МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

федеральное государственное бюджетное образовательное учреждение высшего образования

**«Вологодский государственный университет»**

**Институт математики, естественных и компьютерных наук**

**Информатика и вычислительная техника**

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 3**

Шифр просто замены. Таблица Виженера

Дисциплина: «Защита информации»

Направление подготовки: 09.03.01. Информатика и вычислительная техника

|  |  |
| --- | --- |
| Руководитель | Давыдова.Е.Н |
| Выполнили студенты | Пчелкина О.С. |
| Группа, курс | 4Б09 ВМ-41 4 курс |
| Дата сдачи | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Дата защиты | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  *(подпись преподавателя)* |

Вологда

2023 г.

Цель: ознакомиться с алгоритмами шифрования и реализовать программу с использованием изученных алгоритмов.

1. Процедур шифрования и расшифрования с использованием шифра Цезаря при вводе с клавиатуры ключа и исходного или зашифрованного текста. Учтите регистр вводимого текста.

Исходный код:

def encrypt\_caesar(plaintext, shift):

    encrypted\_text = ""

    for char in plaintext:

        if char.isalpha():

            shifted\_char = chr((ord(char.lower()) - 97 + shift) % 26 + 97)

            if char.isupper():

                shifted\_char = shifted\_char.upper()

            encrypted\_text += shifted\_char

        else:

            encrypted\_text += char

    return encrypted\_text

def decrypt\_caesar(ciphertext, shift):

    decrypted\_text = ""

    for char in ciphertext:

        if char.isalpha():

            shifted\_char = chr((ord(char.lower()) - 97 - shift) % 26 + 97)

            if char.isupper():

                shifted\_char = shifted\_char.upper()

            decrypted\_text += shifted\_char

        else:

            decrypted\_text += char

    return decrypted\_text

plaintext = input("Введите текст для шифрования: ")

shift = int(input("Введите сдвиг: "))

encrypted\_text = encrypt\_caesar(plaintext, shift)

print("Зашифрованное сообщение: ", encrypted\_text)

decrypted\_text = decrypt\_caesar(encrypted\_text, shift)

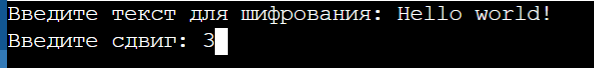
print("Расшифрованное сообщение: ", decrypted\_text)

with open("output.txt", "w") as file:

    file.write("Зашифрованное сообщение: " + encrypted\_text + "\n")

    file.write("Расшифрованное сообщение: " + decrypted\_text)

Пример работы





1. Процедур шифрования и расшифрования с использованием шифра Вижинера при вводе с клавиатуры ключа и исходного или зашифрованного текста. Учтите регистр вводимого текста.

Исходный код:

def encryptvigenere(plaintext, key):

    ciphertext = ""

    keyindex = 0

    for char in plaintext:

        if char.isalpha():

            if char.isalpha() and ord(char) < 128:

                charcode = ord(char.upper()) - 65

            else:

                charcode = ord(char) - 1040

            if key[keyindex].isalpha() and ord(key[keyindex]) < 128:

                keycode = ord(key[keyindex].upper()) - 65

            else:

                keycode = ord(key[keyindex]) - 1040

            if char.isalpha() and ord(char) < 128:

                ciphertext += chr(((charcode + keycode) % 26) + 65)

            else:

                ciphertext += chr(((charcode + keycode) % 32) + 1040).encode('utf-8').decode('utf-8')

            keyindex = (keyindex + 1) % len(key)

        else:

            ciphertext += char

    return ciphertext

def decryptvigenere(ciphertext, key):

    plaintext = ""

    keyindex = 0

    for char in ciphertext:

        if char.isalpha():

            if char.isalpha() and ord(char) < 128:

                charcode = ord(char.upper()) - 65

            else:

                charcode = ord(char) - 1040

            if key[keyindex].isalpha() and ord(key[keyindex]) < 128:

                keycode = ord(key[keyindex].upper()) - 65

            else:

                keycode = ord(key[keyindex]) - 1040

            if char.isalpha() and ord(char) < 128:

                plaintext += chr(((charcode - keycode) % 26) + 65)

            else:

                plaintext += chr(((charcode - keycode) % 32) + 1040).encode('utf-8').decode('utf-8')

            keyindex = (keyindex + 1) % len(key)

        else:

            plaintext += char

    return plaintext

plaintext = input("Введите исходный текст: ")

key = input("Введите ключ: ")

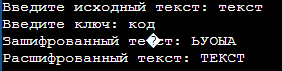
ciphertext = encryptvigenere(plaintext, key)

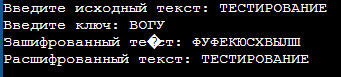
print("Зашифрованный текст:", ciphertext)

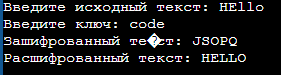
decryptedtext = decryptvigenere(ciphertext, key)

print("Расшифрованный текст:", decryptedtext)

Пример работы:







Вывод: в ходе лабораторной работы мы реализовали программы с использованием алгоритма шифрования Цезаря и Виженера.