Математические основы защиты информации и информационной безопасности

Дарижапов Тимур Андреевич

07 Декабря 2024

РУДН, Москва, Россия

Лабораторная работа 7

p-метод Полларда.

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
```

Рис. 1: Реализация программы

p-метод Полларда.

```
27
28      m, l = 0, ((k[3] - j[3]) * inverse(j[2] - k[2], (p - 1) + d)) % ((p - 1) + d)
29      while m <= d
30          println(m, l)
31          if powermod(g, l, p) == t
32              return l
33          end
34          m, l = m + 1, (l + ((p - 1) + d)) % (p - 1)
35      end
36      return false
37  end
38
39  dlog(10,64,107)
```

Рис. 2: Реализация программы

Результат работы.

```
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

Рис. 3: Вывод программы

Выводы

- Познакомился с дискретным логарифмированием в конечном поле
- Реализовал алгоритм p-метод Полларда

Спасибо за внимание!