Отчёт по лабораторной работе №1

Шифр простой замены

Студент: Гонсалес Ананина Луис Антонио, 1032175329
Группа: НФИмд-02-21
Преподаватель: Кулябов Дмитрий Сергеевич,
д-р.ф.-м.н., проф.

Москва 2021

Содержание

List of Figures

1 Цель работы

Цель данной лабораторной работы- изучить теорию и реализовать шифры простой замены (Шифр Цезаря и Шифр Атбаш)

2 Теоретические сведения

Шифр Цезаря

Также известный как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования [1].

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.

Математическая модель:

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

$$x = (y - k + n) \mod n,$$

Figure 2.1: Формула

$$y = (x + k) \mod n$$

Figure 2.2: Формула

где ~x — символ открытого текста, ~y — символ шифрованного текста, ~n — мощность алфавита, а ~k — ключ.

Шифр Цезаря со сдвигом на 3 (английский алфавит):

A заменяется на D, B заменяется на E, Z заменяется на C и так далее.

Шифр Атбаш

Шифр простой замены, использованный для еврейского алфавита и получивший оттуда свое название. Шифрование происходит заменой первой буквы алфавита на последнюю, второй на предпоследнюю [2].

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

Исходный текст	א	ב	ג	ד	ה	ו	ז	ח	ט	י	כ	ל	מ	נ	ס	ע	פ	צ	ק	ר	ש	ת
Зашифрованный текст	ת	ש	ר	ק	צ	פ	ע	ס	נ	מ	ל	כ	י	ט	ח	ז	ו	ה	ד	ג	ב	א

Figure 2.3: Атбаш

3 Выполнение работы

Шифр Цезарь:

1. Для начала начал разбирать шифр Цезаря, для этого написал функцию code_cesar с двумя нужными параметрами (message, к) где message это сам текст который будем зашифровывать, а к это наш произвольный ключ, моем случае 3.
2. Далее написал нужный алгоритм который взял с файла пдф и с интернета.
3. Потом написал само сообщения и вышло оно зашифровано.

   Шифр Атбаш:

   1. Написал функцию code_atbash с параметром message.
   2. Далее написал нужный алгоритм.
   3. Потом написал само сообщения и вышло оно зашифровано.

In [1]:
```
def code_cesar(message, k):
    message=message.upper()
    stroka=''
    for text in message.split():
        for i in text:
            number=(ord(i)-65+k)%26
            let=chr(65+number)
            stroka+=let
        stroka+=' '
    return stroka
```

In [2]:
```
code_cesar('Veni vidi vici',3)
```

Out[2]:
```
'YHQL YLGL YLFL '
```

In [3]:
```
def code_atbash(message):
    message=message.lower()
    stroka=''
    for i in message:
        if i==' ':
            number=1072
            let=chr(number)
        elif i=='а':
            number=32
            let=chr(number)
        else:
            number=ord(i)-1073
            let=chr(1103-number)
        stroka+=let
    return stroka
```

In [4]:
```
code_atbash('Привет нашему миру')
```

Out[4]:
```
'сршюыоау иыфнафшрн'
```

In [ ]:

Figure 3.1: Код

4 Выводы

В итоге в данной лабораторной работы я изучил теорию и реализовал шифры простой замены (Шифр Цезаря и Шифр Атбаш)

Список литературы

1. Шифр Цезаря [Электронный ресурс]. Википедия, 2021. URL: https://calculatorium.ru/cryptography/caesar-cipher.
2. Шифр Атбаш [Электронный ресурс]. Википедия, 2021. URL: http://kriptografea.narod.ru/atbash.html.