Лабораторная работа №6

Wang Yao

RUDN University, Moscow, Russian Federation

3 января 2026

Цель работы

Изучить теоретические основы алгоритмов разложения чисел на множители, реализовать ρ-метод Полларда и метод квадратов Ферма, провести сравнительный анализ их эффективности и точности.

Ход лабораторной работы

Основные понятия

- **Факторизация**: разложение составного числа на простые множители
- **Нетривиальный делитель**: делитель, отличный от 1 и самого числа
- **ρ-метод**: вероятностный алгоритм, использующий поиск циклов
- **Метод Ферма**: основан на представлении числа как разности квадратов
- **Сложность факторизации**: фундаментальная проблема криптографии

ρ-метод Полларда

Основа: поиск цикла в последовательности $x_{i+1} = f(x_i)$

Алгоритм: 1. Инициализировать $x = y = 2$, $d = 1$ 2. Пока $d = 1$: - $x = f(x) \mod n$ - $y = f(f(y)) \mod n$ - $d = \gcd(|x - y|, n)$ 3. Если $d = n$ → неудача Иначе → найден делитель d

Особенности: - Использует алгоритм “черепахи и зайца” - Эффективен для чисел с малыми делителями - Сложность: $O(\sqrt{p})$, где p - наименьший делитель

Метод квадратов Ферма

Основа: $n = s^2 - t^2 = (s - t)(s + t)$

Алгоритм: 1. Найти наименьшее $s > \sqrt{n}$ 2. Вычислить $t^2 = s^2 - n$ 3. Пока t^2 не является полным квадратом: - Увеличить s на 1 - Пересчитать $t^2 = s^2 - n$ 4. Найден делители: $(s - t)$ и $(s + t)$

Особенности: - Эффективен, когда делители близки к $\sqrt{n}$ - Прост в реализации - Медленный для чисел с сильно различающимися делителями

Пример работы: ρ-метод Полларда

Число n	Функция $f(x)$	Делитель	Второй делитель
1359331	$x^2 + 5$	1181	1151
10403	$x^2 + 5$	103	101

Пример работы: Метод квадратов Ферма

Число n	Найденный s	t	Делители
1359331	1166	15	1151 × 1181
10403	102	1	101 × 103

Сравнительный анализ методов

Параметр	ρ-метод Полларда	Метод квадрат
Сложность	$O(\sqrt{p})$	$O(\frac{\sqrt{n}-\sqrt{p}}{2})$
Эффективность	Лучше для малых делителей	Лучше для бли
Простота реализации	Средняя	Высокая
Вероятностный	Да	Нет
Память	$O(1)$	$O(1)$
Применимость	Числа с небольшими делителями	$p \approx q \approx \sqrt{n}$

Криптографическое значение

- **Безопасность RSA**: основана на сложности факторизации больших чисел
- **Ключевой параметр**: длина модуля RSA определяет стойкость системы
- **Атаки на RSA**: использование эффективных алгоритмов факторизации
- **Рекомендуемая длина**: современные стандарты требуют 2048-битных ключей

Ограничения методов

ρ-метод Полларда: - Может не сходиться для некоторых чисел - Требует выбора подходящей функции $f(x)$ - Эффективен только для небольших делителей

Метод квадратов Ферма: - Очень медленный, если p и q сильно различаются - Неприменим для современных криптографических чисел - Историческое значение больше, чем практическое

Вывод

Изучили и реализовали два алгоритма факторизации: ρ-метод Полларда и метод квадратов Ферма.

Основные выводы:

• **Теоретическая ценность**: Понимание фундаментальных алгоритмов теории чисел

• **Практическая значимость**: Эти методы являются основой для атак на криптосистемы

• **Сравнительный анализ**: - ρ-метод Полларда: эффективен для чисел с малыми делителями - Метод квадратов Ферма: хорош, когда делители близки друг к другу

• **Криптографическое применение**: Оба метода слишком медленны для факторизации современных RSA-модулей, но важны для понимания принципов

• **Итоговый вывод**: Выбор алгоритма факторизации зависит от структуры разлагаемого числа. Для реальных криптографических приложений используются более сложные методы (решето числового поля, эллиптические кривые).

Литература

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