Эссе по курсу: Защита информации
на тему: Алгоритм быстрого возведения в степень
Московский физико-технический институт

17 декабря 2023 г.

Студент:	Михалун Д.О.
Преподаватель:	Семака В.Ю.
Группа:	Б01-003

Содержание

1 Введение

В современном мире, где большинство операций и передача данных осуществляются с использованием компьютерных технологий, безопасность информации становится одной из самых важных проблем. Основной математической операцией, применяемой в защите информации, особенно в криптографии, является возведение числа в степень.

Примеры использования возведения в степень в защите информации:

1. Шифрование: Возведение в степень используется при выполнении операций шифрования и дешифрования. Например, алгоритм RSA (Rivest-Shamir-Adleman) использует возведение в степень для шифрования сообщения с помощью публичного ключа и дешифрования с помощью соответствующего приватного ключа.

2. Хэширование: Возведение в степень может использоваться при создании хэш-функций, которые преобразуют данные переменной длины в фиксированный хэш-код. Например, алгоритм SHA-1 (Secure Hash Algorithm) использует возведение в 2-ю степень для создания хэш-кода.

3. Проверка подлинности: Возведение в степень может использоваться для проверки подлинности данных при помощи электронной подписи

В данном эссе речь пойдет об основных алгоритмах возведения в степень, а именно - возведения в степень по модулю, так как криптография оперирует с модульной арифметикой, описана сложность этих методов и показано, почему возведение числа в степень по простому модулю является важной частью шифрования.

2 Метод повторяющихся возведения в квадрат и умножения

Пусть требуется вычислить: y $= a^x \mod p$

Введем переменную $t = [log2(x)]$

Вычисляем числа ряда

a, $a^2, a^4, \ldots a^{2t}$ mod p (1.1) Каждое число вычисляется путем умножения предыдущего числа на самого себя по модулю p

Переведем x в двоичную систему: (x$_t$, x_{t-1}, $\ldots$, $x_0)_2$ Тогда число y $= a^x modp$ может быть получено так: $y = \prod_{i=0,...,t}$a$^{(x_i * 2^i)}$(1.2)

Приведем наглядный пример использования этого алгоритма.

Допустим мы хотим вычислить 5^{100} по модулю 7

1. Вычислим (a, $a^2, a^4, \ldots a^64$): a $=$ 5 $a^2 =$ 5*5 $=$ 25 $=$ 4 (mod 7) $a^4 =$ 4*4 $=$ 16 $=$ 2 (mod 7) $a^8 =$ 2*2 $=$ 4 (mod 7) Аналогично вычислим a^{16} , a^{32}, a^{64} получим упорядоченный набор (5, 4, 2, 4, 2, 4, 2)

2. Запишем показатель степени в двоичной системе исчисления: 100 $=$ 1100100_2

3. Воспользуемся формулой (1.2): 2*4*1*1*2*1*1 $=$ 8 $=$ 1 (mod 7)

Алгоритмы реализуются двумя способами: слева-направо и справа-налево, в зависимости от того, в каком порядке просматриваются биты показателя степени (от младшего к старшему или от старшего к младшему)

Лемма 2.1. (о сложности вычислений). Количество операций умножения n при вычислении $y = a^x$ mod p не превосходит $\log x$

Доказательство:

Вычисление ряда (1.1) требует t умножений, ряда (1.2) - не более, чем t.

$n <= t = [log2x] <= log2x$

Область применения:

Данный метод применяется в случае, когда степень x - простое число или раскладывается на произведение двух простых чисел.

В противном случае применяется метод с использованием Китайской теоремы об остатках, который будет рассмотрен далее.

3 Метод с использованием Китайской теоремы об остатках

Для описания данного метода потребуется теорема:

Теорема 3.1. Китайская теорема об остатках

Пусть натуральные числа $m_1, m_2, \ldots, m_n$ попарно взаимно просты.
Тогда для любых $a_1, \ldots, a_n$ э Z :0 <= $a_i < m_i$, существует N э N :N = $r_i(moda_i)$; и существует N_1, N_2 э N :N_1 тождественно равно N_2 (mod $a_1 * a_2 ... * a_n$)

Описание метода:

Пусть нам требуется вычислить $y = a^x$ mod p.

Пусть p разбивается на n простых множителей $p_1, \ldots, p_n$.

