

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет Информатика и вычислительная техника

Кафедра Кибербезопасность информационных систем

**Лабораторная работа № 4**

по дисциплине «Криптографические методы защиты информации»

на тему «Шифрование с использованием системы Вижинера и шифра «двойной квадрат» Уитстона»

Выполнил обучающийся гр. ВКБ41

Деев Д.Д.

(Фамилия, Имя, Отчество)

Проверила:

Доцент Рощина Е.В.

(Должность, Фамилия, Имя, Отчество)

Ростов-на-Дону

2019

**Краткие теоретические сведения**

1. **Чем шифры сложной замены отличаются от шифров простой замены?**

Шифры сложной замены называют многоалфавитными шифрами, в таких шифрах для преобразования каждого отдельно взятого элемента естественного алфавита применяют свой шифр простой замены, устраняя при этом статистические демаскирующие признаки.

1. **Что используется в качестве ключа в системе Вижинера?**

Ключевое слово или фразу. Если ключ оказался короче сообщения, то его циклически повторяют.

1. **Как осуществляется шифрование текста с использованием системы Вижинера?**

При шифровании исходного сообщения его выписывают в строку, а под ним записывают ключевое слово или фразу. Если ключ оказался короче сообщения, то его циклически повторяют. В процессе шифрования находят в верхней строке таблицы очередную букву исходного текста и в левом столбце очередное значение ключа. Очередная буква шифртекста находится на пересечении столбца, определяемого шифруемой буквой, и строки, определяемой числовым значением ключа.

1. **Какие требования предъявляются к шифруемому тексту при использовании шифра «двойной квадрат» Уитстона?**

Текст должен иметь четное количество символов, символы должны соответствовать символам шифрующих таблиц.

1. **Как осуществляется шифрование текста с использованием шифра «двойной квадрат» Уитстона?**

Пусть имеются две таблицы со случайно расположенными в них русскими алфавитами. Перед шифрованием исходное сообщение разбивают на биграммы. Каждая биграмма шифруется отдельно. Первую букву биграммы находят в левой таблице, а вторую букву - в правой таблице. Затем мысленно строят прямоугольник так, чтобы буквы биграммы лежали в его противоположных вершинах. Другие две вершины этого прямоугольника дают буквы биграммы шифртекста.

Если обе буквы биграммы сообщения лежат в одной строке, то и буквы шифртекста берут из этой же строки. Первую букву биграммы шифртекста берут из левой таблицы в столбце, соответствующем второй букве биграммы сообщения. Вторая же буква биграммы шифртекста берется из правой таблицы в столбце, соответствующем первой букве биграммы сообщения.

**Цель работы:** формирование умений шифрования с использованием системы Вижинера и шифра «двойной квадрат» Уитстона.

**Ход работы (вариант 8)**

**Задание 1.** Используя систему Вижинера, зашифруйте сообщения.

Сообщение: Оптимист – это человек, который еще не читал утренних газет

Ключевое слово: КАНИКУЛЫ

Программное средство было реализовано на языке Python 3.7. Результаты работы показаны на рисунках 1, 2.

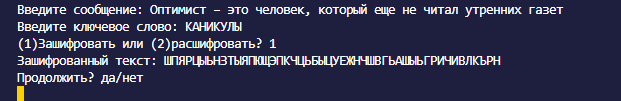


Рисунок 1 – Результат шифрования

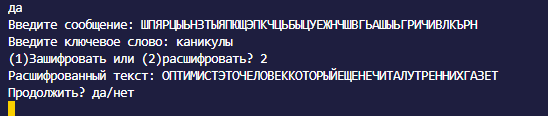


Рисунок 2 – Результат расшифрования

**Задание 2.** Используя шифр «двойной квадрат» Уитстона и шифрующие таблицы, выполните шифрование.

Сообщение: Оптимист это человек, который еще не читал утренних газет

Результаты работы показаны на рисунках 1, 2.

