Penerapan Teori Bilangan Bulat dalam Kriptografi dan Aplikasinya dalam Kehidupan Sehari-hari

Kukuh Nasrul Wicaksono – NIM 13505097

Program Studi Teknik Informatika
Institut Teknologi Bandung
Jl. Ganesha 10 Bandung 40132

E-mail : *if15097@students.if.itb.ac.id*

Abstrak

Seiring dengan perkembangan zaman, maka munculah cabang matematika baru yang disebut dengan matematika diskrit. Perkembangan yang pesat dari ilmu matematika diskrit ini berkaitan erat dengan perkembangan pesat dari dunia komputer digital, karena komputer digital bekerja secara diskrit. Perkembangan matematika diskrit ini juga diikuti dengan perkembangan ilmu lainnya yang memakai matematika sebagai landasan ilmunya. Salah satunya adalah ilmu kriptrografi yang memakai teori bilangan bulat sebagai landasan ilmunya. Dalam paparan di bawah ini akan dijelaskan bahwa matematika diskrit khusunya teori bilangan bulat memiliki hubungan yang sangat erat dengan ilmu kriptografi. Selain itu akan dijelaskan pula mengenai aplikasi dari ilmu keriptografi ini dalam kehidupan sehari-hari.

Kata kunci *: Teori bilangan bulat, kriptografi*

1. Pendahuluan

Dalam kehidupan sehari-hari, kita pasti telah sering menemukan bahwa ilmu pasti, khususnya Matematika dan berbagai cabang ilmu Matematika lainnya sangat banyak digunakan manusia untuk membantu menyelesaikan suatu masalah. Mulai dari masalah kecil dan tradisional, hingga masalah besar dan modern.

Seiring dengan perkembangan zaman, maka munculah cabang matematika baru yang disebut dengan matematika diskrit. Perkembangan yang pesat dari ilmu matematika diskrit ini berkaitan erat dengan perkembangan pesat dari dunia komputer digital, karena komputer digital bekerja secara diskrit. Perkembangan matematika diskrit ini juga diikuti dengan perkembangan ilmu lainnya yang memakai matematika diskrit landasan ilmunya. Salah satunya adalah ilmu kriptrografi yang memakai teori bilangan bulat sebagai landasan ilmunya.

Kriptografi ini adalah suatu cabang ilmu yang digunakan untuk menjaga kerahasiaan pesan dengan cara menyamarkannya dan menjadikan bentuk sandi yang tidak mempunyai makna. Apakah manfaat kriptografi ini dalam kehidupan sehari-hari kita? Dan apa pula hubungan matematika diskrit khususnya teori bilangan bulat dengan kriptografi? Dalam tulisan berikutnya, akan dijelaskan jawaban dari pertanyaan di atas.

2. Matematika Diskrit dan Teori Bilangan Bulat

Matematika diskrit adalah cabang matematika yang mengkaji objek-objek diskrit. Apa yang dimaksud dengan kata **diskrit (**discrete**)**? Benda disebut diskrit jika ia terdiri dari sejumlah berhingga elemen yang berbeda atau elemen-elemen yang tidak berkesinambungan. Himpunan bilangan bulat (integer) dipandang sebagai objek diskrit. Lawan kata diskrit adalah kontinyu atau menerus. Himpunan bilangan riil (real) adalah suatu objek kontinu. Di dalam matematika kita mengenal fungsi diskrit dan fungsi kontinu. Fungsi diskrit digambarkan sebagai sekumpulan titik-titik, sedangkan fungsi kontinu digambarkan sebagai kurva.

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.

Materi yang ada dalam matematika diskrit adalah materi yang khas informatika, sehingga terkadang matematika diskrit ini disebut juga matematika informatika. Salah satu materi di dalam matematika diskrit ini adalah teori bilangan bulat.

Sesuai dengan namanya, teori bilangan bulat sangat erat hubungannya dengan bilangan bulat. Bilangan bulat itu sendiri adalah bilangan yang tidak mempunya pecahan desimal, misalnya adalah 2, 43, 566, -64, 0 dan sebagainnya. Teori bilangan bulat dalam matematika diskrit memberikan penekanan dengan sifat pembagian. Sifat pembagian pada bilangan bulat melahirkan konsep-konsep seperti bilangan prima dan aritmatika modulo. Satu algoritma penting yang berhubungan dengan sifat pembagian ini adalah algoritma Euclidean. Baik bilangan prima, aritmatika modulo, dan algoritma Euclidean memainkan peran yang penting dalam bidang ilmu Kriptografi, yaitu ilmu yang mempelajari kerahasiaan pesan.

2.1. Algoritma Euclidean

Algoritma Euclidean adalah salah satu metode yang mangkus dalam mencari Pembagi Bersama Terbesar (greates), disingkat menjadi PBB. Algoritma ini sudah dikenal sejak berabad-abad yang lalu. Euclid ,penemu Algoritma Euclidean, adalah seorang matematikawan yunani yang menuliskan algoritmanya tersebut dalam bukunya yang terkanal yang berjudul Element.

Secara formal algoritma Euclidean dirumuskan sebagai berikut.

Misalkan m dan n adalah bilangan bulat tak negatif dengan $m \geq n$. Misalkan $r_0 = m$ dan $r_1 = n$, lakukan secara berturut – turut pembagian seperti dibawah ini.

