PERANAN ARITMETIKA MODULO DAN BILANGAN PRIMA PADA ALGORITMA KRIPTOGRAFI RSA (Rivest-Shamir-Adleman)

Dahlia Br Ginting

Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI
Jl. Ir. H. Juanda 96 Bandung 40132

E-mail:dahliaginting@yahoo.co.id

ABSTRAK

Matematika diskrit berkembang sangat pesat dalam dekade terakhir ini. Salah satu alasan yang menyebabkan perkembangan pesat itu adalah karena komputer digital bekerja secara diskrit. Informasi yang disimpan dan dimanipulasi oleh komputer adalah dalam bentuk diskrit. Perkembangan matematika diskrit ini juga diikuti dengan perkembangan ilmu lainnya yang memakai matematika sebagai landasan ilmunya. Salah satunya adalah ilmu kriptrografi yang memakai aritmetika modulo sebagai landasan ilmunya. Algoritma yang menjadi standard algoritma kriptografi nirsimetri (kunci untuk proses enkripsi berbeda dengan kunci untuk proses dekripsi) adalah RSA (Rivest-Shamir-Adleman). RSA mendasarkan proses enkripsi dan deskripsinya pada konsep **bilangan prima** dan **aritmetika modulo.**

Dalam paparan di bawah ini akan dijelaskan bahwa matematika diskrit khusunya aritmetika modulo memiliki hubungan yang sangat erat dengan ilmu kriptografi.

Kata-kata Kunci *: Aritmetika Modulo, plainteks, chiperteks, enkripsi, dekripsi, kriptografi*

1. PENDAHULUAN

1.1 Aritmatika Modulo

Sifat pembagian pada bilangan bulat melahirkan konsep-konsep seperti bilangan prima dan aritmetika modulo. Aritmetika modulo (*modular arithmetic*) memainkan peranan yang penting dalan komputasi integer, khususnya pada aplikasi kriptografi. Operator yang digunakan pada aritmetika modulo adalah **mod**. Operator mod memberikan sisa pembagian.

Definisi:

Misalkan a adalah bilangan bulat dan m adalah bilangan bulat positif. Operasi a mod m (dibaca "a modulo m") memberikan sisa jika a dibagi dengan m. Dengan kata lain, a mod m = r sedemikian sehingga a = mq + r, dengan $0 \leq r < m$.

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, 3, …, m-1 }. Misalnya 27 dibagi 4 memberikan hasil 6 dengan sisa 3, sehingga kita tulis 27 mod 4 = 3

Untuk nilai a yang negatif, caranya: bagi |a| dengan m mendapatkan sisa r'. Maka a mod m = m – r' bila $r' \neq 0$. Misalkan menghitung – 41 mod 9.

Jadi | – 41 | mod 9 = 5, sehingga – 41 mod 9 = 9 – 5 = 4

Jika a mod m = 0, maka dikatakan bahwa a adalah kelipatan dari m, yaitu a habis dibagi dengan m

Misalnya 28 mod 4 = 0, berarti 28 adalah kelipatan 4.

1.1.1 Kongruen

Kadang-kadang dua buah bilangan bulat a dan b, mempunyai sisa yang sama jika dibagi dengan bilangan bulat positif m. Kita katakan bahwa a dan b kongruen dalam modulo m, dan dilambangkan dengan $a \equiv b \pmod{m}$

Misalkan : 38 mod 5 = 3 dan 13 mod 5 = 3, maka $38 \equiv 13 \pmod{5}$

Definisi

Misalkan a dan b adalah bilangan bulat dan m adalah bilangan > 0, maka $a \equiv b \pmod{m}$ jika m habis membagi a – b. Kekongruenan: $a \equiv b \pmod{m}$ dapat pula dituliskan dalam hubungan a = b + km

Sifat-sifat perhitungan pada aritmetika modulo, khususnya terhadap operasi perkalian dan penjumlahan dinyatakan dalam teorema berikut:

Teorema:

Misalkan m adalah bilangan bulat positif.

