---

marp: true title: "Лабораторная работа №7" author: "Имя Фамилия" paginate: true theme: default

Лабораторная работа №7

Дискретное логарифмирование в конечном поле

Тема: Изучение задачи дискретного логарифмирования и ρ-метода Полларда
Автор: Имя Фамилия

Цель работы

Изучить теоретические основы задачи дискретного логарифмирования в конечном поле, понять применение ρ-метода Полларда и реализовать алгоритм для нахождения дискретного логарифма на практике.

Задание

1. Ознакомиться с теоретическими основами дискретного логарифмирования и конечных полей.
2. Рассмотреть ρ-метод Полларда как эффективный вероятностный алгоритм.
3. Программно реализовать алгоритм и применить его для заданных чисел p, a, b с целью нахождения x, такого что $a^x \equiv b \pmod{p}$.

Теоретическое введение (1/3)

Дискретный логарифм:
Дано a, b, p, где p — простое число, a — элемент мультипликативной группы $\mathbb{F}_p^*$. Задача дискретного логарифма — найти x, удовлетворяющее: $$ a^x \equiv b \pmod{p}. $$

Сложность дискретного логарифма гарантирует криптографическую устойчивость многих протоколов, таких как Диффи-Хеллман и DSA.

Теоретическое введение (2/3)

Конечные поля и группы:

- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ — конечное поле с p элементами.
- Мультипликативная группа $\mathbb{F}_p^* = \{1, 2, \ldots, p-1\}$ циклична.
- Если a является образующим элементом этой группы, тогда каждый $b \in \mathbb{F}_p^*$ можно представить как $b = a^x$ для некоторого x.

Теоретическое введение (3/3)

Сложность решения:

- Наивный перебор: экспоненциальная сложность.
- Более быстрые алгоритмы (группа методов «гигантский и крошечный шаг» Шенкса) имеют сложность порядка $O(\sqrt{p})$.
- ρ-метод Полларда также работает за $O(\sqrt{p})$ и часто проще в реализации, чем метод Шенкса, и требует меньше памяти.

ρ-метод Полларда

Идея метода:

1. Определить псевдослучайное отображение $f: \mathbb{F}_p^* \to \mathbb{F}_p^*$.
2. Генерировать последовательность значений, применяя f к некоторому начальному элементу.
3. Найти цикл в последовательности методом «черепаха-заяц» (Флойда).
4. Используя найденную коллизию, составить уравнение для логарифма и решить его по модулю порядка элемента.

Пример ветвящегося отображения

Часто используют разбиение множества на части, например: $$ f(c) = \begin{cases} a \cdot c \pmod{p}, & c < \frac{p}{2}, $$6pt] b \cdot c \pmod{p}, & c \geq \frac{p}{2}. \end{cases} $$

Сопоставляя каждому шагу приращения показателей u, v (чтобы отслеживать логарифм), при обнаружении коллизии получится уравнение для определения x.

Выполнение лабораторной работы (1/2)

Пример кода на Julia (фрагмент):

```
function funf(h, j, k)
    if h < r
        j += 1
        return mod(a * h, p), j, k
    else
        k += 1
        return mod(b * h, p), j, k
    end
end
```

Данная функция реализует ветвящееся отображение f и обновляет счетчики j, k.

Выполнение лабораторной работы (2/2)

После определения функции f выполняется:

1. Инициализация начальных параметров u, v и вычисление $c = a^u b^v \pmod{p}$.
2. Применение f к c (медленный шаг) и к d (быстрый шаг) до тех пор, пока не найдется коллизия $c = d$.
3. При нахождении коллизии, решение уравнения для логарифма: $$ u - U \equiv x(v - V)^{-1} \pmod{r}.$$

Таким образом, определяется искомый x.

Выводы

- На практике продемонстрирован ρ-метод Полларда для решения задачи дискретного логарифмирования.
- Данный метод имеет субэкспоненциальную сложность порядка $O(\sqrt{r})$, что делает его эффективным инструментом при достаточно больших, но не астрономических размерах модулей.
- Понимание и реализация подобных алгоритмов критически важны для оценки устойчивости криптосистем к атакам, что напрямую влияет на кибербезопасность.

Список литературы

Pollard, 1974. Karaarslan E. Primality Testing Techniques and The Importance of Prime Numbers in Security Protocols (англ.) // ICMCA'2000: Proceedings of the Third International Symposium Mathematical & Computational Applications — Konya: 2000. — P. 280—287. Василенко, 2003, с. 60. Ишмухаметов, 2011, с. 53—55. Cohen, 2000, pp. 439.

Montgomery, Silverman, 1990. Циммерман, Поль. Record Factors Found By Pollard's p-1 Method (англ.). Les pages des personnels du LORIA et du Centre Inria NGE. Дата обращения: 10 октября 2016. Архивировано 11 октября 2016 года. InriaForge: GMP-ECM (Elliptic Curve Method): Project Home. Дата обращения: 15 ноября 2012. Архивировано 21 июля 2012 года.

Спасибо за внимание!