$r_0 = r_1 q_1 + r_2 \qquad 0 \leq r_2 \leq r_1$

$r_1 = r_2 q_2 + r_3 \qquad 0 \leq r_3 \leq r_2$

.
.
.

$r_{n-2} = r_{n-1} q_{n-1} + r_n \qquad 0 \leq r_n \leq r_{n-1}$

$r_{n-1} = r_n q_n + 0$

Kemudian PBB dari m dan n **(**PBB(m,n)**)** adalah sisa terakhir dari pembagian tersebut.

Singkatnya algoritma Euclidean akan dituliskan sebagai berikut.

Algoritma Euclidean

1. Jika n = 0 maka
   m adalah PBB(m,n);
   stop
   tetapi jika $n \neq 0$,
   lanjutkan ke langkah 2.
2. Bagilah m dengan n dan misalkan r adalah sisanya.
3. Gantilah nilai m dengan nilai n dan nilai n dengan r, lalu ulang kembali ke langkah 1.

Catatan : jika $m \leq n$, maka pertukarkan nilai m dan n.

2.2. Aritmatika Modulo

Aritmatika modulo (modular arithmethic) memainkan peran yang penting dalam komputasi integer, khususnya pada aplikasi kriptografi. Operator yang digunakan pada aritmatika modulo adalah **mod**. Operator mod, jika digunakan pada pembagian bilangan bulat meberikan sisa pembagian sebagai kembaliannya. Sebagai contoh 53 mod 5 meberikan hasil = 10 dan sisa = 3. Maka 53 mod 5 = 3. Definisi dari operator mod adalah sebagai berikut

Misalkan a adalah bilangan bulat dan m adalah bilangan bulat > 0. operasi a mod m memberikan sisa jika a dibagi dengan m. Dengan kata lain a mod m = r sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$

2.2.1. 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 mosulo m** dan dilambangkan sebagai

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

(notasi '≡' dibaca kongruen)

Jika a tidak kongruen dengan b dalam modulus m, maka ditulis :

$$a \not\equiv b \pmod{m}$$

Sebagai contoh 53 mod 5 = 3 dan 13 mod 5 = 3, maka 53 ≡ 13 (mod 5).

Definisi formal dari kekongruenan dinyatakan sebagai berikut.

Misalkan a dan b adalah bilangan bulat dan m adalah bilangan > 0 maka a ≡ b (mod m) jika m habis membagi a – b

Sifat-sifat perhitungan pada aritmatika modulo, khususnya terhadap operasi perkalian dan penjumlahan, dinyatakan sebagai berikut.

Misalkan m adalah bilangan bulat positif

1. Jika a ≡ b (mod m) dan c adalah sembarang bilangan bulat maka
   i. (a+c) ≡ (b+c) (mod m)
   ii. ac ≡ bc (mod m)
   iii. $a^p \equiv b^p \pmod{m}$ untuk p bilangan bulat > 0
2. Jika a ≡ b (mod m) dan c ≡ d (mod m), maka
   i. (a+c) ≡ (b+d) (mod m)
   ii. ac ≡ bd (mod m)

2.2.2. Chinese Remainder Problem

Pada abad pertama, seorang matematikawan china yang bernama Sun Tse mengajukan pertanyaan sebagai berikut.

Tentukan sebuah bilangan bulat yang bila dibagi dengan 5 menyisakan 3, bila dibagi 7 menyisakan 5, dan bila dibagi 11 menyisakan 7.

Pertanyaan tersebut dapat dirumuskan sebagai berikut

$$X \equiv 3 \pmod{5}$$
$$X \equiv 5 \pmod{7}$$
$$X \equiv 7 \pmod{11}$$

Teorema Chinese Remainder berikut akan digunakan untuk menyelesaikan sistem di atas

Misalkan m_1, m_2, ...,m_n adalah bilangan bulat positid sedemikian sehingga PBB(m_i,m_j) = 1 untuk $i \neq j$. Maka sistem kongruen lanjar

$$X \equiv a_k \pmod{m_k}$$

Mempunyai sebuah solusi unik untuk modulo $m = m_1 . m_2 . m_3$

Solusi akan dicari sebagai berikut. Solusi modulo tersebut m = 5 . 7 . 11 = 5 . 77 = 11 . 35. Karena 77 . 3 ≡ 1 (mod 5), 55 . 6 ≡ 1 (mod 7), dan 35 . 6 ≡ 1 (mod 11), solusi unik dari sistem kongruen tersebut adalah

$$X \equiv (3 . 77 . 3 + 5 . 55 . 6 + 7 . 35 . 6) \pmod{385}$$
$$\equiv 3813 \pmod{385}$$
$$\equiv 348 \pmod{385}$$

2.3. Bilangan Prima

Bilangan bulat positif yang mempunya 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. Secara formal definisi dari bilangan prima adalah sebagai berikut.

Bilangan bulat positif p (p > 1) disebut bilangan prima jika bilangan yang habis membaginya hanya 1 dan p.

Sebagai contoh adalah bilangan 13. Bilangan 13 hanya habis dibagi 1 dan 13. Maka 13 adalah bilangan prima.

Bilangan selain prima adalah bilangan komposit. Misalnya 12 adalah bilangan yang dapat habis dibagi 1,2,4,6,12.

