J. J. Siang

BILANGAN PRIMA : PERKEMBANGAN DAN APLIKASINYA

Intisari

Dalam tulisan ini dipaparkan mengenai sejarah penemuan bilangan prima, pengujian bilangan prima besar, serta salah satu aplikasinya dalam kriptografi yaitu metode RSA

Abstract

This paper explain about the history and developments of prime numbers, primality testing and its application in cryptography, RSA method

Diterima : 6 Maret 2002
Disetujui untuk dipublikasikan : 8 Maret 2002

1. Sejarah dan Perkembangan Bilangan Prima

Bilangan prima adalah bilangan bulat >1 yang hanya habis dibagi 1 dan bilangan itu sendiri. Manusia telah mengenal bilangan prima sejak 6500 SM. Tulang Ishango yang ditemukan pada tahun 1960 (sekarang disimpan di Musee d'Histoire Naturelle di Brussels) membuktikan hal tersebut. Tulang Ishango memiliki 3 baris takik. Salah satu kolomnya memiliki 11, 13, 17, dan 19 takik, yang merupakan bilangan-bilangan prima antara 10 hingga 20.

Meskipun sedikit sekali manfaat yang diketahui, namun di awal masehi orang tetap mencari dan membuktikan bahwa suatu bilangan merupakan bilangan prima. Cara yang paling efisien untuk mencari bilangan prima kecil (misalkan kurang dari 10^7) adalah dengan menggunakan metode Seive of Eratosthenes (240 SM) sebagai berikut : Daftarkanlah semua bilangan bulat antara 2 hingga n. Hapuslah semua bilangan kelipatan bilangan prima yang lebih kecil atau sama dengan $\sqrt{n}$. Maka bilangan yang masih tersisa adalah bilangan prima.

Sebagai contoh, untuk mencari semua bilangan prima $\leq$ 30, pertama-tama didaftarkan semua bilangan bulat antara 2 hingga 30.

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16
17 18 19 20 21 22 23 24 25 26 27 28 29 30

Bilangan pertama (= 2) adalah bilangan prima. Hapuskan semua bilangan kelipatan 2. Didapat

2 3 5 7 9 11 13 15 17 19 21 23 25 27 29

Bilangan prima setelah 2 dalam daftar tersebut adalah 3, yang merupakan bilangan prima kedua. Hapus semua bilangan kelipatan 3 dari daftar. Didapat

2 3 5 7 11 13 17 19 23 25 29

Bilangan setelah 3 yang belum terhapus adalah 5. Hapus semua bilangan dalah daftar yang merupakan kelipatan 5 sehingga didapat

2 3 5 7 11 13 17 19 23 29

Bilangan yang tidak terhapus berikutnya adalah 7 yang kuadratnya = 49 > 30. Maka bilangan yang tersisa dalam daftar merupakan himpunan semua bilangan prima ≤ 30.

Pencarian bilangan prima dengan metode Sieve sangatlah mudah, cepat dan sederhana. Bahkan prosesnya tidak menggunakan operasi pembagian sama sekali. Pencarian secara langsung dengan menjalankan program di komputer bahkan lebih cepat dibandingkan dengan membaca daftar bilangan prima yang tersimpan dalam disket. Akan tetapi untuk keperluan enkripsi yang membutuhkan bilangan prima yang besar, metode Sieve dirasa tidak memadai.

Sebelum komputer ditemukan, perkembangan penemuan bilangan prima masih lambat karena orang belum merasakan manfaatnya. Tabel 1 menunjukkan daftar penemu tabel bilangan prima sebelum era komputer. Meskipun sederhana, tabel tersebut menolong ahli matematika lain untuk pertama kali menebak teorema bilangan prima.

