

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 №1 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 №1**

**Цель работы:** формирование умений шифрования с использованием методов шифрующих таблиц и магического квадрата.

**Ход работы:**

Задание 1. Вариант 24

Расшифруйте шифртекст «\_НОНАВОГЯПЬТЕМ\_Р», полученный методом двойной перестановки (размер таблицы 4 × 4, последовательность номеров столбцов и номеров строк – 2143, 2143).

Шифртекст = \_НОНАВОГЯПЬТЕМ\_Р

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 2 | 1 | 4 | 3 |
| 2 | \_ | Н | О | Н |
| 1 | А | В | О | Г |
| 4 | Я | П | Ь | Т |
| 3 | Е | М | \_ | Р |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 |
| 2 | Н | \_ | Н | О |
| 1 | В | А | Г | О |
| 4 | П | Я | Т | Ь |
| 3 | М | Е | Р | \_ |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 1 | 2 | 3 | 4 |
| 1 | В | А | Г | О |
| 2 | Н | \_ | Н | О |
| 3 | М | Е | Р | \_ |
| 4 | М | Я | Т | Ь |

Полученный текст: Вагон номер пять

|  |  |  |
| --- | --- | --- |
| П | Р | Е |
| К | Р | А |
| С | Н | О |

Задания 2. Вариант 24. Расшифруйте шифртекст «НЕКПРОАСР», полученный при использовании метода магического квадрата 3 × 3.

|  |  |  |
| --- | --- | --- |
| 8 | 3 | 4 |
| 1 | 5 | 9 |
| 6 | 7 | 2 |

|  |  |  |
| --- | --- | --- |
| Н | Е | К |
| П | Р | О |
| А | С | Р |

|  |  |  |
| --- | --- | --- |
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |

НЕКПРОАСР = ПРЕКРАСНО

834159672 = 1 2 3 4 5 6 7 8 91 2 3 4 5 6 7 8 9 и магического квадрата.

Листинг кода:

import numpy as np

def in\_prog(combo):

for i in range(len(combo)):

combo[i] = combo[i] - 1

return combo

def enscryption\_one(word\_matrix, combo\_one, combo\_two):

matrix\_rearranged = np.take(word\_matrix, combo\_one, axis=1)

matrix\_rearranged = np.take(matrix\_rearranged, combo\_two, axis=0)

matrix\_as\_string = ''.join(map(str, matrix\_rearranged.ravel()))

print(matrix\_as\_string)

def check\_summa(s):

new\_s = []

for i in range(len(s)):

new\_s.append(s[i])

a = np.array(new\_s).reshape(3, 3)

a = a.astype(np.int32)

b = np.fliplr(a)

column\_sum = np.sum(a, axis=0)

row\_sum = np.sum(a, axis=1)

diagonal = np.trace(a)

anti\_diagonal = np.trace(b)

if (diagonal != anti\_diagonal) and ([number == diagonal for number in column\_sum]) and ([i == diagonal for i in row\_sum]):

print("Суммы не равны")

exit()

else:

print("суммы равны")

def check\_unicum(s):

new\_s = []

for i in range(len(s)):

new\_s.append(s[i])

set\_combo = set(new\_s)

if len(set\_combo) != len(new\_s):

print("Введены одинаковые значения ")

exit()

def check\_len(s, w):

if len(s) > 3 \* 3 or len(w) > 3\*3:

print("Введено большое значение для квадрата")

exit()

elif len(s) < 3 \* 3 or len(w) < 3 \* 3:

print("Введено малое значение для квадрата")

exit()

number\_of\_quest = input("какое задание 1 - 2 ?")

if number\_of\_quest == '1':

word = input("Введите слово ")

if len(word) > 16:

print("Слишком много символов ")

exit()

word\_matrix = []

for j in range(len(word)):

word\_matrix.append(word[j])

word\_matrix = np.array(word\_matrix).reshape(4, 4)

combo\_one = input("Введите комбинацию 1 ").split()

combo\_one = np.array(combo\_one).astype(int)

combo\_two = input("Введите комбинацию 2 ").split()

combo\_two = np.array(combo\_two).astype(int)

in\_prog(combo\_one)

in\_prog(combo\_two)

enscryption\_one(word\_matrix,combo\_one,combo\_two)

if number\_of\_quest == '2':

decode\_code = input("1:зашифровать или 2:расшифровать ")

if decode\_code == "1":

word = input("Введите слово")

combo = input("Введите комбинацию для зашифрования ")

check\_unicum(combo)

check\_summa(combo)

check\_len(combo, word)

code\_word = ''

for i in combo:

for j in range(len(word)):

if int(i) - 1 == j:

code\_word += word[j]

print(code\_word)

if decode\_code == "2":

word = input("Введите слово ")

combo = input("Введите комбинацию для расшифрования ")

check\_summa(combo)

check\_len(combo,word)

check\_unicum(combo)

check = [1, 2, 3, 4, 5, 6, 7, 8, 9]

code\_word = ''

for i in check:

for j in range(len(combo)):

if i == int(combo[j]):

code\_word += word[j]

print(code\_word)

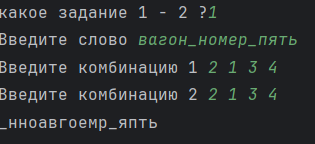


Рис 1 – итог работа программы для зашифрования в 1 задании

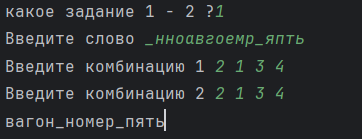


Рис 2 – итог работы программы для расшифрования в 1 задании

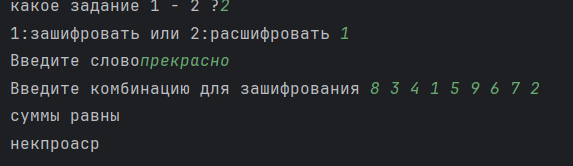
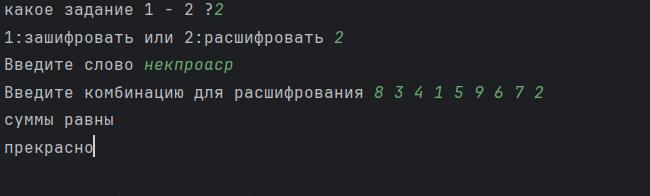


Рис 3 – итог работы программы для зашифрования во 2 задании



Рису 4 – итог работы программы для расшифрования во 2 задании

**Вывод:** в ходе лабораторной работы были изучены методы шифрования текста такие, как метод шифрующих таблиц и шифрование с помощью магического квадрата