Teorema penting menyangkut bilangan prima dinyatakan oleh teorema yang terkenal dalam

teori bilangan yaitu teorema fundamental aritmatik, yang berisi sebagai berikut

Setiap bilangan bulat positif yang lebih besar atau sama dengan 2 dapat dinyatakan sebagai perkalian satu atau lebih baik bilangan prima maupun bilangan komposit, keduanya dapat dinyatakan sebagai perkalian satu atau lebih faktor prima. Misalnya,

$9 = 3 \times 3$	(2 buah faktor prima)
$100 = 2\times2\times5\times5$	(4 buah faktor prima)
$13 = 13$	(1 buah faktor prima)
$12 = 2\times2\times3$	(3 buah faktor prima)

3. Kriptografi

Aritmatika modulo dan bilangan prima mempunyai banyak aplikasi dalam ilmu komputer salah satu aplikasinya yang terpenting adalah ilmu kriptografi.

Kriptografi (cryptography) berasal dari Bahasa Yunani: "cryptós" artinya "secret" (rahasia), sedangkan "gráphein" artinya "writing" (tulisan). Jadi, kriptografi berarti "secret writing" (tulisan rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Definisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih dari sekadar privacy, tetapi juga untuk tujuan data integrity, authentication, dan non-repudiation.

Definisi yang kita pakai di dalam makalah ini mengutip definisi yang dikemukakan di dalam [SCH96]:

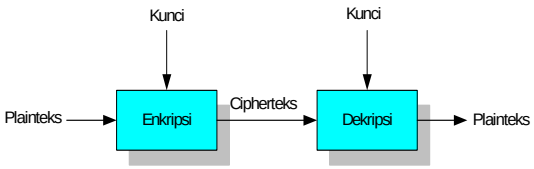
> **Kriptografi** adalah ilmu dan seni untuk menjaga keamanan pesan
> (*Cryptography is the art and science of keeping messages secure*)

Sebagai pembanding, selain definisi tersebut di atas, terdapat pula definisi yang dikemukakan di dalam [MEN96]:

> **Kriptografi** adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi

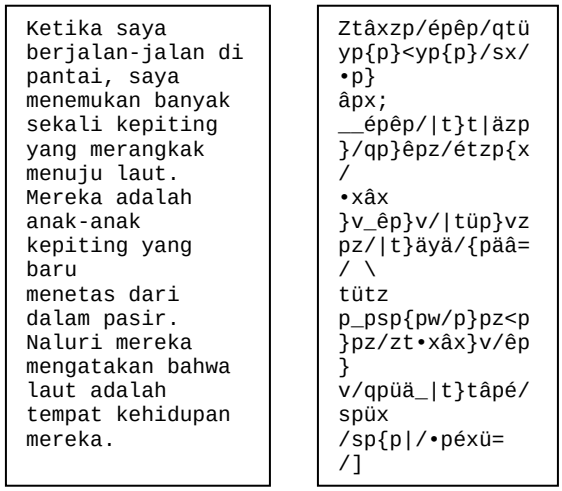
Kata "seni" di dalam definisi di atas berasal dari fakta sejarah bahwa pada masa-masa awal sejarah kriptografi, setiap orang mungkin mempunyai cara yang unik untuk merahasiakan pesan. Cara-cara unik tersebut mungkin berbeda-beda pada setiap pelaku kriptografi sehingga setiap cara menulis pesan rahasia pesan mempunyai nilai estetika tersendiri sehingga kriptografi berkembang menjadi sebuah seni merahasiakan pesan (kata "graphy" di dalam "cryptography" itu sendiri sudah menyiratkan sebuah seni). Kita akan melihat contoh-contoh teknik keriptografi dari zaman dahulu hingga zaman sekarang sehingga kita dapat mamahami bahwa kriptografi dapat dipandang sebagai sebuah seni merahasiakan pesan. Pada perkembangan selanjutnya, kriptografi berkembang menjadi sebuah disiplin ilmu sendiri karena teknik-teknik kriptografi dapat diformulasikan secara matematik sehingga menjadi sebuah metode yang formal.

Dalam kriptografi terdapat beberapa istilah khusus. Pesan yang dirahasiakan dinamakan plainteks (teks jelas dan dapat dimengerti), sedangkan pesan hasil penyamaran disebut chiperteks (teks tersandi). Proses penyamaran dari plainteks ke chiperteks disebut enkripsi dan proses pembalikan dari chiperteks ke plainteks disebut deskripsi. Enkripsi dan deskripsi pada suatu proses penyamaran pesan memiliki suatu kunci tersendiri. Dan hanya orang yang berhak yang mengetahui kunci tersebut. Gambar 1.1 memperlihatkan diagram kedua proses yang dimaksud.



Gambar 1.1

Sebagai contoh, dalam gambar 1.2 sebuah plainteks (sebelah kanan) disandikan menjadi chiperteks (sebelah kiri) dengan suatu teknik kriptografi tersebut.



Gambar 1.2

Chiperteks meskipun sudah tidak bersifat rahasia lagi, namun isinya sudah tidak jelas dan tidak dapat dimengerti maksudnya. Hanya orang yang berhak saja yang dapat mengembalikan pesan tidak jelas tersebut menjadi pesan semula dengan menggunakan suatu kunci.

