Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей
Кафедра информатики
Дисциплина: Информационные сети. Основы безопасности.

ОТЧЁТ
к лабораторной работе №1
на тему

Шифр Цезаря и Виженера

Выполнил: студент группы 153504
Тиханёнок Илья Александрович

Проверил: Лещенко Евгений Александрович

Минск 2024

СОДЕРЖАНИЕ

1 ПОСТАНОВКА ЗАДАЧИ

Целью выполнения лабораторной работы является изучение теоретических сведений по алгоритмам шифрования Цезаря и Виженера, реализация программного средства, читающие данные из файла и шифрующие(дешифрующие) их при помощи шифра Цезаря (шифра сдвига, кода Цезаря) и шифра Виженера.

2 РЕЗУЛЬТАТЫ ВЫПОЛНЕНИЯ ЛАБОРАТОРНОЙ РАБОТЫ

В ходе выполнения лабораторной работы была разработана программа, читающая данные из файла и шифрующие при помощи шифра Цезаря и Виженера соответственно. Блок-схема алгоритма для шифра Цезаря представлена ниже на рисунке 1.

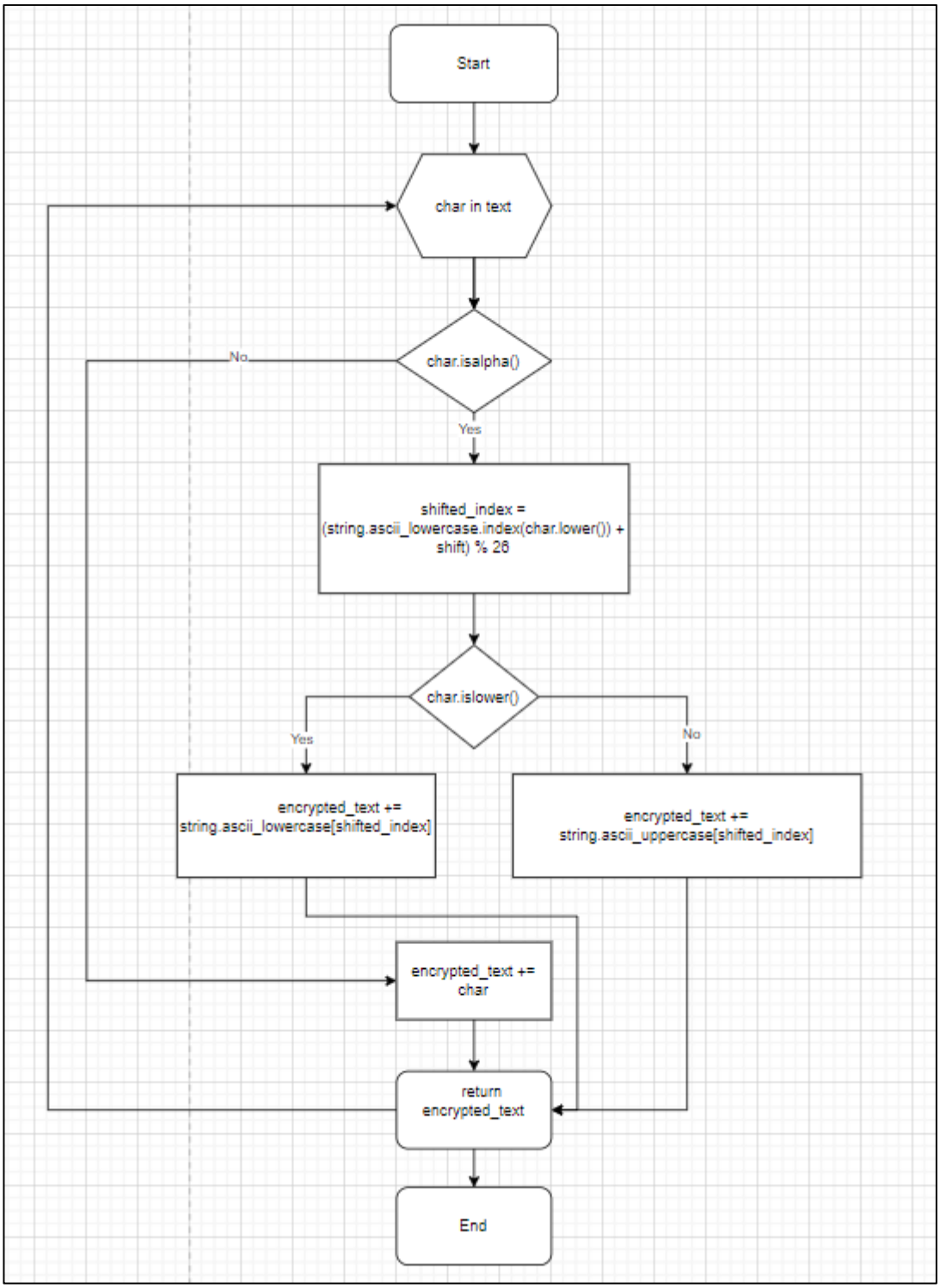

Рисунок 1 – Блок-схема алгоритма для шифра Цезаря

Блок-схема алгоритма для шифра Виженера представлена ниже на (Рисунок 2).

