Шифр простой замены

Кодже Лемонго Арман

30 сентября, 2024, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Целью данной является изучение алгоритмов шифрования Цезаря и Атбаш

Выполнение лабораторной работы

Шифрование

Шифрование – это преобразование данных с использованием математического алгоритма и ключа. Если нет ключа, то зашифрованные данные невозможно прочитать или использовать

Шифр Атбаш

Атбаш — простой шифр подстановки.

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

Шифр Цезаря

Шифр Цезаря — это разновидность шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите.

```
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.

Контрольный пример

```
[20]: s = 'CESAR'
      print (f'{s} : {cesar(s, 4)} : {dec_cesar(cesar(s, 4), 4)}')

      CESAR : GIWEV : CESAR

[37]: s = 'WELCOME'
      print (f'{s} : {cesar(s, 4)} : {dec_cesar(cesar(s, 4), 4)}')

      WELCOME : AIPGSQI : WELCOME
```

Рис. 1: шифр Цезаря

Контрольный пример

```
[33]: s = 'ATBASH'
      print (f'{s} : {atbash(s)} : {dec_atbash(atbash(s))}')

      ATBASH : ZGYZHS : ATBASH

[36]: s = 'WELCOME'
      print (f'{s} : {atbash(s)} : {dec_atbash(atbash(s))}')

      WELCOME : DVOXLNV : WELCOME
```

Рис. 2: шифр Атбаш

Выводы

Результаты выполнения лабораторной работы

в конце нашего лабораторная работа, я изучил алгоритмы шифрования Цезаря и Атбаш.