Лабораторная работа №7

Математические основы защиты информации и информационной безопасности

Колчева Юлия Вячеславовна

Содержание

List of Tables

List of Figures

1 Цель работы

Познакомиться с дискретным логарифмированием в конечном поле.

2 Задание

Реализовать алгоритм, реализующий p-метод Полларда.

3 Выполнение лабораторной работы

Данная работа была выполнена на языке Julia.

Для реализации p-метода Полларда была написана следующая программа (рис. 3.1) (рис. 3.2):

```
In [6]:
using Base.GMP: gcd

function dlog(g, t, p)
    function inverse(x, p)
        return powermod(x, p - 2, p)
    end
    function f(xab)
        x, a, b = xab
        if x < p / 3
            return [(t * x) % p, (a + 1) % (p - 1), b]
        elseif 2 * p / 3 < x
            return [(g * x) % p, a, (b + 1) % (p - 1)]
        else
            return [(x * x) % p, (2 * a) % (p - 1), (2 * b) % (p - 1)]
        end
    end
    i, j, k = 1, [1, 0, 0], f([1, 0, 0])
    while j[1] != k[1]
        println(i, j, k)
        i, j, k = i + 1, f(j), f(f(k))
    end
    println(i, j, k)
    d = gcd(j[2] - k[2], p - 1)
    if d == 1
        return ((k[3] - j[3]) * inverse(j[2] - k[2], p - 1)) % (p - 1)
    end
```

Figure 3.1: Программа реализации p-метода Полларда

```
    m, l = 0, ((k[3] - j[3]) * inverse(j[2] - k[2], (p - 1) + d)) % ((p - 1) + d)
    while m <= d
        println(m, l)
        if powermod(g, l, p) == t
            return l
        end
        m, l = m + 1, (l + ((p - 1) + d)) % (p - 1)
    end
    return false
end

dlog(10,64,107)
```

Figure 3.2: Программа реализации p-метода Полларда

В данной программе:

1 строка: подключение библиотеки для нахождения НОД

3: задание функции

4-16: задание внутренней функции для вывода результатов

17: Задаём начальные значения

18: Начинаем вычисление, пока не получим равенство

18-36: запускаем основной алгоритм, который с помощью вычисления остатков от деления и формул, представленных в лабораторной работе, формирует таблицу ответов.

39: запускаем функцию.

Мы можем видеть результат на (рис. 3.3) . Программа работает верно.

```
39 dlog(10,64,107)
```

```
1[1, 0, 0][64, 1, 0]
2[64, 1, 0][101, 3, 0]
3[30, 2, 0][69, 6, 2]
4[101, 3, 0][27, 24, 8]
5[47, 3, 1][61, 26, 8]
6[69, 6, 2][81, 52, 17]
7[53, 12, 4][83, 104, 36]
8[27, 24, 8][61, 104, 38]
9[16, 25, 8][81, 102, 77]
10[61, 26, 8][83, 98, 50]
11[83, 52, 16][61, 98, 52]
12[81, 52, 17][81, 90, 105]
020
```

```
Out[6]: 20
```

Figure 3.3: Выводы

4 Выводы

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

5 Список литературы

Лабораторная работа №7

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