Отчет по лабораторной работе №1

Шифры простой замены

Легиньких Галина Андреевна

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

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('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  
 result  
end  
  
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  
  
msg = encrypt()  
println(msg)

В качестве параметров скрипт принимает:

* <enc> — Расшивровать 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  
yjxy  
PS D:\> julia project\_1.jl e привет 1  
рсйгжу  
PS D:\> julia project\_1.jl d рсйгжу 1  
привет

## 3.2 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  
end  
  
e = atbash(msg,alp,rev)  
println(e)  
println(atbash(e,rev,alp))

В качестве параметров скрипт принимает:

* <enc> — Расшивровать 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

# 4 Выводы

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