1. Jika $a \equiv b \pmod{m}$ dan c adalah sembarang bilangan bulat maka

   (i) $(a + c) \equiv (b + c) \pmod{m}$

(ii) $ac \equiv bc \pmod{m}$

(iii) $a\,p \equiv b\,p \pmod{m}$ untuk suatu bilangan bulat tak negatif p

2. Jika $a \equiv b \pmod{m}$ dan $c \equiv d \pmod{m}$, maka

(i) $(a + c) \equiv (b + d) \pmod{m}$

(ii) $ac \equiv bd \pmod{m}$

1.1.2 Balikan Modulo (modulo invers)

Jika a dan m relatif prima dan m > 1, maka kita dapat menemukan balikan (invers) dari a modulo m. Balikan dari a modulo m adalah bilangan bulat $\bar{a}$ sedemikian sehingga: $a\,\bar{a} \equiv 1 \pmod{m}$

Bukti:

Pada definisi relatif prima diketahui bahwa PBB(a,m) = 1, maka terdapat bilangan bulat p dan q sedemikian sehingga pa + qm = 1 yang mengimplikasikan bahwa $pa + qm \equiv 1 \pmod{m}$

Yang mengimplikasikan bahwa $pa + qm \equiv 1 \pmod{m}$. Karena $qm \equiv 0 \pmod{m}$ maka $pa \equiv 1 \pmod{m}$

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

1.1.3 Kekongruenan Lanjar

Kekongruenan lanjar adalah kekongruenan yang berbentuk $ax \equiv b \pmod{m}$ dengan m bilangan bulat positif, a dan b sembarang bilangan bulat, dan x adalah peubah. Bentuk kongruen lanjar berarti menentukan nilai-nilai x yang memenuhi kekongruenan tersebut. Metode yang sederhana untuk mencari nilai-nilai x tersebut adalah dengan menggunakan persamaan $ax \equiv b \pmod{m}$ dapat dituliskan dalam hubungan ax = b + km yang dapat disusun menjadi

$$x = \frac{b + km}{a}$$

dengan k sembarang bilangan bulat. Cobakan untuk k = 0 , 1 , 2 , … dan k = -1, -2, … yang menghasilkan x sebagai bilangan bulat.

1.2 Bilangan Prima

Bilangan bulat positif yang mempunyai aplikasi penting dalam ilmu komputer dan matematika diskrit adalah bilangan prima. Bilangan prima adalah bilangan bulat positif yang lebih besar dari 1 yang hanya habis dibagi 1 dan dirinya sendiri.

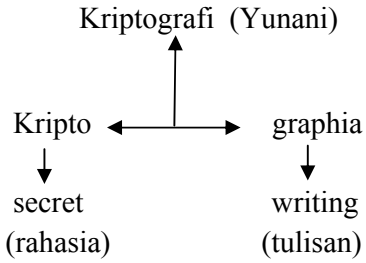
Definisi:

Bilangan bulat positif p (p >1) disebut bilangan prima, jika pembaginya hanya 1 dan p.

2. PEMBAHASAN

2.1 Kriptografi

Arimetika modulo dan bilangan prima mempunyai banyak aplikasi dalam ilmu komputer, salah satu aplikasinya yang terpenting adalah **kriptograf**i.



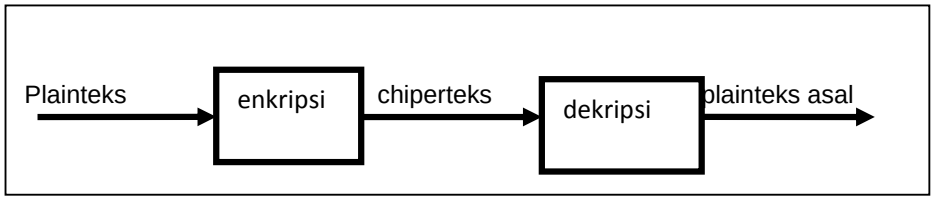
Kegunaannya : Menjaga kerahasiaan pesan (tulisan) yang dikirim dari suatu tempat ke tempat lain.