Tahun	Penemu	Jumlah Digit
1588	Cataldi	6
1772	Euler	10
1883	Pervushin	19
1911	Powers	27
1914	Powers	33

Tabel 1 : Penemu Tabel Bilangan Prima Sebelum Era Komputer

Semua bilangan prima > 2 jelas merupakan bilangan gasal sehingga pada jaman dahulu orang percaya bahwa untuk suatu bilangan prima p, maka 2^p-1 juga merupakan bilangan prima. Namun kemudian terbukti hal tersebut tidak benar. Pada tahun 1536, Regius membuktikan bahwa $2^{11}-1 = 2047$ bukanlah bilangan prima karena $2047 = 23 * 89$

2. Pengujian Bilangan Prima

Mersenne (1588 – 1648) menemukan bahwa bilangan 2^p-1 merupakan bilangan prima hanya untuk p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, dan 257. Meskipun ternyata kemudian terbukti bahwa apa yang ditemukan Mersenne ini salah, tapi bentuk 2^p-1 (yang kemudian dikenal dengan bilangan Mersenne) tetap menarik perhatian

Pertanyaan yang terus ingin dijawab adalah : Pada kondisi apakah bilangan Mersenne $Mp = 2^p-1$ merupakan bilangan prima ? Lucas menemukan syarat perlu dan cukupnya pada tahun 1870 dan Lehmer mengujinya pada tahun 1930.

Uji Lucas – Lehmer : Untuk bilangan gasal p, bilangan Mersenne 2^p-1 adalah bilangan prima bila dan hanya bila $2^p - 1 \mid S(p-1)$ dengan $S(n+1) = (S(n))^2 - 2$ dan $S(1) = 4$.

Dengan bantuan komputer, pengujian bilangan prima yang besar dengan uji Lucas-Lehmer menjadi semakin mudah sehingga bilangan-bilangan prima besar ditemukan, seperti yang tampak pada tabel 2.

Tahun	Penemu	p	Jumlah Digit dalam Mp
1952	Robinson	521	157
1952	Robinson	607	183
1952	Robinson	1279	386
1952	Robinson	2203	664
1952	Robinson	2281	687
1957	Riesel	3217	969
1961	Hurwitz	4253	1281
1961	Hurwitz	4423	1332
1963	Gillies	9689	2917
1963	Gillies	9941	2993
1963	Gillies	11213	3376
1971	Tuckerman	19937	6002
1978	Noll & Nickel	21701	6533
1979	Noll	23209	6987
1979	Nelson & Slowinski	44497	13395
1982	Slowinski	86243	25962
1988	Colquitt & Welsh	110503	33265
1983	Slowinski	132049	39751
1985	Slowinski	216091	65050
1992	Slowinski & Gage	756839	227832
1994	Slowinski & Gage	859433	258716
1996	Slowinski & Gage	1257787	378632
1996	Armengaud, Woltman, et al	1398269	420921
1997	Spence, Woltman, et al	2976221	895932
1998	Clarkson, Woltman, Kurowski, et al	3021377	909526
1999	Hajratwala, Woltman, Kurowski, et al	6972593	2098960

Tabel 2 : Penemu Tabel Bilangan Prima Mersenne

3. Bilangan Prima Semu

Sulitnya menemukan bilangan prima besar menjadi masalah utama bagi praktisi kriptografi karena penggunaan bilangan prima merupakan syarat mutlak dalam implementasinya. Padahal secara praktis, kadang-kadang hanya dibutuhkan bilangan yang "mendekati" prima. Bilangan semacam itu disebut bilangan prima semu (pseudo prime).

Bilangan prima semu bisa didapatkan dari teorema Little Fermat sebagai berikut :
Jika p adalah bilangan prima dan a adalah sembarang bilangan bulat, maka $a^p = a \pmod p$. Secara khusus, jika a bukan faktor p, maka $a^{p-1} = 1 \pmod p$.

Teorema Little Fermat memberikan uji yang baik untuk ketidakprimaan. Dengan diberikan bilangan bulat $n > 1$, pilihlah $a > 1$ dan hitung $a^{n-1} \pmod n$. Jika hasilnya $\neq 1$, maka n bukan bilangan prima. Sebaliknya, jika hasilnya = 1, maka n mungkin bilangan prima sehingga n disebut bilangan prima semu basis a.
Sebagai contoh, untuk $a = 2$ dan $n = 341$, maka $2^{341-1} \pmod{341} = (2^{10})^{34} \pmod{341} = (2^{10} \bmod 341)^{34} = 1^{34} \bmod 341 = 1$.

