

# **Лабораторная Работа No 1**

## **Математические Основы Защиты Информации и Информационной Безопасности**

Хосе Фернандо Леон Атупанья | НФИМд-01-24

# Содержание

1. Цель работы
2. Выполнение лабораторной работы
3. Выводы

## 1. Цель работы

Приобретение практических навыков использования языка программирования "Julia" для выполнения упражнений по шифрованию (Cesar и Atbash).

## 2. Выполнение лабораторной работы

### Шифр Цезаря

Для начала создайте файл "lab1.1.jl", чтобы выполнить первое упражнение в задании. Шифровка Цезаря.

```
lab1.1.jl > ...
1  k = 3
2  text = "HOLA MUNDO"
3  encryption = ""
4
5  for c in text
6      if isuppercase(c)
7          c_unicode = Int(c)
8          c_index = c_unicode - Int('A')
9
10         new_index = (c_index + k) % 26
11
12         new_unicode = new_index + Int('A')
13         new_character = Char(new_unicode)
14
15         encryption *= new_character
16     else
17         encryption *= c
18     end
19 end
20 println("Plain text: $text")
21 println("Encrypted text: $encryption")
```

Для начала мы создали программные переменные 'k' - количество пробелов смещения, которые были сделаны из основы алфавита. 'text' - текст, который будет зашифрован, 'encryption' - зашифрованный текст.

```
k = 3
text = "HOLA MUNDO"
encryption = ""
```

Теперь мы создаем цикл "for", чтобы изменить порядок нашего алфавита, для начала с помощью команды "isuppercase" мы узнаем, что наш текст написан заглавными буквами, а параметр "c" служит для определения местоположения, в котором будет находиться первая буква алфавита (буква "A"). В этом случае, согласно таблице ASCII, каждый символ на клавиатуре имеет значение, мы используем 'c\_unicode' для определения этого значения и 'c\_index' в качестве вычитания, чтобы количество букв алфавита начиналось с 0 до 25.

```
for c in text
  if isuppercase(c)
    c_unicode = Int(c)
    c_index = c_unicode - Int('A')

    new_index = (c_index + k) % 26

    new_unicode = new_index + Int('A')
    new_character = Char(new_unicode)

    encryption *= new_character
  else
    encryption *= c
  end
end
```

В 'new\_index' мы объявляем изменение порядка букв алфавита, а в 'new\_unicode' и 'new\_character' мы присваиваем им новое значение, которое будет иметь в соответствии с таблицей ASCII. Наконец, в переменной encryption мы сохраним зашифрованный текст. В противном случае, если буква является строчной, то никаких изменений в тексте не вносится.

И мы печатаем результат аргументов 'text' и 'encryption':

```
println("Plain text: $text")
println("Encrypted text: $encryption")
```

Наш Output

```
Plain text: HOLA MUNDO
Encrypted text: KROD PXQGR
```

## Шифр Атбаш

Мы создали функцию `atbash_cipher`, которая помогла бы нам полностью изменить порядок алфавита, первую букву в конце и так далее.

```
#Шифр Атбаш
function atbash_cipher(text::String)
    result = []

    for char in text
        if isletter(char)
            ascii_offset = isuppercase(char) ? 'A' : 'a'
            new_char = Char(ascii_offset + (25 - (Int(char) - Int(ascii_offset))))
            push!(result, string(new_char))
        else
            push!(result, string(char))
        end
    end

    return join(result)
end
```

Переменная `'result'` - это пустой массив, в который мы поместим зашифрованный текст в конце нашего цикла. Мы начинаем наш цикл с распознавания каждой буквы текста, который мы пытаемся зашифровать, независимо от того, написано ли оно в верхнем или нижнем регистре.

```
        new_char = Char(ascii_offset + (25 - (Int(char) - Int(ascii_offset))))
        push!(result, string(new_char))
    else
        push!(result, string(char))
    end
```

Мы объявляем новый порядок букв и сохраняем его в нашем массиве результатов, в противном случае, если в тексте есть что-то большее, чем символ, то текст сохраняется без изменений.

```
println("HELLO WORLD")
println(atbash_cipher("HELLO WORLD"))
```

В конце, мы печатаем текст, который собираемся зашифровать, и результат после вызова функции.

Наш Output

```
HELLO WORLD  
SVOOL DLIOW
```

### 3. Выводы

При разработке этой лаборатории мы получили необходимые знания для выполнения шифрования текста на языке программирования Julia и успешно выполнили задачи, поставленные в лаборатории.