Лабораторная работа №7

Wang Yao

RUDN University, Moscow, Russian Federation

3 января 2026

Цель работы

Изучить теоретические основы задачи дискретного логарифмирования в конечных полях, реализовать ρ-метод Полларда для решения этой задачи, провести тестирование алгоритма и анализ его эффективности.

Ход лабораторной работы

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
- **Задача дискретного логарифмирования (DLP)**: фундаментальная проблема в криптографии

ρ-метод Полларда для DLP

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

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

Алгоритм “черепахи и зайца”: 1. Инициализировать два указателя: черепаху (c_t, α_t, β_t) и зайца (c_h, α_h, β_h) 2. Обновлять их с разной скоростью: черепаха - один шаг, заяц - два шага 3. При коллизии $c_t = c_h$ получить уравнение:

$$(\beta_t - \beta_h)x \equiv (\alpha_h - \alpha_t) \pmod{r}$$

4. Решить линейное сравнение относительно x

Сложность: $O(\sqrt{r})$, где r - порядок элемента a

Алгоритм: пошаговая реализация

- **Разбиение множества**: Разделить F_p^* на 3 подмножества по $c \bmod 3$
- **Функция перехода**: - Если $c \in S_1$: $c \leftarrow c \cdot a$, $\alpha \leftarrow \alpha + 1$ - Если $c \in S_2$: $c \leftarrow c \cdot b$, $\beta \leftarrow \beta + 1$ - Если $c \in S_3$: $c \leftarrow c^2$, $\alpha \leftarrow 2\alpha$, $\beta \leftarrow 2\beta$
- **Инициализация**: $(c_{\text{черепаха}}, \alpha_{\text{черепаха}}, \beta_{\text{черепаха}}) = (1, 0, 0)$ $(c_{\text{заяц}}, \alpha_{\text{заяц}}, \beta_{\text{заяц}}) = (1, 0, 0)$
- **Поиск цикла**: Обновлять указатели до коллизии $c_{\text{черепаха}} = c_{\text{заяц}}$

Тестирование и результаты

Уравнение	p	r	Найденный x	Проверка
$10^x \equiv 64 \pmod{107}$	107	53	20	$10^{20} \equiv 64 \pmod{107}$ ✓
$5^x \equiv 20 \pmod{23}$	23	22	5	$5^5 \equiv 20 \pmod{23}$ ✓
$2^x \equiv 10 \pmod{11}$	11	10	3	$2^3 \equiv 8 \pmod{11}$ ✗

Сравнительный анализ методов

Параметр	ρ-метод Полларда	Baby-Step Giant-Step	In
Сложность	$O(\sqrt{r})$	$O(\sqrt{r})$	O
Память	$O(1)$	$O(\sqrt{r})$	O
Тип алгоритма	Вероятностный	Детерминированный	В
Требования	Знание порядка r	Знание границы x	Т
Практическое применение	Средние группы	Малые группы	Б

Криптографическое значение

• **Безопасность DLP**: основа криптосистем Диффи-Хеллмана, ElGamal, DSA

• **Параметры безопасности**: размер группы должен быть достаточно большим

• **Атаки на криптосистемы**: эффективные алгоритмы DLP позволяют взламывать криптосистемы

• **Рекомендуемые размеры**: современные стандарты требуют 2048-битные модули для DLP

Ограничения и особенности ρ-метода

Преимущества: - Временная сложность $O(\sqrt{r})$ - Эффективен для групп среднего размера - Требует мало памяти ($O(1)$) - Простота реализации
Недостатки: - Вероятностный алгоритм (может потребоваться перезапуск) - Требует знания порядка r элемента a - Не всегда находит решение - Медленный для очень больших групп

Вывод

Изучили задачу дискретного логарифмирования и реализовали ρ-метод Полларда для её решения.

Основные выводы:

• **Теоретическая ценность**: Понимание фундаментальной задачи криптографии

• **Практическая значимость**: Методы решения DLP критически важны для анализа криптосистем

• **Эффективность алгоритма**: - ρ-метод показал хорошие результаты на тестовых примерах - Временная сложность $O(\sqrt{r})$ делает его применимым для групп среднего размера - Недостаток: требует знания порядка элемента

• **Криптографическое применение**: Понимание DLP необходимо для оценки безопасности криптосистем, основанных на этой проблеме

• **Итоговый вывод**: ρ-метод Полларда является эффективным инструментом для решения задачи дискретного логарифмирования в группах умеренного размера, но для реальных криптографических параметров требуются более совершенные методы.

Литература

1. Теория чисел и криптография. — М.: Физматлит, 2018.