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

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).

```
PS D:\Studies\BSUIR\Semester_6\ISOB\lab1> python 1.py
Text from file:
ATTACKATDAWN
Input key (integer): 3
Choose the action (encrypt - 'e', decrypt - 'd'): e
Encrypted text:
DWWDFNDWGDZQ
```

а

```
PS D:\Studies\BSUIR\Semester_6\ISOB\lab1> python 1.py
Text from file:
DWWDFNDWGDZQ
Input key (integer): 3
Choose the action (encrypt - 'e', decrypt - 'd'): d
Decrypted text:
ATTACKATDAWN
```

б

а – шифрование; б – дешифрование

Рисунок 1 – Шифр Цезаря

```
PS D:\Studies\BSUIR\Semester_6\ISOB\lab1> python 2.py
Text from file:
ATTACKATDAWN
Input key (string): LEMON
Choose the action (encrypt - 'e', decrypt - 'd'): e
Encrypted text:
LXFOPVEFRNHR
```

а

```
PS D:\Studies\BSUIR\Semester_6\ISOB\lab1> python 2.py
Text from file:
LXFOPVEFRNHR
Input key (string): LEMON
Choose the action (encrypt - 'e', decrypt - 'd'): d
Decrypted text:
ATTACKATDAWN
```

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