Kriptografi juga dapat dituliskan dalam notasi matematis. Jika chiperteks dilambangkan dengan C dan plainteks dilambangkan dengan P, maka fungsi enkripsi E memetakan P ke C, dapat ditulis sebagai berikut

$$E(P) = C$$

Pada proses kebalikannya yaitu proses deskripsi, fungsi deskripsi D memetakan C ke P, dapat ditulis sebagai berikut

$$D(C) = P$$

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

$$D(E(P)) = P$$

4. Hubungan Teori Bilangan Bulat dengan Kriptografi

Seperti yang telah diungkapkan diatas bahwa kriptografi sangat erat hubungannya dengan matematika diskrit terutama fungsi dan teori bilangan bulat yang berisi tentang.

- Integer dan sifat-sifat pembagian
- Algoritma Euclidean
- Aritmetika modulo
- Bilangan prima

Hal yang diungkapkan di atas sangat relevan karena saat ini kriptografi modern tidak lagi mendasarkan kekuatan kriptografi pada algoritmanya. Namun kriptografi saat ini mendasarkan kekuatan kriptografinya pada kunci. Sebelum melangkah lebih jauh, alangakah lebih baiknya jika dijelaskan mengenai kekuatan kriptrografi berdasarkan algoritma maupun kunci sebagai berikut.

Algoritma kriptografi atau chipper adalah fungsi matematika yang digunakan untuk enkripsi dan deskripsi. Kekeuatan suatu algoritma kriptografi diukur dari banyaknya kerja yang dibutuhkan untuk memecahkan data chipperteks menjadi plainteksnya. Semakin banyak usaha yang diperlukan, yang berarti semakin banyak waktu yang dubutuhkan, maka semakin kuat algoritma kriptografinya, yang berarti semakin aman digunakan untuk menyandikan pesan.

Jika kekuatan kriptografi ditentukan dengan menjaga kerahasiaan algoritmanya, maka algoritma kriptografinya dinamakan algoritma *restricted*. Misalkan di dalam sebuah kelompok orang meraka sepakat untuk menyadikan setiap pesan-pesan dengan algoritma yang sama, Algoritmanya adalah mempertukarkan setiap kata karakter pertama dengan karakter kedua, karakter ketiga dengan karakter keempat dan seterusnya. Contohnya,

Plainteks : `STRUKTUR DISKRIT`
Chiperteks : `TSURTKRU IDKSIRT`

Untuk mendeskripsikan pesan, algoritma yang sama digunakan kembali. Sayangnya, algoritma restricted tidak cocok saat ini. Bila salah seorang keluar dari kelompok, maka algoritma penyandian pesan harus diubah lagi karena kerahasiaannya tidak lagi dapat diandalkan.

Kriptografi modern tidak lagi mendasarkan kekuatan pada algoritmanya. Jadi algoritma tidak lagi dirahasiakan dan boleh diketahui oleh umum. Kekuatan kriptografinya terletak pada kunci,

yang berupa dereten karakter atau deretan bilangan bulat, dijaga kerahasiaannya. Hanya orang uang mengetahui kunci yang dapat melakukan enkripsi dan deskripsi. Kunci ini analog fungsinya dengan password pada sistem komputer, PIN pada ATM atau kartu kredit. Bedanya jika password bertujuan untuk otorisasi akses, maka kunci pada kriptografi digunakan pada proses enkripsi dan deskripsi.

Kriptografi yang mendasarkan kekuatan pada kunci sering menggunakan dasar teori bilangan bulat diatas sebagai dasar algoritma dan juga kuncinya. Selanjutnaya akan dijelaskan dalam sub bab berikut ini.

4.1. Caesar Chiper

Teknik kriptografi ini digunakan oleh Julius Caesar, kaisar Romawi, untuk menyandikan pesan yang ia kirim kepada gubernurnya. Pada caesar chiper, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan alfabet. Dalam hal ini kuncinya adalah jumlah pergeseran huruf (yaitu 3).

Plainteks p_i :
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 c_i :
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

Dengan mengkodekan setiap huruf alfabet dengan integer: A = 0, B = 1, … , Z = 25, maka secara matematis caesar chiper menyandikan plainteks p_i menjadi c_i dengan aturan sebagai berikut

$$c_i = E(p_i) = (p_i + 3) \bmod 26$$

Persoalan di atas dapat digenerik-an sebagai berikut.

Jika pergeseran huruf sejauh *k*, maka:

Enkripsi: $ci = E(pi) = (pi + k) \bmod 26$
Dekripsi: $pi = D(ci) = (ci - k) \bmod 26$
k = kunci rahasia

Untuk 256 karakter ASCII, maka:

Enkripsi: $ci = E(pi) = (pi + k) \bmod 256$
Dekripsi: $pi = D(ci) = (ci - k) \bmod 256$
k = kunci rahasia

Namun teknik ini memiliki kelemahan yaitu mudah dipecahkan dengan *exhaustive key search* karena jumlah kuncinya sangat sedikit (hanya ada 26 kunci).

4.2. Vigènere Cipher

Algoritma kriptografi ini dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigènere pada abad 16 (tahun 1586).
Vigènere Cipher digunakan oleh Tentara Konfederasi (*Confederate Army*) pada Perang Sipil Amerika (*American Civil war*).
Vigènere Cipher menggunakan Bujursangkar *Vigènere* untuk melakukan enkripsi. Setiap baris di dalam bujursangkar menyatakan huruf-huruf cipherteks yang diperoleh dengan *Caesar Cipher*. Pada dasarnya teknik yang digunakan hampir sama dengan *Caesar Cipher*.

Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik. Bila panjang kunci adalah *m*, maka periodenya dikatakan *m*. Berikut ini contoh penggunaan *Vigènere Cipher*.

kunci = sony
Plainteks :THIS PLAINTEXT
Kunci :sony sonysonys

Hasil enkripsi seluruhnya adalah sebagai berikut:

Plainteks :THIS PLAINTEXT
Kunci :sony sonysonys
Cipherteks : **LVVQ HZNGFHRVL**

Pada dasarnya, setiap enkripsi huruf adalah *Caesar cipher* dengan kunci yang berbeda-beda.

c('T') = ('T' + 's') mod 26 = L
c('H') = ('H' + 'o') mod 26 = V, dst

Keunggulan dari penggunaan *Vignere Cipher* adalah huruf yang sama tidak selalu dienkripsi menjadi huruf cipheteks yang sama pula sehingga lebih sukar untuk mengubah cipherteks menjadi plainteks asal jika tidak mengetahui kuncinya.

4.3. RSA (Rivest-Shamir-Adleman)

Algoritma RSA diperkenalkan oleh tiga orang peneliti dari MIT (Massachussets Institute of Technology), yaitu Ron Rivest, Adi Shamir, dan Len Adleman, pada tahun 1976. RSA mendasarkan proses enkripsi dan deskripsinya pada konsep bilangan prima dan aritmatika modulo. Baik kunci enkripsi maupun kunci deskripsi keduanya merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diketahui umum (sehingga dinamakan juga kunci publik), namun kunci untuk deskripsi bersifat rahasia. Kunci deskripsi dibangkitkan oleh beberapa buah bilangan prima bersama-sama dengan kunci enkripsi. Untuk menemukan kunci enkripsi, seseorang harus memfaktorkan suatu bilangan non proma menjadi faktor primanya. Kenyataannya, memfaktorkan bilangan non-prima menjadi faktor primanya bukanlah pekerjaan yang mudah. Belum ada algoritma yang efisien yang ditemukan untuk pemfaktoran itu. Semakin besar bilangan non-primanya tentu akan semakin sulit menemukan faktor primanya. Semakin sulit pemfaktorannya, semakin kuat pula algoritma RSA. Algoritma RSA sebenarnya sederhana sekali. Secara ringkas, algoritma RSA adalah sebagai berikut.

Algoritma RSA

1. Pilih dua buah bilangan prima sembarang, sebut a dan b. Jaga kerahasiaan a dan b ini.
2. Hitung n = a × b. Besaran n tidak dirahasiakan.
3. Hitung m = (a – 1) × (b – 1). Sekali m telah dihitung, a dan b dapat dihapus untuk mencegah diketahui pihak lain.
4. Pilih sebuah bilangan bulat untuk kunci publik, sebut namanya e, yang relatif prima terhadap m.
5. Bangkitkan kunci deskripsi, d, dengan kekongruenan ed ≡ 1 (mod m). Lakukan enkripsi terhadap isi pesan dengan persamaan $c_i = p_i^{\,e} \bmod n$, 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, …, n – 1 untuk menjamin hasil perhitungan tidak berada di luar himpunan.
6. Proses deskripsi dilakukan dengan menggunakan persamaan $p_i = c_i^{\,d} \bmod n$, yang dalam hal ini d adalah kunci deskripsi.

Pehatikan bahwa dalam langkah 4 kekongruenan ed ≡ 1 (mod m) sama dengan ed mod m = 1. ed mod m = 1 ekivalen dengan ed = km + 1 sehingga akan menghasilkan persamaan

$$d = (1 + km) / e$$

akan terdapat bilangan bulat k yang menyebabkan persaman diatas memberikan bilangan bulat d.

Kekuatan dan Keamanan RSA

Seperti yang telah dikatakan sebelumnya, kekuatan RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non-prima menjadi faktor primanya, yang dalam hal ini n = a × b. Sekali n berhasil difaktorkan menjadi a dan b maka m = (a – 1) × (b – 1) dapat dihitung. Selanjutnya, karena kunci enkripsi e diumumkan (tidak rahasia), maka kunci deskripsi d dapat dihitung dari persamaan e × d ≡ 1 (mod m). Ini berarti proses deskripsi dapat dilakukan oleh orang yang tidak berhak.

Penemu algortima RSA menyarankan nilai a dan b yang dipakai panjangnya lebih dari 100 digit. dengan demikian hasil kali n = a × b akan berukuran lebih dari 200 digit. Bayangkan berapa besar usaha kerja yang diperlukan untuk memfaktorkan bilangan bulat 200 digit menjadi faktor primanya. Menurut Rivest dan kawan-kawan, usaha untuk mencari faktor bilangan 200 digit membutuhkan waktu komputasi selama 4 milyar tahun. (Dengan asumsi bahwa algoritma pemfaktoran yang digunakan adalah algoritma tercepat saat ini dan komputer yang dipakai mempunyai kecepatan 1 milidetik).

