# Шифрование гаммированием

Лабораторная работа №3

Данилова А.С.

# Цели и задачи

Изучить шифрование гаммированием, реализовать алгоритм шифрования гаммированием конечной гаммой на языке программирования Julia.

### Шифрование гаммированием

*Гаммирование* - процедура наложения при помощи некоторой функции F на исходный текст гаммы шифра, т.е. псевдослучайной последовательности (ПСП) с выходов генератора G.

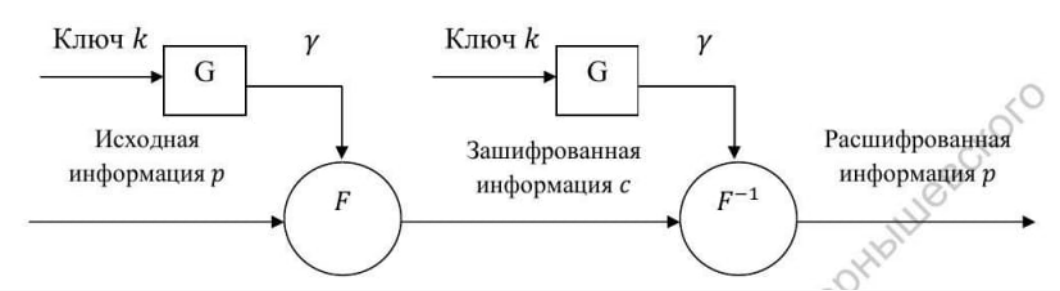


Рис. 1: Схема гаммирования

Стойкость шифров, основанных на процедуре гаммирования, зависит от характеристик гаммы - длины и равномерности распределения вероятностей появления знаков гаммы. При использовании генератора ПСП получаем бесконечную гамму. Однако, возможен режим шифрования конечной гаммы. В роли конечной гаммы может выступать фраза. Как и ранее, используется алфавитный порядок букв, т.е. буква «а» имеет порядковый номер 1, «б» - 2 и т.д.

# Выполнение работы

```julia
using Dates

function encrypt(text, gamma)
    shtext = ""
    key = iterate(gamma)
    values = [Int(c) for c in text]
    for p in values
        if key === nothing
            key = iterate(gamma)
        end
        k, state = key
        c = Char(((p - 1040) + (Int(k) - 1040)) % 32 + 1040)
        shtext *= string(c)
        key = iterate(gamma, state)
    end
    return shtext
end

function decrypt(shtext, gamma)
    text = ""
    key = iterate(gamma)
    for c in shtext
        if key === nothing
            key = iterate(gamma)
        end
        k, state = key
        p = Char(((Int(c) - 1040) - (Int(k) - 1040)) % 32 + 1040)
        text *= string(p)
        key = iterate(gamma, state)
    end
    return text
end

println("Введите текст: ")
text = readline()
println("Введите гамму: ")
gamma = readline()
```

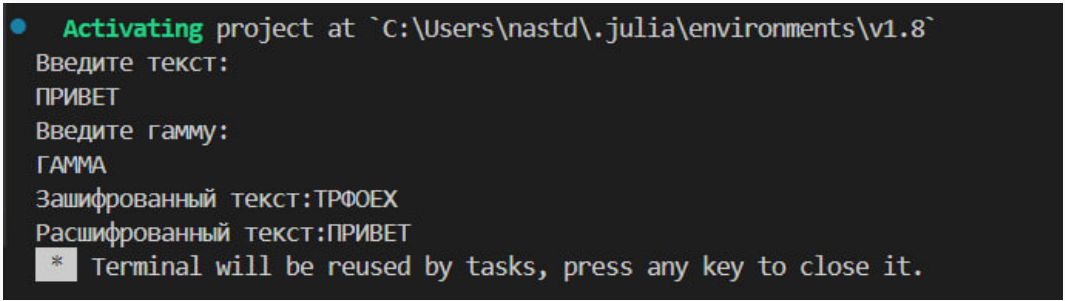


Рис. 3: Зашифрованный и дешифрованный текст

# Выводы

Мы изучили шифрование гаммированием, а также реализовали алгоритм шифрования гаммированием конечной гаммой на языке программирования Julia.