

# **Лабораторная работа №6**

**Математические основы защиты информации и информационной  
безопасности**

Колчева Юлия Вячеславовна

# Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	9
5	Список литературы	10

# List of Tables

# List of Figures

3.1 Программа реализации теста Ферма . . . . . 7

# 1 Цель работы

Познакомиться с алгоритмом разбора числа на множители.

## 2 Задание

Реализовать алгоритм, реализующий р-метод Полларда.

### 3 Выполнение лабораторной работы

Данная работа была выполнена на языке Julia.

Для реализации теста Ферма была написана следующая программа (рис. 3.1) :

```
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
```

Figure 3.1: Программа реализации теста Ферма

В данной программе:

1-2 строки: подключение библиотек для случайного числа и для нахождения НОД

4: задание функции

5-9: Задаём сжимающую функцию, в данном случае степенную. Со случайно выбранным числом делаем операцию  $a^B \bmod n$ .

10: находим НОД чисел  $a-1$  и  $n$

11: проводим проверку условия, если числитель нетривиальный, то выводим его, в ином случае алгоритм необходимо повторить

18: задаём число, которое нужно разложить

19: запускаем функцию.

Мы можем видеть результат на (рис. 3.1 ). Программа работает верно.



## 4 Выводы

Познакомилась с алгоритмом разбора числа на множители и реализовала алгоритм р-метод Полларда.

## 5 Список литературы

Лабораторная работа №6

Разложение чисел на множители [Электронный ресурс]. URL: <https://esystem.rudn.ru/mod/fold>