Akan tetapi 341 bukan bilangan prima karena 341 = 11*31, sehingga 341 adalah bilangan prima semu basis 2.

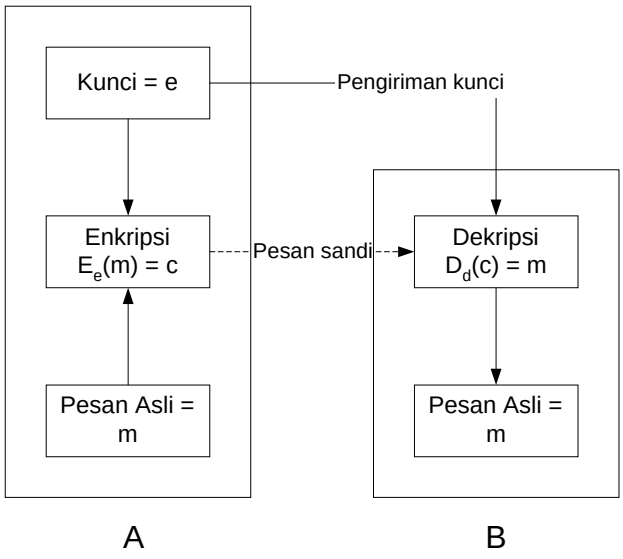
Terdapat lebih dari 10^9 buah bilangan prima yang lebih kecil dari $25*10^9$, tapi hanya ada 21.853 buah bilangan prima semu basis 2. Ini berarti bahwa persentase menjadi bilangan prima semu jauh lebih kecil dari bilangan prima.

4. Kriptografi

4.1 Kriptografi Simetris vs Kriptografi Kunci Publik

Kriptografi adalah teknik untuk menyamarkan suatu pesan. Kriptografi meliputi enkripsi, yaitu transformasi data ke bentuk yang tidak mungkin dibaca pihak lain tanpa mengetahui kuncinya, serta dekripsi, yang merupakan kebalikan dari enkripsi, yaitu mengembalikan data yang ditrans-formasi ke bentuk semula. Baik enkripsi maupun dekripsi selalu membutuhkan suatu informasi rahasia yang disebut kunci.

Berdasarkan sifat kuncinya, terdapat 2 jenis kriptografi yaitu kriptografi simetris (kunci rahasia) dan kriptografi dengan kunci publik. Dalam kriptografi simetris, kunci yang sama dipakai dalam enkripsi dan dekripsi sehingga baik pengirim maupun penerima informasi harus memiliki kunci yang sama untuk mengolahnya. Keadaan ini dapat digambarkan dalam gambar 1.

