

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

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

**(ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Кибербезопасность информационных систем»

**Отчет**

**Лабораторная работа №3 по дисциплине «Методы и средства криптографической защиты»**

Выполнил:   
обучающийся гр. ВКБ41

Ушаков М.А.

Проверила:   
 Сафарьян Ольга Александровна

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Ростов-на-Дону

2024

**Лабораторная работа №3**

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

**Ход работы**

Ключ слово – ПАПКА

Текст - В системах прозрачного шифрования преобразования осуществляются незаметно для пользователя

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| п | а | к | б | в | г | д | е |
| ж | з | и | й | л | м | н | О |
| р | с | т | у | ф | х | ц | Ч |
| ш | щ | ъ | ы | ь | э | ю | я |

Шифр текст – афзтчкзгргчжжсесожемъжхследзоъжшочпузследзоъзчсыачфкоьъцчщодсзогцинеоьежфвижгкчкоь

Листинг программы:

import numpy as np

def check\_copy(word,s):

word = list(word)

new\_word = ''

if s==1:

for i in range(0,len(word),2):

if word[i] == word[i+1]:

word.insert(i+1,'x')

for j in word:

new\_word += j

if len(new\_word) % 2 != 0:

new\_word += "x"

else:

for i in range(0,len(word),2):

if word[i] == word[i + 1]:

word.insert(i + 1, 'ъ')

for j in word:

new\_word += j

if len(new\_word) % 2 != 0:

new\_word += "ъ"

return new\_word

def delete\_copy(key, alphabet, s):

used\_letters = []

for char in key:

if char not in used\_letters:

used\_letters.append(char)

for char in alphabet:

if char not in used\_letters:

used\_letters.append(char)

if s == 1:

square = np.array(used\_letters).reshape(5, 5)

else:

square = np.array(used\_letters).reshape(4, 8)

print(square)

return square

def find\_position(square, char):

if alp\_change == 1:

for i in range(5):

for j in range(5):

if square[i][j] == char:

return i, j

else:

for i in range(4):

for j in range(8):

if square[i][j] == char:

return i, j

return None

def encrypt(plaintext, matrix, s):

if s == 1:

encrypted\_text = ''

for i in range(0, len(plaintext), 2):

char1 = plaintext[i]

char2 = plaintext[i + 1]

row1, col1 = find\_position(matrix, char1)

row2, col2 = find\_position(matrix, char2)

if row1 == row2: # Одна строка

encrypted\_text += matrix[row1][(col1 + 1) % 5]

encrypted\_text += matrix[row2][(col2 + 1) % 5]

elif col1 == col2: # Один столбец

encrypted\_text += matrix[(row1 + 1) % 5][col1]

encrypted\_text += matrix[(row2 + 1) % 5][col2]

else:

encrypted\_text += matrix[row1][col2]

encrypted\_text += matrix[row2][col1]

return encrypted\_text

else:

encrypted\_text = ''

print(len(plaintext))

for i in range(0, len(plaintext), 2):

char1 = plaintext[i]

char2 = plaintext[i + 1]

row1, col1 = find\_position(matrix, char1)

row2, col2 = find\_position(matrix, char2)

# print(f'первый символ {char1},{row1},{col1}')

# print(f'второй символ {char2},{row2},{col2}')

if row1 == row2: # Одна строка

encrypted\_text += matrix[row1][(col1 + 1) % 8]

encrypted\_text += matrix[row2][(col2 + 1) % 8]

elif col1 == col2: # Один столбец

encrypted\_text += matrix[(row1 + 1) % 4][col1]

encrypted\_text += matrix[(row2 + 1) % 4][col2]

else:

encrypted\_text += matrix[row1][col2]

encrypted\_text += matrix[row2][col1]

return encrypted\_text

def decrypt(ciphertext, matrix, s):

decrypted\_text = ''

if s == 1:

for i in range(0, len(ciphertext), 2):

char1 = ciphertext[i]

char2 = ciphertext[i + 1]

row1, col1 = find\_position(matrix, char1)

row2, col2 = find\_position(matrix, char2)

# print(f'первый символ {char1},{row1},{col1}')

# print(f'второй символ {char2},{row2},{col2}')

if row1 == row2: # Одна строка

decrypted\_text += matrix[row1][(col1 - 1) % 5]

decrypted\_text += matrix[row2][(col2 - 1) % 5]

elif col1 == col2: # Один столбец

decrypted\_text += matrix[(row1 - 1) % 5][col1]

decrypted\_text += matrix[(row2 - 1) % 5][col2]

else:

decrypted\_text += matrix[row1][col2]

decrypted\_text += matrix[row2][col1]

return decrypted\_text

else:

for i in range(0, len(ciphertext), 2):

char1 = ciphertext[i]

char2 = ciphertext[i + 1]

row1, col1 = find\_position(matrix, char1)

row2, col2 = find\_position(matrix, char2)

# print(f'первый символ {char1},{row1},{col1}')

# print(f'второй символ {char2},{row2},{col2}')

if row1 == row2: # Одна строка

decrypted\_text += matrix[row1][(col1 - 1) % 8]

decrypted\_text += matrix[row2][(col2 - 1) % 8]

elif col1 == col2: # Один столбец

decrypted\_text += matrix[(row1 - 1) % 4][col1]

decrypted\_text += matrix[(row2 - 1) % 4][col2]

else:

decrypted\_text += matrix[row1][col2]

decrypted\_text += matrix[row2][col1]

return decrypted\_text

alphabet = 'абвгдежзийклмнопрстуфхцчшщъыьэюя'

alphabet\_lat = 'abcdefghiklmnopqrstuvwxyz'

alp\_change = int(input("Какой алфавит 1-латинский 2-кириллица"))

keyword = input("Введите ключевое слово ").replace(" ", "")

text = input("Введите предложение ").replace(" ", "")

# "папка"

# "всистемахпрозрачногошифрованияпреобразованияосуществляютсянезаметнодляпользователя"

# "hello"

# 'ushakovmaksimaleksandrovich'

if alp\_change == 1:

if len(text) % 2 != 0:

text += "x"

text = check\_copy(text, 1)

print(text)

keyword = delete\_copy(keyword, alphabet\_lat, alp\_change)

else:

if len(text) % 2 != 0:

text += "ъ"

text = check\_copy(text, 2)

print(text)

keyword = delete\_copy(keyword, alphabet, alp\_change)

encrypted\_text = encrypt(text, keyword, alp\_change)

print(f"Зашифрованный текст: {encrypted\_text}")

decrypted\_text = decrypt(encrypted\_text, keyword, alp\_change)

print(f"Расшифрованный текст: {decrypted\_text}")

**Вывод:** в ходе лабораторной работы было освоен и реализован на языке программирования Pyhton алгоритм шифрования Плейфейра.