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 3](#_Toc146728177)

[2 Результаты выполнения лабораторной работы 4](#_Toc146728179)

[Выводы 7](#_Toc146728180)

[Приложение А (обязательное) Листинг кода 8](#_Toc146728182)

## 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.

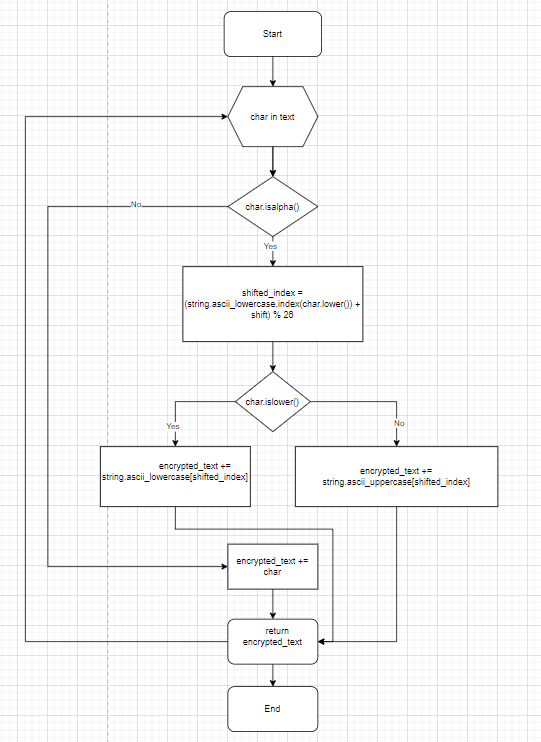


Рисунок 1 – Блок-схема алгоритма для шифра Цезаря

Блок-схема алгоритма для шифра Виженера представлена ниже на рисунке 2.

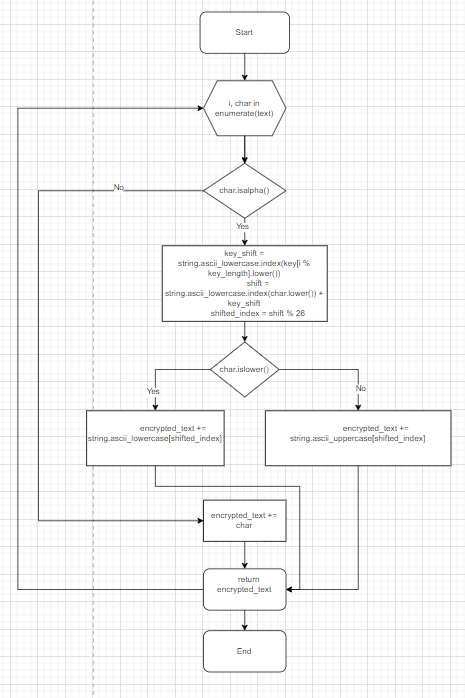


Рисунок 2 – Блок-схема алгоритма для шифра Виженера

Входные данные, записанные в файл для шифрования при помощи шифра Цезаря представлены на рисунке 3.

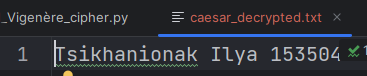


Рисунок 3 – Входные данные

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

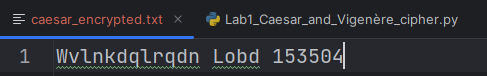


Рисунок 4 ─ Зашифрованная информация при помощи шифра Цезаря

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

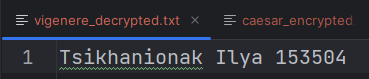


Рисунок 5 – Входные данные

Зашифрованные данные отражены на рисунке 6.

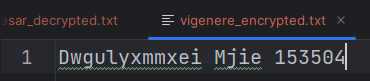


Рисунок 6 – Зашифрованная информация при помощи шифра Виженера

## 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")