

Презентация к лабораторной работе 3

Математические основы защиты информации и информационной безопасности

Аристова Арина Олеговна

07 октября 2025

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

- Аристова Арина Олеговна
- студентка группы НФИмд-01-25
- Российский университет дружбы народов имени Патриса Лумумбы
- 1032259382@rudn.ru
- <https://github.com/aoaristova>



Цель работы

Изучить шифрование гамилизацией, реализовать соответствующий алгоритм на языке Julia.

Задание

- Реализовать шифр гаммированием

Выполнение лабораторной работы

Реализация шифрования гаммированием

В коде задан русский алфавит. Необходимые переменные содержат текст, который необходимо зашифровать и гамма-ключ.

```
alphabet = ['А', 'Б', 'В', 'Г', 'Д', 'Е', 'Ж', 'З', 'И', 'Й', 'К', 'Л', 'М', 'Н',
```

```
text = "ПРИКАЗ"
```

```
gamma = "ГАММА"
```

Реализация шифрования гаммированием

Две функции реализуют переходы от текста к номерам в алфавите и наоборот.

```
function text_to_numbers(text)
    [findfirst==(c), alphabet) for c in collect(text)]
end
```

```
function numbers_to_text(numbers)
    join([alphabet[n] for n in numbers])
end
```

Реализация шифрования гаммированием

Сперва необходимо перевести тексты в массивы номеров символов, а также зациклить гамма-ключ так, чтобы символов хватило для шифрования строки длиной $\text{length}(\text{text})$.

Затем реализуем шифрование текста нахождением остатка от деления на 33 суммы индексов каждого из символов текста и гамма-ключа.

```
gamma_extended = join(first(collect(repeat(gamma, ceil(Int,length(text))/length(text)))))

text_numbers = text_to_numbers(text)
gamma_numbers = text_to_numbers(gamma_extended)
```

Реализация шифрования гаммированием

Для расшифровки текста находим остатки от деления на 33 разности числового значения символа в шифре и соответствующего значения гамма-ключа.

Затем переводим массивы числовых значений в текст и выводим результаты.

```
encrypted_numbers = [mod(t+g-1, 33) + 1 for (t, g) in zip(text_numbers, gamma_numbers)]
decrypted_numbers = [mod(e - g - 1, 33) + 1 for (e, g) in zip(encrypted_numbers, gamma_numbers)]

encrypted_text = numbers_to_text(encrypted_numbers)
decrypted_text = numbers_to_text(decrypted_numbers)

println("Исходный текст:", text)
println("Зашифрованный текст:", encrypted_text)
println("Расшифрованный текст:", decrypted_text)
```

Проверка работы кода

Проверяю работу кода, получаю результат, идентичный тому, что был получен в приведенном тексте лабораторной работы

```
PS C:\Users\arist\Github\study_2025-2026_mathsec\labs\lab03> julia .\gamm.jl
Исходный текст:ПРИКАЗ
Зашифрованный текст:УСХЧБЛ
Расшифрованный текст:ПРИКАЗ
```

Рис. 1: Результат работы программы

Вывод

В ходе выполнения данной лабораторной работы мною были получены знания о шифровании гаммированием, а также создана программа для реализации шифрования и расшифрования с помощью гаммирования.