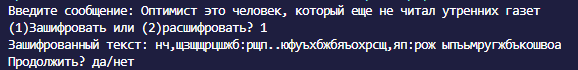


Рисунок 1 – Результат шифрования

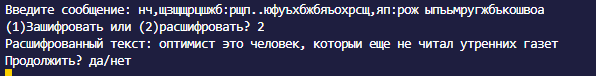


Рисунок 2 – Результат расшифрования

Листинг программного средства:

def isstring(string):

try:

ABC = string\_abc()

for i in string:

if not (i in ABC or i in ['–', ',', '.', ' ']):

int(None)

return string

except TypeError:

print('Введите строку, состоящую из букв русского алфавита, без цифр')

string = isstring(input().upper())

return string

def string\_abc():

abc = ''

for i in range(1040, 1072):

abc += chr(i)

return abc

def clear\_text(text):

new\_text = ''

for symbol in text:

if 1040 <= ord(symbol) < 1072:

new\_text += symbol

return new\_text

def encipher(key, string):

ABC = string\_abc()

string = clear\_text(string)

ret = ''

for (i, c) in enumerate(string):

i = i % len(key)

ret += ABC[(ABC.index(c) + ABC.index(key[i])) % 32]

return ret

def decipher(key, string):

ABC = string\_abc()

string = clear\_text(string)

ret = ''

for (i, c) in enumerate(string):

i = i % len(key)

ret += ABC[(ABC.index(c) - ABC.index(key[i])) % 32]

return ret

# Шифр Вижинера

if \_\_name\_\_ == "\_\_main\_\_":

while True:

print('Введите сообщение: ', end='')

text = isstring(input().upper())

print('Введите ключевое слово: ', end='')

key = isstring(input().upper())

print('(1)Зашифровать или (2)расшифровать? ', end='')

case = input()

if case == '1':

print('Зашифрованный текст:', encipher(key, text))

elif case == '2':

print('Расшифрованный текст:', decipher(key, text))

print('Продолжить? да/нет')

fail\_condition = input()

if fail\_condition == 'нет':

break

def clear\_text(text, key):

new\_text = ''

for symbol in text:

if symbol not in key:

new\_text += symbol

return new\_text

def isstring(string, key):

try:

for i in string:

if i not in key:

int(None)

return string

except TypeError:

print('Введите строку, состоящую из букв русского ', end='')

print('алфавита, или символов ":", ",", "."')

string = isstring(input().lower(), key)

return string

def cipher\_pair(key1, key2, a, b):

arow, acol = int(key1.index(a) / 5), key1.index(a) % 5

brow, bcol = int(key2.index(b) / 5), key2.index(b) % 5

if arow == brow:

return (key2[arow \* 5 + (acol) % 5] +

key1[brow \* 5 + (bcol) % 5])

else:

return (key2[arow \* 5 + bcol] +

key1[brow \* 5 + acol])

def cipher(key1, key2, string):

ret = ''

for c in range(0, len(string), 2):

ret += cipher\_pair(key1, key2, string[c], string[c + 1])

return ret

# Шифр «двойной квадрат» Уитстона

if \_\_name\_\_ == "\_\_main\_\_":

while True:

key1 = 'жщнюритьцбяме.свыпч :дуокзэфгшха,лъ'

key2 = 'ичгят,жьмозюрвщц:пелъан.хэксшдбфуы '

print('Введите сообщение: ', end='')

text = input().lower().replace('й', 'и')

text = isstring(text, key1)

if len(text) % 2 == 1:

text += ' '

print('(1)Зашифровать или (2)расшифровать? ', end='')

case = input()

if case == '1':

print('Зашифрованный текст:', cipher(key1, key2, text))

elif case == '2':

print('Расшифрованный текст:', cipher(key2, key1, text))

print('Продолжить? да/нет')

fail\_condition = input()

if fail\_condition == 'нет':

break

**Заключение.** В ходе выполнения лабораторной работы были получены навыки шифрования с использованием системы Вижинера и шифра «двойной квадрат» Уитстона. Таким образом, цель работы была достигнута.