Kriptografi adalah ilmu sekaligus seni untuk menjaga kerahasiaan pesan (data atau informasi) dengan cara menyamarkannya (*to crypt*) menjadi bentuk yang tidak mempunyai makna. Kerahasiaan informasi merupakan suatu hal yang sangat penting, agar tidak diketahui oleh orang yang tidak berhak. Misalnya, perdagangan elektronis (*e-commerce*) yang menggunakan kriptografi untuk menyediakan nomor PIN *customer*, karena pembayaran di dalam *e-commerce* umumnya menggunakan kartu kredit.

Pesan yang sudah disandikan dapat dikembalikan lagi ke pesan aslinya hanya oleh orang yang berhak (orang yang berhak yang dimaksudkan adalah orang yang memiliki suatu metode atau kunci untuk mengembalikan isi sistem)

Pesan yang dirahasiakan dinamakan **plainteks** (*plaintext*), artinya teks jelas yang dapat dimengerti, sedangkan pesan hasil penyamaran disebut **chiperteks** (*chipertext*), yang artinya teks tersandi.

Proses penyamaran dari plainteks ke chiperteks disebut **enkripsi** (*encryption*) dan proses pembalikan dari chiperteks ke plainteks disebut **dekripsi** (*decryption*).



Gambar 2.1 Enkripsi dan Dekripsi

Sebagai contoh, sebuah pesan rahasia (plainteks) berikut:

Uang disimpan di balik buku x

Disandikan menjadi chiperteks dengan suatu teknik kriptografi tertentu

j&kloP(d$gkhtpuBn%6^klp..t@

Aspek-aspek keamanan data

1. *Integrity* (Integritas), yaitu keaslian pesan yang dikirim melalui jaringan
2. *Authentication* (Pembuktian Keaslian), yaitu penerima info yakin keaslian pesan berasal dari orang yang dikehendaki.
3. *Confidentiality*, yaitu usaha untuk menjaga informasi dari orang yang tidak berhak mengakses.

Kriptografi lazim digunakan di dalam komputer, baik untuk pengiriman data maupun untuk penyimpanan data di dalam *disk storge*. Data yang ditransmisikan melalui saluran komunikasi direpresentasikan dalam bentuk chiperteks. Di tempat penerima chiperteks dikembalikan lagi menjadi plainteks hanya oleh pihak yang berhak saja, yang biasanya menggunakan kunci rahasia juga.

File di dalam media penyimpanan komputer (seperti *hard disk*) disimpan dalam bentuk chiperteks. Untuk membacanya, hanya orang yang berhak yang dapat mengembalikan chiperteks menjadi plainteks.

Notasi Matematis

Jika chiperteks dilambangkan dengan C dan plainteks dilambangkan dengan P, maka fungsi enkripsi E memetakan P ke C,

$E(P) = C$

Pada proses kebalikannya, fungsi dekripsi D memetakan C ke P,

$D(C) = P$

Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan asal, maka kesamaan berikut harus benar,

$D(E(P)) = P$

Algoritma kriptografi atau *chiper* adalah fungsi matematik yang digunakan untuk enkripsi dan dekripsi.

Kekuatan kriptografi ditentukan dengan menjaga kerahasiaan algoritmanya. Algoritma kriptografii dinamakan algoritma *restricted*.

Misalnya dalam sebuah kelompok orang, mereka sepakat menyandikan setiap pesan dengan algoritma yang sama. Algoritmanya adalah mempertukarkan pada setiap kata karakter pertama dengan karakter ketiga, karakter kedua dengan karakter keempat dan seterusnya.

Contohnya:

Plainteks	:	MATEMATIKA DISKRIT
Chiperteks	:	TEMATIMAKA SKDITIR

Untuk mendiskripsikan pesan, algoritma yang sama digunakan kembali. Namun algoritma *restricted* ini, mempunyai kelemahan yakni bila seorang dari anggota keluar dari kelompok, maka penyandian pesan harus diubah lagi. Kriptografi modern tidak lagi mendasarkan kekuatan pada algoritmanya, namun kekuatan kriptografinya terletak pada kunci, yang berupa deretan karakter atau bilangan bulat. Algoritmanya tidak dirahasiakan lagi, tapi bisa diketahui oleh semua orang.

