

Отчёт по лабораторной работе №1

Шифр простой замены

Шевляков Илья Николаевич НФИмд-01-21

Содержание

Цель работы	4
Теоретические сведения	5
Шифр Цезаря	5
Шифр Атбаш	6
Выполнение работы	7
Реализация шифра Цезаря и Атбаш на языке Python	7
Контрольный пример	8
Выводы	9
Список литературы	10

Список иллюстраций

0.1	Работа алгоритмов	8
-----	-----------------------------	---

Цель работы

Изучение алгоритмов шифрования Цезаря и Атбаш

Теоретические сведения

Шифр Цезаря

Шифр Цезаря, также известный, как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования.

Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом 3 А была бы заменена на Г, Б станет Д, и так далее.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и все ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет практически никакого применения на практике.

Если сопоставить каждому символу алфавита его порядковый номер (нумеруя с 0), то шифрование и дешифрование можно выразить формулами модульной арифметики:

$$y = (x + k) \bmod n$$

$$x = (y - k + n) \bmod n$$

где x — символ открытого текста, y — символ шифрованного текста n — мощность алфавита k — ключ.

С точки зрения математики шифр Цезаря является частным случаем аффинного шифра.

Шифр Атбаш

Атбаш — простой шифр подстановки, изначально придуманный для иврита. Правило шифрования состоит в замене i -й буквы алфавита буквой с номером $n - i + 1$, где n — число букв в алфавите.

Выполнение работы

Реализация шифра Цезаря и Атбаш на языке Python

```
alphabet_ru = 'абвгдеёжзийклмнопрстуфхцчщъыьэюя'
```

```
alphabet_en = 'abcdefghijklmnopqrstuvwxyz'
```

```
def atbash(alphabet, s):
```

```
    return s.translate(str.maketrans(alphabet + alphabet.upper(), alphabet[::-1] + alphabet.upper()[::-1]))
```

```
def ceasar(alphabet, s, k):
```

```
    s = s.strip()
```

```
    result = ''
```

```
    for i in s:
```

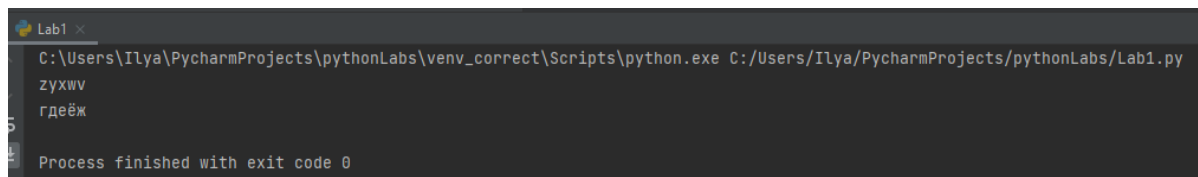
```
        result += alphabet[(alphabet.index(i) + k) % len(alphabet)]
```

```
    return result
```

```
print(atbash(alphabet_en, 'abcde'))
```

```
print(ceasar(alphabet_ru, 'абвгд', 3))
```

Контрольный пример



The image shows a terminal window titled 'Lab1'. The command prompt displays the full path to the Python interpreter and the script: `C:\Users\Ilya\PycharmProjects\pythonLabs\venv_correct\Scripts\python.exe C:/Users/Ilya/PycharmProjects/pythonLabs/Lab1.py`. The script's output consists of two lines of Cyrillic text: `зухвв` and `гдеёж`. At the bottom of the terminal, a status message reads: `Process finished with exit code 0`.

Рис. 0.1: Работа алгоритмов

Выводы

Во время выполнения данной лабораторной работы были изучили алгоритмы шифрования Цезаря и Атбаш.

Список литературы

1. Шифр Цезаря
2. Шифр Атбаш