Отчёт по лабораторной работе №1

Шифр простой замены

Шевляков Илья Николаевич НФИмд-01-21

Содержание

# 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) mod n  
x = (y - k + n) mod 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

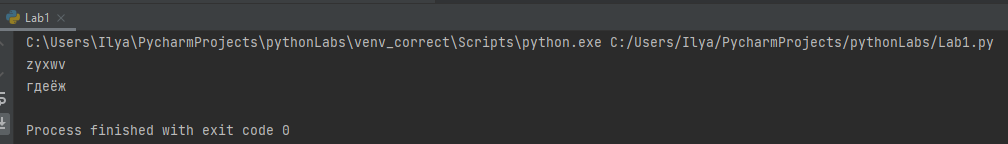
Атбаш — простой шифр подстановки, изначально придуманный для иврита. Правило шифрования состоит в замене i-й буквы алфавита буквой с номером n − i + 1, где n — число букв в алфавите.

# Выполнение работы

## Реализация шифра Цезаря и Атбаш на языке Python

alphabet\_ru = 'абвгдеёжзийклмнопрстуфхцчшщъыьэюя'  
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



Работа алгоритмов

# Выводы

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

# Список литературы

1. [Шифр Цезаря](https://ru.wikipedia.org/wiki/%D0%A8%D0%B8%D1%84%D1%80_%D0%A6%D0%B5%D0%B7%D0%B0%D1%80%D1%8F)
2. [Шифр Атбаш](https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B1%D0%B0%D1%88)