Hanya orang yang mengetahui kunci yang dapat melakukan enkripsi dan diskripsi. Kunci ini analog fungsinya dengan *password* pada sistem komputer.

Misalnya pada Caesar chipper, teknik yang digunakan oleh Julius Caesar, kaisar Romawi, untuk menyandikan pesan yang ia kirim kepada para gubernurnya. Pada Caesar chipper, tiap huruf disubstitusikan dengan huruf ke tiga berikutnya dari susunan alfabet. Dalam hal ini kuncinya adalah
jumlah pergeseran huruf, yaitu 3.

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	Z

Dengan mengkodekan setiap huruf alfabet dengan integer

A=0, B=1, C=2, D=3, E=4, F=5, G=6, H=7, I=8, J=9, K=10, L=11, M=12, N=13, O=14, P=15, Q=16, R=17, S=18, T=19, U=20, V=21, W=22, X=23, Y=24, Z=25

maka secara matematis plainteks p_i disandikan menjadi c_i dengan aturan

$$c_i = E(p_i) = (p_i + 3) \ mod \ 26 \qquad \textbf{(2.1)}$$

Misalkan pesan

AWASI GERAK GERIK ASTERIX DARI JAUH

Disandikan dengan persamaan (2.1) menjadi

DZDVL JHUDN JHULN DVWHULA GDUL MDXK

Penerima pesan mengembalikan lagi chiperteks dengan operasi kebalikan, yang secara matematis dapat dinyatakan dengan persamaan

$$p_i = D(c_i) = (c_i - 3) \ mod \ 26 \qquad \textbf{(2.2)}$$

Sehingga chiperteks:

DZDVL JHUDN JHULN DVWHULA GDUL MDXK

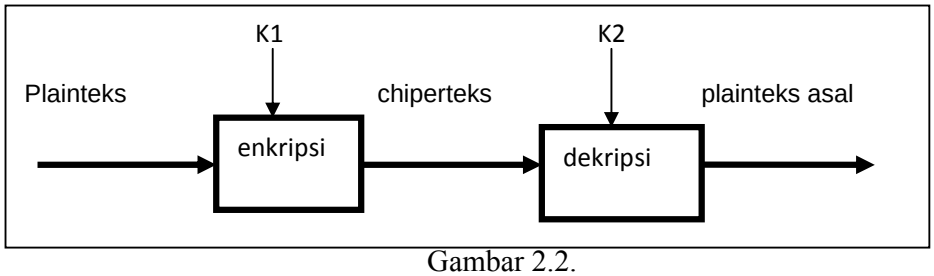
Dikembalikan menjadi plainteks asal dengan persamaan (2.2) menjadi

AWASI GERAK GERIK ASTERIX DARI JAUH

Secara matematis, pada system kriptografi yang menggunakan kunci K, maka fungsi enkripsi dan dekripsi menjadi

$E_{K1}(P) = C$ dan $D_{K1}(C) = P$

Kedua fungsi ini memenuhi $D_{K2}(E_{K1}(P)) = P$



Gambar 2.2.

Diagram proses enkripsi dan deskripsi pada algoritma kriptografi modern

Jika K1 = K2 (yaitu, kunci untuk proses enkripsi sama dengan kunci untuk dekripsi), maka algoritma kriptografinya disebut **algoritma simetri** (algoritma kunci pribadi atau *private key*).

Contoh algoritma yang menjadi standard algoritma kriptografi simetri adalah DES (*Data Encyption Standard).* Sebaliknya, jika K1 ≠ K2 (yaitu, kunci untuk proses enkripsi berbeda dengan kunci untuk dekripsi), maka algoritma kriptografinya disebut

algoritma nirsimetri (algoritma kunci publik atau *publice key*). Algoritma ini yang umum dipakai di lingkungan jaringan komputer.

