Лабораторная работа №1

Дисциплина: Математические основы защиты информации и информационной безопасности

Аветисян Давид Артурович

Содержание

List of Tables

List of Figures

1 Цель работы

Познакомиться с шифрами Цезаря и Атбаш.

2 Задание

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

3 Выполнение лабораторной работы

1) Сначала я реализовал шифр Цезаря на языке Python. Я использовал переменную k в качестве сдвига. При проверке слова берётся конкретный символ (char). Далее при помощи match-case я реализовал проверки на наличие выбранного символа в русском или английском алфавите. При этом я учёл регистр символа. Если символ находится в алфавите, то берётся его код ASCII, из которого вычитается код ASCII первой буквы алфавита. Затем прибавляется сдвиг k и берётся остаток от количества символов в алфавите (русский - 32, английский 26). После чего мы определяем, какая по счёту буква в алфавите, и прибавляем код ASCII первой буквы алфавита. Затем вписываем каждый символ в result и возвращаем его.

Figure 3.1: Шифр Цезаря на языке Python

2) Далее я реализовал запрос текста у пользователя и вывод результата алго-

ритма шифра Цезаря.

```
37   text = input ("Введите текст:\t")
38   encrypted_caesar = caesar_cipher(text, k)
39   print("Шифр Цезаря:\t", encrypted_caesar)
```

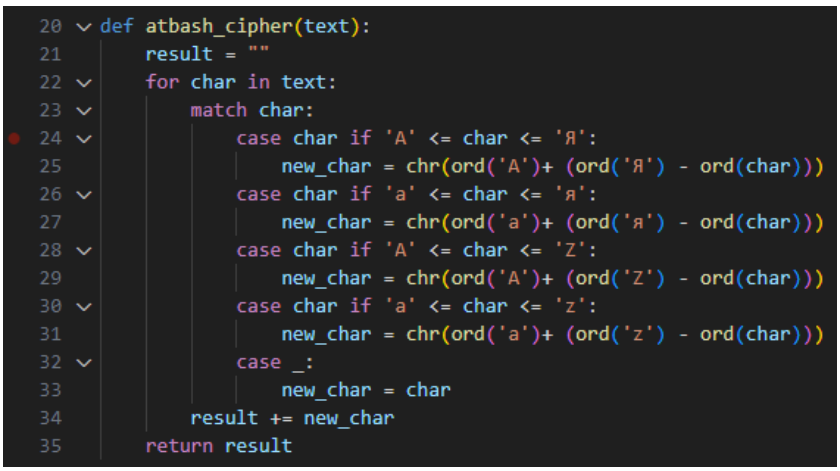
Figure 3.2: Запрос текста и вывод результата шифра Цезаря

3) После я вызвал написанный метод через командную строку и проверил все русские и английские буквы.

```
C:\Users\yaeda\OneDrive\Рабочий стол\rudn\МОЗИиИБ>py lab01.py
Введите текст:  АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
Шифр Цезаря:     ГДЕЖЗИЙКЛНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ

C:\Users\yaeda\OneDrive\Рабочий стол\rudn\МОЗИиИБ>py lab01.py
Введите текст:   абвгдежзиклмнопрстуфхцчшщъыьэюя
Шифр Цезаря:      гдежзийклнопрстуфхцчшщъыьэюяабв

C:\Users\yaeda\OneDrive\Рабочий стол\rudn\МОЗИиИБ>py lab01.py
Введите текст:  ABCDEFGHIJKLMNOPQRSTUVWXYZ
Шифр Цезаря:     DEFGHIJKLMNOPQRSTUVWXYZABC

C:\Users\yaeda\OneDrive\Рабочий стол\rudn\МОЗИиИБ>py lab01.py
Введите текст:  abcdefghijklmnopqrstuvwxyz
Шифр Цезаря:     defghijklmnopqrstuvwxyzabc

C:\Users\yaeda\OneDrive\Рабочий стол\rudn\МОЗИиИБ>
```

Figure 3.3: Проверка метода шифра Цезаря

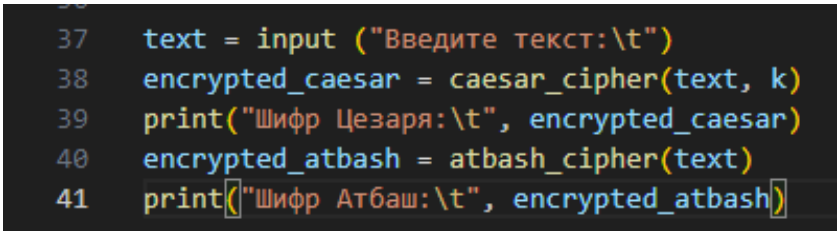
4) Затем я реализовал шифр Атбаша. При проверке слова берётся конкретный символ (char). match-case я реализовал проверки на наличие выбранного символа в русском или английском алфавите. При этом я учёл регистр символа. Если символ находится в алфавите, то берётся код ASCII последней буквы алфавита, из которого вычитается код ASCII выбранного символа. С помощью этого мы определяем, какое значение имеет симметричный центру символ алфавита. Затем мы прибавляем код ASCII первой буквы алфавита, чтобы определить нужный нам символ. Затем вписываем каждый символ в result и возвращаем его.



```python
def atbash_cipher(text):
    result = ""
    for char in text:
        match char:
            case char if 'А' <= char <= 'Я':
                new_char = chr(ord('А')+ (ord('Я') - ord(char)))
            case char if 'а' <= char <= 'я':
                new_char = chr(ord('а')+ (ord('я') - ord(char)))
            case char if 'A' <= char <= 'Z':
                new_char = chr(ord('A')+ (ord('Z') - ord(char)))
            case char if 'a' <= char <= 'z':
                new_char = chr(ord('a')+ (ord('z') - ord(char)))
            case _:
                new_char = char
        result += new_char
    return result
```

