Отчёт по лабораторной работе №1  
Шифры простой замены

Студент: Леонова Алина Дмитриевна, 1032212306

Группа: НФИмд-01-21

Преподаватель: Кулябов Дмитрий Сергеевич,

д-р.ф.-м.н., проф.

Москва 2021

Содержание

# 1 Цель работы

Целью данной работы является ознакомление с двумя шифрами простой замены: шифром Цезаря и шифром Атбаш, кроме того, их реализация на языке выбранном программирования.

# 2 Задание

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

# 3 Теоретическое введение

## 3.1 Шифр Цезаря

Шифр Цезаря относится к группе одноалфавитных шифров подстановки. При использовании шифров этой группы каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ того же алфавита [1].

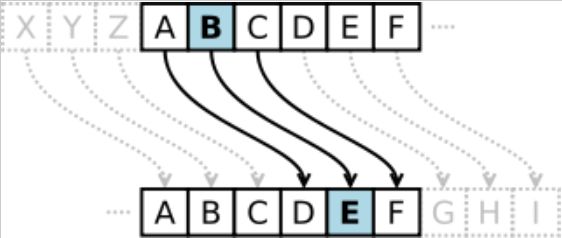


Figure 1: Фрагмент шифра Цезаря для латиницы со сдвигом на 3

В шифре Цезаря ключом служит произвольное целое число k. Каждая буква открытого текста заменяется буквой, стоящей на k знаков дальше нее в алфавите. К примеру, пусть ключом будет число 3. Тогда буква A английского алфавита будет заменена буквой D, буква B — буквой E и так далее (см. рис. 1).

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

где — символ открытого текста, — символ шифрованного текста, — мощность алфавита, а — ключ, - операция нахождения остатка от деления [2].

## 3.2 Шифр Атбаш.



Figure 2: Шифр Атбаш

Правило шифрования состоит в замене -й буквы алфавита на -ю букву алфавита с конца, букву с номером , где — число букв в алфавите (см. рис. 2) [3].

# 4 Выполнение лабораторной работы

## 4.1 Реализация шифра Цезаря с произвольным ключом k

Поскольку в задании алфавит для шифрования не был задан, сперва реализую вариант шифра Цезаря для всех unicode символов. Функция Cesar0 для шифрования и de\_Cesar0 для дешифрования текста со сдвигом k.

# 1. Реализовать шифр Цезаря с произвольным ключом k  
  
# с изменением всех символов  
print('Шифр Цезаря с изменением всех символов')  
  
def Cesar0(text, k):  
 res = ''  
 for i in text:  
 e = ord(i) + k  
 res += chr(e)  
 return res  
  
def de\_Cesar0(text, k):  
 res = ''  
 for i in text:  
 e = ord(i) - k  
 res += chr(e)  
 return res  
  
k = 3  
r = Cesar0('Veni, vidi, vici',k)  
print(r)  
print(de\_Cesar0(r,k))

Но обычно принято рассматривать алфавит в пределах какого-то конкретного языка, поэтому далее я создаю списки букв, составляющих кириллицу (ru) и латиницу (en), сначала все заглавные бугвы, потом все строчные.

# алфавиты  
print('\nАлфавиты:')  
ru = [chr(i) for i in range ( ord('А'), ord('я') + 1)]  
en = [chr(i) for i in range ( ord('A'), ord('Z') + 1)] \  
 + [chr(i) for i in range ( ord('a'), ord('z') + 1)]  
print('ru = ',ru)  
print('\nen = ',en)

Теперь создаю функции Cesar и de\_Cesar для шифрования и дешифрования текста шифром Цезаря на заданном алфавите (ru или en) со сдвигом k. В таком случае все символы, не входящие в алфавит, не будут изменяться при шифровании. А также число k может превосходить размер алфавита и шифрование всегда будет производиться символами, входящими в алфавит.

# по заданному алфавиту  
print('\nШифр Цезаря по заданному алфавиту')  
  
def Cesar(text, k, abc):  
 res = ''  
 for i in text:  
 if i in abc:  
 n = abc.index(i)  
 e = (n+k) % len(abc)  
 res += abc[e]  
 else:  
 res += i  
 return res  
  
def de\_Cesar(text, k, abc):  
 res = ''  
 for i in text:  
 if i in abc:  
 n = abc.index(i)  
 e = (n-k) % len(abc)  
 res += abc[e]  
 else:  
 res += i  
 return res  
  
k = 3  
r = Cesar('Veni, vidi, vici', k, en)  
print(r)  
print(de\_Cesar(r, k, en))  
k = 1000  
r = Cesar('Торопись медленно', k, ru)  
print(r)  
print(de\_Cesar(r, k, ru))

## 4.2 Реализация шифра Атбаш

Шифрования и дешифрования текста шифром Атбаш на заданном алфавите (ru или en) реализовано функцией Atbash. Все символы, не входящие в алфавит, не будут изменяться при шифровании.

# 2. Реализовать шифр Атбаш  
print('\nШифр Атбаш')  
  
def Atbash(text, abc):  
 res = ''  
 for i in text:  
 if i in abc:  
 e = abc.index(i)  
 res += abc[-e-1]  
 else:  
 res += i  
 return res  
  
r = Atbash('абвгд', ru)  
print(r)  
print(Atbash(r,ru))  
r = Atbash('Hello, world!', en)  
print(r)  
print(Atbash(r,en))

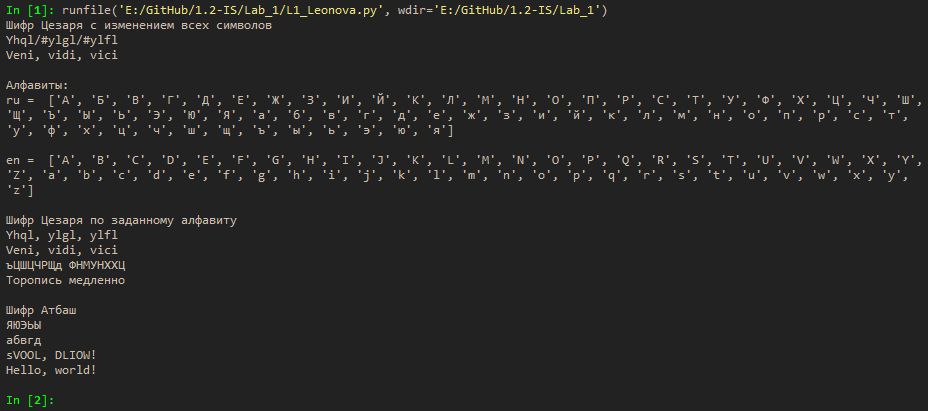


Figure 3: Результат выполнения L1\_Leonova.py

Реализованные функции шифрования и дешифрования шифрами Цезаря и Атбаш были проверены для английского и русского языка (латиницы и кириллицы) на нескольких примерах из задания к лаборатоной работе (см. рис. 3).

# 5 Выводы

Цель лабораторной работы была достигнута, два шифра простой замены, шифр Цезаря и шифр Атбаш, были реализованы на языке программирования Python.

# Список литературы

1. NeverWalkAloner. Классический криптоанализ [Электронный ресурс]. Хабр, 2015. URL: <https://habr.com/ru/post/271257/>.

2. Шифр Цезаря [Электронный ресурс]. Википедия, 2021. URL: <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>.

3. Атбаш [Электронный ресурс]. Википедия, 2021. URL: <https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B1%D0%B0%D1%88>.