Отчёт по лабораторной работе 1

Шифры простой замены

Каримов Зуфар НФИ-01-22

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Приобретение навыков программной реализации простых шифров подстановки и замены.

2 Теоретические сведения

Шифр Цезаря (также он является шифром простой замены) - это моноалфавитная подстановка, т.е. каждой букве открытого текста ставится в соответствие одна буква шифртекста. На практике при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит, но с нарушенным порядком букв алфавитная перестановка).

При достижении конца алфавита выполнялся циклический переход к его началу. Таким образом, шифр-алфавит циклически сдвинут влево на K позиций относительно нормативного алфавита.

Цезарь использовал этот шифр замены при смещении. k = 3. Такой шифр можно задать таблицей подстановок, содержащей соответствующие пары букв открытого текста и шифротекста [1]. (рис. -fig. 2.1)

Порядковый номер символа	0	1	2	3	4		23	24	25
Нормативный алфавит	a	b	c	d	e		x	y	z
	↓	↓	↓	↓	↓	...	↓	↓	↓
Алфавит шифрования	d	e	f	g	h		a	b	c
Порядковый номер символа	3	4	5	6	7		0	1	2

Рис. 2.1: Шифр Цезаря

Шифр Атбаш:

Еще один шифр простой (моноалфавитной) замены. Шифрование осуществляется путем замены первой буквы алфавита на последнюю, второй на предпоследнюю и так далее. (рис. -fig. 2.2)

Этот шифр использовался для еврейского алфавита и отсюда получил свое название. Первая буква - алеф, заменяется на тау (последнюю), вторая буква - бет,

заменяется на шин (предпоследнюю). Из этих букв и сформировалось название.
[]

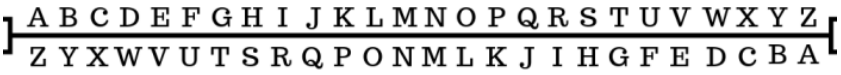

Рис. 2.2: Шифр Атбаш

3 Выполнение лабораторной работы

1. Написал функцию caesar для шифрования и расшифровки текста. (рис. -fig. 3.1)

Сначала написал алфавит в виде списки.

Для расшифровки умножил ключ на -1.

Написал цикл для проверки каждой буквы в нашем слове, а затем определил ее позицию в алфавите с помощью index метода, который возвращает индекс указанного элемента в списке. Как определил позицию, сложил на него ключ (shift). потом распечатал зашифрованный текст.

```
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 caeser(start, shift, direction):
    end_text = ""
    if direction == "decode":
        shift *= -1
    for char in start:
        if char in alphabet:
            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_rext}")
```

Рис. 3.1: Функция для кодирования текста шифром Цезаря

2. Написал функцию atbash для шифрования и расшифровки текста. (рис. -fig. 3.2)

Для атбаша сделал аналогично, для сдвига на всю длину алфавита нам нужно умножить позицию на -1.

```python
def albash(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_rext}")
```

Рис. 3.2: Функция для кодирования текста шифром Атбаша

3. Написал блок выбора нужного метода и ввода текста. (рис. -fig. 3.3)

```python
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. 3.3: Код для выбора метод шифрования и ввода текста

4. Зашифровал и расшифровал слова password с помощью шифра Цезаря. (рис. -fig. 3.4) (рис. -fig. 3.5)

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

Рис. 3.4: Получение шифрования текста методом Цезаря

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

Рис. 3.5: Получение шифрования текста методом Цезаря

5. Зашифровал и расшифровал слова password с помощью Атбаша. (рис. - fig. 3.6)

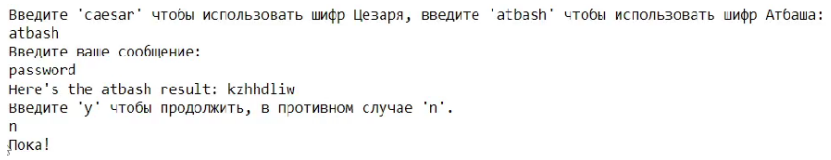

Рис. 3.6: Получение шифрования текста методом Атбаша

4 Выводы

Приобрел навыки программной реализации простых шифров подстановки и замены.

5 Список литературы

1. Шифры простой замены. — URL: https://studme.org/239550/informatika/shifry_prostoy_zameny.
2. Шифр Атбаш. — URL: https://studbooks.net/2215784/informatika/shifr_atbash.