

Лабораторная работа №1

Шифры простой замены

Легиньких Г.А.

Российский университет дружбы народов, Москва, Россия

Информация

- Легиньких Галина Андреевна
- НПМмд-02-25
- Российский университет дружбы народов
- 1032259346@pfur.ru
- <https://github.com/galeginkikh>

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

```
enc = ARGS[1]
msg = ARGS[2]
key = parse{Int, ARGS[3]}
```

```
function encrypt()
    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')
```


Шифр Цезаря

```
if enc == "e"
    key = key
elseif enc == "d"
    if 1041 < Int(msg[1]) < 1104
        # 31 - так как в ASCII ё -- пропущена в списке
        key = 31 - key
    else
        key = 26 - key
    end
else
    println("Wrong argument. Possible values are 'd' or 'e'")
    exit(1)
end
```

В качестве параметров скрипт принимает:

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

Запрос и результат:

```
PS D:\> julia project_1.jl e test 5  
yјху
```

```
PS D:\> julia project_1.jl e привет 1  
рсйгжу
```

```
PS D:\> julia project_1.jl d рсйгжу 1  
привет
```

Шифр Атбаш

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

```
enc = ARGS[1]
```

```
msg = ARGS[2]
```

```
alp = ARGS[3]
```

```
rev = reverse(ARGS[3])
```

```
function atbash(msg,alp,rev)
```

```
    result=""
```

```
    for i in msg
```

```
        c = rev[findfirst(i,alp)]
```

```
        result = result * c
```

```
    end
```

```
    result
```

В качестве параметров скрипт принимает:

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

Запрос и вывод:

```
PS D:\> julia Атбаш.jl e "test test" " abcdefghijklmnopqrstuvwxyz"  
fugfzfugf  
test test  
PS D:\> julia Атбаш.jl e "function" " abcdefghijklmnopqrstuvwxyz"  
telwfqkl  
function
```

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