Математические основы защиты информации и информационной безопасности. Лабораторная работа №7. Дискретное логарифмирование в конечном поле

Лесков Данила Валерьевич: НФИмд-02-21
Преподаватель: Кулябов Дмитрий Сергеевич

11 декабря, 2021, Москва, Россия

Российский Университет Дружбы Народов

Цели и задачи

Цель лабораторной работы

Изучение алгоритма p-Полларда для задач дискретного логарифмирования.

Задачи

Реализовать программно алгоритм, реализующий p-метод Полларда для задач дискретного логарифмирования

Выполнение лабораторной работы

Дискретное логарифмирование

Задача обращения функции g^x в некоторой конечной мультипликативной группе G.

Дискретное логарифмирование

Наиболее часто задачу дискретного логарифмирования рассматривают в мультипликативной группе кольца вычетов или конечного поля, а также в группе точек эллиптической кривой над конечным полем. Эффективные алгоритмы для решения задачи дискретного логарифмирования в общем случае неизвестны.

Дискретное логарифмирование

Для заданных g и a решение x уравнения $g^x = a$ называется дискретным логарифмом элемента a по основанию g.

ρ-метод Полларда для задач дискретного логарифмирования

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

ρ-метод Полларда для задач дискретного логарифмирования

1. Выбрать произвольные числа u, v и положить $c = a^u b^v (mod p), d = c$
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 $c \equiv d(mod p)$
3. Приравняв логарифы для c и d, вычислить логарифм x решением сравнения по модулю r. Результат: x или “Решений нет”.

Пример работы p-алгоритма Полларда

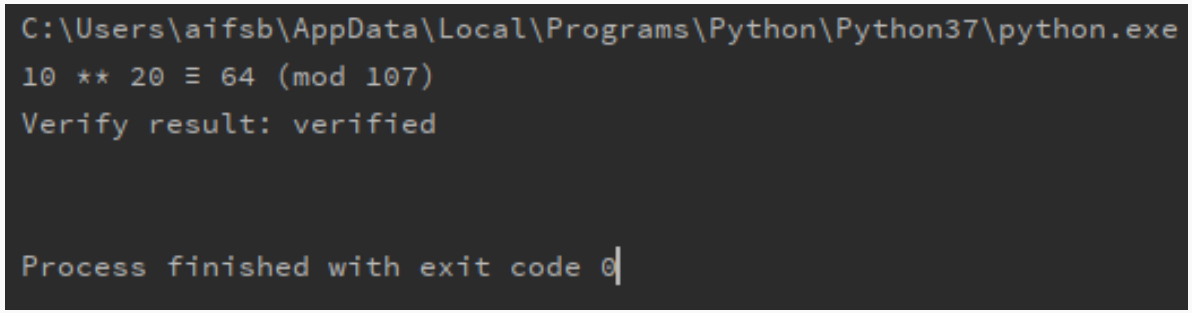

Figure 1: Пример работы p-алгоритма Полларда

Выводы

Результаты выполнения лабораторной работы

В ходе выполнения работы был успешно изучен p-метод Полларда для задач дискретного логарифмирования, а также был реализован программно программно на языке Python.