

Лабораторная работа №1

Шифры простой замены

Федюшина Ярослава Андреевна

Содержание

Цель работы	5
Задание	6
Выполнение лабораторной работы	7
Выводы	9

Список иллюстраций

1	Шифр Цезаря	7
2	Шифр Атбаш	8

Список таблиц

Цель работы

Целью работы является изучение алгоритмов шифрования Цезаря и Атбаш, принцип работы, реализация на Julia.

Задание

1. Реализовать шифр Цезаря с произвольным ключом k
2. Реализовать шифр Атбаш

Выполнение лабораторной работы

Суть шифра Цезаря заключается в том, что происходит смещение всех букв по алфавиту в сообщении на некоторый коэффициент k . Декодирование происходит путем смещения в обратную сторону. (рис. [-@fig:001]).

```
function caesar_cipher(text::String, shift::Int)
    alphabet = 'A':'Z'
    encrypted_text = ""

    for char in uppercase(text)
        if char in alphabet
            pos = findfirst(isequal(char), alphabet)
            new_pos = mod(pos + shift - 1, length(alphabet)) + 1
            encrypted_text *= alphabet[new_pos]
        else
            encrypted_text *= char
        end
    end
    return encrypted_text
end

text = "hello"
shift = 3
println("зашифрованный текст: |", caesar_cipher(text, shift))
```

Рис. 1: Шифр Цезаря

Шифр Атбаш похож на шифр Цезаря, но в данном алгоритме разворачивается весь алфавит, а не какой то маленький сдвиг. (рис. [-@fig:002]).

```
function atbash_cipher(text::String)
    alphabet = 'A':'Z'
    encrypted_text = ""
    for char in uppercase(text)
        if char in alphabet
            pos = findfirst(isequal(char), alphabet)
            new_char = alphabet[length(alphabet) - pos + 1]
            encrypted_text *= new_char
        else
            encrypted_text *= char
        end
    end
    return encrypted_text
end

text = "hello world"
println("зашифрованный текст: ", atbash_cipher(text))
```

Рис. 2: Шифр Атбаш

Выводы

В результате выполнения лабораторной данной работы мы научились реализовывать два алгоритма шифрования - Цезарь и Атбаш. Оба алгоритма были реализованы на языке Julia.