

# **Лабораторная работа №3**

**Математические основы защиты информации и информационной  
безопасности**

Дарижапов Тимур Андреевич

# Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	9
5	Список литературы	10

## List of Tables

# List of Figures

3.1	Программа реализации шифра . . . . .	7
3.2	Вывод программы . . . . .	8

# 1 Цель работы

Познакомиться с алгоритмом шифрования гаммированием конечной гаммой и применить его на практике.

## 2 Задание

Реализовать алгоритм шифрования гаммированием конечной гаммой

### 3 Выполнение лабораторной работы

Данная работа была выполнена на языке Julia.

Для реализации алгоритм шифрования гаммированием конечной гаммой мной была написана следующая программа (рис. 3.1) :

```
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))
```

Figure 3.1: Программа реализации шифра

В данной программе:

1 строка: подключение библиотеки для реализации выбора случайной гаммы.

2-14 строки: реализация функции для шифрования.

2-5: проверка условия, что длины текста и гаммы совпадают, иначе алгоритм не будет реализован.

8-11: основной цикл, который взаимодействует с кодами чисел и возвращает

третий код, который затем преобразуется в новый символ шифр-текста.

13: возвращаем результат работы программы - шифр-текст.

16: задаём пустую гамму для дальнейшего заполнения

17: задаём текст, который хотим зашифровать

19: задаём гамму случайным образом длиной текста.

21: вызываем функцию.

23-26: вывод результатов программы.

Далее представлен результат работы программы (рис. 3.2 )

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

Figure 3.2: Вывод программы

Как видно, программа работает верно.



## 4 Выводы

Я познакомился с алгоритмом шифрования гаммированием конечной гаммой и применил его на практике.

## 5 Список литературы

Лабораторная работа №3

Шифрование гаммированием [Электронный ресурс]. URL: <https://esystem.rudn.ru/mod/folder/>