Цель работы

Изучение алгоритмов шифрования Цезаря и Атбаш

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.

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.

Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

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.

С точки зрения математики шифр Цезаря является частным случаем аффинного шифра.

Шифр Атбаш

Атбаш — простой шифр подстановки, изначально придуманный для иврита. 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

```
def tsesar():
    letters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'
    step = 5
    text = input("Цезарь - шифрование :)")
    result = ''
    for i in text:
        ind = letters.find(i)
        newind = ind + step
        if i in letters:
            result += letters[newind]
        else:
            result += i
    print(result)
```

Блок дешифровки

```
def tsesar_deshifr():
    letters = 'ABCDEFGHIJKLMNOPQRSTUVWXYZABCDEFGHIJKLMNOPQRSTUVWXYZ'
    smeshenie = 5
    text = input("Цезарь - дешифровка")
    result = ''

    for i in text:
        ind = letters.find(i)
        newind = ind - smeshenie
        if i in letters:
            result += letters[newind]
        else:
            result += i
    print(result)
```

Реализация шифра Атбаш на языке Python

Блок шифрования

```
def atbash():
    letters = [chr(x) for x in range(65, 91)]
    letters_r = [x for x in letters]
    letters_r.reverse()

    text = input("Атбаш - шифрование")
    result = ""
    for i in text:
        for j,l in enumerate(letters):
            if i == l: # если буквы i и l равны, то
                result += letters_r[j]
    print(result)
```

Блок дешифровки

```
def atbash_desh():
    letters = [chr(x) for x in range(65, 91)]
    letters_r = [x for x in letters]
    letters_r.reverse()

    text = input("Атбаш - дешивровка")
    result = ""
    for i in text:
        for j, l in enumerate(letters_r):
            if i == l:
                result += letters[j]
    print(result)
```

Контрольный пример

```
if __name__ == "__main__":
    main()
```

```
Цезарь - шифрование : FMIAT
KRNFY
Цезарь - дешифровка : KRNFY
FMIAT
Атбаш - шифрование : FMIAT
UNRZG
Атбаш - дешивровка : UNRZG
FMIAT
```

Выводы

Изучили алгоритмы шифрования Цезаря и Атбаш.

Список литературы{.unnumbered}

1. Шифр Цезаря
2. Шифр Атбаш