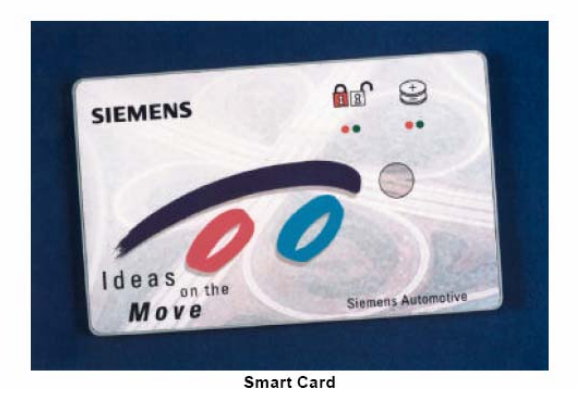
Untunglah algoritma yang paling mangkus untuk memfaktorkan bilangan yang besar belum ditemukan. Inilah yang membuat algoritma RSA tetap dipakai hingga saat ini. Selagi belum ditemukan algoritma yang mangkus untuk memfaktorkan bilangan bulat menjadi faktor primanya, maka algoritma RSA masih direkomendasikan untuk penyandian pesan.

5. Kriptografi Dalam Kehidupan Sehari-hari

Kehidupan kita saat ini dikelililingi oleh kriptografi. Kriptografi sudah digunakan dalam berbagai aplikasi, mulai dari penarikan uang di ATM, penggunaan kartu kredit, penggunaan kartu cerdas (smart card), percakapan dengan telepon genggam, *password* komputer, televisi, transaksi *e-commerce* di internet, sampai pada pengaktifan peluru kendali dan bom nuklir. Bab ini membahas secara ringkas penerapan kriptografi dalam kehidupan sehari-hari.

5.1. Kartu Cerdas (Smart Card)

Salah satu aplikasi yang menggunakan kriptografi adalah kartu cerdas (*smart card*). Kartu cerdas (gambar 1.3) saat ini tumbuh sangat pesat. Kartu cerdas yang mirip dengan kartu kredit dapat melayani banyak fungsi, mulai dari otentikasi sampai penyimpanan data. Dengan menggunakan kartu cerdas, pengguna dapat mengakses informasi dari berbagai peralatan dengan kartu cerdas yang sama.



Gambar 1.3 Sebuah smart card dari Siemens

Kartu cerdas yang paling populer adalah *memory card* dan *microprocessor card*. *Memory card* mirip dengan *floppy disk*, sedangkan *microprocessor card* mirip dengan komputer kecil dengan sistem operasi, sekuriti, dan penyimpanan data. Kartu cerdas mempunyai beberapa jenis antarmuka (*interface*) yang berbeda. Jenis antarmuka yang umum adalah *contact interface*, yang dalam hal ini kartu cerdas dimasukkan ke dalam alat pembaca (*card reader*) dan secara fisik terjadi kontak fisik antara alat dan kartu (Gambar 1.4).

Gambar 1.4 Pembaca kartu cerdas

Kartu cerdas menyimpan kunci privat, sertifikat digital, dan informasi lainnya. Kartu cerdas juga menyimpan nomor kartu kredit dan informasi kontak personal (no telpon). Sertifikat digital ditandatangani oleh *card issuer* (*CA*) untuk mensertifikasi kunci publik pemilik kartu.

Penggunaan kartu cerdas dikombinasikan dengan *PIN* (*Personal Identification Number*). Jadi, ada dua level yang harus dari penggunaan kartu cerdas, yaitu memiliki kartu cerdas itu sendiri dan mengetahui *PIN* yang mengakses informasi yang disimpan di dalam kartu. Komputer *server* mengotentikasi kartu dengan cara mengirimkan suatu nilai atau *string* (yang disebut *challenge*) ke kartu untuk ditandatangani dengan menggunakan kunci privat (yang tersimpan di dalam kartu), lalu tanda-tangan tersebut diverifikasi oleh mesin dengan menggunakan kunci publik pemilik kartu. Komputer *server* perlu menyimpan kunci publik *card issuer* untuk memvalidasi sertifikat digital.

Banyak peralatan *mobile* yang menggunakan kartu cerdas untuk otentikasi. Namun kartu cerdas masih tidak menjamin keamanan secara total. Jika peralatan *mobile* hilang atau dicuri, sertifikat digital dan kunci privat di dalam kartu cerdas (yang terdapat di dalam peralatan tersebut) berpotensi diakses oleh pencuri untuk mengakses informasi rahasia. Telpon seluler dengan teknologi *GSM* memiliki kartu cerdas yang terintegrasi di dalam *handphone*. Pemilik *handphone* memiliki opsi untuk men-set *PIN* untuk proteksi tambahan, sehingga jika *handphone* hilang atau dicuri, *handphone* tidak dapat digunakan tanpa mengetahui *PIN* tersebut.

Kartu cerdas *Wireless Identity Module* (*WIM*) termasuk di dalam *Wireless Application Protocol* (*WAP*). Kartu *WIM* memproteksi komunikasi dan transaksi *mobile* dengan tandatangan digital. Kartu *WIM* menyediakan keamanan untuk sertifikat digital, manajemen kode *PIN*, kunci, dan tanda-tangan digital. *WIM* menyimpan algoritma enkripsi yang diperlukan di dalam kartu cerdas. Semua fungsi yang diperlukan untuk sistem keamanan dan privatisasi dimasukkan ke dalam kartu cerdas.

5.2. Transaksi Melalui Anjungan Tunai Mandiri (ATM)

Anjungan Tunai Mandiri atau *Automatic Teller Machine* (*ATM*) digunakan nasabah bank untuk melakukan transaski perbankan. Utamanya, kegunaan *ATM* adalah untuk menarik uang secara tunai (*cash withdrawal*), namun saat ini *ATM* juga digunakan untuk transfer uang (pemindahbukuan), mengecek saldo, membayar tagihan kartu ponsel, membeli tiket kereta api, dan sebagainya.

