Aplikasi Teori Bilangan dalam Algoritma Kriptografi

Veren Iliana Kurniadi 13515078
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13515078@std.stei.itb.ac.id

***Abstrak*—Teori bilangan memiliki banyak aplikasi dalam kehidupan, salah satunya yaitu dalam bidang kriptografi. Teori bilangan yang banyak digunakan dalam kriptografi adalah aritmatika modulo. Makalah ini berisi pembahasan mengenai keterkaitan teori bilangan dan kriptografi, contoh algoritma kriptografi, kelebihan dan kekurangan algoritma tersebut, serta bagaimana cara memilih algoritma yang tepat untuk menyelesaikan persoalan.**

***Kata kunci*—kriptografi, algoritma, simetri, asimetri**

I. PENDAHULUAN

Dewasa ini, teknologi informasi berkembang dengan pesat. Penyampaian informasi atau pesan semakin mudah dilakukan. Saat ini , media yang paling banyak digunakan untuk menyampaikan informasi adalah internet. Internet menghubungkan jutaan orang sebagai media pertukaran dan penyimpanan informasi. Dengan segala kemudahan tersebut, keamanan informasi semakin rentan.

Kemanan informasi menjadi hal yang krusial pada era digital seperti sekarang ini. Kemudahan penyampaian informasi dan penyimpanan data di internet dapat dimanfaatkan oleh orang-orang tidak bertanggung jawab yang ingin menyalahgunakan informasi tersebut. Oleh karena itu, kemanan informasi harus ditingkatkan, salah satunya dengan cara mengenkripsi pesan yang dikirim. Ilmu untuk menjaga kerahasiaan informasi ini disebut kriptografi.

Selain untuk mengenkripsi pesan, sangat banyak aplikasi kriptografi dalam kehidupan sehari-hari, seperti *e-commerce* , *digital signatures*, penggunaan ATM, dan password komputer. Hal-hal tersebut sangat dekat dengan kehidupan kita di tengah kemajuan teknologi saat ini. Algoritma asimetri merupakan salah satu jenis algoritma dalam kriptografi yang dapat diaplikasikan untuk hal-hal tersebut. Dalam tulisan ini, akan dijelaskan mengenai algoritma asimetri dalam kriptografi, hubungannya dengan aritmatika modulo, dan aplikasinya dalam kehidupan sehari-hari.

II. TEORI BILANGAN

A. Pembagian Bilangan Bulat

Misalkan a dan b adalah dua buah bilangan bulat dengan syarat $a \neq 0$. Kita menyatakan bahwa a habis membagi b jika terdapat bilangan bulat c sedemikian sehingga b = ac. Notasi: a | b jika b = ac, c elemen Z dan $a \neq 0$. (Z = himpunan bilangan bulat).

Misalkan m dan n adalah dua buah bilangan bulat dengan syarat n > 0. Jika m dibagi dengan n maka terdapat dua buah bilangan bulat unik q (quotient) dan (remainder), sedemikian sehingga

$$m = nq + r$$

dengan $0 \leq r < n$.

Dua buah bilangan bulat dapat memiliki factor pembagi yang sama. Faktor pembagi bersama yang terpenting adalah faktor pembagi bersama terbesar. Misalkan a dan b adalah dua buah bilangan bulat tidak nol. Pembagi bersama terbesar (PBB – greatest common divisor atau gcd) dari a dan b adalah bilangan bulat terbesar d sedemikian sehingga d | a dan d | b. Dalam hal ini kita nyatakan bahwa PBB(a, b) = d.

B. Aritmatika Modulo

Arimatika modulo merupakan salah satu cabang ilmu matematika yang memegang peranan penting dalam komputasi, khususnya pada aplikasi kriptografi. Operator yang digunakan dalam aritmatika modulo adalah mod.

Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0. Operasi a mod m (dibaca “a modulo m”) memberikan sisa jika a dibagi dengan m.

Notasi: a mod m = r sedemikian sehingga

$$a = mq + r,$$

dengan $0 \leq r < m$. Bilangan m disebut modulus atau modulo, dan hasil aritmetika modulo m terletak di dalam himpunan {0, 1, 2, …, m – 1}

Kadang, dua buah bilangan bulat a dan b mempunyai sisa yang sama jika dibagi dengan bilangan positif m. Kita katakan bahwa a dan b kongruen dalam modulo m, dan dilambangkan sebagai :

$$a \equiv b \pmod{m}$$

(Notasi ‘≡’ dibaca ‘kongruen’.) Definisi kekongruenan secara formal dinyatakan sebagai berikut : Misalkan a and b adalah bilangan bulat dan m adalah bilangan bulat positif, maka $a \equiv b \pmod{m}$ jika m habis membagi a-b.

