

Лабораторная работа №6

**Дисциплина: Математические основы защиты информации и
информационной безопасности**

Аветисян Давид Артурович

Содержание

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

List of Tables

List of Figures

3.1	Алгоритм, реализующий р-метод Полларда, на языке Julia	7
-----	--	---

1 Цель работы

Реализовать алгоритм, реализующий р-метод Полларда.

2 Задание

1. Реализовать алгоритм, реализующий p -метод Полларда.
2. Разложить на множители данное преподавателем число.

3 Выполнение лабораторной работы

Данная работа была выполнена на языке Julia.

Для реализации алгоритм, реализующего р-метод Полларда, была написана следующая программа.

```
[1]: using Printf

[2]: function pollard_p(n, f = x -> (x^2 + 1) % n, x0 = 2)
    x = x0
    y = x0
    d = 1

    while d == 1
        x = f(x)
        y = f(f(y))

        d = gcd(abs(x - y), n)
    end

    if d == n
        return :failure
    else
        return d
    end
end

[2]: pollard_p (generic function with 3 methods)

[3]: n = 8851
divisor = pollard_p(n)

if divisor != :failure
    @printf("Найден делитель числа %d: %d\n", n, divisor)
else
    @printf("Метод не нашёл делитель числа %d\n", n)
end

Найден делитель числа 8851: 97

[4]: n = 1359331
divisor = pollard_p(n)

if divisor != :failure
    @printf("Найден делитель числа %d: %d\n", n, divisor)
else
    @printf("Метод не нашёл делитель числа %d\n", n)
end

Найден делитель числа 1359331: 1151
```

Figure 3.1: Алгоритм, реализующий р-метод Полларда, на языке Julia

В данной программе:

- 1-й блок. Импорт необходимых модулей
- 2-й блок. Реализация самого алгоритма: Задаются начальные значения x и y и НОД d . С помощью цикла вычисляется медленный и быстрый шаги x и y . Затем они сравниваются, чтобы найти НОД. В конце проверяется результат выполнения алгоритма.
- 3-й блок. Задаётся значение n , для которого нужно найти делитель и вызывается

функция, описанная выше.

- 4-й блок. Вывод ответа в зависимости от результат выполнения алгоритма.

Мы можем видеть результат для чисел 8051 и 1359331 (данное преподавателем число) на рисунке выше. Программа работает верно.

4 Выводы

Я реализовал алгоритм, реализующий р-метод Полларда.