Дискретная математика

Теория чисел и криптография

Константин Чухарев

Осень 2026

Безопасность и делимость

> *Математика — царица наук, а теория чисел — царица математики.*
>
> ***— Карл Фридрих Гаусс***

Керкгоффс

Безопасность не постулируется — она проверяется атакой.

Определение 1 (Принцип Керкгоффса)

Система должна оставаться безопасной, даже если известно всё, кроме ключа.

Секретность — в ключе, а не в алгоритме.

Спрятать алгоритм надолго невозможно.

Секретным может быть только ключ — то, что передают по защищённому каналу.

Взлом

Пример (Перебор)

Шифр Цезаря: ключ — сдвиг, всего 32 варианта.

Ломается за секунды: перебор всех ключей.

Пример (Частотный анализ)

Простая замена: частая буква шифротекста — частая буква языка.

Структура сообщения выдаёт его без перебора.

- Перебор (*brute force*) атакует длину ключа.
- Частотный анализ — структуру сообщения.

НОД и алгоритм Евклида

Определение 2 (НОД)

Наибольший общий делитель $\gcd(a, b)$ — наибольшее d, делящее и a, и b.

$\gcd(a, b) = 1$ — числа взаимно просты (*coprime*).

Теорема 1 (Алгоритм Евклида)

$\gcd(a, b) = \gcd(b, a \bmod b)$, $\gcd(a, 0) = a$.

Пример

$\gcd(48, 18) = \gcd(18, 12) = \gcd(12, 6) = \gcd(6, 0) = 6$.

Число шагов — $O(\log a)$.

Не нужна факторизация.

Коэффициенты Безу

Определение 3

Для $\gcd(a, m) = 1$ расширенный алгоритм Евклида находит x, y с

$$ax + my = 1.$$

Пример

Для $\gcd(7, 26) = 1$: $7 \cdot (-11) + 26 \cdot 3 = 1$, поэтому $7^{-1} \equiv -11 \equiv 15 \pmod{26}$.

Если $ax + my = 1$, то $ax \equiv 1 \pmod{m}$.

$x \bmod m$ — обратный элемент к a.

Первый кирпичик открытых ключей.

Модулярная арифметика

Сравнения

Определение 4

Сравнение (*congruence*):

$$a \equiv b (\mathrm{mod}\, m)$$

тогда и только тогда, когда m делит $a - b$.

Пример

$14 \equiv 2 (\mathrm{mod}\, 12)$ — циферблат.

Все числа, кратные 12, сравнимы с 0.

Сложение и умножение работают как обычно.

Один лишний шаг — взятие остатка.

Обратный элемент

Определение 5

Обратный к a по модулю m: $a \cdot a^{-1} \equiv 1 (\mathrm{mod}\, m)$.

a^{-1} существует тогда и только тогда, когда $\gcd(a, m) = 1$.

Взаимная простота решает, у кого есть обратный.

Пример

$7^{-1} \bmod 26$: $7 \cdot 15 = 105 \equiv 1 (\mathrm{mod}\, 26)$.

Значит, $7^{-1} \equiv 15$.

Малая теорема Ферма

Теорема 2 (Малая теорема Ферма)

Если p простое и a не делится на p:

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

Умножение на a переставляет ненулевые остатки.

Отсюда и перестановочное доказательство.

Пример

$3^6 \equiv 1 (\mathrm{mod}\, 7)$: $729 = 7 \cdot 104 + 1$.

Функция Эйлера

Определение 6

$\varphi(n)$ — число чисел от 1 до n, взаимно простых с n.

Пример

- $\varphi(p) = p - 1$ для простого p.
- $\varphi(pq) = (p-1)(q-1)$ для разных простых.

Теорема Эйлера

Теорема 3 (Теорема Эйлера)

Если $\gcd(a, n) = 1$: $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$.

Пример

$a = 3$, $n = 10$: $\varphi(10) = 4$, и $3^4 = 81 \equiv 1 (\mathrm{mod}\, 10)$.

Эйлер обобщил Ферма на составной модуль.

Ровно то, что нужно для RSA.

RSA

Генерация ключей

Определение 7 (Ключи RSA)

1. Выбрать различные простые p, q.
2. Модуль $n = pq$, функция $\varphi(n) = (p-1)(q-1)$.
3. Открытый показатель e, взаимно простой с $\varphi(n)$.
4. Закрытый $d = e^{-1} \bmod \varphi(n)$.

Открытый ключ: (n, e). Закрытый: (n, d).

Шифрование: $c = m^e \bmod n$. Дешифрование: $m = c^d \bmod n$.

p и q после генерации можно уничтожить.

В открытом ключе — только произведение n.

Китайская теорема об остатках

Доказательство RSA ниже опирается на один факт, который сформулируем заранее.

Теорема 4 (Китайская теорема об остатках)

Для взаимно простых p и q система

$$x \equiv a (\mathrm{mod}\, p), \quad x \equiv b (\mathrm{mod}\, q)$$

имеет единственное решение по модулю pq.