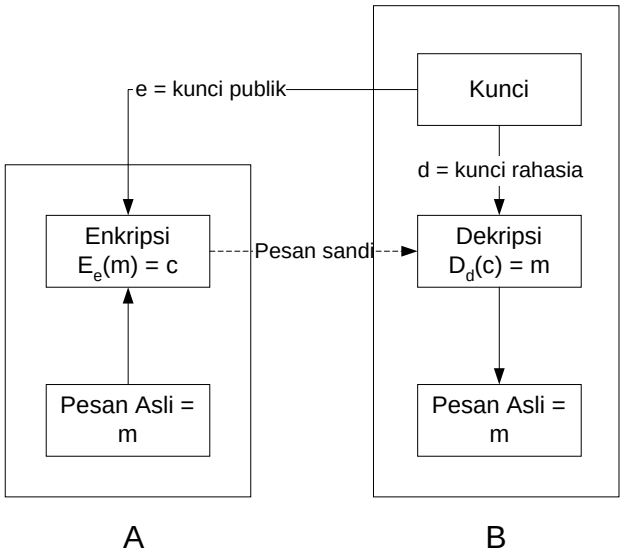


Gambar 1 : Skema Enkripsi pada Kriptografi Simetris

Misalkan A hendak mengirim pesan m pada B. Pesan m dienkrip dengan menggunakan kunci e menjadi c. Selanjutnya pesan sandi c dikirimkan pada B. Ada kemungkinan pihak ketiga bisa memperoleh pesan sandi c. Tetapi ia tidak bisa membacanya karena tidak mengetahui kunci pembukanya. B yang menerima pesan sandi c dapat membukanya dengan kunci pembuka d (yang bisa diturunkan dari e). Dalam hal ini, baik A maupun B harus sama-sama memiliki kunci e (dan d), dan kunci ini tidak boleh diketahui pihak ketiga. Kelemahan metode ini adalah jika A dan B tinggal di tempat yang berjauhan sehingga kunci e harus dikomunikasikan lewat media (telpon, surat, internet, dls) yang kemungkinan tidak aman.

Sebaliknya, dalam kriptografi dengan kunci publik, penerima memiliki 2 buah

kunci yaitu kunci publik dan kunci rahasia. Kunci publik bisa diketahui oleh banyak orang, tetapi kunci rahasia hanya diketahui oleh penerima saja. Bahkan pengirimpun tidak mengetahui kunci rahasia sehingga tidak bisa mendekrip kembali pesan yang telah dienkripnya. Keadaan ini dapat digambarkan dalam gambar 2. Misalkan A mengirim pesan pada B, maka A mengenkrip pesan asli dengan kunci publik (= e) dan mengirimkannya pada B. Selanjutnya B mendekrip pesan yang diterimanya dengan kunci rahasia (= d) yang hanya diketahuinya sendiri.



Gambar 2 : Skema Enkripsi pada Kriptografi dengan Kunci Publik

Keuntungan utama metode ini adalah tidak diperlukannya media komunikasi antara A dan B untuk menentukan kunci rahasia sehingga keamanannya dapat lebih terjamin. Jika B hendak membalas pesan m' pada A, maka ia akan mengenkripnya dengan menggunakan kunci publik e' yang ditentukan A. A akan mendekripnya dengan kunci rahasia d'. Kunci rahasia d tidak sama dengan d'.

Sebenarnya kunci rahasia d bisa dihitung dari kunci publik e. Tapi tanpa informasi tambahan yang hanya diketahui oleh B, perhitungan tersebut membutuhkan waktu yang sangat lama sehingga secara praktis tidak dapat dilakukan.

4.2 Enkripsi Dengan Metode RSA

Kriptografi kunci publik yang paling terkenal adalah metode RSA (Rivest, Shamir dan Adleman). Kuncinya dibentuk dari sepasang bilangan prima (dalam prakteknya sering dipakai bilangan prima semu yang besar). Algoritmanya adalah sebagai berikut :

1. Tentukan sembarang 2 bilangan prima p dan q, dan hitung n = pq.
2. Pilih sembarang bilangan bulat positif e yang relatif prima dengan (p-1)(q-1). Ini berarti bahwa e harus dipilih sehingga GCD (e, (p-1)(q-1)) = 1. Pasangan (n, e) merupakan kunci publik

Untuk mengenkripsi, dilakukan langkah-langkah sebagai berikut :

1. Ubah tiap karakter teks asli menjadi bilangan bulat 01-26 (A = 01, B =

02, … , Z = 26), dan bagi teks menjadi beberapa blok b yang besar tiap bloknya lebih kecil dari n.
2. Untuk tiap blok, hitung $c = b^e \pmod n$. c menjadi blok teks sandi yang dikirimkan.

Untuk mendekripkan kembali teks sandi, dilakukan langkah-langkah sebagai berikut :
1. Hitung bilangan bulat d sedemikian hingga $d.e = 1 \pmod{(p-1)(q-1)}$. Pasangan (n, d) merupakan kunci rahasia.
2. Untuk setiap blok sandi c yang diterima, hitung $b = c^d \pmod n$.

