

# Математические основы защиты информации и информационной безопасности

---

Колчева Юлия Вячеславовна

23 Ноября 2024

РУДН, Москва, Россия

## Лабораторная работа 6

---

## р-метод Полларда.

```
In [56]: 1 using Random
          2 using Base.GMP: gcd
          3
          4 function pollard(n)
          5     B = 30
          6     a = rand(2:n-1)
          7     for j in 2:B
          8         a = powermod(a, j, n)
          9     end
         10     d = gcd(a - 1, n)
         11     if 1 < d < n
         12         return d
         13     else
         14         return nothing
         15     end
         16 end
         17
         18 n = 21
         19 factor = pollard(n)
         20 if factor != nothing
         21     println(" $n = $factor * $(n ÷ factor)")
         22 else
         23     println("Множители числа $n не найдены")
         24 end

21 = 7 * 3
```

Рис. 1: Реализация программы

- Познакомилась с алгоритмом разбора числа на множители
- Реализовала алгоритм р-метод Полларда

Спасибо за внимание!