Transaksi lewat *ATM* memerlukan kartu magnetik (disebut juga kartu *ATM*) yang terbuat dari plastik dan kode *PIN* (*Personal Information Number*) yang berasosiasi dengan kartu tersebut. *PIN* terdiri dari 4 angka yang harus dijaga kerahasiannya oleh pemilik kartu *ATM*, sebab orang lain yang mengetahui *PIN* dapat menggunakan kartu *ATM* yang dicuri atau hilang untuk melakukan penarikan uang.

arah antara *ATM* dan komputer *host*. *ATM* mengirim *PIN* dan informasi tambahan pada kartu ke komputer *host*, *host* melakukan verifikasi dengan cara membandingkan *PIN* yang di-*entry*-kan oleh nasabah dengan *PIN* yang disimpan di dalam basisdata komputer *host*, lalu mengirimkan pesan tanggapan ke *ATM* yang menyatakan apakah transaksi dapat dilanjutkan atau ditolak.

Selama transmisi dari *ATM* ke komputer *host*, *PIN* harus dilindungi dari penyadapan oleh orang yang tidak berhak. Bentuk perlindungan yang dilakukan selama transmisi adalah dengan mengenkripsikan *PIN*. Di sisi bank, *PIN* yang disimpan di dalam basisdata juga dienkripsi (lihat Gambar 1.5).

Algoritma enkripsi yang digunakan adalah *DES* dengan mode *ECB*. Karena *DES* bekerja dengan mengenkripsikan blok 64-bit, maka *PIN* yang hanya terdiri dari 4 angka (32 bit) harus ditambah dengan *padding bits* sehingga panjangnya menjadi 64 bit. *Padding bits* yang ditambahkan berbeda-beda untuk setiap *PIN*, bergantung pada informasi tambahan pada setiap kartu *ATM*-nya [PIN02].

Karena panjang *PIN* hanya 4 angka, maka peluang ditebak sangat besar. Seseorang yang memperoleh kartu *ATM* curian atau hilang dapat mencoba semua kemungkinan kode *PIN* yang mungkin, sebab hanya ada $10 \times 10 \times 10 \times 10 = 10.000$ kemungkinan kode *PIN* 4- angka. Untuk mengatasi masalah ini, maka kebanyakan *ATM*

Gambar 1.5 Mekanisme enkripsi dan deskripsi *PIN* pada transaksi dengan mesin ATM

PIN digunakan untuk memverifikasi kartu yang dimasukkan oleh nasabah di *ATM*. Proses verifikasi dilakukan di komputer pusat (*host*) bank, oleh karena itu harus ada komunikasi dua

hanya membolehkan peng*entry*-an *PIN* maksimum 3 kali, jika 3 kali tetap salah maka *ATM* akan 'menelan' kartu *ATM*. Masalah ini juga menunjukkan bahwa kriptografi tidak selalu dapat menyelesaikan masalah keamanan data.

Beberapa jaringan *ATM* sekarang menggunakan kartu cerdas sehingga memungkinkan penggunaan kriptografi kunci publik. Kartu *ATM* pengguna mengandung kunci privat dan sertifikat digital yang ditandatangani oleh *card issuer* (*CA*) untuk mensertifikasi kunci publiknya. *ATM* mengotentikasi kartu dengan cara mengirimkan suatu *string* ke kartu untuk ditandatangani dengan menggunakan kunci privat, lalu tanda-tangan tersebut diverifikasi oleh *ATM* dengan menggunakan kunci publik pemilik kartu. Seperti semua sistem yang berbasis sertifikat digital, terminal *ATM* perlu memiliki salinan kunci publik *card issuer* dengan maksud untuk memvalidasi sertifikat digital. Hal ini direalisasikan dengan menginstalasi kunci publik tersebut ke dalam mesin *ATM*.

5.3. Komunikasi dengan Telepon Seluler

Penggunaan telepon seluler (ponsel) atau lebih dieknal dengan nama telepon genggam (*handphone*) yang bersifat *mobile* memungkinkan orang berkomunikasi dari tempat mana saja. Telepon seluler bersifat nirkabel (*wireless*), sehingga pesan yang dikirim dari ponsel ditransmisikan melalui gelombang mikro (*microwave*) atau radio sampai ia mencapai *base station* (*BST*) terdekat, selanjutnya ditransfer ke ponsel penerim. *GSM* merupakan teknologi telepon seluler yang paling banyak digunakan di seluruh dunia.

Karena menyadap sinyal radio jauh lebih mudah daripada menyadap sinyal pada saluran kabel, maka ini berarti *GSM* tidak lebih aman daripada telepon *fixed* konvensional. Untuk membuat komunikasi lewat ponsel aman, maka pesan dienkripsi selama transmisi dari ponsel ke *BST* terdekat. Metode enkripsi yang digunakan adalah metode *cipher* aliran (*stream cipher*).

Masalah keamanan lain adalah identitas penelpon. Operator seluler harus dapat mengidentifikasi suatu panggilan (*call*) dan mengetahui identitas penelpon (apakah penelpon merupakan pengguna/pelanggan dari operator seluler tersebut atau pengguna/ pelanggan dari operator lain).

