

Лабораторная работа №1

**Дисциплина: Математические основы защиты информации и
информационной безопасности**

Мохаммад хоссейн фарзанфар

Содержание

Цель работы	5
Задание	6
Выполнение лабораторной работы	7
Выводы	12

Список иллюстраций

1	Шифр Цезаря на языке Python	7
2	Запрос текста и вывод результата шифра Цезаря	8
3	Проверка метода шифра Цезаря	8
4	Шифр Атбаш на языке Python	9
5	Вывод результата шифра Атбаш	9
6	Проверка метода шифра Атбаш	10
7	Итоговый код	11

Список таблиц

Цель работы

Познакомиться с шифрами Цезаря и Атбаш.

Задание

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

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.

```
lab01.py > ...
1  k = 3
2
3  def caesar_cipher(text, k):
4      result = ""
5      for char in text:
6          match char:
7              case char if 'А' <= char <= 'Я':
8                  new_char = chr((ord(char) - ord('А') + k) % 32 + ord('А'))
9              case char if 'а' <= char <= 'я':
10                 new_char = chr((ord(char) - ord('а') + k) % 32 + ord('а'))
11              case char if 'A' <= char <= 'Z':
12                 new_char = chr((ord(char) - ord('A') + k) % 26 + ord('A'))
13              case char if 'a' <= char <= 'z':
14                 new_char = chr((ord(char) - ord('a') + k) % 26 + ord('a'))
15              case _:
16                 new_char = char
17             result += new_char
18     return result
```

Рис. 1: Шифр Цезаря на языке Python

- 2) Далее я реализовал запрос текста у пользователя и вывод результата алгоритма шифра Цезаря.

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

Рис. 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\alghai\OneDrive\Рабочий стол\rudn\МОЗИИИБ>py lab01.py
Введите текст: АБВГДЕЖЗИКЛМНОПРСТУФХЦШЩЬЬЪЮЯ
Шифр Цезаря: ГДЕЖЗИЙКЛНОПРСТУФХЦШЩЬЬЪЮЯАБВ

C:\Users\alghai\OneDrive\Рабочий стол\rudn\МОЗИИИБ>py lab01.py
Введите текст: абвгдежзиклмнопрстуфхцщшьььюя
Шифр Цезаря: гдежзийклнопрстуфхцщшьььюяабв

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

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

C:\Users\alghai\OneDrive\Рабочий стол\rudn\МОЗИИИБ>
```

Рис. 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.

```
20 def atbash_cipher(text):
21     result = ""
22     for char in text:
23         match char:
24             case char if 'A' <= char <= 'Я':
25                 new_char = chr(ord('A') + (ord('Я') - ord(char)))
26             case char if 'a' <= char <= 'я':
27                 new_char = chr(ord('a') + (ord('я') - ord(char)))
28             case char if 'A' <= char <= 'Z':
29                 new_char = chr(ord('A') + (ord('Z') - ord(char)))
30             case char if 'a' <= char <= 'z':
31                 new_char = chr(ord('a') + (ord('z') - ord(char)))
32             case _:
33                 new_char = char
34         result += new_char
35     return result
```

Рис. 4: Шифр Атбаш на языке Python

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

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

Рис. 5: Вывод результата шифра Атбаш

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

```

C:\Users\alghai\OneDrive\Рабочий стол\rudn\МОЗИиИБ>py lab01.py
Введите текст: АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЬЬЪЮЯ
Шифр Цезаря: ГДЕЖЗИЙКЛНОПРСТУФХЦЧШЩЬЬЪЮЯАБВ
Шифр Атбаш: ЯЮЭЬЫЩШЧХФУТСРПОНМЛКЙИЗЖЕДГВБА

C:\Users\alghai\OneDrive\Рабочий стол\rudn\МОЗИиИБ>py lab01.py
Введите текст: абвгдежзиклмнопрстуфхцчшщъьёюя
Шифр Цезаря: ггдежзийклнопрстуфхцчшщъьёюяабв
Шифр Атбаш: яюэьыщшчхфутсрпонмлкйизжедгвба

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

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

```

Рис. 6: Проверка метода шифра Атбаш

7) Итоговый код можно увидеть на картинке ниже.

```

lab01.py > ...
1   k = 3
2
3   def caesar_cipher(text, k):
4       result = ""
5       for char in text:
6           match char:
7               case char if 'A' <= char <= 'Я':
8                   new_char = chr((ord(char) - ord('A') + k) % 32 + ord('A'))
9               case char if 'a' <= char <= 'я':
10                  new_char = chr((ord(char) - ord('a') + k) % 32 + ord('a'))
11               case char if 'A' <= char <= 'Z':
12                  new_char = chr((ord(char) - ord('A') + k) % 26 + ord('A'))
13               case char if 'a' <= char <= 'z':
14                  new_char = chr((ord(char) - ord('a') + k) % 26 + ord('a'))
15               case _:
16                  new_char = char
17           result += new_char
18       return result
19
20  def atbash_cipher(text):
21      result = ""
22      for char in text:
23          match char:
24              case char if 'A' <= char <= 'Я':
25                  new_char = chr(ord('A') + (ord('Я') - ord(char)))
26              case char if 'a' <= char <= 'я':
27                  new_char = chr(ord('a') + (ord('я') - ord(char)))
28              case char if 'A' <= char <= 'Z':
29                  new_char = chr(ord('A') + (ord('Z') - ord(char)))
30              case char if 'a' <= char <= 'z':
31                  new_char = chr(ord('a') + (ord('z') - ord(char)))
32              case _:
33                  new_char = char
34          result += new_char
35      return result
36
37  text = input ("Введите текст:\t")
38  encrypted_caesar = caesar_cipher(text, k)
39  print("Шифр Цезаря:\t", encrypted_caesar)
40  encrypted_atbash = atbash_cipher(text)
41  print(["Шифр Атбаш:\t", encrypted_atbash])

```

Рис. 7: Итоговый код

Выводы

Я реализовал шифр Цезаря с произвольным ключом k и реализовал шифр Ат-баш.