Лабораторная работа №7

Решение задачи дискретного логарифмирования

Студент: Ван Яо
Группа: НФИмд-01-25
РУДН, 2025

Цель работы

1. Изучение теоретических основ задачи дискретного логарифмирования в конечных полях.
2. Реализация алгоритма ρ Полларда для решения этой задачи.
3. Проведение тестирования алгоритма на различных примерах и анализ его эффективности.

Основные понятия

- **Конечное поле** F_p: множество вычетов по простому модулю p
- **Дискретный логарифм**: для $a^x \equiv b \pmod p$,найти $x = \log_a b$
- **Порядок элемента a**: наименьшее r>0, такое что$a^r \equiv 1 \pmod p$
- **ρ-метод Полларда**:вероятностный алгоритм поиска коллизий в псевдослучайной последовательности

ρ-метод Полларда для DLP

Основа: поиск цикла в последовательности $c_{i+1} = f(c_i)$, где

$$c_i = a^{\alpha_i} b^{\beta_i} \quad mod \quad p$$

Особенности: 1. Использует "черепаху и зайца" для поиска цикла
2. При коллизии $c_t = c_h$ получаем уравнение:
$(\beta_t - \beta_h)x \equiv (\alpha_h - \alpha_t)(mod \quad r)$ 3. Сложность: $O(\sqrt{r})$ где r - порядок элемента a

Алгоритм: пошагово

- Разбить F_p^* на 3 подмножества (по cmod3)
- Определить функцию перехода:
  - $S_1 : c \leftarrow c \cdot a, \alpha \leftarrow \alpha + 1$
  - $S_2 : c \leftarrow c \cdot b, \beta \leftarrow \beta + 1$
  - $S_3 : c \leftarrow c^2, \alpha \leftarrow 2 \cdot \alpha, \beta \leftarrow 2 \cdot \beta$
- Инициализировать два указателя:$(c, \alpha, \beta) = (1, 0, 0)$
- Обновлять указатели до тех пор, пока $c_{turtle} = c_{hare}$
- Решить линейное сравнение и проверить решение

Тестирование и результаты

Уравнение	Порядок r	x	Проверка
$10^x \equiv 64(mod 107)$	53	20	$10^{20} \equiv 64(mod 107)$
$5^x \equiv 20(mod 23)$	22	5	$5^5 \equiv 20(mod 23)$

Анализ и сравнение

Метод	Преимущества	Недостатки
ρ -метод Полларда (DLP)	- Временная сложность $O(\sqrt{r})$- Эффективен для групп среднего размера - Требует мало памяти	- Вероятностный алгоритм (может потребоваться перезапуск) - Требует знания порядка r элемента a

Заключение

- Мы успешно реализовали алгоритм ρ Полларда для решения задачи дискретного логарифмирования и протестировали его на нескольких примерах.
- Программа показала свою корректность и эффективность.
- Мы также изучили важность задачи дискретного логарифмирования в криптографии и возможности использования данного алгоритма для анализа криптографических систем.

Спасибо за внимание!