

Математические основы защиты информации и информационной безопасности

Супонина Анастасия Павловна

5 Октября 2024

РУДН, Москва, Россия

Лабораторная работа 3

`randstring` - создает рандомную строку из заданных данных, заданной длины
`xor` - производит побитовое сложение
`codepoint` - возвращает кодовую точку Unicode соответствующую символу

```
using Random  
  
k = ""  
text = "Have a nice day"  
k *= randstring(['A':'Z'; 'a':'z'; '0':'9'], length(text))
```

Рис. 1: 'Введение функции и запись переменных'

```
for i in 1:length(text)
    cipher_text_bit = xor(codepoint(text[i]), codepoint(k[i]))
    cipher_text *= Char(cipher_text_bit)
end
```

Рис. 2: 'Создание цикла for с побитовым сложением'

```
function cipher(text, k) #функция шифрования и дешифровки
    if length(text) == length(k)
        cipher_text = ""
        for i in 1:length(text)
            cipher_text_bit = xor(codepoint(text[i]), codepoint(k[i]))
            cipher_text *= Char(cipher_text_bit)
        end
    end
    return cipher_text
end
```

Рис. 3: 'Функция шифровки и дешифровки'

```
cipher_text = cipher(text, k)

printstyled("Текст:", text; color = :green)
println(" Ключ шифра:", k)
printstyled("Зашифрованный текст:", cipher_text; color = :blue)
printstyled(" Дешифрованный текст:", cipher(cipher_text, k); color = :green)
```

Рис. 4: 'Вывод переменных'

ШифрованиеГаммированием.jl U X

MathSec > ШифрованиеГаммированием.jl > cipher

```
1 using Random
2
3 k = ""
4 text = "Have a nice day"
5 k *= randstring(['A':'Z'; 'a':'z'; '0':'9'], length(text)) #создание случайного ключа длины текста
6
7 function cipher(text, k) #функция шифрования и дешифровки
8     if length(text) == length(k)
9         cipher_text = ""
10         for i in 1:length(text)
11             cipher_text_bit = xor(codepoint(text[i]), codepoint(k[i]))
12             cipher_text *= Char(cipher_text_bit)
13         end
14     end
15     return cipher_text
16 end
17
18 cipher_text = cipher(text, k)
19
20 printstyled("Текст:", text; color = :green)
21 println(" Ключ шифра:", k)
22 printstyled("Зашифрованный текст:", cipher_text; color = :blue)
23 printstyled(" Дешифрованный текст:", cipher(cipher_text, k); color = :green)
```

PROBLEMS 4 OUTPUT DEBUG CONSOLE TERMINAL PORTS COMMENTS

Зашифрованный текст:2,?N9y=«QDQ,. Дешифрованный текст:Have a nice day
Текст:Have a nice day Ключ шифра:KpHkKEU8GY0jrgP
Зашифрованный текст:~>Jk\$u^.:UJ~&) Дешифрованный текст:Have a nice day
Текст:Have a nice day Ключ шифра:635BxBeSDA64zGf
Зашифрованный текст:~RC'X#E~"S\$A&v Дешифрованный текст:Have a nice day
Текст:Have a nice day Ключ шифра:EGP2f5rgIITuxCS
&WfTrov *1U"L Дешифрованный текст:Have a nice day
Текст:Have a nice day Ключ шифра:mZ7b00Vj3vqVF57
Зашифрованный текст:%;A~.v+Z\$9v"TN Дешифрованный текст:Have a nice day
Текст:Have a nice day Ключ шифра:mQLYHzQtvgKIZW8
Зашифрованный текст:%0:ch~\$ iA6A Дешифрованный текст:Have a nice day


```
Текст:Have a nice day Ключ шифра:635BxBеSDA64zGf  
Зашифрованный текст:~RC'X#E=-"Sj▲&▼ Дешифрованный текст:Have a nice day
```

Рис. 6: 'Результат выполнения программы'

В процессе выполнения работы, я разобралась с принципом работы шифрования гаммированием. Изучила новые функции Julia, такие как `randstring`, `xor` и `codepoint`. Реализовала шифрование гаммированием на языке программирования Julia.

Спасибо за внимание!