Лабораторная работа №3

Морозова Ульяна

Российский университет дружбы народов, Москва, Россия

Цели

Целью работы является изучение алгоритмов шифрования гаммированием и реализация его на языке Julia.

Шифрование гаммированием

Шифрование гаммированием (в англоязычной версии — stream cipher) — метод симметричного шифрования, при котором последовательность случайных символов (гамма) накладывается на открытый текст. Гамма вырабатывается по определённому алгоритму и используется для шифровки открытых данных и дешифровки шифротекста.

Принцип работы

- Генерация гаммы. Можно использовать генератор псевдослучайных чисел или аппаратный источник случайных чисел. Длина гаммы должна быть не меньше длины защищаемого сообщения (открытого текста).
- Наложение гаммы на открытый текст. Процедура может быть различной: например, символы исходного текста и гаммы заменяются цифровыми эквивалентами, которые затем складываются или вычитаются, или символы представляются в виде двоичного кода, затем соответствующие разряды складываются по модулю 2 (XOR).
- Дешифрование — повторная генерация гаммы и наложение гаммы на зашифрованные данные.

```julia
using Random

function gamma_cipher(text::AbstractString, key::AbstractString; encrypt::Boo
    # Преобразуем текст и ключ в массивы байтов
    text_bytes = Vector{UInt8}(text)
    key_bytes = Vector{UInt8}(key)

    # Если ключ короче текста, повторяем его
    if length(key_bytes) < length(text_bytes)
        key_bytes = repeat(key_bytes, ceil(Int, length(text_bytes) / length(k
        key_bytes = key_bytes[1:length(text_bytes)]
    end

    result = Vector{UInt8}(undef, length(text_bytes))
```

Результат работы шифра

```
julia> demo()
Исходный текст: All I want for Christmas is you!
Ключ (hex): b82a3af92aa5d3026365c938858f79a7
Зашифрованный текст (hex): f94656d96385a4630d11e95eeafd59e4d058538a5ec8b27143
Дешифрованный текст: All I want for Christmas is you!
Проверка: true
```

Выводы

Мы изучили работу алгоритмов шифрования гаммированием, а также реализовали его на языке Julia.