Отчёт по лабораторной работе №1.

Студентка: Царитова Нина Аведиковна, 1132236907

Группа: НФИмд-02-21

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Москва 2023

Содержание

1 Цель работы

Целью данной лабораторной работы является ознакомление с двумя методами шифрования: шифром Цезаря и шифром Атбаш, – а также их реализация на произвольном языке программирования.

2 Задание

1. Реализовать шифр Цезаря.
2. Реализовать шифр Атбаш.

3 Теоретическое введение

Математическая часть подробно описана в задании к лабораторной работе. Я поставила перед собой задачу найти факты о методах шифрования.

В основе функционирования шифров простой замены лежит следящий принцип: для получения шифртекста отдельные символы или группы символов исходного алфавита заменяются символами или группами символов шифралфавита.

Шифр Цезаря – (также он является шифром простой замены) – это моноалфавитная подстановка, т.е. каждой букве открытого текста ставится в соответствие одна буква шифртекста. На практике при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит, но с нарушенным порядком букв (алфавитная перестановка). Для запоминания нового порядка букв перемешивание алфавита осуществляется с помощью пароля. В качестве пароля могут выступать слово или несколько слов с неповторяющимися буквами. Шифровальная таблица состоит из двух строк: в первой записывается стандартный алфавит открытого текста, во второй- начиная с некоторой позиции размещается пароль (пробелы опускаются), а далее идут в алфавитном порядке оставшиеся буквы, не вошедшие в пароль. В случае несовпадения начала пароля с началом строки процесс после ее завершения циклически продолжается с первой позиции. Ключом шифра служит пароль вместе с числом, указывающим положение начальной буквы пароля. Таблица шифрования на ключе 4 пароль будет иметь вид:

а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я

ы э ю я п а р о л ь б в г д е ж з и й к м н с т у ф х ц ч ш щ ъ

Шрифт Атбаш является шифром сдвига на всю длину алфавита. Для алфавита, состоящего только из русских букв и пробела, таблица шифрования будет иметь следующий вид:

а б в г д е ж з и й к л м н о п р с т у ф х ц ч ш щ ъ ы ь э ю я _

_ ы э ю я п а р о л ь б в г д е ж з и й к м н с т у ф х ц ч ш щ ъ

4 Выполнение лабораторной работы

Примечание: комментарии по коду представлены на скриншотах к каждому из проделанных заданий.

4.1 Шифр Цезаря

В соответствии с заданием, первой была написана программа для шифра Цезаря. Программный код представлен ниже.

```
alfavit_EU =  'ABCDEFGHIJKLMNOPQRSTUVWXYZ'
alfavit_RU = 'АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЬЫЬЭЮЯ'
smeshenie = int(input('Шаг шифровки: '))
message = input("Сообщение для шифровки: ").upper()
itog = ''
lang = input('Выберите язык RU/EU: ')
if lang == 'RU':
    for i in message:
        mesto = alfavit_RU.find(i)
        new_mesto = mesto + smeshenie
        if i in alfavit_RU:
            itog += alfavit_RU[new_mesto]
        else:
            itog += i
else:
    for i in message:
        mesto = alfavit_EU.find(i)
        new_mesto = mesto + smeshenie
        if i in alfavit_EU:
            itog += alfavit_EU[new_mesto]
        else:
            itog += i
print (itog)
```

Figure 1: Реализация шифра Цезаря

```
Шаг шифровки: 4
Сообщение для ДЕшифровки: apple turk me
Выберите язык RU/EU: EU
ETTPI XYVO QI
```

Figure 2: Результат шифра Цезаря

4.2 Шрифт Атбаш

```
import os

def Atbash_crypt(cistring):
  string = ""
  cistring = formatString(cistring)
  for x in range(0, len(cistring)):
    string += flipChar(cistring[x])
  return(string)

def formatString (string):
  fmtString = string.lower()
  fmtString = "".join(fmtString.split())
  return fmtString

def flipChar(char):
  flip = abs((ord(char) - 96) - 27)
  return chr(flip + 96) if flip > 0 and flip <= 26 else ""

def Atbash():
  os.system('cls')
  cistring = input()
  print("\nСообщение для шифровки: ")
  print (cistring,"\n")
  print("Шифровка:")
  print(Atbash_crypt(cistring),"\n")
  print("Дешифровка:")
  print(Atbash_crypt(Atbash_crypt(cistring)),"\n")


print(Atbash())
```

Figure 3: Реализации шрифта Атбаш

```
world come true

Сообщение для шифровки:
world come true

Шифровка:
dliowxlnvgifv

Дешифровка:
worldcometrue
```

Figure 10: Результат шрифта Атбаш

5 Выводы

Таким образом, была достигнута цель, поставленная в начале лабораторной работы: я ознакомилась с двумя методами шифрования – шифром Цезаря и шифром Атбаш, – а также мне удалось реализовать их на языке программирования Python.

Список литературы

1. Википедия. Атбаш [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: https://ru.wikipedia.org/wiki/Атбаш

2. Википедия. Шифр Цезаря [Электронный ресурс]. Википедия, свободная энциклопедия, 2021. URL: https://ru.wikipedia.org/wiki/Шифр_Цезаря