**, **"u"**:**"43"**, **"v"**:**"44"**, **"w"**:**"45"**, **"x"**:**"46"**,  
 **"y"**:**"51"**, **"z"**:**"52"**}  
  
 s=**""  
 for** i **in** text:  
 **if** i **in** dictRus:  
 temp=int(dictRus.get(i))+10  
 **if** temp > 70:  
 temp -= 60  
 **elif** temp > 63:  
 temp -= 50  
 **for** k **in** dictRus.items():  
 **if** str(temp) == k[1]:  
 s+=k[0]  
 **break  
 elif** i **in** dictRusUp:  
 temp=int(dictRusUp.get(i))+10  
 **if** temp > 70:  
 temp -= 60  
 **elif** temp > 63:  
 temp -= 50  
 **for** k **in** dictRusUp.items():  
 **if** str(temp) == k[1]:  
 s+=k[0]  
 **break  
 elif** i **in** dictEngUp:  
 temp=int(dictEngUp.get(i))+10  
 **if** temp > 60:  
 temp -= 50  
 **elif** temp > 52:  
 temp -= 40  
 **for** k **in** dictEngUp.items():  
 **if** str(temp) == k[1]:  
 s+=k[0]  
 **break  
 elif** i **in** dictEng:  
 temp=int(dictEng.get(i))+10  
 **if** temp > 60:  
 temp -= 50  
 **elif** temp > 52:  
 temp -= 40  
 **for** k **in** dictEng.items():  
 **if** str(temp) == k[1]:  
 s+=k[0]  
 **break  
 elif** i **in** dictSymb:  
 s+=i  
 **else**:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Введите текст!"**)  
 msgBox.exec\_()  
 **return**(**""**)  
 **return** s  
  
**def** decodingPolybius(text):  
 dictSymb = **" `~!@#№$;%^:?\*&()-+=\_,./1234567890"** dictRusUp = {**"А"**:**"11"**, **"Б"**:**"12"**, **"В"**:**"13"**, **"Г"**:**"14"**, **"Д"**:**"15"**, **"Е"**:**"16"**,  
 **"Ё"**:**"21"**, **"Ж"**:**"22"**, **"З"**:**"23"**, **"И"**:**"24"**,**"Й"**:**"25"**, **"К"**:**"26"**,  
 **"Л"**:**"31"**, **"М"**:**"32"**, **"Н"**:**"33"**, **"О"**:**"34"**, **"П"**:**"35"**, **"Р"**:**"36"**,  
 **"С"**:**"41"**, **"Т"**:**"42"**, **"У"**:**"43"**, **"Ф"**:**"44"**, **"Х"**:**"45"**, **"Ц"**:**"46"**,  
 **"Ч"**:**"51"**, **"Ш"**:**"52"**, **"Щ"**:**"53"**, **"Ъ"**:**"54"**, **"Ы"**:**"55"**, **"Ь"**:**"56"**,  
 **"Э"**:**"61"**, **"Ю"**:**"62"**, **"Я"**:**"63"**}  
  
 dictRus = {**"а"**:**"11"**, **"б"**:**"12"**, **"в"**:**"13"**,  
 **"г"**:**"14"**, **"д"**:**"15"**, **"е"**:**"16"**, **"ё"**:**"21"**,  
 **"ж"**:**"22"**, **"з"**:**"23"**, **"и"**:**"24"**,**"й"**:**"25"**,  
 **"к"**:**"26"**, **"л"**:**"31"**, **"м"**:**"32"**, **"н"**:**"33"**,  
 **"о"**:**"34"**, **"п"**:**"35"**, **"р"**:**"36"**, **"с"**:**"41"**,  
 **"т"**:**"42"**, **"у"**:**"43"**, **"ф"**:**"44"**, **"х"**:**"45"**,  
 **"ц"**:**"46"**, **"ч"**:**"51"**, **"ш"**:**"52"**, **"щ"**:**"53"**,  
 **"ъ"**:**"54"**, **"ы"**:**"55"**, **"ь"**:**"56"**, **"э"**:**"61"**,  
 **"ю"**:**"62"**, **"я"**:**"63"**}  
  
 dictEngUp = {**"A"**:**"11"**, **"B"**:**"12"**, **"C"**:**"13"**, **"D"**:**"14"**, **"E"**:**"15"**, **"F"**:**"16"**,  
 **"G"**:**"21"**, **"H"**:**"22"**, **"I"**:**"23"**, **"J"**:**"24"**, **"K"**:**"25"**, **"L"**:**"26"**,  
 **"M"**:**"31"**, **"N"**:**"32"**, **"O"**:**"33"**, **"P"**:**"34"**, **"Q"**:**"35"**, **"R"**:**"36"**,  
 **"S"**:**"41"**, **"T"**:**"42"**, **"U"**:**"43"**, **"V"**:**"44"**, **"W"**:**"45"**, **"X"**:**"46"**,  
 **"Y"**:**"51"**, **"Z"**:**"52"**}  
  