Kekongruenan $a \equiv b \pmod{m}$ dapat pula dituliskan sebagai berikut :

$$a = b + km$$

yang dalam hal ini k adalah bilangan bulat. Berdasarkan definisi aritmetika modulo, kita dapat menuliskan a mod

m = r sebagai a ≡ r (mod m).

Jika a dan m relatif prima dan m > 1, maka kita dapat menemukan invers dari a mod m. Invers dari a mod m adalah bilangan bulat $\bar{a}$ sedemikian sehingga

$$a\bar{a} \equiv mod\ m$$

Dari definisi relatif prima diketahui bahwa bilangan pembagi bersama terbesar a dan m = 1, maka terdapat bilangan bulat p dan q sedemikian sehingga

pa + qm = 1

yang mengimplikasikan bahwa

pa ≡ 1 (mod m)

Kekongruenan yang terakhir ini berarti bahwa p adalah balikan dari a modulo m.

Kekongruenan lanjar adalah kongruen yang berbentuk

ax ≡ b (mod m)

dengan m adalah bilangan bulat positif, a dan b sembarang bilangan bulat, dan x adalah peubah bilangan bulat. Nilai-nilai x dapat dicari dengan persamaan ax = b + km yang dapat disusun menjadi

x = (b + km) / a

dengan k sembarang bilangan bulat.

C. Bilangan Prima

Bilangan bulat lebih dari 1 yang hanya habis dibagi oleh 1 dan bilangan itu sendiri disebut bilangan prima. Bilangan prima membentuk bilangan bulat positif. Hal ini sesuai dengan teorema fundamental aritmatik (The Fundamental Theorem of Arithmetic) yang berbunyi : Setiap bilangan bulat positif yang lebih besar atau sama dengan 2 dapat dinyatakan sebagai perkalian satu atau lebih bilangan prima.

Untuk menguji apakah n merupakan bilangan prima atau komposit, kita cukup membagi n dengan sejumlah bilangan prima, mulai dari 2, 3, … , bilangan prima £ Ön. Jika n habis dibagi dengan salah satu dari bilangan prima tersebut, maka n adalah bilangan komposit, tetapi jika n tidak habis dibagi oleh semua bilangan prima tersebut, maka n adalah bilangan prima.

III. KRIPTOGRAFI

A.Pengertian dan Sejarah Kriptografi

Kriptografi berasal dari bahasa Yunani, *crypto* yang berarti *secret* (rahasia) dan *graphia* yang berarti *writing* (tulisan). Kriptografi adalah ilmu dan seni untuk menjaga kemanan pesan (data atau informasi) dengan cara menyamarkannya (*to crypt* artinya menyamar) menjadi pesan tersandi.

Sejarah kriptografi sudah dimulai sejak sangat lama. Pada awal tahun 400 SM, kriptografi digunakan oleh tentara Sparta di Yunani. Mereka menggunakan alat yang bernama *scytale*. Scytale terdiri dari pita panjang dari daun papyrus dan sebatang silinder (Gambar 1). Pesan yang akan dikirim ditulis horizontal (baris per baris). Bila pita dilepaskan, maka huruf-huruf di dalamnya telah tersusun membentuk pesan rahasia. Untuk membaca pesan, penerima harus melilitkan kembali pita ke silinder yang diameternya sama dengan diameter silinder pengirim.

Gambar 1. Scytale
(sumber : http://www.oxfordmathcenter.com/drupal7/node/486)

Dalam kriptografi, ada beberapa istilah penting yang sering digunakan. Istilah-istilah tersebut antara lain : plaintext, chipertext, enkripsi, dan dekripsi. Berikut ini akan diberikan sedikit penjelasan mengenai istilah-istilah tersebut. Pesan yang jelas dan dapat dimengerti maknanya disebut *plaintext*, sedangkan pesan yang sudah diubah ke bentuk pesan tersandi dan tidak dapat dimengerti maknanya oleh pihak lain disebut *chipertext*. Proses mengubah bentuk *plaintext* ke *chipertext* disebut enkripsi, sedangkan proses balikannya yang mengembalikan *chipertext* ke *plaintext* disebut dekripsi. Berikut ini ilustrasi proses enkripsi dan dekripsi (Gambar 2).