Набросок: числа $a, a + p, a + 2p, \ldots, a + (q - 1)p$ дают все остатки по модулю q, поэтому одно из них сравнимо с b.

Если решений два, их разность делится и на p, и на q, а значит, на pq.

Пример

Китайская теорема об остатках [2]

$x \equiv 1 (\mathrm{mod}\, 3)$, $x \equiv 3 (\mathrm{mod}\, 5)$. Перебираем $1, 4, 7, 10, 13$ — подходит 13, поэтому $x \equiv 13 (\mathrm{mod}\, 15)$.

Почему работает

Доказательство

d выбран так, что $ed = 1 + k\varphi(n)$.

Тогда $c^d = (m^e)^d = m^{ed} = m \cdot \left(m^{\varphi(n)}\right)^k$, поэтому $c^d \equiv m \cdot \left(m^{\varphi(n)}\right)^k (\mathrm{mod}\, n)$.

Если " gcd "$(m, n) = 1$, теорема Эйлера даёт $m^{\varphi(n)} \equiv 1 (\mathrm{mod}\, n)$, откуда $c^d \equiv m (\mathrm{mod}\, n)$. Если m делится на p, то по модулю p сравнение тривиально ($0 \equiv 0$), а по модулю q малая теорема Ферма даёт $m^{ed} = m \cdot \left(m^{q-1}\right)^{k(p-1)} \equiv m (\mathrm{mod}\, q)$. Китайская теорема об остатках склеивает оба сравнения в $c^d \equiv m (\mathrm{mod}\, n)$.

Стойкость RSA

Обратный шаг — восстановить d — требует знания $\varphi(n)$.

А оно эквивалентно разложению $n = pq$.

Квантовый алгоритм Шора факторизует n за полиномиальное время.

Отсюда — постквантовая криптография.

Подпись и податливость

Определение 8 (Подпись)

$s = m^d \bmod n$ — закрытым ключом.

Проверка: $s^e \equiv m (\bmod n)$ — открытым.

Подписать может только владелец d.

Пример (Податливость)

RSA мультипликативен: $c_1 c_2 \equiv (m_1 m_2)^e (\bmod n)$.

Злоумышленник, не зная ключа, умножает шифротекст на $r^e \bmod n$ и меняет сумму перевода m на $m \cdot r$.

Поэтому «голый» RSA не используют: нужен padding (OAEP).

Диффи–Хеллман

Дискретный логарифм

Определение 9

Возведение в степень по модулю — односторонняя функция.

Дискретный логарифм: по $h = g^x \bmod p$ найти x.

Прямой шаг быстр: метод квадратов.

Обратный — предположительно труден при больших p.

Пример

3 — образующий $\mathbb{Z}_7^*$: степени пробегают все ненулевые остатки.

Протокол

Определение 10 (Обмен ключами)

1. Алиса выбирает a и отправляет $A = g^a \bmod p$. Боб выбирает b и отправляет $B = g^b \bmod p$.
2. Алиса: $s = B^a$. Боб: $s = A^b$.
3. Общий секрет: $s = g^{ab} \bmod p$.

Ключ нигде не путешествует.

Перехватчик видит p, g, A, B — но не знает a или b.

Пример

$p = 23$, $g = 5$: $A = 5^6 \bmod 23 = 8$, $B = 5^{15} \bmod 23 = 19$.

Общий секрет: $19^6 \equiv 8^{15} \equiv 2 (\bmod 23)$.

Атака посередине

Дыра в Диффи–Хеллмане — не в математике, а в протоколе.

Алиса и Боб не знают, что разговаривают с тем, с кем думают.

Злоумышленник встаёт посередине: с Алисой он — Боб, с Бобом — Алиса.

Решение — аутентификация: подпись или сертификаты.

Математика честна, протокол требует проверки личности.

Что мы поняли?

- Безопасность держится на ключе. Перебор атакует длину ключа, а частотный анализ — структуру сообщения.
- Расширенный алгоритм Евклида находит обратный элемент: a обратим по модулю m ровно тогда, когда $\gcd(a, m) = 1$.
- Малая теорема Ферма и теорема Эйлера — двигатель RSA: $c^d \equiv m^{ed} \equiv m (\mathrm{mod}\, n)$.
- Диффи–Хеллман даёт общий секрет g^{ab} без передачи ключа. Стойкость — трудность дискретного логарифма, а протокол требует аутентификации против атаки посередине.

Вопросы для самопроверки

- Сформулируйте принцип Керкгоффса.
- Вычислите $\gcd(154, 98)$ алгоритмом Евклида.
- Почему a имеет обратный по модулю m тогда и только тогда, когда они взаимно просты?
- Сформулируйте малую теорему Ферма.
- Чему равно $\varphi(77)$?
- Опишите генерацию ключей RSA.
- Почему дешифрование RSA возвращает исходное сообщение?
- В чём податливость RSA и почему это атака?
- Как Алиса и Боб получают общий секрет по Диффи–Хеллману?