 dictEng = {**"a"**:**"11"**, **"b"**:**"12"**, **"c"**:**"13"**, **"d"**:**"14"**, **"e"**:**"15"**, **"f"**:**"16"**,  
 **"g"**:**"21"**, **"h"**:**"22"**, **"i"**:**"23"**, **"j"**:**"24"**, **"k"**:**"25"**, **"l"**:**"26"**,  
 **"m"**:**"31"**, **"n"**:**"32"**, **"o"**:**"33"**, **"p"**:**"34"**, **"q"**:**"35"**, **"r"**:**"36"**,  
 **"s"**:**"41"**, **"t"**:**"42"**, **"u"**:**"43"**, **"v"**:**"44"**, **"w"**:**"45"**, **"x"**:**"46"**,  
 **"y"**:**"51"**, **"z"**:**"52"**}  
  
 s=**""  
 for** i **in** text:  
 **if** i **in** dictRus:  
 temp=int(dictRus.get(i))-10  
 **if** temp < 4:  
 temp+=60  
 **elif** temp < 7:  
 temp+=50  
 **for** k **in** dictRus.items():  
 **if** str(temp) == k[1]:  
 s+=k[0]  
 **break  
 elif** i **in** dictRusUp:  
 temp=int(dictRusUp.get(i))-10  
 **if** temp < 4:  
 temp+=60  
 **elif** temp < 7:  
 temp+=50  
 **for** k **in** dictRusUp.items():  
 **if** str(temp) == k[1]:  
 s+=k[0]  
 **break  
 elif** i **in** dictEngUp:  
 temp=int(dictEngUp.get(i))-10  
 **if** temp < 3:  
 temp+=50  
 **elif** temp < 7:  
 temp+=40  
 **for** k **in** dictEngUp.items():  
 **if** str(temp) == k[1]:  
 s+=k[0]  
 **break  
 elif** i **in** dictEng:  
 temp=int(dictEng.get(i))-10  
 **if** temp < 3:  
 temp+=50  
 **elif** temp < 7:  
 temp+=40  
 **for** k **in** dictEng.items():  
 **if** str(temp) == k[1]:  
 s+=k[0]  
 **break  
 elif** i **in** dictSymb:  
 s+=i  
 **else**:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Введите текст!"**)  
 msgBox.exec\_()  
 **return**(**""**)  
 **return** s  
  
**def** codingPolybius1(text, flag):  
 dict = {**"a"**:**"11"**, **"b"**:**"12"**, **"c"**:**"13"**, **"d"**:**"14"**, **"e"**:**"15"**, **"f"**:**"16"**, **"g"**:**"17"**, **"h"**:**"18"**,  
 **"i"**:**"21"**, **"j"**:**"22"**, **"k"**:**"23"**, **"l"**:**"24"**, **"m"**:**"25"**, **"n"**:**"26"**, **"o"**:**"27"**, **"p"**:**"28"**,  
 **"q"**:**"31"**, **"r"**:**"32"**, **"s"**:**"33"**, **"t"**:**"34"**, **"u"**:**"35"**, **"v"**:**"36"**, **"w"**:**"37"**, **"x"**:**"38"**,  
 **"y"**:**"41"**, **"z"**:**"42"**, **"а"**:**"43"**, **"б"**:**"44"**, **"в"**:**"45"**, **"г"**:**"46"**, **"д"**:**"47"**, **"е"**:**"48"**,  
 **"ё"**:**"51"**, **"ж"**:**"52"**, **"з"**:**"53"**, **"и"**:**"54"**,**"й"**:**"55"**, **"к"**:**"56"**, **"л"**:**"57"**, **"м"**:**"58"**,  
 **"н"**:**"61"**, **"о"**:**"62"**, **"п"**:**"63"**, **"р"**:**"64"**, **"с"**:**"65"**, **"т"**:**"66"**, **"у"**:**"67"**, **"ф"**:**"68"**,  
 **"х"**:**"71"**, **"ц"**:**"72"**, **"ч"**:**"73"**, **"ш"**:**"74"**, **"щ"**:**"75"**, **"ъ"**:**"76"**, **"ы"**:**"77"**, **"ь"**:**"78"**,  
 **"э"**:**"81"**, **"ю"**:**"82"**, **"я"**:**"83"**, **"."**:**"84"**, **","**:**"85"**, **" "**:**"86"**, **"!"**:**"87"**, **"?"**:**"88"**}  
  