Bagi pembuat sandi, dengan memilih 2 buah bilangan prima p dan q, tidaklah sulit untuk menghitung kunci publik n = pq, serta mendekripkannya kembali. Kevalidan dekripsi dengan metode RSA dapat dibuktikan [4]. Akan tetapi bagi orang lain yang mencoba mendekripsinya, ia harus mencari p dan q dari kunci publik n. Jika berhasil, maka kunci rahasia d dapat dihitung. Akan tetapi sangatlah sulit untuk memperoleh p dan q dari n yang sangat besar (umumnya dibuat 100 digit atau lebih). Rivest, Shamir dan Adleman telah mencoba mengenkripsi pesan dengan menggunakan bilangan bulat 129 digit pada tahun 1977. Pesan tersebut baru berhasil dipecahkan orang 17 tahun kemudian [2]. Ini berarti bahwa secara praktis hanya pemilik kunci rahasia saja yang mampu membukanya.

Sebagai contoh, andaikan B memilih p = 13 dan q = 17. Maka n = pq = 221.
Berikutnya, misalkan secara acak B memilih e = 5 yang merupakan bilangan yang relatif prima dengan (p-1)(q-1) = 192. Maka kunci publiknya adalah (n, e) = (221, 5).
Jika A hendak mengirim teks "TAMAN", maka ia harus mengubahnya menjadi barisan angka-angka sebagai (A = 01, B = 02 , …) : 20 01 13 01 14.
Misalkan A mengambil blok dengan panjang 3 digit, maka ia memiliki 4 blok untuk disandikan, masing-masing adalah 200, 113, 011, 4

200 disandikan menjadi $(200)^5 \pmod{221} = 200$
113 disandikan menjadi $(113)^5 \pmod{221} = 146$
011 disandikan menjadi $(11)^5 \pmod{221} = 163$
4 disandikan menjadi $(4)^5 \pmod{221} = 140$

Maka A mengirimkan 4 blok pesan rahasia 200 146 163 140

B yang menerima pesan sandi dari A harus mencari kunci rahasia yang didapat dari relasi e.d = 5d = 1 (mod 192). Didapat d = 77. Maka :

blok sandi 200 didekrip menjadi $(200)^{77} \pmod{221} = 200$
blok sandi 146 didekrip menjadi $(146)^{77} \pmod{221} = 113$
blok sandi 163 didekrip menjadi $(163)^{77} \pmod{221} = 11 = 011$ (karena 3 digit)
blok sandi 140 didekrip menjadi $(140)^{77} \pmod{221} = 4$

didapat pesan asli 200 113 011 4 yang jika dikelompokkan dalam 2 digit menjadi 20 01 13 01 14 atau teks "TAMAN" seperti pesan semula.

5. Penutup

Semakin pesat perkembangan komputer, semakin terasalah pentingnya peranan bilangan prima. Bilangan prima yang dulunya dianggap sebagai sesuatu yang tidak memiliki manfaat, kini menjadi

bagian yang tak terpisahkan dalam keamanan data. Kriptografi dewasa ini lebih dari sekedar enkripsi dan dekripsi. Tanda tangan digital (digital signature) mulai banyak dipakai untuk mencegah pemalsuan dokumen elektronik. Semuanya itu membutuhkan bilangan prima.

Pustaka

[1] Caldwell, C.K., *The Largest Known Prime by Year : A Brief History*, http://www.utm.edu/research/primes/ notes/by_year.html, 2001

[2] Caldwell, C.K., http://www.utm.edu/research/primes/glossary/index.htm, 2001

[3] Caldwell, C.K., *Mersenne Primes : History, Theorems and Lists*, http://www.utm.edu/research/primes/ mersenne.shtml, 2001

[4] Menezes, A., P.van Oorschot, Vanstone, S., *A Handbook of Applied Cryptography*, CRC Press, 1997

[5] RSA Laboratories, *RSA Laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1*, RSA Security Inc, 2000

Penulis

J.J. Siang adalah dosen Jurusan Matematika, Fakultas MIPA, Universitas Kristen Immanuel, Yogyakarta