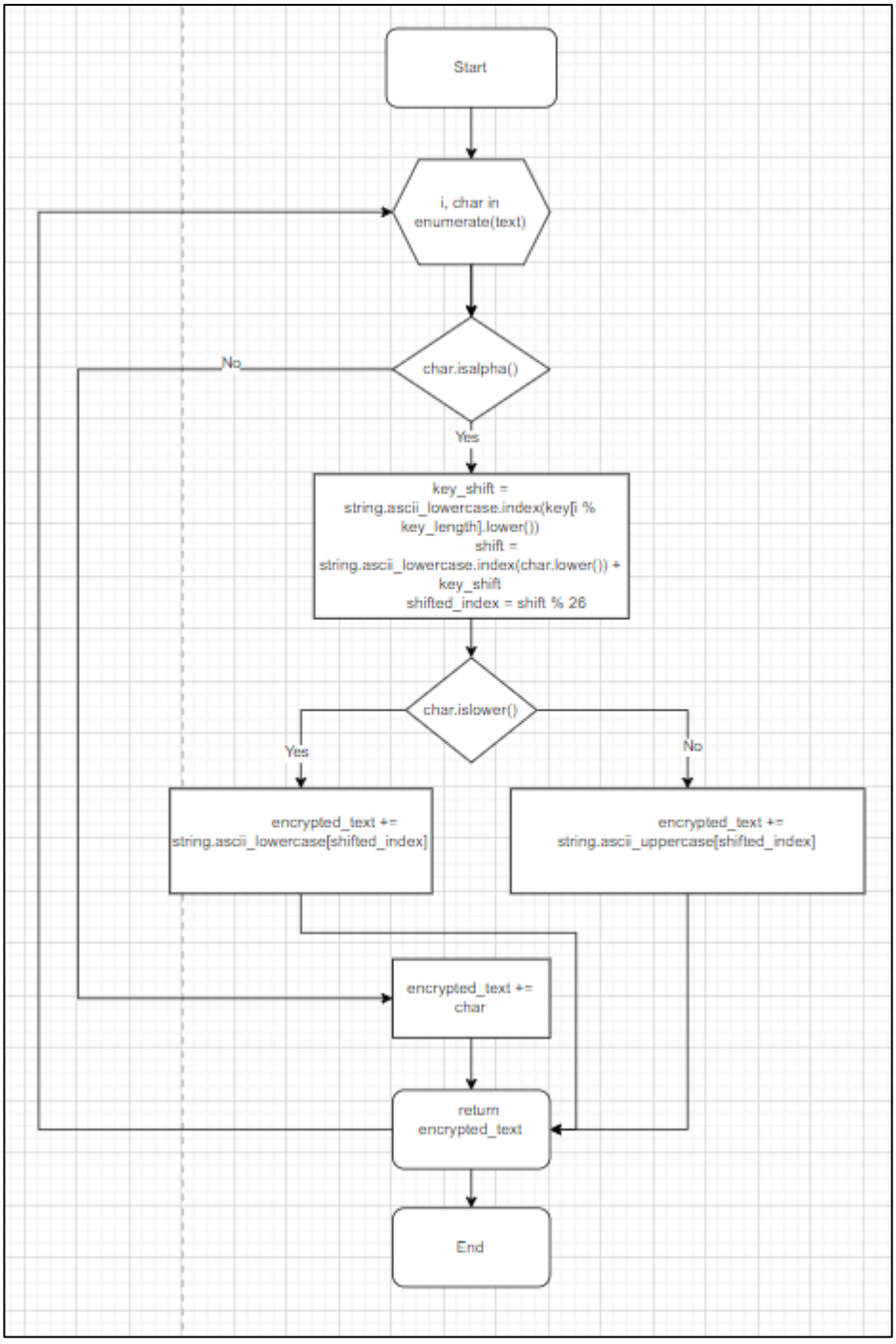

Рисунок 2 – Блок-схема алгоритма для шифра Виженера

Входные данные, записанные в файл для шифрования при помощи шифра Цезаря представлены на (Рисунок 2).

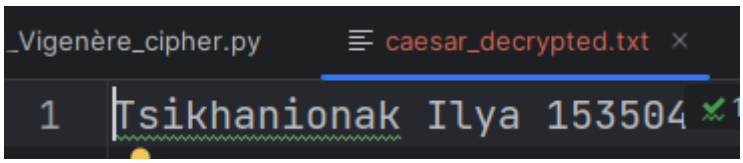

Рисунок 3 – Входные данные

После использования шифра был получен следующий результат представленный на рисунок 4.

