Отчет по лабораторной работе №1

*дисциплина: Математические основы защиты информации и информационной безопасности*

Морозова Ульяна Константиновна

Содержание

# 1 **Цель работы**

Целью работы является изучение алгоритмов шифрования Цезаря и Атбаша и реализация их на языке Julia.

# 2 Выполнение лабораторной работы

## 2.1 Шифр Цезаря

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

Далее приведена реализация шифра на языке Julia для русского и английского алфавита.

function caeser\_cipher(text::AbstractString, k::int, encrypt::Bool=true)  
 rus\_alphabet = collect("АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЬЭЮЯ")  
 eng\_alphabet = collect("ABCDEFGHIJKLMNOPQRSTUWXYZ")  
  
 result=IOBuffer()  
  
 for c in uppercase(text)  
 if c in rus\_alphabet  
 alphabet = rus\_alphabet  
 elseif c in eng\_alphabet  
 alphabet = eng\_alphabet  
 else  
 print(result, c)  
 print("Unknown language")  
 continue  
 end  
   
 n = length(alphabet)  
 index\_c = findfirst(==(c), alphabet)  
 if encrypt  
 new\_index = mod(index\_c - 1 + k, n) + 1  
 else  
 new\_index = mod(index\_c - 1 - k, n) + 1  
 end  
 print(result, alphabet[new\_index])  
 end  
 return String(take!(result))  
end

На вход функция принимает слово, которое нужно (де)шифровать, шаг шифра, а также булевый параметр, отвечающий за (де)шифрование.

Результат работы шифра:

julia> caesar\_cipher("EVENING", 3, encrypt=true)  
"HYHQLQJ"

julia> caesar\_cipher("HYHQLQJ", 3, encrypt=false)  
"EVENING"

## 2.2 Шифр Атбаша

Шифр представляет собой шифр сдвига на всю длину алфавита.

Его реализация:

function atbash\_cipher(text::String)  
 result = IOBuffer()  
 for c in text  
 if 'A' <= c <= 'Z'  
 write(result, Char('Z' - (c - 'A')))  
 elseif 'a' <= c <= 'z'  
 write(result, Char('z' - (c - 'a')))  
 else  
 write(result, c)  
 end  
 end  
 return String(take!(result))  
end

Выполнение работы кода:

julia> atbash\_cipher("TOMORROW")  
"GLNLIILD"

# 3 Выводы

Мы изучили работу алгоритмов шифрования Цезаря и Атбаша, а также реализовали их на языке Julia.