Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет компьютерных систем и сетей

Кафедра информатики

Дисциплина: Информационные сети. Основы безопасности

ОТЧЕТ

к лабораторной работе №1

на тему

**ШИФР ЦЕЗАРЯ. ШИФР ВИЖЕНЕРА**

Студент Д. С. Кончик

Преподаватель Е. А. Лещенко

Минск 2024

СОДЕРЖАНИЕ

[Введение 3](#_Toc157471308)

[1 Результат выполнения 4](#_Toc157471309)

[Заключение 5](#_Toc157471310)

[Приложение А (обязательное) Листинг кода 6](#_Toc157471311)

[Приложение Б (обязательное) Блок-схема алгоритма 8](#_Toc157471312)

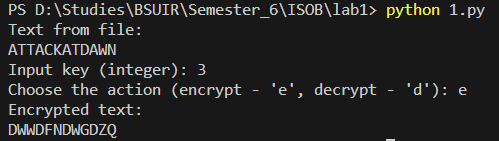
**ВВЕДЕНИЕ**

Лабораторная работа ставит перед собой задачу разработки программных средств для шифрования и дешифрования текстовых файлов с использованием двух классических методов шифрования: шифра Цезаря и шифра Виженера.

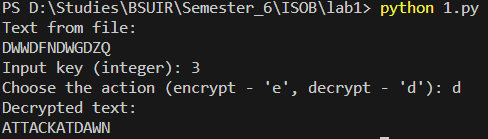
Основная цель работы – изучение принципов работы указанных алгоритмов и их реализация на языке программирования *Python*. В ходе работы будет осуществлен анализ методов шифрования, разработка алгоритмов шифрования и дешифрования, а также создание программного продукта, позволяющего осуществлять шифрование и дешифрование текстовых файлов.

1. **РЕЗУЛЬТАТ ВЫПОЛНЕНИЯ**

В результате работы было создано два приложения для шифрования и дешифрования текстовых файлов: с использованием шифра Цезаря   
(рисунок 1) и шифра Виженера (рисунок 2).



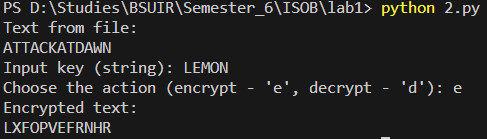
а



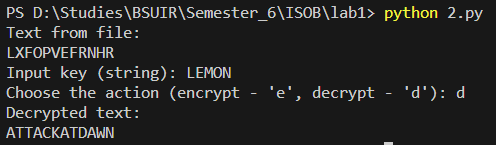
б

а – шифрование; б – дешифрование

Рисунок 1 – Шифр Цезаря



а



б

а – шифрование; б – дешифрование

Рисунок 2 – Шифр Виженера

# ЗАКЛЮЧЕНИЕ

В результате выполнения данной лабораторной работы были разработаны программные средства для шифрования и дешифрования текстовых файлов с применением шифра Цезаря и шифра Виженера на языке программирования *Python*.

Был проведен анализ методов шифрования и алгоритмов работы с текстовыми файлами, разработана блок-схема алгоритма, написаны и отлажены программы для шифрования и дешифрования файлов.

При выполнении работы были использованы теоретические сведения о принципах работы шифра Цезаря и шифра Виженера и получены практические навыки работы с данными алгоритмами.

# ПРИЛОЖЕНИЕ А (обязательное) Листинг кода

Листинг 1 – Файл *common.py*

import re

def caesar\_encrypt(text, k):

    result = ''

    for x in text:

        y = chr((ord(x) - ord('A') + k) % 26 + ord('A'))

        result += y

    return result

def caesar\_decrypt(text, k):

    result = ''

    for y in text:

        x = chr((ord(y) - ord('A') - k + 26) % 26 + ord('A'))

        result += x

    return result

def is\_english\_letters\_only(string):

    return bool(re.match("^[A-Z]+$", string))

Листинг 2 – Файл *1.py*

from common import caesar\_encrypt, caesar\_decrypt, is\_english\_letters\_only

def main():

    file\_name = "example.txt"

    try:

        with open(file\_name, 'r', encoding='utf-8') as file:

            text = file.read()

    except FileNotFoundError:

        print(f"File '{file\_name}' not found.")

        return

    print(f"Text from file:\n{text}")

    if is\_english\_letters\_only(text):

        k = int(input("Input key (integer): "))

        action = input("Choose the action ('e', 'd'): ").lower()

        if action == 'e':

            result = caesar\_encrypt(text, k)

            print(f"Encrypted text:\n{result}")

        elif action == 'd':

            result = caesar\_decrypt(text, k)

            print(f"Decrypted text:\n{result}")

        else:

            print("Incorrect action. Choose 'e' or 'd'.")

    else:

        print("Source text is incorrect. Use only english letters.")

if \_\_name\_\_ == "\_\_main\_\_":

    main()

Листинг 3 – Файл *2.py*

from common import caesar\_encrypt, caesar\_decrypt, is\_english\_letters\_only

def adjust\_key(text: str, key: str):

    extended\_key = key

    while len(extended\_key) < len(text):

        extended\_key += key

    return extended\_key[:len(text)]

def main():

    file\_name = "example.txt"

    try:

        with open(file\_name, 'r', encoding='utf-8') as file:

            text = file.read()

    except FileNotFoundError:

        print(f"File '{file\_name}' not found.")

        return

    print(f"Text from file:\n{text}")

    if is\_english\_letters\_only(text):

        key = input("Input key (string): ")

        if is\_english\_letters\_only(key):

            key = adjust\_key(text, key)

            action = input("Choose the action ('e', 'd'): ").lower()

            result = ''

            if action == 'e':

                for i in range(len(text)):

                    result += caesar\_encrypt(text[i], ord(key[i]) - ord('A'))

                print(f"Encrypted text:\n{result}")

            elif action == 'd':

                for i in range(len(text)):

                    result += caesar\_decrypt(text[i], ord(key[i]) - ord('A'))

                print(f"Decrypted text:\n{result}")

            else:

                print("Incorrect action. Choose 'e' or 'd'.")

        else:

            print("Key is incorrect. Use only caps english letters.")

    else:

        print("Source text is incorrect. Use only caps english letters.")

if \_\_name\_\_ == "\_\_main\_\_":

    main()

# ПРИЛОЖЕНИЕ Б (обязательное) Блок-схема алгоритма