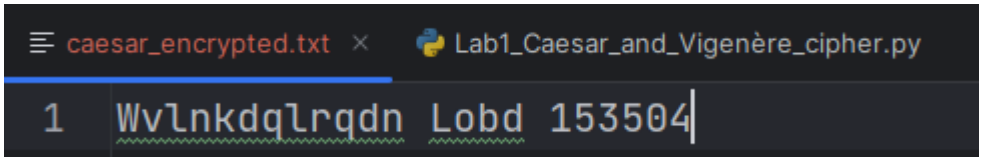

Рисунок 4 — Зашифрованная информация при помощи шифра Цезаря

Аналогичным образом были записаны входные данные в другой файл для шифрования при помощи шифра Виженера. Данные представлены на (Рисунок 5).

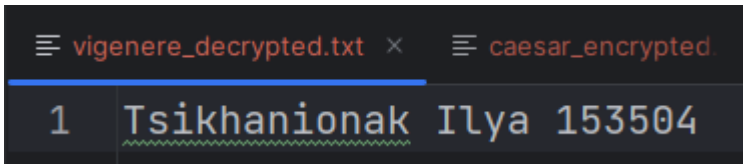

Рисунок 5 – Входные данные

Зашифрованные данные отражены на (Рисунок 6).

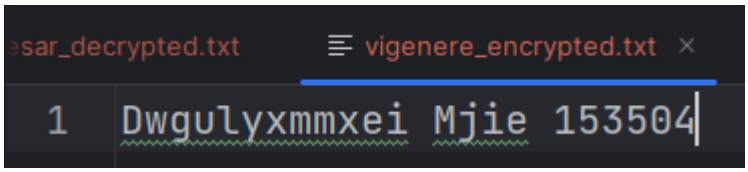

Рисунок 6 – Зашифрованная информация при помощи шифра Виженера

ВЫВОДЫ

В ходе выполнения данной лабораторной работы были изучены теоретические сведения по шифрованию, на примере шифра Цезаря и шифра Виженера, которые позволили реализовать программное средство шифрования и дешифрования текстовых файлов.

ПРИЛОЖЕНИЕ А
(обязательное)
Листинг кода

Lab1.py

```
import string


def caesar_cipher(text, shift):
    encrypted_text = ""
    for char in text:
        if char.isalpha():
            shifted_index = (string.ascii_lowercase.index(char.lower()) + shift) % 26
            if char.islower():
                encrypted_text += string.ascii_lowercase[shifted_index]
            else:
                encrypted_text += string.ascii_uppercase[shifted_index]
        else:
            encrypted_text += char
    return encrypted_text


def vigenere_cipher(text, key):
    key_length = len(key)
    encrypted_text = ""
    for i, char in enumerate(text):
        if char.isalpha():
            key_shift = string.ascii_lowercase.index(key[i % key_length].lower())
            shift = string.ascii_lowercase.index(char.lower()) + key_shift
            shifted_index = shift % 26
            if char.islower():
                encrypted_text += string.ascii_lowercase[shifted_index]
            else:
                encrypted_text += string.ascii_uppercase[shifted_index]
        else:
            encrypted_text += char
    return encrypted_text


def encrypt_file_caesar(input_file, output_file, shift):
    with open(input_file, 'r') as file:
        plaintext = file.read()
    encrypted_text = caesar_cipher(plaintext, shift)
    with open(output_file, 'w') as file:
        file.write(encrypted_text)
```

```
def decrypt_file_caesar(input_file, output_file, shift):
    with open(input_file, 'r') as file:
        ciphertext = file.read()
    decrypted_text = caesar_cipher(ciphertext, -shift)
    with open(output_file, 'w') as file:
        file.write(decrypted_text)


def encrypt_file_vigenere(input_file, output_file, key):
    with open(input_file, 'r') as file:
        plaintext = file.read()
    encrypted_text = vigenere_cipher(plaintext, key)
    with open(output_file, 'w') as file:
        file.write(encrypted_text)


def decrypt_file_vigenere(input_file, output_file, key):
    with open(input_file, 'r') as file:
        ciphertext = file.read()
    decrypted_text = vigenere_cipher(ciphertext, key)
    with open(output_file, 'w') as file:
        file.write(decrypted_text)


encrypt_file_caesar("input.txt", "caesar_encrypted.txt", 3)
decrypt_file_caesar("caesar_encrypted.txt", "caesar_decrypted.txt", 3)

encrypt_file_vigenere("input.txt", "vigenere_encrypted.txt", "key")
decrypt_file_vigenere("vigenere_encrypted.txt", "vigenere_decrypted.txt", "key")
```