

Математические основы защиты информации и информационной безопасности

Дарижапов Тимур Андреевич

12 Октября 2024

РУДН, Москва, Россия

Лабораторная работа 3

Шифрование гаммированием

```
In [2]: using Random

function text_f(text, key)
    if length(text) != length(key)
        return "Длины не совпадают"
    end

    ctext = ""
    for i in 1:length(text)
        ctext_s = xor(Int(codepoint(text[i])), Int(codepoint(key[i])))
        ctext *= Char(ctext_s)
    end

    return ctext
end
```

Out[2]: text_f (generic function with 1 method)

```
In [4]: key = ""
text = "Hello, world!"
Random.seed!(5)
global key = key * randstring(['A':'Z';'0':'9'], length(text))

ctext = text_f(text, key)

println("Текст: ", text)
println("Гамма: ", key)
println("Зашифрованный текст: ", ctext)
println("Дешифрованный текст: ", text_f(ctext, key))
```

Рис. 1: Реализация программы

```
Текст: Hello, world!  
Гамма: 97ATM03RN61VC  
Зашифрованный текст: qR-8"cD%!D]2b  
Дешифрованный текст: Hello, world!
```

Рис. 2: Вывод программы

- Познакомился с алгоритмом шифрования гаммированием конечной гаммой.
- Применил алгоритм на практике.

Спасибо за внимание!