 res=**""** text1 = text.split(**"\n"**)  
 **for** string **in** text1:  
 coord = **""** s = **""  
 for** i **in** string:  
 **if** i **in** dict:  
 **for** k **in** dict.items():  
 **if** k[0] == i:  
 coord+=k[1]  
 **else**:  
 msgBox = QtWidgets.QMessageBox()  
 msgBox.setWindowTitle(**"Ошибка"**)  
 msgBox.setText(**"Введите строчные английские и русские символы!"**)  
 msgBox.exec\_()  
 **return**(**""**)  
 **if** flag == 1:  
 **for** i **in** range(len(coord)):  
 **if** i % 2 == 0:  
 s += coord[i]  
 **for** i **in** range(len(coord)):  
 **if** i % 2 == 1:  
 s += coord[i]  
 **else**:  
 **for** i **in** range(len(coord) // 2):  
 s += coord[i]  
 s += coord[i + len(coord) // 2]  
 **for** i **in** range(0, len(s), 2):  
 **for** k **in** dict.items():  
 **if** k[1] == s[i]+s[i+1]:  
 res += k[0]  
 res+=**'\n'** *#print(coord)  
 #print(s)  
 # print(res)* **return** res

1. **Примеры работы программы**

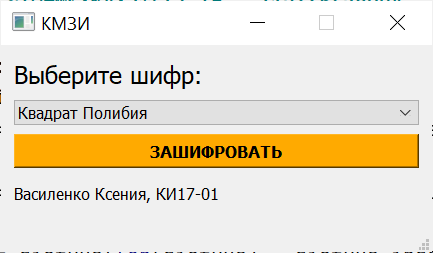


Рисунок 1 – Главное окно.

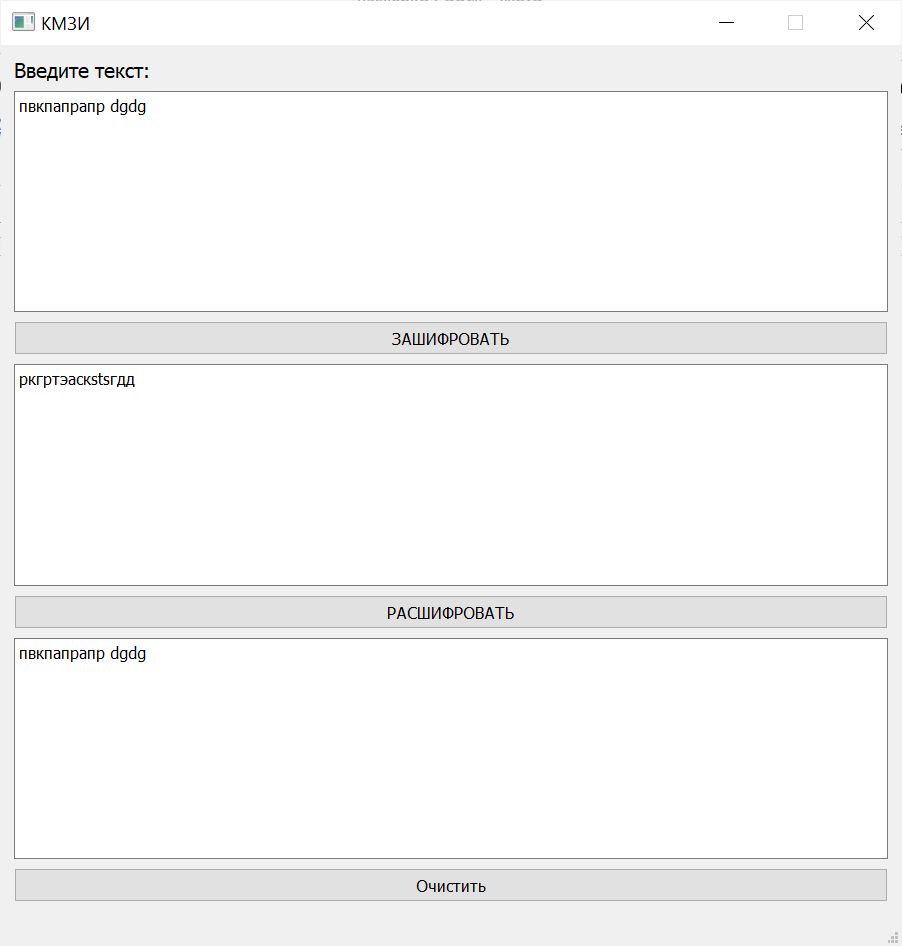


Рисунок 2 – Шифр Полибия.

# ЗАКЛЮЧЕНИЕ

Во время выполнения лабораторной работы №3 мною был изучен и реализован программно шифр Полибия, а также предусмотрен графический интерфейс с помощью PyQt5 и Qt designer.