

Шифры простой замены

Тагиев Б. А.

08 сентябрь 2024

Российский университет дружбы народов, Москва, Россия

Цель работы

Целью данной работы является изучение алгоритмов шифрования Цезарь и Атбаш, принцип его работы, реализация на Julia.

1. Реализовать шифр Цезаря с произвольным ключем k .
2. Реализовать шифр Атбаш.

Выполнение лабораторной работы

Суть шифра Цезаря заключается в том, что происходит смещение всех букв по алфавиту в сообщении на некоторый коэффициент k . Декодирование происходит путем смещения в обратную сторону.

Далее приведена реализация как для русского так и для английского алфавита одновременно

Шифр Цезаря

```
result = ""
for c in msg
    if 1041 < Int(c) < 1104
        base = (uppercase(c) == c) ? codepoint('A') : codepoint('a')
        # 31 - так как в ASCII ё -- пропущена в списке
        t = base + (Int(Char(c)) % base + key) % 31
    else
        base = (uppercase(c) == c) ? codepoint('A') : codepoint('a')
        t = base + (Int(Char(c)) % base + key) % 26
    end
    key_rot = Char(t)
    result = result * key_rot
end
```

В качестве параметров скрипт принимает:

- `<enc>` — (Тип: Char) Расшифровать или шифровать сообщение (Возможные значения: d, e).
- `<msg>` — (Тип: String) Сообщение, с которым нужно прозвести действие.
- `<key>` — (Тип: Int) Значение сдвига в шифре Цезаря. (Для русского алфавита в промежутке $[0, 31]$, для английского алфавита в промежутке $[0, 26]$)

Шифр Цезаря

```
$ julia caesar.jl e test 3  
whvw
```

```
$ julia caesar.jl d whvw 3  
test
```


Шифр Атбаш

Шифр Атбаш, отчасти, похож на шифр Цезаря, но в данном алгоритме разворачивается весь алфавит, а не происходит сдвиг.

```
function atbash(msg, alp, rev)
    result = ""
    for i in msg
        c = rev[findfirst(i, alp)]
        result = result * c
    end
    result
end
```

В качестве параметров скрипт принимает:

- `<enc>` — (Тип: Char) Расшифровать или шифровать сообщение (Возможные значения: d, e).
- `<msg>` — (Тип: String) Сообщение, с которым нужно прозвести действие.
- `<alp>` — (Тип: String) Словарь из которого, можно составить данное сообщение.

```
$ julia atbash.jl e "test test" " abcdefghijklmnopqrstuvwxyz"  
fugfzfugf  
test test
```

В данной лабораторной работе были изучены два алгоритма шифрования: Цезарь и Атбаш, оба алгоритма были реализованы на языке Julia и работают корректно.