Отчёт по лабораторной работе №1. Шифры простой замены

Дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Леонова Алина Дмитриевна, 1032212306
Группа: НФИмд-01-21
Преподаватель: д-р.ф.-м.н., проф. Кулябов Дмитрий Сергеевич

14 ноября, 2021, Москва

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.

Задание

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

Теоретическое введение

Шифр Цезаря

Каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ того же алфавита.

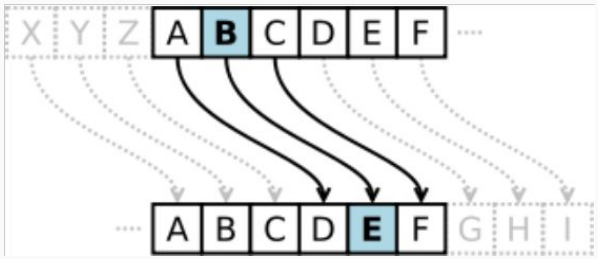

Figure 1: Фрагмент шифра Цезаря для латиницы со сдвигом на 3

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 (см. рис. 1).

Шифр Цезаря

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

$$y = (x + k) \; mod \; m$$

$$x = (y - k) \; mod \; m$$

где x — символ открытого текста, y — символ шифрованного текста, m — мощность алфавита, а k — ключ, mod - операция нахождения остатка от деления.

Шифр Атбаш.

Исходный текст	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Зашифрованный текст	Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

Исходный текст	А	Б	В	Г	Д	Е	Ё	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
Зашифрованный текст	Я	Ю	Э	Ь	Ы	Ъ	Щ	Ш	Ч	Ц	Х	Ф	У	Т	С	Р	П	О	Н	М	Л	К	Й	И	З	Ж	Ё	Е	Д	Г	В	Б	А

Figure 2: Шифр Атбаш

Правило шифрования состоит в замене i-й буквы алфавита на i-ю букву алфавита с конца, букву с номером $n - i + 1$, где n — число букв в алфавите (см. рис. 2).

Выполнение лабораторной работы

Реализация шифра Цезаря с произвольным ключом k

```
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
```

Реализация шифра Цезаря с произвольным ключом k

```
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))
```

Алфавиты

```
# 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)
```

Реализация шифра Цезаря с произвольным ключом k

```
# 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
```

Реализация шифра Цезаря с произвольным ключом k

```
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
```

Реализация шифра Цезаря с произвольным ключом k

```
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))
```

Реализация шифра Атбаш

```
# 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
```

Реализация шифра Атбаш

```
r = Atbash('абвгд', ru)

print(r)

print(Atbash(r,ru))

r = Atbash('Hello, world!', en)

print(r)

print(Atbash(r,en))
```

Результаты

```
In [1]: runfile('E:/GitHub/1.2-IS/Lab_1/L1_Leonova.py', wdir='E:/GitHub/1.2-IS/Lab_1')
Шифр Цезаря с изменением всех символов
Yhql/#ylgl/#ylfl
Veni, vidi, vici

Алфавиты:
ru =  ['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', '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']

en =  ['A', 'B', 'C', 'D', 'E', 'F', 'G', 'H', 'I', 'J', 'K', 'L', 'M', 'N', 'O', 'P', 'Q', 'R', 'S', 'T', 'U', 'V', 'W', 'X', 'Y',
'Z', 'a', 'b', 'c', 'd', 'e', 'f', 'g', 'h', 'i', 'j', 'k', 'l', 'm', 'n', 'o', 'p', 'q', 'r', 's', 't', 'u', 'v', 'w', 'x', 'y',
'z']

Шифр Цезаря по заданному алфавиту
Yhql, ylgl, ylfl
Veni, vidi, vici
ъЦШЦЧРЩд ФНМУНХХЦ
Торопись медленно

Шифр Атбаш
ЯЮЭЬЫ
абвгд
sVOOL, DLIOW!
Hello, world!

In [2]:
```

Figure 3: Результат выполнения L1_Leonova.py

Выводы

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