Шифры простой замены

Тагиев Байрам Алтай оглы

Содержание

# 1 Цель работы

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

# 2 Задание

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

# 3 Выполнение лабораторной работы

## 3.1 Шифр Цезаря

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

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

result = ""  
for c in msg  
 if 1041 < Int(c) < 1104  
 base = (uppercase(c) == c) ? codepoint('А') : codepoint('а')  
 # 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) Расшивровать 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])

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

## 3.2 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) Расшивровать 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

# 4 Выводы

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