

Цель работы

Освоить на практике применение Шифры простой замены [1].

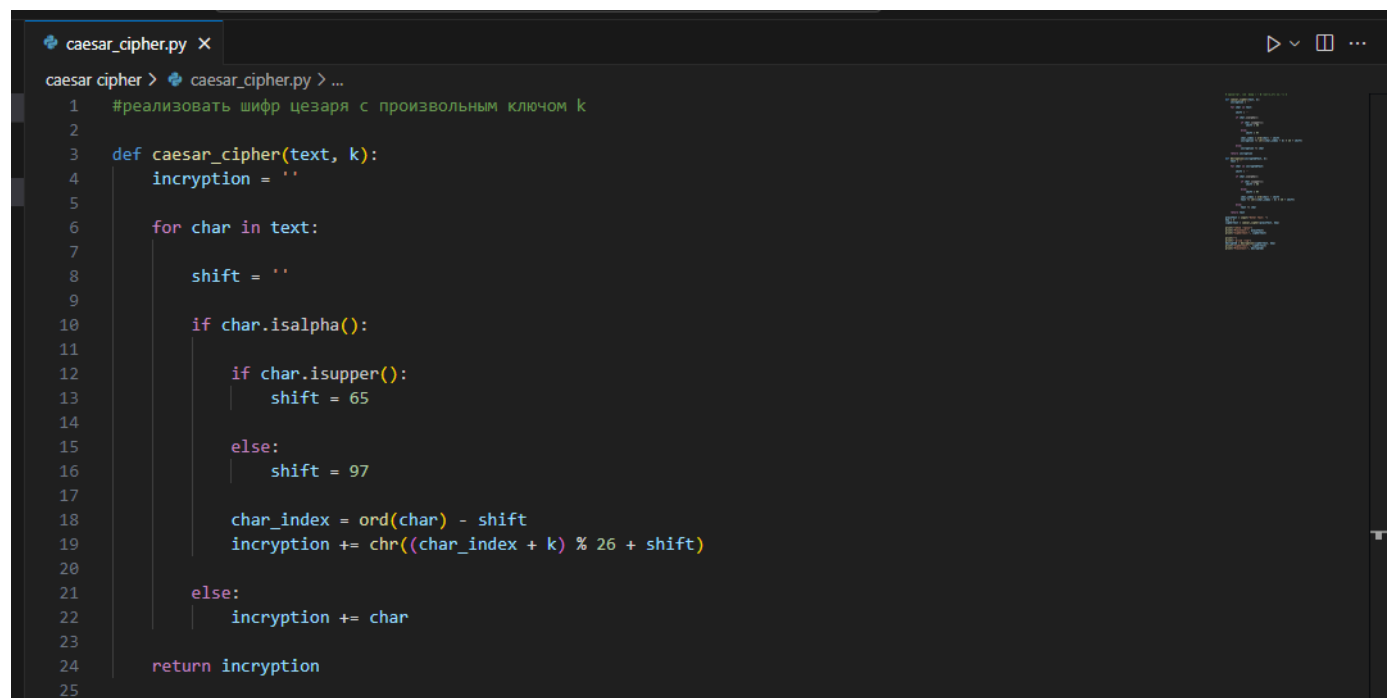
Задание

1 реализовать шифр цезаря с произвольным ключом k.

2 реализовать шифр Атбаш.

Выполнение лабораторной работы

Для выполнения работы была написана программа (@fig:1 - @fig:4) с помощью языка программирования Python, которая получает исходных текста от пользователя и произвольным ключом $k = 3$, затем шифрует исходные тексты методом шифр цезаря.



```
caesar_cipher.py x
caesar cipher > caesar_cipher.py > ...
1  #реализовать шифр цезаря с произвольным ключом k
2
3  def caesar_cipher(text, k):
4      incryption = ''
5
6      for char in text:
7
8          shift = ''
9
10         if char.isalpha():
11
12             if char.isupper():
13                 shift = 65
14
15             else:
16                 shift = 97
17
18             char_index = ord(char) - shift
19             incryption += chr((char_index + k) % 26 + shift)
20
21         else:
22             incryption += char
23
24     return incryption
25
```

```

25
26 def decryption(encryptedText, k):
27     text = ''
28
29     for char in encryptedText:
30
31         shift = ''
32
33         if char.isalpha():
34
35             if char.isupper():
36                 shift = 65
37
38             else:
39                 shift = 97
40
41             char_index = ord(char) - shift
42             text += chr((char_index - k) % 26 + shift)
43
44         else:
45             text += char
46
47     return text
48

```

```

48
49 plainText = input("Enter Text: ")
50 key = 3
51 ciphertext = caesar_cipher(plainText, key)
52
53 print("\nШифрование")
54 print("Plaintext:", plainText)
55 print("Ciphertext:", ciphertext)
56
57 print("")
58 print("Расшифровка")
59 decrypted = decryption(ciphertext, key)
60 print("Ciphertext:", ciphertext)
61 print("Plaintext:", decrypted)
62

```

MINGW64:/e/RUDN_Lessons/Semester1/Mathematical foundations of information protection and information security/Laps/Lap1/work/2023-2024/MOZiiIB/laboratory/lab01/caesar cipher

```

Liban@DESKTOP-DV306IP MINGW64 /e/RUDN_Lessons/Semester1/Mathematical foundations of information protection and information security/Laps/Lap1/work/2023-2024/MOZiiIB/laboratory/lab01/caesar cipher
$ python caesar_cipher.py
Enter Text: Mohamed Liban Abdullahi

Шифрование
Plaintext: Mohamed Liban Abdullahi
Ciphertext: Prkdphg Oledq Degxoodk1

Расшифровка
Ciphertext: Prkdphg Oledq Degxoodk1
Plaintext: Mohamed Liban Abdullahi

Liban@DESKTOP-DV306IP MINGW64 /e/RUDN_Lessons/Semester1/Mathematical foundations of information protection and information security/Laps/Lap1/work/2023-2024/MOZiiIB/laboratory/lab01/caesar cipher
$ |

```

Выводы

Освоено на практике применение Шифры простой замены.

Список литературы

1. Методические материалы курса