

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 №5 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 №5**

**Цель работы**: изучить и реализовать тюремный шифр.

**Ход работы:**

Задание выполнить шифрование с помощью тюремного шифра

ВСИСТЕМАХПРОЗРАЧНОГОШИФРОВАНИЯПРЕОБРАЗОВАНИЯОСУЩЕСТВЛЯЮТСЯНЕЗАМЕТНОДЛЯПОЛЬЗОВАТЕЛЯ

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 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 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| В | С | И | С | Т | Е | М | А | Х | П | Р | О | З | Р | А | Ч | Н | О | Г | О |
| 15 | 32 | 23 | 32 | 33 | 18 | 26 | 12 | 36 | 11 | 31 | 28 | 22 | 31 | 12 | 38 | 27 | 28 | 16 | 28 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Ш | И | Ф | Р | О | В | А | Н | И | Я | П | Р | Е | О | Б | Р |
| 41 | 23 | 35 | 31 | 28 | 15 | 12 | 27 | 23 | 48 | 11 | 31 | 18 | 28 | 14 | 31 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| А | З | О | В | А | Н | И | Я | О | С | У | Щ | Е | С | Т | В | Л | Я | Ю | Т | С |
| 12 | 22 | 28 | 15 | 12 | 27 | 23 | 48 | 28 | 32 | 34 | 42 | 18 | 32 | 33 | 15 | 25 | 48 | 47 | 33 | 32 |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Я | Н | Е | З | А | М | Е | Т | Н | О | Д | Л | Я | П |
| 48 | 27 | 18 | 22 | 12 | 26 | 18 | 33 | 27 | 28 | 17 | 25 | 48 | 11 |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| О | Л | Ь | З | О | В | А | Т | Е | Л | Я |
| 11 | 28 | 25 45 | 22 | 28 | 15 | 12 | 33 | 18 | 25 | 48 |

15322332331826123611312822311238272816284123353128151227234811311828143112222815122723482832344218323315254847333248271822122618332728172548112825452228151233182548

Листинг программы:

import numpy as np

def find\_position(square, char, alp\_change):

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 delete\_copy(key, s):

alphabet = ''

if s == 1:

alphabet = 'abcdefghiklmnopqrstuvwxyz'.upper()

else:

alphabet = 'абвгдежзийклмнопрстуфхцчшщъыьэюя'.upper()

used\_letters = []

for char in key:

if char == "J":

char ='I'

if char == "Ё":

char == "Е"

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 encrypt(text, matrix, s):

encrypted\_text = ''

for i in text:

row, col = find\_position(matrix, i, s)

encrypted\_text += str(row + 1)

encrypted\_text += str(col + 1)

return encrypted\_text

def dencrypt(text, matrix):

decrypted\_text = ''

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

row, col = int(text[i]), int(text[i+1])

decrypted\_text += matrix[row-1][col-1]

return decrypted\_text

alphabet = 'абвгдежзийклмнопрстуфхцчшщъыьэюя'.upper()

alphabet\_lat = 'abcdefghiklmnopqrstuvwxyz'.upper()

keyword =''

text =''

path = input("Введите путь до файла с текстом, который необходимо шифровать")

d = input("Что сдлетать з - зашифровать, р - расшифровать")

print("полученная информация ")

with open (path, "r", encoding="utf-8") as file:

lines = file.readlines()

keyword = lines.pop(0)

keyword = keyword.strip()

for line in lines:

text += line.strip()

keyword = keyword.upper()

s = 0

if 64 < ord((keyword[0])) < 91:

s = 1

else:

s = 2

text = text.upper()

print(keyword)

print(text)

square = delete\_copy(keyword,s)

if d == "з":

encrypt\_text = encrypt(text, square,s)

print(encrypt\_text)

Lines = [keyword, encrypt\_text]

path\_res = input("Введите путь сохранения результата ")

print("результат работы сохранен в файл по пути D:/dec.txt")

with open(path\_res, "w", encoding="utf-8") as out\_file:

for line in Lines:

out\_file.write(line + "\n")

if d == "р":

dencrypt\_text = dencrypt(text,square)

print(dencrypt\_text)

path\_res = input("Введите путь сохранения результата ")

Lines = [keyword, dencrypt\_text]

print("результат работы сохранен в файл по пути D:/dec.txt")

with open (path\_res, "w", encoding="utf-8") as out\_file:

for line in Lines:

out\_file.write(line + "\n")

**Вывод:** в ходе лабораторной работы был изучен и реализован тюремный шифр.