Шифры простой замены

Гурбангельдиев Мухаммет [1]

2022 Moscow, Russia

RUDN University, Moscow, Russian Federation

Цель работы

Цель лабораторной работы

Приобретение навыков программной реализации простых шифров подстановки и замены.

Задание

Задания к лабораторной работе

1. Реализовать шифр Цезаря с произвольным ключом k.
2. Реализовать шифр Атбаш.

Реализация

Реализация шифра Цезаря

Функция caesar для шифрования и расшифровки текста. (рис. -fig. 1)

```
alphabet = ['a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u',
            'v', 'w', 'x', 'y', 'z', 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p',
            'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y', 'z']
```

```
def caesar(start, shift, direction):
    end_text = ""
    if direction == "decode":
        shift *= -1
    for char in start:
        position = alphabet.index(char)
        new_position = (position + shift) % 26
        end_text += alphabet[new_position]
    else:
        end_text += char
    print(f"Here's the {direction}d result: {end_text}")
```

Рис. 1: Функция для кодирования текста шифром Цезаря

Реализация шифра Атбаша

Функция atbash для шифрования и расшифровки текста. (рис. -fig. 2)

```
def atbash(start):
    end_text = ""
    for char in start:
        if char in alphabet:
            position = alphabet.index(char)+1
            end_text += alphabet[position*(-1)]
    else:
        end_text += char
    print(f"Here's the atbash result: {end_text}")
```

Рис. 2: Функция для кодирования текста шифром Атбаша

Процесс выполнения

Описан блок выбора нужного метода и ввода текста. (рис. -fig. 3)

```
should_continue = True
while should_continue:
    cipher = input("Введите 'caesar' чтобы использовать шифр Цезаря, введите 'atbash' чтобы использовать шифр Атбаша:\n")
    text = input("Введите ваше сообщение:\n").lower()

    if cipher == "caesar":
        direction = input("Введите 'encode' для шифрования, а 'decode' для расшифрования:\n")
        shift = int(input("Введите количество сдвигов:\n"))
        shift = shift % 26
        caesar(start=text, shift=shift, direction = direction)
    else:
        atbash(start=text)

    restart = input("Введите 'y' чтобы продолжить, в противном случае 'n'.\n")
    if restart == "n":
        should_continue == False
        print("Пока!")
```

Рис. 3: Код для выбора метод шифрования и ввода текста

Результат

Результат

```
Введите 'caesar' чтобы использовать шифр Цезаря, введите 'atbash' чтобы использовать шифр Атбаша:
caesar
Введите ваше сообщение:
privet
Введите 'encode' для шифрования, а 'decode' для расшифрования:
encode
Введите количество сдвигов:
3
Here's the encoded result: sulyhwt
Введите 'y' чтобы продолжить, в противном случае 'n'.
y
```

Рис. 4: Получение шифрования и расшифровки текста методом Цезаря

Результат

```
Введите 'caesar' чтобы использовать шифр Цезаря, введите 'atbash' чтобы использовать шифр Атбаша:
caesar
Введите ваше сообщение:
privet
Введите 'encode' для шифрования, а 'decode' для расшифрования:
decode
Введите количество сдвигов:
3
Here's the decoded result: mofsbqt
Введите 'y' чтобы продолжить, в противном случае 'n'.
y
```

Рис. 5: Получение шифрования и расшифровки текста методом Цезаря

Результат

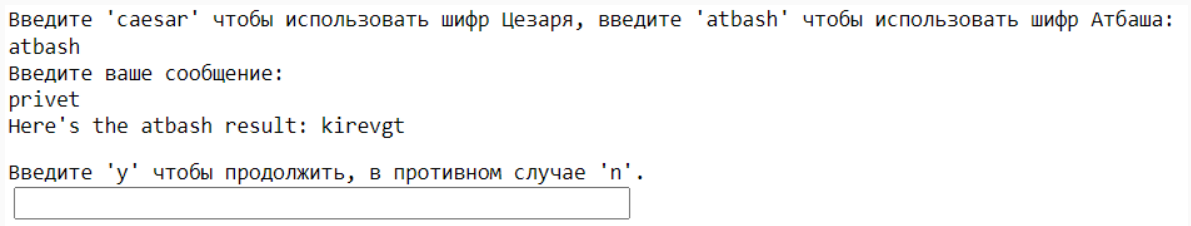

Рис. 6: Получение шифрования текста методом Атбаша

Вывод

Вывод

Приобрел навыки программной реализации простых шифров подстановки и замены.