Gambar 2. Proses Enkripsi dan Dekripsi

Kegunaan kriptorafi berhubungan dengan aspek-aspek keamanan informasi, antara lain :

1. *Confidentiality* : menjaga informasi dari orang-orang yang tidak berhak mengaksesnya. Ada banyak cara untuk meningkatkan confidentiality atau kerahasiaan, mulai dari perlindungan fisik hngga algoritma matematika untuk melindungi data.
2. *Data Integrity* : memastikan keaslian data dengan mendeteksi apakah ada manipulasi dari pihak-pihak yang tidak berhak. Manipulasi data termasuk penambahan, pengurangan, dan penyisipan.
3. *Authentication* : identifikasi pihak yang berkomunikasi maupun verifikasi informasi yang disampaikan. Proses identifikasi ini akan menunjukkan keasilan data.
4. *Non-repudiation* : mencegah pengirim untuk menyangkal bahwa dia yang mengirim pesan.

Kriptografi memiliki notasi matematis sebagai berikut. Misalkan chiperteks dilambangkan C dan plainteks dilambangkan P. Fungsi enkripsi E memetakan P ke C ,

E(P) = C

Fungsi dekripsi D memetakan C ke P,

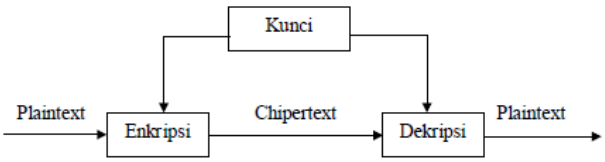
D(C) = P

C. Algoritma Kriptografi

Algoritma adalah urutan langkah-langkah logis penyelesaian masalah yang disusun secara sistematis. Algoritma kriptografi berarti langkah-langkah untuk menjaga keamanan pesan atau informasi. Algoritma kriptografi terdiri dari 3 fungsi dasar, yaitu enkripsi, dekripsi, dan kunci. Kunci yang dimaksud disini adalah kunci yang dipakai untuk enkripsi dan dekripsi pesan. Berdasarkan kunci yang dipakainya, algoritma kriptografi dapat dibagi menjadi 2 :

1. Algoritma Simetri

Algoritma simetri sering disebut juga algoritma klasik. Algoritma ini menggunakan 1 kunci dalam implementasinya. Dalam algoritma simetri, kunci yang digunakan saat enkripsi maupun dekripsi pesan adalah kunci yang sama (Gambar 3).



Gambar 3. Algoritma Simetri
(sumber : widuri.raharja.info)

Algoritma simetri disebut algoritma klasik karena sudah ada sejak lama, contohnya adalah teknik c*aesar chiper* yang digunakan oleh Julius Caesar pada zaman romawi kuno. Pada *caesar chiper*, tiap huruf dalam alfabet "digeser" susunannya sehingga suatu huruf disubtitusi dengan huruf setelahnya sesuai dengan jumlah pergeseran. Kunci dari *caesar chiper* adalah jumlah pergeseran huruf.
Contoh penggunaan caesar chiper dengan pergeseran 3 huruf. Enkripsi plainteks p ke chiperteks c dengan caesar chiper dapat ditulis secara matematis :

$$c = E(p) = (p+3) \bmod 26$$

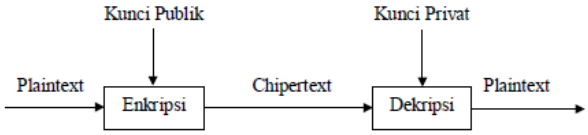
Plainteks : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Chiperteks : D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
Jika ingin menulis pesan "MARKAS DISERANG", dengan menggunakan chiperteks yang telah digeser 3 kali, pesan menjadi "PDUNDV GLVHUDQJ"
Penerima dapat mengembalikan pesan seperti semula dengan menggunakan kunci yang sama yaitu 3 kali pergeseran. Dekripsi chiperteks c ke plainteks p dengan caesar chiper dapat ditulis secara matematis :

$$p = D(c) = (c-3) \bmod 26$$

Contoh algoritma simetri : AES, DES, A5, dll.
Aplikasi kriptografi simetri : enkripsi/dekripsi (untuk menjaga kerahasiaan pesan).

2. Algoritma Asimetri

Algoritma asimetri sering disebut juga algoritma modern atau algoritma kunci publik. Algoritma ini menggunakan 2 kunci dalam implementasinya. Dalam algoritma asimetri, kunci yang digunakan saat enkripsi maupun dekripsi pesan adalah kunci yang berbeda (Gambar 4).



Gambar 4. Algoritma Asimetri
(sumber : widuri.raharja.info)

Pada algoritma asimetri, kunci terbagi menjadi 2 :

1. Kunci publik : kunci yang boleh diketahui semua orang, digunakan untuk enkripsi pesan
2. Kunci privat : kunci yang dirahasiakan, hanya diketahui orang tertentu, digunakan untuk dekripsi pesan.