Сначала вычисляются вычеты a^x mod pi при помощи теоремы Ферма.

В результате получаем систему сравнений: $a^x = r_1 modp_1, 0 <= r_1 < p_1 a^x = r_2 modp_2, 0 <= r_2 < p_2 \ldots\ldots a^x = r_n modp_n, 0 <= r_n < p_n$

Положим $a^x = t$.

Решая по Китайской теореме об остатках эту систему сравнений относительно t, находим значение R э Z/n.

Поскольку a^x - тоже решение этой системы, и все решения сравнимы между собой, то a^x = R.

Область применения:

В криптографии в большинстве случаев возведение в степень осуществляется по простому модулю, поэтому данный метод применяется редко.

4 Одностороняя функция

Обратная функция к возведению в степень по модулю - дискретное логарифмирование. Данная операция вычисляется гораздо дольше, чем возведение в степень. Наиболее лучшие алгоритмы вычисления данной функции:

Алгоритмы с экспоненциальной сложностью

1. Алгоритм Шенкса (алгоритм больших и малых шагов, baby-step giant-step)
2. Алгоритм Полига — Хеллмана
3. -Метод Полларда

Данные алгоритмы имеют экспоненциальную сложность - O($p^{1/2}$), где p - модуль, по которому вычисляется степень.
Именно высокая вычислительная сложность этих алгоритмов определяет стойкость криптографических схем. Функции, подобные функции возведения в степень по модулю, имеют собственное определение - односторонние функции

Односторонняя функция в криптографии - это функция, которая легко вычисляется в обратном направлении, но трудно создать прообраз, значение которого соответствует заданному значению функции.
Односторонние функции используются в криптографии, например, в структуре Меркла-Дамгора и в криптографических хеш-функциях. Они часто строятся на основе блочных шифров и могут быть использованы для хранения паролей или создания электронной подписи. Также существуют односторонние функции с потайным входом, которые используются в асимметричных методах шифрования, таких как RSA и NTRUEncrypt. Односторонние функции с потайным входом позволяют найти прообраз для любого значения функции, что делает их полезными в криптографии.

Покажем, что при больших p функция возведения в степень по модулю p действительно односторонняя.

Выше мы оценили время вычисления прямой функции как не большее чем $log2p$

Допустим для вычисления обратной функции мы будем использовать метод "шаг младенца шаг великана"(baby-step giant-step) (t $\sim 2\sqrt{p}$)

Количество десятичных знаков в записи p	Вычисление (2.3) ($2 \log p$ умножений)	Вычисление (2.4) ($2 \cdot \sqrt{p}$ умножений)
12	$2 \cdot 40 = 80$	$2 \cdot 10^6$
60	$2 \cdot 200 = 400$	$2 \cdot 10^{30}$
90	$2 \cdot 300 = 600$	$2 \cdot 10^{45}$

Рис. 1: *Таблица: количество умножений для вычисления прямой и обратной функции*

Можно сделать вывод, что с увеличением числа знаков в десятичной записи p сложность возведения в степень по этому модулю растет линенейно, в то время как сложность вычисления обратной функции растет экспоненциально.

Проиллюстрируем это свойство на примере первой системы с открытым ключом – системы Диффи - Хелмана:

Алиса и Боб выбирают общие параметры: основание g (допустим, 5) и большое простое число p (допустим, 23).

Алиса генерирует свой секретный ключ a (допустим, 6) и вычисляет свой публичный ключ A:
$A = g^a mod p = 5^6 mod 23 = 15625 mod 23 = 8$.

Боб генерирует свой секретный ключ b (допустим, 9) и вычисляет свой публичный ключ B:
$B = g^b mod p = 5^9 mod 23 = 1953125 mod 23 = 11$.
Алиса и Боб обмениваются публичными ключами: Алиса отправляет свой ключ A (8) Бобу, а Боб отправляет свой ключ B (11) Алисе.
Алиса вычисляет общий секретный ключ s:
$s = B^a mod p = 11^6 mod 23 = 1771561 mod 23 = 9$.
Боб вычисляет общий секретный ключ s:
$s = A^b mod p = 8^9 mod 23 = 134217728 mod 23 = 9$.

Теперь Алиса и Боб имеют общий секретный ключ s, который равен 9.
Этот ключ может быть использован для дальнейшего зашифрования и расшифрования сообщений между ними.

