

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 № 3**

по дисциплине «Криптографические методы защиты информации»

на тему «Реализация алгоритма шифрования Плейфейра»

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. Как формируется шифрующая таблица для реализации алгоритма Плейфейра?**

В основе алгоритма Плейфейра – использование шифрующей таблицы, формируемой аналогично таблице подстановок Трисемуса. Составной ключ шифрования также включает ключевое слово и размер шифрующей таблицы.

**2. Какие ограничения накладываются на шифруемый текст?**

Шифруемый текст должен иметь четное количество букв, и в нем не должно быть биграмм, содержащих две одинаковые буквы.

**3. Что такое биграмма?**

Одна пара букв открытого текста.

**4. В чем заключается процедура шифрования с помощью алгоритма Плейфейра?**

Последовательность биграмм открытого текста преобразуется с помощью шифрующей таблицы в последовательность биграмм шифртекста по следующим правилам:

а) если обе буквы биграммы открытого текста не попадают на одну строку или столбец, тогда находят буквы в углах прямоугольника, определяемого данной парой букв. Последовательность букв в биграмме шифртекста должна быть зеркально расположенной по отношению к последовательности букв в биграмме открытого текста;

б) если обе буквы биграммы открытого текста принадлежат одному столбцу таблицы, то буквами шифртекста считаются 2 буквы, которые лежат под ними. Если при этом буква открытого текста находится в нижней строке, то для шифртекста берется соответствующая буква из верхней строки того же столбца;

в) если обе буквы биграммы открытого текста принадлежат одной строке таблицы, то буквами шифртекста считаются буквы, которые лежат справа от них. Если при этом буква открытого текста находится в крайнем правом столбце, то для шифра берут соответствующую букву из левого столбца в той же строке.

**Цель работы:** формирование умений шифрования с использованием алгоритма шифрования Плейфейра.

**Ход работы (вариант 8)**

**Задание 1.** Зашифруйте сообщение, используя алгоритм Плейфейра согласно своему варианту. Размер шифрующей таблицы 4 × 8.

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

Ключевое слово: КАНИКУЛЫ

Программное средство было реализовано на языке Python 3.6. Результаты работы показаны на рисунках 1, 2.

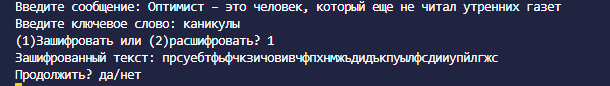


Рисунок 1 – Результат шифрования

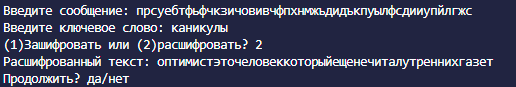


Рисунок 2 – Результат расшифрования

Листинг программного средства:

def clear\_text(text):

new\_text = ''

for symbol in text:

if 1072 <= ord(symbol) < 1104:

new\_text += symbol

return new\_text

def check\_nearby(text):

for i in range(1, len(text), 2):

if text[i] in text[i-1]:

return True

def remove\_duplicates(key, new\_key):

for symbol in key:

if symbol not in new\_key:

new\_key += symbol

return new\_key

def isstring(string):

try:

for i in string:

if i not in "абвгдеёжзийклмнопрстуфхцчшщъыьэюя":

int(None)

return string

except TypeError:

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

strings = isstring(input().lower())

return string

def allint(string):

try:

int(string)

print('Введите строку, в которой есть буквы русского алфавита')

string = allint(input().lower())

return string

except ValueError:

return string

def encipher\_pair(key, a, b):

arow, acol = int(key.index(a) / 8), key.index(a) % 8

brow, bcol = int(key.index(b) / 8), key.index(b) % 8

if arow == brow:

return (key[arow \* 8 + (acol + 1) % 8] +

key[brow \* 8 + (bcol + 1) % 8])

elif acol == bcol:

return (key[((arow + 1) \* 8 + acol) % 32] +

key[((brow + 1) \* 8 + bcol) % 32])

else:

return (key[(arow \* 8 + bcol) % 32] +

key[(brow \* 8 + acol) % 32])

def decipher\_pair(key, a, b):

arow, acol = int(key.index(a) / 8), key.index(a) % 8

brow, bcol = int(key.index(b) / 8), key.index(b) % 8

if arow == brow:

return (key[arow \* 8 + (acol - 1) % 8] +

key[brow \* 8 + (bcol - 1) % 8])

elif acol == bcol:

return (key[((arow - 1) \* 8 + acol) % 32] +

key[((brow - 1) \* 8 + bcol) % 32])

else:

return (key[(arow \* 8 + bcol) % 32] +

key[(brow \* 8 + acol) % 32])

def encipher(key, string):

ret = ''

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

ret += encipher\_pair(key, string[c], string[c + 1])

return ret

def decipher(key, string):

ret = ''

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

ret += decipher\_pair(key, string[c], string[c + 1])

return ret

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

while True:

ABC = "абвгдежзийклмнопрстуфхцчшщъыьэюя"

text = ''

while True:

print('Введите сообщение: ', end='')

text = allint(input().lower())

text = clear\_text(text)

if len(text) % 2 == 1:

print('Текст должен иметь четное количество букв')

continue

if check\_nearby(text):

print('Введите текст без биграмм, ', end='')

print('содержащих две одинаковые буквы.')

continue

break

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

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

new\_key = ''

new\_key = remove\_duplicates(key, new\_key)

new\_key = remove\_duplicates(ABC, new\_key)

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

case = input()

if case == '1':

print('Зашифрованный текст:', encipher(new\_key, text))

elif case == '2':

print('Расшифрованный текст:', decipher(new\_key, 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 алгоритма шифрования Плейфейра. Таким образом, цель работы была достигнута.