Отчёт по лабораторной работе №1

Шифр простой замены

Наботов Шахзод НПМмд-02-22

Содержание

Цель работы

Создание программы для шифрования методом простой замены

Теоретические сведения

Шифр Цезаря

Шифр Цезаря, также известный, как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования. Он является моноалфавитным, то есть имеет подстановочный тип, где каждая буква в открытом тексте заменяется на другую букву, смещенную на определенное количество позиций в алфавите.

Шифр Цезаря называется так благодаря Юлию Цезарю, который использовал его со сдвигом 3, чтобы защищать военные сообщения. Несмотря на то, что Цезарь считается первым зафиксированным человеком, использующим эту схему, другие шифры подстановки, как известно, использовались и раньше.

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

Пример шифрования со сдвигом 5:

Сообщение	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Номер п/п	12	18	10	17	20	16	4	18	1	22	10	33
Номер п/п +5	17	23	15	22	25	21	9	23	6	27	15	5
Шифр	П	Х	Н	Ф	Ч	У	З	Х	Е	Щ	Н	Д

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и все ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет практически никакого применения на практике.

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
x = (y - k + n) mod n
```

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

Шифр Атбаш

Шифр простой замены Атбаш использовался для еврейского алфавита и оттуда же получил свое название. Шифрование происходит заменой первой буквы алфавита на последнюю, второй на предпоследнюю. (алеф(первая буква) заменяется на тау(последнюю), бет(вторая) заменяется на шин(предпоследняя) из этих сочетаний шифр и получил свое название).

Шифр Атбаш для английского алфавита:

Исходный алфавит	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
Алфавит замены:	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

Правило шифрования состоит в замене i-й буквы алфавита буквой с номером $n - i + 1$, где n — число букв в алфавите. # Выполнение работы

Реализация шифра Цезаря на языке Python

Блок шифрования

```
#Функция, шифр Цезаря

def shifr_Caesar():
    alph = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz'
    sdvig = 5
```

```
    print('Цезарь:')
    text = input('Зашифровка: ')
    resultat = ""
    for i in text:
        index = alph.find(i)
        new_index = index + sdvig
        if i in alph:
            resultat += alph[new_index]
        else:
            resultat += i
    print('Результат: ', resultat)
```

Блок дешифровки

```
#Функция, дешифр Цезаря
def deshifr_Caesar():
    alph2 = 'ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz'
    sdvig = 5
    text = input('Дешифровка: ')
    resultat = ""
    for i in text:
        index = alph2.find(i)
        new_index = index - sdvig
        if i in alph2:
            resultat += alph2[new_index]
        else:
            resultat += i
    print('Результат: ', resultat)
```

Реализация шифра Атбаш на языке Python

Блок шифрования

```
#Функция, шифр Атбаша
def atbash():
    alph = [chr(x) for x in range(32, 122)]
    alph_reverse = [x for x in alph]
    alph_reverse.reverse()
    print('Атбаш: ')
    text = input('Зашифровка: ')
    resultat = ""
    for i in text:
        for j, k in enumerate(alph):
            if i == k:
                resultat = resultat + alph_reverse[j]
    print('Результат: ', resultat)
```

Блок дешифровки

```
#Функция, дешифр Атбаша
def deshifr_atbash():
    alph = [chr(x) for x in range(32, 122)]
    alph_reverse = [x for x in alph]
```

```
    alph_reverse.reverse()
    text = input('Дешифровка: ')
    resultat = ""
    for i in text:
        for j, k in enumerate(alph_reverse):
            if i == k:
                resultat = resultat + alph[j]
    print('Результат: ', resultat)
```

Контрольный пример

```
In [19]: if __name__ == "__main__":
             main()

         Цезарь:
         Зашифровка: Abcd
         Результат:  Fghi
         Дешифровка: Fghi
         Результат:  Abcd
         Атбаш:
         Зашифровка: Abcd
         Результат:  X765
         Дешифровка: X765
         Результат:  Abcd
```

Результат работы алгоритмов

Выводы

Я освоил шифрование методом простой замены и реализовал программу для шифрования на языке Python.

Список литературы

1. Шифр Цезаря
2. Шифр Цезаря из Википедии
3. Шифр Атбаш