При этом для тех, кто не знает числа a и b, вычисление s заняло бы продолжительное время по доказанному выше.

5 Заключение

В статье были рассмотрены различные методы возведения в степень по модулю, которые широко используются в современной математике и криптографии. Описано, как эти методы могут быть применены для решения различных задач, включая вычисление корней и факторизацию чисел. Особое внимание уделено методам, основанным на использовании логарифмов и элементарных операций. Эти методы являются наиболее эффективными и могут быть использованы для работы с большими числами и вычислениями высокой точности.

В заключении можно отметить, что методы возведения в степень по модулю являются важным инструментом в современной математике и криптографии и позволяют решать множество важных задач Вот некоторые из них:

1. Вычисление корней и факторизация чисел: Методы возведения в степень по модулю могут использоваться для вычисления корней квадратных уравнений и факторизации больших чисел. Это особенно полезно в криптографии, где необходимо работать с большими числами и обеспечивать безопасность данных.

2. Решимость уравнений: Методы возведения в степень по модулю могут быть использованы для решения различных уравнений, включая уравнения с комплексными числами. Это позволяет решать сложные задачи в алгебре и геометрии.

3. Генерация псевдослучайных чисел: Методы возведения в степень по модулю могут быть использованы для генерации псевдослучайных чисел. Это особенно полезно в криптографии, где требуется создавать безопасные ключи и пароли.

4. Работа с большими числами: Методы возведения в степень по модулю позволяют работать с большими числами высокой точности. Это особенно важно в научных и инженерных расчетах, где требуется высокая точность при работе с большими числами.

5. Шифрование данных: Методы возведения в степень по модулю широко используются в криптографии для шифрования данных. Они позволяют создавать безопасные шифры, которые защищают данные от несанкционированного доступа.

Вот некоторые из методов шифрования которые используют быстрое возведение в степень по модулю :

1. Шифрование: В алгоритмах шифрования, таких как RSA, используется быстрое возведение в степень для вычисления больших составных чисел, которые являются основой для шифрования и дешифрования сообщений. Метод Ньютона используется для эффективного вычисления этих чисел, что позволяет сохранить криптографическую стойкость алгоритма.

2. Подпись сообщений: В алгоритмах цифровой подписи, таких как DSA, используется быстрое возведение в степень для вычисления значений, связанных с ключами подписи. Это позволяет эффективно создавать и проверять цифровые подписи сообщений.

3. Хеширование: В некоторых алгоритмах хеширования, таких как MD5 и SHA, используется быстрое возведение в степень для вычисления определенных значений. Например, в алгоритме MD5, используется быстрое возведение в степень для вычисления значений, связанных с хеш-функцией.

4. Публичные системы ключей: В алгоритмах публичных систем ключей, таких как алгоритмы Эллиптической кривой, используется быстрое возведение в степень для вычисления значений, связанных с ключами. Например, в алгоритме Эллиптической кривой, используется быстрое возведение в степень для вычисления значений, связанных с эллиптической кривой.

5. Симметричное шифрование: В некоторых симметричных алгоритмах шифрования, таких как алгоритм AES, используется быстрое возведение в степень для выполнения определенных операций. Например, в алгоритме AES, используется быстрое возведение в степень для выполнения определенных операций с использованием расширений поля.

В каждом из этих случаев, метод быстрого возведения в степень позволяет эффективно выполнять операции с большими числами, что повышает скорость и криптографическую стойкость соответствующих алгоритмов.

Это лишь некоторые примеры задач, которые можно решать с помощью методов возведения в степень по модулю. Их важность и разнообразие применения делают эти методы ключевыми инструментами в современной математике и криптографии.

При этом, развитие и совершенствование этих методов продолжается, что открывает новые возможности для их применения в будущем.

6 Список использованной литературы

1. Рябко Б. Я., Фионов А. Н. Основы современной криптографии для специалистов в информационных технологиях — Научный мир, 2004. — С. 15. — 173 с. — ISBN 978-5-89176-233-6

2. Молдовян Н. А. Теоретический минимум и алгоритмы цифровой подписи. — СПб.: БВХ-Петербург: Книжный Дом «ЛИБРОКОМ», 2010. — 304 с. — ISBN 978-5-9775-0585-7.