Отчёт по лабораторной работе №1

Шифр простой замены

Мадаманов Аллаберды

Содержание

[1 Цель работы 1](#_Toc158471261)

[2 Теоретические сведения 1](#_Toc158471262)

[2.1 Шифр Цезаря 1](#_Toc158471263)

[2.2 Шифр Атбаш 2](#_Toc158471264)

[3 Выполнение работы 2](#_Toc158471265)

[3.1 Реализация шифра Цезаря на языке Python 2](#_Toc158471266)

[3.2 Реализация шифра Атбаш на языке Python 3](#_Toc158471267)

[3.3 Контрольный пример 4](#_Toc158471268)

[4 Выводы 4](#_Toc158471269)

[Список литературы 4](#_Toc158471270)

# 1 Цель работы

Изучение алгоритмов шифрования Цезаря и Атбаш

# 2 Теоретические сведения

## 2.1 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.

## 2.2 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.

# 3 Выполнение работы

## 3.1 Реализация шифра Цезаря на языке Python

Блок шифрования

def caesar():

letters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'  
 step = 5  
 text = input("Шифрование Цезаря")  
 result = ''  
 for i in text:  
 ind = letters.find(i)   
 newind = ind + step   
 if i in letters:  
 result += letters[newind]   
 else:  
 result += i  
 print(result)

Блок дешифровки

def caesar\_deshifr():  
 letters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'  
 smeshenie = 5  
 text = input("Дешифровка Цезаря")  
 result = ''  
  
 for i in text:  
 ind = letters.find(i)  
 newind = ind - smeshenie  
 if i in letters:  
 result += letters[newind]  
 else:  
 result += i  
 print(result)

## 3.2 Реализация шифра Атбаш на языке Python

Блок шифрования

def atbash():  
   
 letters = [chr(x) for x in range(65, 91)]  
 letters\_r = [x for x in letters]  
 letters\_r.reverse()  
  
 text = input("Шифрование Атбаш")  
 result = ""

for i in text:  
 for j,l in enumerate(letters):  
 if i == l:   
 result += letters\_r[j]   
 print(result)

Блок дешифровки

def atbash\_desh():  
 letters = [chr(x) for x in range(65, 91)]  
 letters\_r = [x for x in letters]  
 letters\_r.reverse()  
  
 text = input("Дешивровка Атбаш")  
 result = ""  
 for i in text:  
 for j, l in enumerate(letters\_r):  
 if i == l:  
 result += letters[j]  
 print(result)

## 3.3 Пример работы

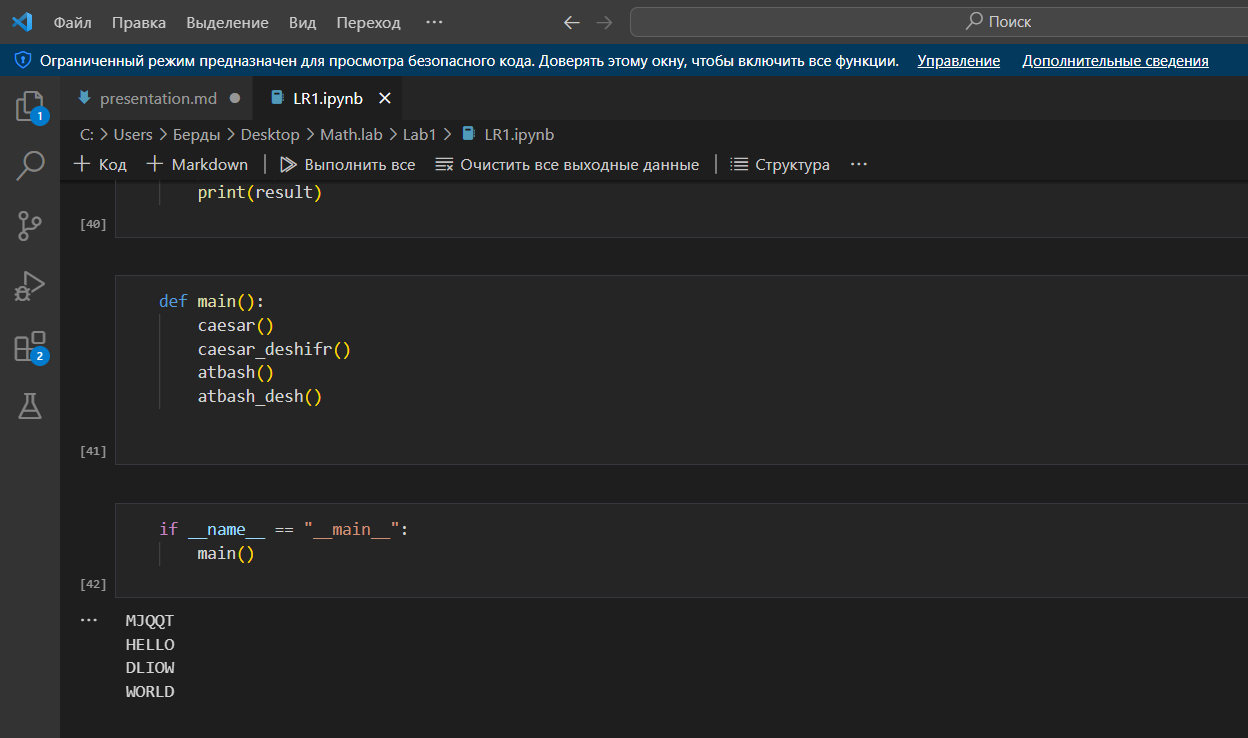


Figure 1: Работа алгоритмов

# 4 Выводы

В данной работе мы изучили алгоритмы шифрования Цезаря и Атбаш.