Отчет по лабораторной работе №6

дисциплина: Математические основы защиты информации и информационной безопасности

Морозова Ульяна

Содержание

1 Цель работы

Целью работы является изучение алгоритм разложение чисел на множителей и реализация его на языке Julia.

2 Выполнение лабораторной работы

2.1 Алгоритм p-метода Полларда

Идея метода основана на малой теореме Ферма: если p — простое число, являющееся делителем натурального числа a, то a^(p – 1) ≡ 1 mod p.

Алгоритм состоит из двух стадий: - Определение границы гладкости (B1). Чем больше B1, тем больше времени займёт вычисление, но большое B1 увеличивает шансы найти делитель на первой стадии. - Сбор в виде произведения M как можно большего числа степеней простых сомножителей так, чтобы M делилось на каждый сомножитель, входящий в разложение (p – 1). - Определение искомого делителя p по формуле: p = НОД(n, a^M – 1).

Далее приведена реализация шифра на языке Julia.

```
using Random

function pollard_rho(n::Integer, c::Integer=1, f::Function=x -> x^2+1)
    a = c
    b = c

    while true
        a = f(a)%n
        b = f(f(b)%n) % n

        d = gcd(abs(a-b),n)
```

```
        if 1<d<n
            return d
        elseif d==n
            return 0
        end
    end
end

function test_pollard()
    println("Тестирование p-метода Полларда")
    println('='^40)

    test_cases = [
        (8051, 1, "8051"),
        (10403, 1, "10403"),
        (15251, 1, "15251"),
        (123456789, 1, "123456789"),
        (987654321, 1, "987654321"),
        (15, 1, "15"),
        (21, 1, "21"),
        (35, 1, "35")
    ]

    for (n, c, desc) in test_cases
        println("\nТест: $desc")
        println("n = $n, c = $c")

        result = pollard_rho(n, c)
```

```
        if result == 0
            println("Результат: Делитель не найден")
        else
            println("Результат: Найден делитель p = $result")
            println("Проверка: $n = $result × $(n ÷ result)")
            println("Верность: $(result * (n ÷ result) == n)")
        end
        println('-'^40)
    end
end
```

И результат его работы

```
Тестирование p-метода Полларда
========================================

Тест: 8051
n = 8051, c = 1
Результат: Найден делитель p = 97
Проверка: 8051 = 97 × 83
Верность: true
----------------------------------------

Тест: 10403
n = 10403, c = 1
Результат: Найден делитель p = 101
Проверка: 10403 = 101 × 103
Верность: true
----------------------------------------
```

```
Тест: 15251
n = 15251, c = 1
Результат: Найден делитель p = 151
Проверка: 15251 = 151 × 101
Верность: true
----------------------------------------

Тест: 123456789
n = 123456789, c = 1
Результат: Найден делитель p = 3
Проверка: 123456789 = 3 × 41152263
Верность: true
----------------------------------------

Тест: 987654321
n = 987654321, c = 1
Результат: Найден делитель p = 3
Проверка: 987654321 = 3 × 329218107
Верность: true
----------------------------------------

Тест: 15
n = 15, c = 1
Результат: Найден делитель p = 3
Проверка: 15 = 3 × 5
Верность: true
----------------------------------------

Тест: 21
```

```
n = 21, c = 1
Результат: Найден делитель p = 3
Проверка: 21 = 3 × 7
Верность: true
----------------------------------------

Тест: 35
n = 35, c = 1
Результат: Найден делитель p = 7
Проверка: 35 = 7 × 5
Верность: true
----------------------------------------
```

3 Выводы

Мы изучили работу алгоритма, а также реализовали его на языке Julia.