Лабораторная работа №6

Математические основы защиты информации и информационной безопасности

Дарижапов Тимур Андреевич

Содержание

List of Tables

List of Figures

1 Цель работы

Познакомиться с алгоритмом разбора числа на множители.

2 Задание

Реализовать алгоритм, реализующий p-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]:

```
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
```

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! mod 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

Познакомился с алгоритмом разбора числа на множители и реализовал алгоритм p-метод Полларда.

5 Список литературы

Лабораторная работа №6

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