Лабораторная работа №3

Математические основы защиты информации и информационной безопасности

Колчева Юлия Вячеславовна

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) :

```
1  using Random
2  function text_f(text, key)
3      if length(text) != length(key)
4          return "Длины не совпадают"
5      end
6
7      ctext = ""
8      for i in 1:length(text)
9          ctext_s = Int(codepoint(text[i])) ⊻ Int(codepoint(key[i]))
10         ctext *= Char(ctext_s)
11     end
12
13     return ctext
14 end
15
16 key = ""
17 text = "Hello, world"
18 Random.seed!(4)
19 global key = key * randstring(['A':'Z'; '0':'9'], length(text))
20
21 ctext = text_f(text, key)
22
23 println("Текст: ", text)
24 println("Гамма: ", key)
25 println("Зашифрованный текст: ", ctext)
26 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 случайны образом длинной текста.

21: вызываем функцию.

23-26: вывод результатов программы.

Далее представлен результат работы программы (рис. 3.2)

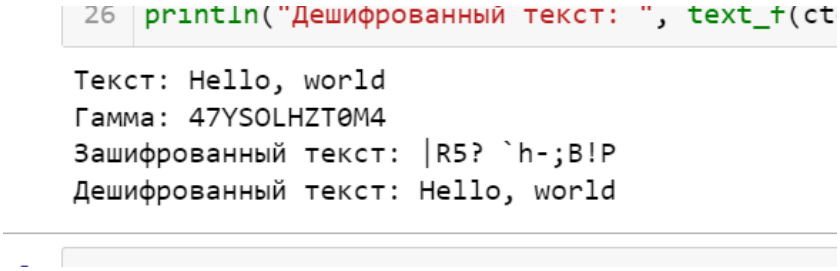

Figure 3.2: Вывод программы

Как видно, программа работает верно.

4 Выводы

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/view.php?id=1150972