Algoritma ini mempunyai dua buah kunci, yaitu kunci publik (untuk enkripsi) yang tidak rahasia, dan kunci rahasia (*secret key*) untuk dekripsi.

Contoh algoritma yang menjadi standard algoritma kriptografi nirsimetri adalah RSA (Rivest-Shamir-Adleman). RSA mendasarkan proses enkripsi dan deskripsinya pada konsep **bilangan prima** dan **aritmetika modulo.**

2.2 RSA (Rivest-Shamir-Adleman)

Algoritma RSA diperkenalkan oleh tiga peneliti dari MIT (*Massachussest Institute of Technology*) pada tahun 1976. RSA mendasarkan proses enkripsi dan deskripsinya pada konsep **bilangan prima** dan **aritmetika modulo.** Baik kunci enkripsi maupun deskripsi merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diketahui umum (sehingga dinamakan juga kunci publik), namun kunci untuk deskripsi dirahasiakan.

ALGORITMA RSA

1. Pilih dua buah bilangan prima sembarang, sebut *a* dan *b*. Jaga kerahasiaan *a* dan *b* ini.
2. Hitung $n = a \times b$. Besaran *n* tidak dirahasiakan.
3. Hitung $m = (a - 1) \times (b - 1)$. Sekali *m* telah dihitung, *a* dan *b* dapat dihapus untuk mencegah diketahuinya oleh pihak lain.
4. Pilih sebuah bilangan bulat untuk kunci pablik, sebut namanya *e*, yang relatif prima terhadap *m*
5. Bangkitkan kunci dekripsi, *d* , dengan kekongruenan $e \equiv 1 (\mathrm{mod}\ m)$
   Lakukan enkripsi terhdap isi pesan dengan persamaan $c_i \equiv p_i (\mathrm{mod}\ n)$ yang dalam hal ini p_i adalah blok plainteks, c_i adalah chiperteks yang diperoleh, dan *e* adalah kunci enkripsi (kunci publik). Harus dipenuhi persyaratan bahwa nilai p_i harus terletak dalam himpunan nilai 0, 1, 2, 3, …, n – 1 untuk menjamin hasil perhitungan tidak berada di luar himpunan.
6. Proses dekripsi dilakukan dengan menggunakan persamaan $p_i \equiv c_i^{\,d} \bmod n$ yang dalam hal ini *d* adalah kunci enkripsi.

Kekongruenan $e \equiv 1 (\mathrm{mod}\ m)$ pada langkah 5, sama dengan $ed \bmod m = 1$.

$a \equiv b \pmod{m}$ ekivalen dengan $a = b + km$, maka $ed \equiv 1 \pmod{m}$ ekivalen dengan $ed = 1 + km$, sehingga d dapat dihitung dengan

$$d = \frac{1+km}{e} \qquad \textbf{(2.3)}$$

Sebagai ilustrasi, misalnya kita mengambil $a = 47$ dan $b = 71$ (keduanya prima), maka dapat dihitung nilai $n = a \times b = 3337$ dan $m = (a - 1)x(b - 1) = 3220$. Pilih kunci publik $e = 79$ (bilangan yang relative prima dengan 3220, karena pembagi bersama terbesarnya adalah 1). Nilai *e* dan *m* dapat dipublikasikan ke umum.

Selanjutnya akan dihitung kunci dekripsi d seperti pada langkah ke 4

$$e \times d \equiv 1 \pmod{m}$$

Dengan menggunakan rumus (2.3), kita dapat menghitung kunci dekripsi *d* sebagai berikut

$$d = \frac{1+(kx3220)}{79}$$

Dengan mencoba nilai-nilai k = 1, 2, 3, …, diperoleh nilai d yang bulat adalah 1019. Jadi angka **1019** inilah yang menjadi **kunci dekripsi yang harus dirahasiakan**.