Jadi, pada *GSM* diperlukan dua kebutuhan keamanan lainnya, yaitu:

1. otentikasi penelpon (*user authentication*), yang merupakan kebutuhan bagi sistem,
2. kerahasiaan (*confidentiality*) pesan (data atau suara), yang merupakan kebutuhan bagi pelanggan,

Dua kebutuhan ini dipenuhi dengan penggunaan kartu cerdas (*smart card*) personal yang disebut kartu *SIM* (*Subscriber Identity Module card*). Kartu *SIM* berisi:

1. identitas pelanggan/pengguna operator seluler berupa *IMSI* (*International Mobile Subscriber Identity*) yang unik nilainya,
2. kunci otentikasi rahasia sepanjang 128-bit yang diketahui hanya oleh operator. Nilai ini digunakan sebagai kunci pada protokol otentikasi dengan menggunakan program enkripsi yang dipilih oleh operator (algoritma *A2*, *A3*, atau *A5*),
3. *PIN* (jika di-set oleh pengguna).
4. Program enkripsi.

Secara keseluruhan, sistem keamanan *GSM* terdiri atas dalam 3 komponen, yaitu:

1. kartu *SIM,*
2. *handset* (pesawat telepon seluler),
3. jaringan *GSM* (seperti jaringan *ProXL*, *Simpati*, *IM3*). Setiap jaringan dioperasikan oleh operatornya masing-masing (*Excelcomindo*, *Telkomsel*, *Satelindo*). Komputer operator (*host*) memiliki basisdata yang berisi identitas (*IMSI*) dan kunci otentikasi rahasia semua pelanggan/pengguna *GSM*.

5.3.1. Otentikasi Penelpon

Otentikasi penelpon dilakukan melalui protokol otentikasi dengan mekanisme *challenge – response*. Ketika pengguna ponsel melakukan panggilan (*call*), identitasnya dikirim ke komputer operator via *BST* untuk keperluan otentikasi. Karena *BST* tidak mengetahui kunci otentikasi kartu *SIM*, dan bahkan tidak mengetahui algoritma otentikasi, maka komputer operator melakukan verifikasi pengguna dengan cara mengirimkan suatu nilai acak (128 bit) yang disebut *challenge* ke *SIM card* penelpon. Kartu *SIM* mengeluarkan *response* dengan cara

mengenkripsi *challenge* 128-bit tersebut dengan menggunakan kunci otentikasi yang terdapat di dalam kartu.

Enkripsi terhadap *challenge* menghasilkan keluaran 128-bit; dari 128-bit keluaran ini hanya 32 bit yang dikirim dari kartu *SIM* ke *BST* sebagai *response*. *BST* meneruskan *response* ke komputer operator. Ketika *response* sampai di komputer operator, komputer operator melakukan perhitungan yang sama dengan yang dilakukan oleh kartu *SIM*; yang dalam hal ini komputer mengenkripsi *challenge* yang dikirim tadi dengan menggunakan kunci otentikasi penelpon (ingat, komputer operator mengetahui kunci otentikasi semua kartu *SIM*), lalu membandingkan hasil enkripsi ini (yang diambil hanya 32 bit) dengan *response* yang ia terima. Jika sama, maka otentikasi berhasil, dan penelpon dapat melakukan percakapan.

Sebagaimana dijelaskan di atas, dari 128-bit hasil enkripsi, hanya 32 bit yang dikirim sebagai *response*. Jadi, masih ada 96 bit sisanya yang hanya diketahui oleh kartu *SIM*, *BST*, dan komputer operator.

5.3.2. Kerahasiaan Pesan

SIM card juga berisi program *stream cipher* (algoritma *A5*) untuk mengenkripsi pesan dari ponsel ke *BST*. Kunci enkripsi panjangnya 64 bit, yang diambil dari 96 bit sisa dari *response SIM card*. Perhatikan bahwa kunci enkripsi 64-bit ini berbeda setiap kali proses otentikasi dilakukan. Hal ini memenuhi prinsip algoritma *OTP* (*one-time pad*).

6. Kesimpulan

Dari paparan di atas, kita dapat menyimpulkan bahwa matematika diskrit khusunya teori bilangan bulat memiliki hubungan yang sangat erat dengan ilmu kriptografi seperti yang telah dijelaskan di atas. Karena dalam dekade terakhir ini komputer digital yang bekerja secara diskrit mengalami perkembangan yang sangat pesat, maka matematika diskrit dan juga kriptrografi juga mengalami perkembangan yang pesat secara langsung.

Ilmu kriptrografi yang saat ini erat hubungannya dengan sistem komputer digital dalam menjaga keamanan dan privasi data, menjadi banyak kita temukan dalam kehidupan sehari-hari karena perkembangan komputer digital itu sendiri. Boleh dikatakan bahwa kehidupan manusia saat ini dikelilingi oleh kriptografi dan juga matematika diskrit. Oleh karena itu, sebagai manusia yang hidup di zaman modern ini, kita diharapkan untuk dapat mengembangkan setidaknya memahami kedua ilmu tersebut.

Daftar Pustaka

[1] Handbook of Applied Cryptography, http://www.cacr.math.uwaterloo.ca/hac/ Diakses tanggal 30 Desember 2006, pukul 14.05 WIB

[2] Munir, Rinaldi. (2004). Diktat Kuliah IF 2153 Matematika Diskrit, Edisi Keempat. Departemen Teknik Informatika, Institut Teknologi Bandung. 2006

[3] Munir, Rinaldi. (2004). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.