Author

Старикова Евгения Дмитриевна

email: 1032259343@pfur.ru

Российский университет дружбы народов

Российская Федерация

Москва

"Лабораторная работа №3" "Шифрование гаммированием"

Цель работы

Цель работы -- изучить и реализовать шифрование гаммированием.

Задание

С помощью языка программирования Julia реализовать:

- шифрование гаммированием.

Теоретическое введение

Julia — высокоуровневый свободный язык программирования с динамической типизацией, созданный для математических вычислений[@julialang]. Эффективен также и для написания программ общего назначения. Синтаксис языка схож с синтаксисом других математических языков, однако имеет некоторые существенные отличия.

Для выполнения заданий была использована официальная документация Julia[@juliadoc].

Выполнение лабораторной работы

Шифрование гаммированием — это симметричный метод шифрования, при котором к открытым данным (тексту) применяется операция наложения (обычно XOR) с последовательностью случайных чисел, называемой гаммой. Эта гамма должна быть не короче сообщения и обеспечивает обратимость операции, позволяя расшифровать данные при наличии той же гаммы. Такой метод обеспечивает высокую стойкость при условии использования случайной и одноразовой гаммы.

```
function gamma_cypher(text, gamma; mod=33)
    russian_alphabet = collect("абвгдежзийклмнопрстуфхцчшщьыъэюя")

    # Фильтруем текст, оставляя только буквы и приводим к нижнему регистру
    filtered_text = [c for c in lowercase(text) if c in russian_alphabet]

    # Преобразуем гамму в числовые значения
    gamma_nums = [findfirst(==(c), russian_alphabet) for c in gamma]
```

```
    # Создаем повторяющуюся гамму нужной длины
    repeated_gamma = repeat(gamma_nums, ceil(Int, length(filtered_text) / length(gamma_nums)))

    cyphered_text = ""

    for (a, b) in zip(filtered_text, repeated_gamma)
        # Находим индекс буквы в алфавите
        char_index = findfirst(==(a), russian_alphabet)
        # Вычисляем новый индекс
        new_index = (char_index + b) % mod
        if new_index == 0
            new_index = mod
        end
        # Добавляем соответствующую букву
        cyphered_text *= russian_alphabet[new_index]
    end

    return cyphered_text
end
```

Также реализуем простую программу для проверки работы шифра:

```
function main()
    text = "приказ"
    gamma = "гамма"
    cyphered_text = gamma_cypher(text, gamma)
    println("Исходный текст: ", text)
    println("Гамма: ", gamma)
    println("Зашифрованный текст: ", cyphered_text)
end
```

```
Результат:

Исходный текст: приказ

Гамма: гамма

Зашифрованный текст: усхчбл
```

Выводы

С помощью языка программирования Julia были реализованы:

- шифрование гаммированием.

Список литературы{.unnumbered}

::: {#refs} :::