Contoh penggunaan algoritma asimetri jika A ingin mengirim pesan ke B. Pertama B harus memberikan kunci publiknya pada A untuk mengenkripsi pesan yang akan dikirim A. Kemudian B dapat mendekripsi pesan dari A menggunakan kunci privat B. Begitu juga sebaliknya jika B ingin mengirim pesan ke A.

Algoritma asimetri lebih aman disbanding algoritma simetri. Sistem kriptografi asimetri didasarkan pada fakta:

1. Komputasi untuk enkripsi/dekripsi pesan mudah dilakukan.
2. Secara komputasi hampir tidak mungkin (infeasible) menurunkan kunci privat, d, bila diketahui kunci publik, e, pasangannya.

Kedua fakta diatas dapat dianalogikan dengan perkalian dan pemfaktoran. Cukup mudah jika kita ingin mengalikan bilangan a x b = n, tapi akan jadi sulit jika kita ingin memfaktorkan bilangan n.
Contoh algoritma asimetri : RSA, DSA, ElGamal, dll.
Aplikasi kriptografi asimetri :

1. Enkripsi/ dekripsi : algoritma asimetri dapat digunakan untuk menjaga kerahasiaan pesan.
2. *Digital signatures* : algoritma asimetri dapat digunakan untuk membuktikan otentikasi pesan maupun otentikasi pengirim.
3. Pertukaran kunci : algoritma asimetri dapat digunakan untuk mengirim kunci simetri supaya tetap aman.

D. Algoritma RSA

Dalam sistem kriptografi asimetri, salah satu algoritma yang cukup populer dan paling banyak digunakan adalah algoritma RSA. Algoritma RSA dibuat oleh tiga peneliti dari MIT (Massachusetts Institute of Technology), yaitu Ron Rivest, Adi Shamir, dan Len Adleman pada tahun 1976. RSA mendasarkan proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmatika modulo. Kunci enkripsi dan dekripsi merupakan bilangan bulat.
Besaran-besaran yang digunakan pada algoritma RSA:

1. a dan b bilangan prima (rahasia)
2. $n = a \times b$ (tidak rahasia)
3. $m = (a - 1)(a - 1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
5. d (kunci dekripsi) (rahasia)

6. p (plainteks) (rahasia)
7. c (cipherteks) (tidak rahasia)

Algoritma membangkitkan pasangan kunci (menggunakan besaran-besaran di atas) :

1. Pilih 2 buah bilangan prima sembarang a dan b
2. Hitung n = a × b dengan n > 255 (nilai maksimum ASCII = 255)
3. Hitung m = (a – 1)(a – 1)
   Setelah m dihitung, a dan b dapat dihapus untuk menjaga kerahasiaan.
4. Pilih sebuah bilangan bulat untuk kunci publik e yang relatif prima terhadap m (PBB(e,m) =1)
5. Bangkitkan kunci dekripsi d dengan kekongruenan e.d ≡ 1 (mod m)
6. Lakukan enkripsi terhadap isi pesan dengan persamaan $c = p^e \bmod n$. Harus dipenuhi persyaratan bahwa nilai p terletak dalam himpunan nilai 0,1,2,…,n-1 untuk menjamin hasil perhitungann tidak berada di luar himpunan.
7. Proses dekripsi dilakukan dengan persamaan $p = c^d \bmod n$

Misalkan B ingin mengirim pesan yang terenkripsi menggunakan algoritma RSA untuk A yang akan mendekripsinya. Berikut ini langkah untuk enkripsi :

1. B menerima kunci public A (n,e)
2. Ubah pesan menjadi integer m (bentuk ASCII) dalam interval [0,n-1]
3. Hitung $c = m^e \bmod n$.
4. Kirim chiperteks ke A

Kemudian A melakukan dekripsi pesan menggunakan kunci privat d dengan persamaan $m = c^d \bmod n$

Kekuatan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi faktor primanya, dalam hal ini n = a × b. Penemu algoritma RSA menyarankan panjang a dan b lebih dari 100 digit. Dengan demikian hasil perkaliannya akan lebih dari 200 digit. Menurut Rivest dan kawan-kawan, usaha untuk mencari faktor untuk mencari faktor bilangan 200 digit membutuhkan waktu komputasi selama 4 milyar tahun (dengan asumsi bahwa algoritma pemfaktoran yang digunakan adalah algoritma yang tercepat saat ini dan komputer yang dipakai mempunyai kecepatan 1 milidetik).

