

Шифры простой замены

Лабораторная работа №1

Данилова А.С.

01 января 1970

Российский университет дружбы народов, Москва, Россия

Объединённый институт ядерных исследований, Дубна, Россия

- Изучить теоретическую часть
- Реализовать шифр Цезаря и шифр Атбаш.

Шифр Цезаря (также он является шифром простой замены) - это моноалфавитная подстановка, т.е. каждой букве открытого текста ставится в соответствие одна буква шифртекста. На практике при создании шифра простой замены в качестве шифроалфавита берется исходный алфавит, но с нарушенным порядком букв (алфавитная перестановка).

Шифр Атбаш - это один из древнейших криптографических методов, который был впервые описан в Талмуде и использовался еще в Древнем Вавилоне. Основная идея шифра Атбаш заключается в замене каждой буквы текста на букву, находящуюся на противоположном конце алфавита. Например, в латинском алфавите 'a' заменяется на 'z', 'b' на 'y', и так далее.

```
1 function caesar(text::String, k::Int)
2     alph = collect("abcdefghijklmnopqrstuvwxyz")
3     etext = ""
4
5     for char in text
6         if char in alph
7             index = findfirst(isequal(char), alph)
8             new_index = ((index - 1 + k) % length(alph)) + 1
9             e_char = alph[new_index]
10            etext *= e_char
11        else
12            etext *= char
13        end
14    end
15
16    return etext
17 end
18
19 print("Введите текст: ")
20 text = readline()
21 print("Введите ключ: ")
22 key = parse{Int, readline()}
23
24 encrypted = caesar(text, key)
25 println("Зашифрованный текст: ", encrypted)
```

Рис. 1: Шифр Цезаря

Введите текст:

hello world

Введите ключ:

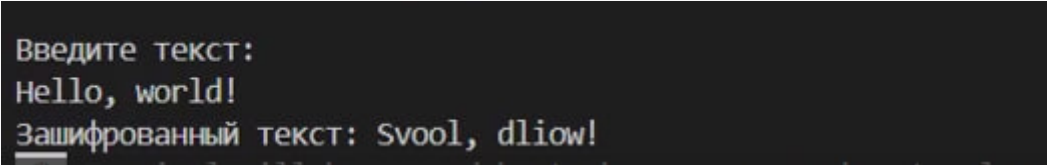
7

Зашифрованный текст: olssv dvysk

Рис. 2: Зашифрованный текст

```
1 function atbash(text)
2   alph = collect("abcdefghijklmnopqrstuvwxyz")
3   reversed_alph = reverse(alph)
4   etext = ""
5
6   for char in text
7     index = findfirst(letter -> lowercase(char) == letter, alph)
8     if index != nothing
9       e_char = reversed_alph[index]
10      if char == uppercase(char)
11        e_char = uppercase(e_char)
12      end
13      etext *= e_char
14    else
15      etext *= char
16    end
17  end
18
19  return etext
20 end
21
22 println("Введите текст: ")
23 text = readline()
24 encrypted = atbash(text)
25 println("Зашифрованный текст: ", encrypted)
```

Рис. 3: Шифр Атбаш



```
Введите текст:  
Hello, world!  
Зашифрованный текст: Svoool, dliow!
```

Рис. 4: Зашифрованный текст

Мы изучили то, как работают два метода шифрования, а также реализовали их самостоятельно на языке программирования Julia.