

# Шифры простой замены

---

Гебриал Ибрам Есам Зекри <sup>1</sup>

2022 Moscow, Russia

<sup>1</sup>RUDN University, Moscow, Russian Federation

## Цель работы

---

Приобретение навыков программной реализации простых шифров подстановки и замены.

## Задание

---

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

## Реализация

---

# Реализация шифра Цезаря

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

```
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']  
2  
3 def caesar(start, shift, direction):  
4     end_text = ""  
5     if direction == "decode":  
6         shift *= -1  
7     for char in start:  
8         if char in alphabet:  
9             position = alphabet.index(char)  
10            new_position = (position + shift) % 26  
11            end_text += alphabet[new_position]  
12        else:  
13            end_text += char  
14    print(f"Here's the {direction}d result:  
    {end_text}")  
15
```

Figure 1: Функция для кодирования текста шифром Цезаря

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

```
15
16 ▼ def atbash (start):
17     end_text = ""
18 ▼   for char in start:
19 ▼       if char in alphabet:
20           position = alphabet.index(char)+1
21           end_text += alphabet[position*(-1)]
22 ▼       else:
23           end_text += char
24
25     print(f"Here's the atbash result: {end_text}")
26
```

Figure 2: Функция для кодирования текста шифром Атбаша



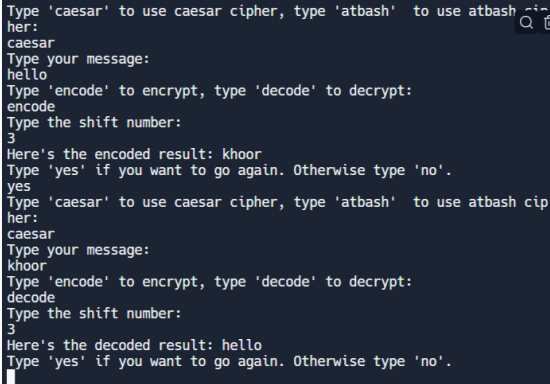
Описан блок выбора нужного метода и ввода текста. (рис. 3)

```
27 should_continue = True
28 ▼ while should_continue:
29     cipher= input("Type 'caesar' to use caesar cipher,
    type 'atbash' to use atbash cipher:\n")
30     text = input("Type your message:\n").lower()
31
32 ▼     if cipher == "caesar":
33         direction = input("Type 'encode' to encrypt,
    type 'decode' to decrypt:\n")
34         shift = int(input("Type the shift number:\n"))
35         shift = shift % 26
36         caesar(start=text, shift=shift,
    direction=direction)
37
38 ▼     else:
39         atbash(start=text)
40
41     restart = input("Type 'yes' if you want to go
    again. Otherwise type 'no'. \n")
42 ▼     if restart == "no":
43         should_continue = False
44         print("Goodbye")
45
```

Figure 3: Код для выбора метод шифрования и ввода текста

Результат

---



A terminal window with a dark blue background and white text. The text shows a sequence of commands and prompts for a Caesar cipher program. The first part shows the program being started with 'caesar', the message 'hello' being entered, and the shift number '3' being specified. The result 'khour' is displayed. The second part shows the program being started again with 'caesar', the message 'khour' being entered, and the shift number '3' being specified. The result 'hello' is displayed. In the top right corner of the terminal window, there are icons for search and trash.

```
Type 'caesar' to use caesar cipher, type 'atbash' to use atbash
her:
caesar
Type your message:
hello
Type 'encode' to encrypt, type 'decode' to decrypt:
encode
Type the shift number:
3
Here's the encoded result: khour
Type 'yes' if you want to go again. Otherwise type 'no'.
yes
Type 'caesar' to use caesar cipher, type 'atbash' to use atbash cip
her:
caesar
Type your message:
khour
Type 'encode' to encrypt, type 'decode' to decrypt:
decode
Type the shift number:
3
Here's the decoded result: hello
Type 'yes' if you want to go again. Otherwise type 'no'.
█
```

Figure 4: Получение шифрования и расшифровки текста методом Цезаря



```
Type 'caesar' to use caesar cipher, type 'atbash' to use atbash ^i~  
her:    
atbash  
Type your message:  
hello  
Here's the atbash result: svoool  
Type 'yes' if you want to go again. Otherwise type 'no'.  
█
```

Figure 5: Получение шифрования текста методом Атбаша

Приобрел навыки программной реализации простых шифров подстановки и замены..

Спасибо за внимание