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 № 6**

Шифры замены.

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 работы***: реализация блочного шифра.

**Задание на лабораторную работу**

Согласно варианту реализовать один из блочных шифров.

Программа просит ввести пользователю сообщение и сдвиг, затем шифрует и расшифровывает сообщение с помощью шифра Цезаря и выводит результаты на экран. Затем она сохраняет зашифрованный и расшифрованный текст в файл "output.txt".

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)

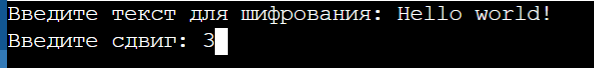
print("Расшифрованное сообщение: ", decrypted\_text)

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

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

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

Пример работы





Вывод: в ходе лабораторной работы реализовали блочный шифр Цезаря.