Отчёт по лабораторной работе №1. Шифры простой замены

Дисциплина: Математические основы защиты информации и информационной безопасности

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

15 ноября, 2021, Москва

Цели и задачи

Цель лабораторной работы

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

Выполнение лабораторной работы

Шифрование

Шифрование – это технология кодирования и раскодирования данных. Зашифрованные данные -это результат применения алгоритма для кодирования данных с целью сделать их недоступными для чтения. Данные могут быть раскодированы в исходную форму только путем применения специальный ключа. Шифрование является важной частью обеспечения безопасности данных, поскольку оно защищает конфиденциальную информацию от угроз, в числе которых использование вредоносного ПО и несанкционированный доступ третьих сторон. Шифрование данных - это универсальное защитное решение: оно может применяться к части данных, например, к паролю, к информации в файле или даже ко всем данным, содержащимся на носителе.‘

Шифр Цезаря

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. Например, в шифре со сдвигом 3 А была бы заменена на Г, Б станет Д, и так далее.

Математическая модель:

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

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

Figure 1: Формула

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.

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 3: Атбаш

Результат выполнения работы

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=='a':
            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 4: Код

Выводы

Выводы

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