Sampai saat ini, belum ditemukan algoritma yang paling efisien untuk memfaktorkan bilangan yang besar. Inilah yang membuat algoritma RSA tetap dipakai hingga saat ini. Selagi belum ditemukan algoritma yang efisien untuk memfaktorkan bilangan bulat menjadi faktor primanya, maka algoritma RSA masih termasuk salah satu algoritma kriptografi yang aman.

D. Algoritma Simetri vs Algoritma Asimetri

Kelebihan algoritma simetri:

1. Algoritma kriptografi simetri dirancang sehingga proses enkripsi/dekripsi membutuhkan waktu yang singkat.
2. Ukuran kunci simetri relatif pendek.
3. Algoritma kriptografi simetri dapat digunakan untuk membangkitkan bilangan acak.
4. Algorima kriptografi simetri dapat dikombinasikan untuk menghasilkan cipher yang lebih kuat.
5. Otentikasi pengirim pesan langsung diketahui dari cipherteks yang diterima, karena kunci hanya diketahui oleh pengirim dan penerima pesan saja.

Kelemahan algoritma simetri:

1. Kunci simetri harus dikirim melalui saluran yang aman. Kedua entitas yang berkomunikasi harus menjaga kerahasisan kunci ini.
2. Kunci harus sering diubah, mungkin pada setiap sesi komunikasi.

Kelebihan kriptografi asimetri:

1. Hanya kunci privat yang perlu dijaga kerahasiaannya oleh seiap entitas yang berkomuniaksi (tetapi, otentikasi kunci publik tetap harus terjamin).
2. Pasangan kunci publik/kunci privat tidak perlu diubah, bahkan dalam periode waktu yang panjang.
3. Dapat digunakan untuk mengamankan pengiriman kunci simetri.
4. Beberapa algoritma kunci-publik dapat digunakan untuk memberi tanda tangan digital pada pesan.

Kelemahan kriptografi asimetri:

1. Enkripsi dan dekripsi data umumnya lebih lambat daripada sistem simetri, karena enkripsi dan dekripsi menggunakan bilangan yang besar dan melibatkan operasi perpangkatan yang besar.
2. Ukuran cipherteks lebih besar daripada plainteks (bisa dua sampai empat kali ukuran plainteks).
3. Ukuran kunci relatif lebih besar daripada ukuran kunci simetri.
4. Karena kunci publik diketahui secara luas dan dapat digunakan setiap orang, maka cipherteks tidak memberikan informasi mengenai otentikasi pengirim.

Berdasarkan kelebihan dan kelemahan masing-masing algoritma yang telah dijelaskan di atas, dapat diketahui, algoritma asimetri cocok untuk jaringan data yang besar karena tidak perlu membangkitkan pasangan kunci berbeda untuk setiap data. Sedangkan algoritma simetri cocok untuk jaringan data yang lebih kecil dan keterbatasan waktu karena ukuran kunci yang relatif pendek dan waktu untuk proses enkripsi/dekripsi yang cukup cepat.

VII. KESIMPULAN

Algoritma kriptografi, baik yang simetri maupun asimetri, memiliki kelebihan dan kekurangan masing-masing. Kedua algoritma tersebut memiliki aplikasi yang berbeda dalam kehidupan sehari-hari. Kita tidak bisa memilih atau menentukan mana algoritma yang paling baik. Kita hanya dapat menentukan mana algoritma yang paling cocok untuk menyelesaikan persoalan tertentu.

IV. UCAPAN TERIMA KASIH

Penulis mengucap syukur pada Tuhan YME untuk berkat dan rahmatnya sehingga penulis bisa menyelesaikan makalah ini. Penulis juga mengucapkan terima kasih pada Bapak Rinaldi Munir sebagai dosen pengajar Matematika Diskrit yang telah memberi bimbingan selama satu semester ini dan telah mengenalkan kriptografi sehingga penulis dapat mengembangkan ketertarikan pada kriptografi untuk ditulis dalam makalah ini.

REFERENCES

[1] Ayirus, Dony. 2008. "Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi". Yogyakarta: ANDI
[2] Munir, Rinaldi. 2006. "Diktat Kuliah IF2120 Matematika Diskrit". Bandung: Penerbit Informatika ITB.
[3] Rosen, Kenneth H. 2012. "Discrete mathematics and its applications". New York: McGraw-Hill
[4] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/ diakses pada 8 Desember 2016, 20.06
[5] https://www.ciphercloud.com/blog/cloud-information-protection-symmetric-vs-asymmetric-encryption/ diakses pada 9 Desember 2016, 12.25
[6] http://www.metode-algoritma.com/2013/06/algoritma-rsa.html diakses pada 9 Desember 2016, 14.28

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 9 Desember 2016

Veren Iliana Kurniadi
13515078