

Отчёт по лабораторной работе №2

Аветисян Давид Артурович

27 Сентября 2024

РУДН, Москва, Россия

1. Программно реализовать маршрутное шифрование.
2. Программно реализовать шифрование с помощью решёток.
3. Программно реализовать шифр Виженера.

Реализация маршрутного шифрования

- Сначала я реализовал возможность выбора одного из трёх шифров пользователем. Затем начал с маршрутного шифрования. Я сделал запрос текста и пароля у пользователя, их фильтрацию и добавил проверки на соответствие требованиям для шифрования.

```
print('Выберите один из шифров перестановки:')
print('1. Маршрутное шифрование')
print('2. Шифрование с помощью решёток')
print("3. Таблица Виженера")
choice = input('Введите номер выбранного шифра: ')
match choice:
    case '1':
        text = input('Введите текст: ')
        filter_text = ''.join(filter(str.isalnum, text)).upper()
        password = input('Введите пароль: ')
        filter_password = ''.join(filter(str.isalnum, password)).upper()
        if len(filter_text) > len(filter_password):
            if len(set(filter_password)) == len(filter_password):
                encrypter_route = route_cipher(filter_text, filter_password)
                print("Криптограмма:", encrypter_route)
            else:
                print('Буквы пароля не должны повторяться!')
        else:
            print('Текст должен быть длиннее пароля!')
    case '2':
        print('2. Шифрование с помощью решёток')
    case '3':
        print("3. Таблица Виженера")
    case _:
```

Реализация маршрутного шифрования

- Я реализовал русский алфавит для удобного заполнения массивов. Далее я реализовал функцию `route_cipher`, в которой создал матрицу размером с текст пользователя и шириной с его пароль.

```
import math
import random

russian_letter = [chr(i) for i in range(ord('А'), ord('Я') + 1)]

def cryptogram(matrix, password):
    return

def route_cipher(text, password):
    rows = math.ceil(len(text)/len(password))
    cols = len(password)
    matrix = []
    for _ in range(rows):
        row = [random.choice(russian_letter) for _ in range(cols)]
        matrix.append(row)

    i, j = 0, 0
    for char in text:
        matrix[i][j] = char
        j += 1
        if j >= cols:
```

Реализация маршрутного шифрования

- После я реализовал общую для первого и второго шифрования функцию cryptogram, которая из заданного массива и введённого пользователем пароля создаёт таблицу, которую выводит, а затем создаётся криптограмму.

```
def cryptogram(matrix, password):
    matrix.append[''] * len(password)
    matrix.append[''] * len(password)
    j = 0
    for char in password:
        matrix[-2][j] = char
        matrix[-1][j] = ord(char)
        j += 1

    for i in range(len(matrix[:-1])):
        for j in range(len(matrix[i])):
            value = matrix[i][j]
            if i == len(matrix[:-2]):
                print(Fore.GREEN + str(value) + Style.RESET_ALL, end=' ')
            else:
                print(value, end=' ')
        print()

    last_row = matrix[-1]
    sorted_indices = sorted(range(len(last_row)), key=lambda x: last_row[x])
    sorted_matrix = []
    for row in matrix[:-2]:
        sorted_row = [row[i] for i in sorted_indices]
        sorted_matrix.append(sorted_row)
    transposed_matrix = [[row[i] for row in sorted_matrix] for i in range(len(sorted_matrix[0]))]
    result = ''.join('').join(row) for row in transposed_matrix
    return result
```

Реализация маршрутного шифрования

- Далее я запустил два теста через командную строку. Шифрование совпало с тестом в лабораторной работе №2, и реализовано верно.

```
C:\Users\yaeda\OneDrive\Рабочий стол\RUDN\МОЗИИИБ>py lab02.py
Выберите один из шифров перестановки:
```

1. Маршрутное шифрование
2. Шифрование с помощью решёток
3. Таблица Виженера

Введите номер выбранного шифра: 1

Введите текст: нельзя недооценивать противника

Введите пароль: пароль

Маршрутное шифрование:

Н Е Л Ь З Я

Н Е Д О О Ц

Е Н И В А Т

Ь П Р О Т И

В Н И К А О

П А Р О Л Ь

Криптограмма: ЕЕНПНЗОАТАЬОВОКННЕЬВЛДИРИЯЦИО

```
C:\Users\yaeda\OneDrive\Рабочий стол\RUDN\МОЗИИИБ>py lab02.py
Выберите один из шифров перестановки:
```

1. Маршрутное шифрование
2. Шифрование с помощью решёток
3. Таблица Виженера

Введите номер выбранного шифра: 1

Введите текст: математические основы информационной безопасности

Введите пароль: физмат

Маршрутное шифрование:

