Математические основы защиты информации и информационной безопасности

Отчёт по лабораторной работе №3:Шифрование гаммированием

Ахлиддинзода Аслиддин

Содержание

# Цель работы

Основная цель работы — освоить шифрование гаммированием.

# Выполнение лабораторной работы

## Шифрование гаммированием

Реализация алгоритма шифрования гаммированием конечной гаммой Примеры использования цикла while

## Код программы

function build\_keystream(data\_len::Int, key::Vector{UInt8}; repeat\_key::Bool=true)  
 if length(key) == 0  
 throw(ArgumentError("Ключ не может быть пустым!"))  
 end  
 if length(key) >= data\_len  
 return key[1:data\_len]  
 elseif repeat\_key  
 n = ceil(Integer, data\_len / length(key))  
 replicated = repeat(key, n)  
 return replicated[1:data\_len]  
 else  
 throw(ArgumentError("Ключ короче текста, а repeat\_key=false"))  
 end  
end  
function encrypt\_bytes(data::Vector{UInt8}, key::Vector{UInt8}; repeat\_key::Bool=true)  
 ks = build\_keystream(length(data), key; repeat\_key=repeat\_key)  
 return xor.(data, ks)  
end  
function bytes\_to\_hex(b::Vector{UInt8})  
 hexbytes = map(x -> lpad(string(x, base=16), 2, '0'), b)  
 return join(hexbytes, "")  
end  
function hex\_to\_bytes(hexstr::AbstractString)  
 if length(hexstr) % 2 != 0  
 throw(ArgumentError("Длина hex-строки должна быть чётной"))  
 end  
 return [parse(UInt8, hexstr[i:i+1], base=16) for i in 1:2:length(hexstr)]  
end  
println("Введите текст, который нужно зашифровать:")  
plaintext = readline()  
  
println("Введите ключ для шифрования:")  
key\_str = readline()  
  
# Преобразуем в массивы байт  
pt\_bytes = collect(codeunits(plaintext))  
key\_bytes = collect(codeunits(key\_str))  
  
# Шифрование  
cipher\_bytes = encrypt\_bytes(pt\_bytes, key\_bytes; repeat\_key=true)  
cipher\_hex = bytes\_to\_hex(cipher\_bytes)  
  
println("\nЗашифрованный текст (hex): $cipher\_hex")  
  
# Дешифрование (для проверки)  
dec\_bytes = encrypt\_bytes(cipher\_bytes, key\_bytes; repeat\_key=true)  
recovered\_text = String(dec\_bytes)  
  
println("Дешифрованный текст: $recovered\_text")

# Вывод

В ходе выполнения лабораторной работы был реализован алгоритм шифрования гаммированием конечной гаммой.