Математические основы защиты информации и информационной безопасности

Дарижапов Тимур АНдреевич

23 Ноября 2024

РУДН, Москва, Россия

Лабораторная работа 6

p-метод Полларда.

In [56]:

```
using Random
using Base.GMP: gcd

function pollard(n)
    B = 30
    a = rand(2:n-1)
    for j in 2:B
        a = powermod(a, j, n)
    end
    d = gcd(a - 1, n)
    if 1 < d < n
        return d
    else
        return nothing
    end
end

n = 21
factor = pollard(n)
if factor !== nothing
    println(" $n = $factor * $(n ÷ factor)")
else
    println("Множители числа $n не найдены")
end
```

```
21 = 7 * 3
```

Рис. 1: Реализация программы

Выводы

- Познакомился с алгоритмом разбора числа на множители
- Реализовал алгоритм p-метод Полларда

Спасибо за внимание!