Разложение чисел на множители

Аль-Агуар Абдурахман Абдалла Мухаммад

3 января, 2024, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение задачи дискретного логарифмирования.

Выполнение лабораторной работы

Задача дискретного логарифмирования

Решение задачи дискретного логарифмирования состоит в нахождении некоторого целого неотрицательного числа x, удовлетворяющего уравнению. Если оно разрешимо, у него должно быть хотя бы одно натуральное решение, не превышающее порядок группы.

р-алгоритм Поллрада

- Вход. Простое число p, число a порядка r по модулю p, целое число bб $1 < b < p$; отображение f, обладающее сжимающими свойствами и сохраняющее вычислимость логарифма.
- Выход. показатель x, для которого $a^x = b(modp)$, если такой показатель существует.

1. Выбрать произвольные целые числа u, v и положить $c = a^u b^v (modp), d = c$
2. Выполнять $c=f(c)(mod p), d=f(f(d))(mod p), вычисляя при этом логарифмы для c и d как линейные функции от x по модулю r, до получения равенства $c = d(modp)$
3. Приняв логарифмы для c и d, вычислить логарифм x решением сравнения по модулю r. Результат x или РЕШЕНИЯ НЕТ.

Оценка сложности

Алгоритм полного перебора нашёл бы решение за число шагов не выше порядка данной группы.

Пример работы алгоритма

```
args = [
    (10, 64, 107),
]

for arg in args:
    res = pollard(*arg)
    print(arg, ': ', res)
    print("Validates: ", verify(arg[0], arg[1], arg[2], res))
    print()
```

```
(10, 64, 107) :  20
Validates:  True
```

Рис. 1: Работа алгоритма

Выводы

Результаты выполнения лабораторной работы

Изучили задачу дискретного логарифмирования.