М А Т Е М А

Т И Ч Е С К

И Е О С Н О

Реализация шифрования с помощью решёток

- Затем я перешёл к реализации шифрования с помощью решёток. Я аналогично предыдущему шифрованию запросил текст у пользователя, но в данном случае я запрашиваю пароль необходимой длины $2k$, как сказано в теории к лабораторной работы.

```
case '2':
    text = input('Введите текст: ')
    filter_text = ''.join(filter(str.isalnum, text)).upper()
    sqrt_text = math.ceil(math.sqrt(len(filter_text)))
    if sqrt_text % 2 == 1:
        sqrt_text += 1
    while len(filter_text) < (sqrt_text**2):
        filter_text += random.choice(russian_letters)
    password = input(f'Введите пароль длиной {sqrt_text} букв(ы): ')
    filter_password = ''.join(filter(str.isalnum, password)).upper()
    if len(set(filter_password)) == len(filter_password):
        if sqrt_text == len(filter_password):
            encrypted_lattice = lattice_cipher(filter_text, filter_password)
            print("Криптограмма:", encrypted_lattice)
        else:
            print(f'В пароле должно быть {sqrt_text} букв(ы)!!')
    else:
        print('Буквы пароля не должны повторяться!')
```

Рис. 5: Начало реализации шифрования с помощью решёток

Реализация шифрования с помощью решёток

- Далее я реализовал функцию `lattice_cipher`, в которой я создал матрицу размера $2k$ и заполнил её нулями.

```
def lattice_cipher(text, password):
    rows, cols = len(password), len(password)
    matrix = [[0 for _ in range(cols)] for _ in range(rows)]
    k = int(len(password)/2)

    for _ in range(4):
        i, j, number = 0, 0, 0
        for i in range(k):
            for j in range(k):
                number += 1
                matrix[i][j] = number
            matrix = rotate_matrix_clocwise(matrix)

    unique_values = set()
    for row in matrix:
        unique_values.update(row)
    coordinates = {value: [] for value in unique_values}
    for i in range(len(matrix)):
        for j in range(len(matrix[i])):
            value = matrix[i][j]
            if value in coordinates:
                coordinates[value].append((i, j))
    selected_coordinates = {}
    for number in range(1, k**2+1):
        if coordinates[number]:
            selected_coordinates[number] = random.choice(coordinates[number])

    print("Решето:")
    for i in range(len(matrix)):
        for j in range(len(matrix[i])):
            value = matrix[i][j]
```


- Для того чтобы заполнить матрицу значениями от 1 до k^2 , я реализовал функцию вращения матрицы на 90 градусов по часовой стрелке.

```
def rotate_matrix_clocwise(matrix):  
    transposed_matrix = []  
    for j in range(len(matrix[0]) - 1, -1, -1):  
        new_row = []  
        for i in range(len(matrix)):  
            new_row.append(matrix[i][j])  
        transposed_matrix.append(new_row)  
    return transposed_matrix
```

Рис. 7: Функция вращения матрицы на 90 градусов по часовой стрелк

Реализация шифрования с помощью решёток

- Далее для правильного заполнения матрицы текстом пользователя, я реализовал 4 похожих, но разных цикла. Я заполнял все уникальные значения побуквенно текстом пользователя.

```
letter, i, j, count = 0, 0, 0, 0
while count < k**2:
    if (i,j) in selected_coordinates.values():
        matrix[i][j] = text[letter]
        letter += 1
        count += 1
    j += 1
    if j >= cols:
        i += 1
        j = 0
    matrix = rotate_matrix_clocwise(matrix)

i, j, count = rows - 1, 0, 0
while count < k**2:
    if (i,j) in selected_coordinates.values():
        matrix[i][j] = text[letter]
        letter += 1
        count += 1
    j += 1
    if j >= cols:
        i -= 1
        j = 0
    matrix = rotate_matrix_clocwise(matrix)
```

Реализация шифрования с помощью решёток

- Далее я запустил два теста через командную строку. Шифрование совпало с тестом в лабораторной работе №2, и реализовано верно.

```
C:\Users\yaeda\OneDrive\Рабочий стол\RUDN\МОЗНИИБ>py lab02.py
Выберите один из шифров перестановки:
1. Маршрутное шифрование
2. Шифрование с помощью решёток
3. Таблица Виженера
Введите номер выбранного шифра: 2
Введите текст: договор подписали
Введите пароль длиной 4 букв(ы): шифр
Решето:
1 2 3 0
0 0 4 0
0 4 0 0
0 3 2 1
Шифрование с помощью решёток:
Д О О В
О С Г Р
А Д П Л
И О П И
Ш И Ф Р
Криптограмма: ОСДОВРЛИОГППДОИИ
```

