Лабораторная работа №3

Шифрование гаммированием

Коняева Марина Александровна
НФИмд-01-25
Студ. билет: 1032259383

2025

RUDN

Теоретическое введение

Шифр гаммирования — симметричный потоковый шифр, в котором каждый символ открытого текста объединяется с соответствующим символом гаммы с помощью операции сложения по модулю.

Ключевые особенности: - Относится к классу потоковых шифров - Криптостойкость зависит от длины и случайности гаммы - При одноразовом ключе — абсолютная криптостойкость

Цель работы

Целью данной работы является изучение алгоритма шифрования гаммированием, принципа его работы и реализация на языке программирования Julia.

Задание

1. Реализовать алгоритм шифрования гаммированием
2. Реализовать алгоритм дешифрования
3. Протестировать работу алгоритма на примере

Реализация шифрования

```
function gamma_encrypt(text::Vector{Int}, gamma::Ve
                       mod_value::Int=33)
    # Формируем ключевое слово
    keyText = Int[]
    for i in 1:(textLen ÷ gammaLen)
        append!(keyText, gamma)
    end
    # Шифрование
    for i in 1:textLen
        result = (text[i] + keyText[i]) % mod_value
        push!(encrypted, result)
    end
    return encrypted
end
```

Реализация дешифрования

```
function gamma_decrypt(encrypted::Vector{Int}, gamm
                       mod_value::Int=33)
    # Формируем ключевое слово
    keyText = Int[]
    for i in 1:(encryptedLen ÷ gammaLen)
        append!(keyText, gamma)
    end
    # Расшифрование
    for i in 1:encryptedLen
        result = (encrypted[i] - keyText[i]) % mod_
        if result <= 0
            result += mod_value
        end
        push!(decrypted, result)
    end
    return decrypted
end
```

Тестирование алгоритма

```
text = [16, 17, 9, 11, 1, 8] # ПРИКАЗ
gamma = [4, 1, 13, 13, 1] # ГАММА
mod_value = 33

encrypted = gamma_encrypt(text, gamma, mod_value)
decrypted = gamma_decrypt(encrypted, gamma, mod_val
```

Выполнение лабораторной работы

Результаты выполнения

```
Исходный текст: [16, 17, 9, 11, 1, 8]
Гамма: [4, 1, 13, 13, 1]
Зашифрованный текст: [20, 18, 22, 24, 2, 12]
Расшифрованный текст: [16, 17, 9, 11, 1, 8]
Исходный текст восстановлен: true
```

Вывод

В данной лабораторной работе был успешно реализован алгоритм шифрования гаммированием на языке Julia. Алгоритм корректно выполняет как шифрование, так и дешифрование, что подтверждается тестовыми примерами. Реализация демонстрирует принципы работы потоковых шифров и модульной арифметики в криптографии.

Список литературы

[1] Методические материалы курса.

[2] Wikipedia: Stream cipher

[3] Официальная документация по языку Julia