Figure 3.4: Шифр Атбаш на языке Python

5) Далее я реализовал вывод результата алгоритма шифра Атбаш после вывода результата алгоритма шифра Цезаря.



```python
text = input ("Введите текст:\t")
encrypted_caesar = caesar_cipher(text, k)
print("Шифр Цезаря:\t", encrypted_caesar)
encrypted_atbash = atbash_cipher(text)
print("Шифр Атбаш:\t", encrypted_atbash)
```

Figure 3.5: Вывод результата шифра Атбаш

6) После я вызвал написанный метод через командную строку и проверил все русские и английские буквы.

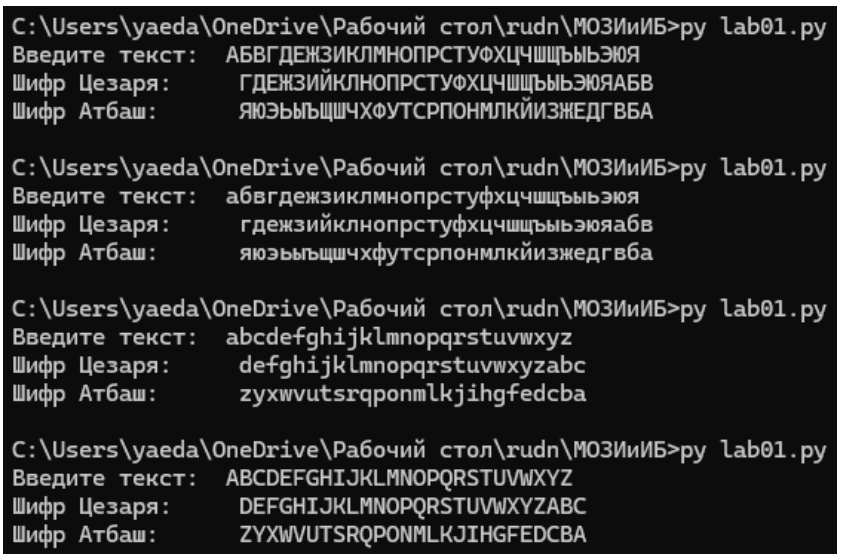


Figure 3.6: Проверка метода шифра Атбаш

7) Итоговый код можно увидеть на картинке ниже.

lab01.py > ...

```python
k = 3

def caesar_cipher(text, k):
    result = ""
    for char in text:
        match char:
            case char if 'А' <= char <= 'Я':
                new_char = chr((ord(char) - ord('А') + k) % 32 + ord('А'))
            case char if 'а' <= char <= 'я':
                new_char = chr((ord(char) - ord('а') + k) % 32 + ord('а'))
            case char if 'A' <= char <= 'Z':
                new_char = chr((ord(char) - ord('A') + k) % 26 + ord('A'))
            case char if 'a' <= char <= 'z':
                new_char = chr((ord(char) - ord('a') + k) % 26 + ord('a'))
            case _:
                new_char = char
        result += new_char
    return result

def atbash_cipher(text):
    result = ""
    for char in text:
        match char:
            case char if 'А' <= char <= 'Я':
                new_char = chr(ord('А')+ (ord('Я') - ord(char)))
            case char if 'а' <= char <= 'я':
                new_char = chr(ord('а')+ (ord('я') - ord(char)))
            case char if 'A' <= char <= 'Z':
                new_char = chr(ord('A')+ (ord('Z') - ord(char)))
            case char if 'a' <= char <= 'z':
                new_char = chr(ord('a')+ (ord('z') - ord(char)))
            case _:
                new_char = char
        result += new_char
    return result

text = input ("Введите текст:\t")
encrypted_caesar = caesar_cipher(text, k)
print("Шифр Цезаря:\t", encrypted_caesar)
encrypted_atbash = atbash_cipher(text)
print("Шифр Атбаш:\t", encrypted_atbash)
```

Figure 3.7: Итоговый код

4 Выводы

Я реализовал шифр Цезаря с произвольным ключом k и реализовал шифр Атбаш.