

Лабораторная работа №1

Реализация шифра Цезаря с произвольным ключом k, реализация шифра Атбаш.

автор

Кюнкристов Д.С. -

принадлежность

Российский университет дружбы народов, Москва, Россия

-

Информация

Докладчик

- Кюнкристов Даниил Саналович
- студент уч. группы НПИМД-01-24
- Российский университет дружбы народов
- 1132249574@pfur.ru
- https://github.com/DanzanK/2025-2026_math-sec/tree/main

Вводная часть

Актуальность

- Создание кода на Julia (шифра простой замены), чтобы понять принципы работы алгоритмов.

Объект и предмет исследования

- Шифры простой замены (шифр Цезаря и шифр Атбаш)
- Распределенная система управления версиями Git.
- Веб-сервис GitHub
- Язык разметки Markdown

Цели и задачи

- Реализовать шифр Цезаря с произвольным ключом k, Реализовать шифр Атбаш

Процесс выполнения работы

Реализация шифра Цезаря с произвольным ключом k на языке

программирования Julia

```
function main()
    alphabet = collect("абвгдеёжзийклмнопрстуфхцчишъыъюъ")
    n = length(alphabet)
    while true
        println("ш - шифрование, р - расшифровка, в - выход")
        menu = lowercase(strip(readline()))
        if menu == "в"
            break
        elseif menu == "ш"
            operation = "шифрование"
        elseif menu == "р"
            operation = "расшифровка"
        else
            println("Ошибка команды")
            continue
        end

        print("Введите сообщение:")
        message = lowercase(strip(readline()))
        print("Введите ключ (число):")
        try
            key = parse(Int,readline())
        catch e
            println("Ошибка catch")
            continue
        end
        if menu == "р"
            key = -key
        end
        output = ""

        for letter in message
            idx = findfirst(isequal(letter), alphabet)
            if idx !== nothing
                new_idx = mod(idx+key-1,n)+1
                output *= string(alphabet[new_idx])
            else
                output *= string(letter)
            end
        end
        println("Result $operation: $output")
    end
end

main() | ⌂
```

```
ш - шифрование, р - расшифровка, в - выход
julia> ш
ш
Введите сообщение:сообщение
Введите ключ (число):4
Result шифрование: хттеэисми
ш - шифрование, р - расшифровка, в - выход
р
Result шифрование: хттеэисми
ш - шифрование, р - расшифровка, в - выход
р
ш - шифрование, р - расшифровка, в - выход
р
Введите сообщение:хттеэисми
Введите ключ (число):4
Введите сообщение:хттеэисми
Введите ключ (число):4
Result расшифровка: сообщение
Введите ключ (число):4
Result расшифровка: сообщение
Result расшифровка: сообщение
ш - шифрование, р - расшифровка, в - выход
```

Реализация шифра Атбаш на языке программирования Julia

```
function Atbash(message::AbstractString, alphabet::Vector{Char})
    n = length(alphabet)
    output = IOBuffer()

    for letter in message
        idx = findfirst==(letter), alphabet)
        if idx !== nothing
            new_idx = n - idx + 1
            write(output, alphabet[new_idx])
        else
            write(output, letter)
        end
    end
    return String(take!(output))
end

function main()
    alphabet = collect("абвгдеёжзийклмнопрстуфхцчишъыъэюя")
    while true
        println("ш - шифрование, р - расшифровка, в - выход")
        menu = lowercase(strip(readline()))
        if menu == "в"
            break
        elseif menu == "ш"
            operation = "шифрование"
        elseif menu == "р"
            operation = "расшифровка"
        else
            println("Ошибка команды")
            continue
        end

        print("Введите сообщение:")
        message = lowercase(strip(readline()))

        output = Atbash(message, alphabet)

        println("Result $operation: $output")
    end
end
```

main() | ⌂

```
ш - шифрование, р - расшифровка, в - выход
julia> ш
ш
Введите сообщение:сообщение
Введите сообщение:сообщение
Result шифрование: нррюёсьсъ
ш - шифрование, р - расшифровка, в - выход
[]
```

Результаты

- Выполнены все необходимые действия для реализации задач лабораторной работы.

Вывод

Реализованы шифры простой замены (шифр Цезаря и шифр атбаш)