

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ  
Факультет физико-математических и естественных наук  
Кафедра прикладной информатики и теории вероятностей

## 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: Кулябов Дмитрий Сергеевич,  
д-р.ф.-м.н., проф.

Москва 2021

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>5</b>
<b>2</b>	<b>Задание</b>	<b>6</b>
<b>3</b>	<b>Теоретическое введение</b>	<b>7</b>
3.1	Шифр Цезаря . . . . .	7
3.2	Шифр Атбаш. . . . .	8
<b>4</b>	<b>Выполнение лабораторной работы</b>	<b>9</b>
4.1	Реализация шифра Цезаря с произвольным ключом $k$ . . . . .	9
4.2	Реализация шифра Атбаш . . . . .	12
<b>5</b>	<b>Выводы</b>	<b>14</b>
	<b>Список литературы</b>	<b>15</b>

# List of Figures

3.1	Фрагмент шифра Цезаря для латиницы со сдвигом на 3 . . . . .	7
3.2	Шифр Атбаш . . . . .	8
4.1	Результат выполнения L1_Leonova.py . . . . .	13

## List of Tables

# 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 так называемых одноалфавитных шифров подстановки. При использовании шифров этой группы «каждый символ открытого текста заменяется на некоторый, фиксированный при данном ключе символ того же алфавита.

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 А английского алфавита будет заменена буквой D, буква В — буквой Е и так далее.

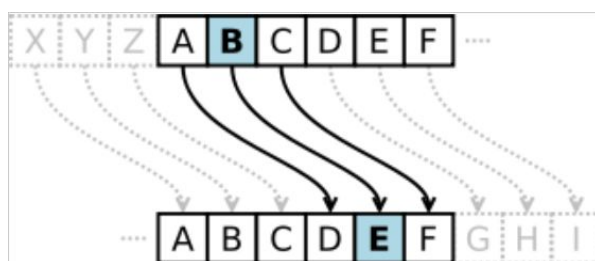


Figure 3.1: Фрагмент шифра Цезаря для латиницы со сдвигом на 3

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

$$y = (x + k) \bmod m$$

$$x = (y - k) \bmod m$$

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

### 3.2 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.

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 3.2: Шифр Атбаш



## 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 буквы, 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'),  
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))
```

```

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
Yhq1/#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
Yhq1, ylg1, ylf1
Veni, vidi, vici
ьЦЩЦЧРЩд фНМУНХХЦ
Торопись медленно

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

In [2]:

```

Figure 4.1: 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 лабораторной работе (см. рис. 4.1).

## 5 Выводы

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

## **Список литературы**