

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ПРЕЗЕНТАЦИЯ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 3

дисциплина: Математические основы защиты информации и информационной безопасности

Студент: Пиняева Анна Андреевна

Группа: НПИмд-01-24

МОСКВА

2025

Цель работы

Изучение и реализация шифрования гаммированием на языке Julia.

Ход работы

1. Функция получения номера буквы

```
alphabet=collect("АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ")
```

```
function letter(c::Char)
    pos = findfirst(isequal(c), alphabet)
    if pos === nothing
        error("Буквы в алфавите нет")
    end
    return pos
end
```

2. Функция получения буквы по номеру

```
function num(n::Int)
    if n ==0
        n=32
    elseif n<1 || n>32
        error("Номер не в диапазоне")
    end
    return alphabet[n]
end
```

3. Функция шифрования

```
function gamma(message::String, key::String, mod_val::Int=32)
    p_nums = [letter(c) for c in message]
    k_nums=[letter(c) for c in key]
    k_len=length(k_nums)

    c_nums=Vector{Int}(undef, length(p_nums))
    for i in 1:length(p_nums)
        ki=k_nums[(i-1) % k_len+1]
        c_nums[i]=(p_nums[i] + ki) % mod_val
        if c_nums[i] ==0
            c_nums[i]=mod_val
        end
    end

    return join([num(n) for n in c_nums])
end
```

4. Функция дешифрования

```
function gamma_de(ciphertext::String, key::String, mod_val::Int=32)
    c_nums=[letter(c) for c in ciphertext]
    k_nums=[letter(c) for c in key]
    k_len=length(k_nums)

    p_nums=Vector{Int}(undef, length(c_nums))
    for i in 1:length(c_nums)
        ki=k_nums[(i-1) % k_len+1]
        p_nums[i]=(c_nums[i] - ki) % mod_val
        if p_nums[i] ==0
            p_nums[i]=mod_val
        end
    end

    return join([num(n) for n in p_nums])
end
```

5. Вывод результатов

```
message="ПРИКАЗ"  
key="ГАММА"  
encrypted=gamma(message,key)  
decrypted=gamma_de(encrypted, key)  
  
println("открытый текст: $message")  
println("ключ: $key")  
println("зашифрованный текст: $encrypted")  
println("расшифрованный текст: $decrypted")
```

Результат тестирования представлен на рис.1

Рис. 1 Тестирование шифрования гаммированием:

```
println("Зашифрованный текст: $encrypted")  
println("Расшифрованный текст: $decrypted")
```

Открытый текст: ПРИКАЗ

Ключ: ГАММА

Зашифрованный текст: УСХЧБЛ

Расшифрованный текст: ПРИКАЗ

:

|

Вывод: В ходе данной работы мной был изучен и реализован метод шифрования гаммированием. Написан программный код на языке Julia и протестирован.