Рис. 9: Тест реализации маршрутного шифрования из лабораторной работы №2

- В конце я перешёл к реализации шифра Виженера. В первую очередь для его реализации нам потребуется таблица с русским алфавитом, где каждая следующая строка сдвигается на одну букву.

```
import math
import random
import numpy as np
from colorama import Fore, Style, init

init(autoreset=True)

russian_letters = [chr(i) for i in range(ord('А'), ord('Я') + 1)]
russian_matrix = np.empty(len(russian_letters). len(russian_letters), dtype='<U1')
for i in range(len(russian_letters)):
    for j in range(len(russian_letters)):
        letter_index = (i + j) % len(russian_letters)
        russian_matrix[i][j] = russian_letters[letter_index]
```

Рис. 10: Реализация таблицы с русским алфавитом

Реализация шифра Виженера

- Затем я перешёл к реализации шифра Виженера. Я аналогично предыдущим шифрованиям запросил текст и пароль у пользователя, отфильтровал их, а также проверил на соответствие требованиям для шифрования.

```
print('Буквы пароля не должны повторяться')
case '3':
    text = input('Введите текст: ')
    filter_text = ''.join(filter(str.isalnum, text)).upper()
    password = input('Введите пароль: ')
    filter_password = ''.join(filter(str.isalnum, password)).upper()
    if len(filter_text) > len(filter_password):
        if all('А' <= char <= 'Я' for char in filter_text):
            if all('А' <= char <= 'Я' for char in filter_password):
                vigenere_cipher(filter_text, filter_password)
            else:
                print('Пароль должен быть только из русских букв (и без ё)!')
        else:
            print('Текст должен быть только из русских букв (и без ё)!')
    else:
        print('Текст должен быть длиннее пароля!')
case _:
    print('Некорректный выбор!')
```

Рис. 11: Начало реализации шифра Виженера

Реализация шифра Виженера

- Далее я реализовал функцию `vigener_cipher`, в которой создаётся матрица, где первая строка - текст пользователя, вторая строка - повторяющийся пароль пользователя, а третья строка пуста (для будущей криптограммы).

```
def vigener_cipher(text, password):
    row1 = list(text)
    repeated_password = (password * (len(text) // len(password) + 1))[:len(text)]
    row2 = list(repeated_password)
    row3 = ['' for _ in range(len(text))]
    matrix = [row1, row2, row3]

    n, index_i, index_j = 0, -1, -1
    for n in range(len(text)):
        for j in range(len(russian_matrix[0])):
            if russian_matrix[0][j] == matrix[0][n]:
                index_j = j
                break
        for i in range(len(russian_matrix)):
            if russian_matrix[i][0] == matrix[1][n]:
                index_i = i
                break
        matrix[2][n] = russian_matrix[index_i][index_j]

    print("Шифр Виженера:")
    for i in range(len(matrix)):
        for j in range(len(matrix[i])):
            value = matrix[i][j]
            if i == len(matrix[:1]):
                print(Fore.GREEN + str(value) + Style.RESET_ALL, end=' ')
            else:
```

Реализация шифра Виженера

- Далее я запустил два теста через командную строку. Шифрование совпало с тестом в лабораторной работе №2, и реализовано верно.

```
C:\Users\yaeda\OneDrive\Рабочий стол\RUDN\МОЗИИИБ>py lab02.py
Выберите один из шифров перестановки:
1. Маршрутное шифрование
2. Шифрование с помощью решёток
3. Таблица Виженера
Введите номер выбранного шифра: 3
Введите текст: криптография серьёзная наука
Введите пароль: математика
Шифр Виженера:
К Р И П Т О Г Р А Ф И Я С Е Р Ь Е З Н А Я Н А У К А
М А Т Е М А Т И К А М А Т Е М А Т И К А М А Т Е М А
Ц Р Ь Ф Ю О Х Ш К Ф Ф Я Г К Ь Ъ Ч П Ч А Л Н Т Ш Ц А

C:\Users\yaeda\OneDrive\Рабочий стол\RUDN\МОЗИИИБ>py lab02.py
Выберите один из шифров перестановки:
1. Маршрутное шифрование
2. Шифрование с помощью решёток
3. Таблица Виженера
Введите номер выбранного шифра: 3
Введите текст: математические основы защиты информации
Введите пароль: шифр
Шифр Виженера:
М А Т Е М А Т И Ч Е С К И Е О С Н О В Ы З А Щ И Т Ы И Н Ф О Р М А Ц И И
Ш И Ф Р Ш И Ф Р Ш И Ф Р Ш И Ф Р Ш И Ф Р Ш И Ф Р Ш И Ф Р Ш И Ф Р
Д И Ж Х Д И Ж Ш П Н Е Ъ А Н В Б Е Ц Ц Л Я И Н Ш К Г Ъ Э М Ц Д Ъ Ш Ю Ъ Ш
```

Рис. 13: Проверка реализации шифра Виженера

- Я программно реализовал шифры перестановки.