Misalkan plainteks yang akan dienkripsikan adalah P = HARI INI (atau di dalam desimal ASCII-nya adalah 7265827332737873). Pecah P menjadi blok yang lebih kecil, misalnya P dipecah menjadi 6 blok yang berukuran 3 digit:

p1 = 726 p2 = 582 p3 = 733 p4 = 273 p5 = 787 p6 = 003

Nilai-nilai pi ini masih terletak dalam rentang nilai 0 sampai 3337 – 1 .

Blok pertama dienkripsikan sebagai $726^{79} \bmod 3337 \equiv 215 = c1$

Blok kedua dienkripsikan sebagai $582^{79} \bmod 3337 \equiv 776 = c2$

Blok ketiga dienkripsikan sebagai $733^{79} \bmod 3337 \equiv 1743 = c3$

Blok keempat dienkripsikan sebagai $273^{79} \bmod 3337 \equiv 933 = c4$

Blok kelima dienkripsikan sebagai $787^{79} \bmod 3337 \equiv 1731 = c5$

Blok keenam dienkripsikan sebagai $003^{79} \bmod 3337 \equiv 158 = c6$

Sehingga dihasilkan chiperteks **C = 215 776 1743 933 1731 158**.

Proeses dekripsi dilakukan dengan menggunakan kunci rahasia **d = 1019**.

Jadi: blok c1 didekripsikan sebagai $215^{1019} \bmod 3337 \equiv 726 = p1$

blok c2 didekripsikan sebagai $776^{1019} \bmod 3337 \equiv 582 = p2$

blok c3 didekripsikan sebagai $1743^{1019} \bmod 3337 \equiv 733 = p3$

blok c4 didekripsikan sebagai $933^{1019} \bmod 3337 \equiv 273 = p4$

blok c5 didekripsikan sebagai $1731^{1019} \bmod 3337 = 787 = p5$

blok c6 didekripsikan sebagai $156^{1019} \bmod 3337 = 003 = p6$

Akhirnya kita peroleh kembali plainteks semula **P = 7265827332737873** yang karakternya adalah P = HARI INI.

Perhitungan perpangkatan pada proses enkripsi ($c_i = p_i^e \bmod n$) dan dekripsinya ($p_i = c_i^d \bmod n$) membutuhkan bilangan yang sangat besar. Untuk menghindari penggunaan bilangan yang besar, maka dapat digunakan penyederhanaan dengan persamaan berikut:

$$ab \bmod m = [(a \bmod m)(b \bmod m)] \bmod m$$

3. KESIMPULAN

Kekuatan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi factor primanya, yang dalam hal ini $n = a \times b$. Sekali n berhasil difaktorkan menjadi a dan b, maka $m = (a - 1) \times (b - 1)$ dapat dihitung. Selanjutnya karena kunci enkripsi *e* diumumkan (tidak dirahasiakan), maka kunci dekripsi d dapat dihitung dari persamaan $e \times d = 1 \pmod m$. Ini berarti proses dekripsi dapat dilakukan oleh orang yang tidak berhak.

Nilai *a* dan *b* disarankan panjangnya lebih dari 100 digit. Dengan demikian hasil kali $n = a \times b$ akan berukuran lebih dari 200 digit. Menurut Rivest dan kawan-kawan, usaha untuk mencari factor bilangan 200 digit membutuhkan waktu komputasi selama 4 milyar tahun, dengan asumsi bahwa algoritma pemfaktoran yang dipakai adalah algoritma yang tercepat saat ini dan komputar yang dipakai mempunyai kecepatan 1 milidetik.

Hingga saat ini algoritma yang paling mangkus untuk memfaktorkan bilangan yang besar belum ditemukan. Inilah yang membuat algoritma RSA masih tetap dipakai. Sampai saat ini, algoritma RSA masih direkomendasikan untuk penyandian pesan.

4. DAFTAR PUSAKA

1. Douglas R. Stinson ," *Cryptography : Theory and Practice*"
2. *Cryptography and Network Security: Principles and Practice*, 2nd ed., Prentice Hall 1999
3. Rinaldi Munir, "Matematika Diskrit"