MAKALAH MATA KULIAH MATEMATIKA DISKRIT

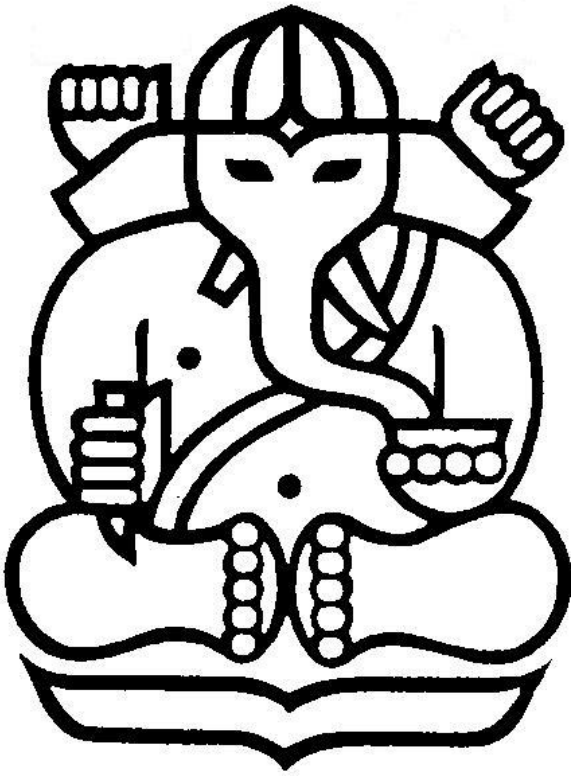
(IF 2152)

KRIPTOGRAFI

Oleh

YURI ANDRI GANI

(13506118)



SEKOLAH TEKNIK ELEKTERO DAN INFORMATIKA

PROGRAM STUDI TEKNIK INFORMATIKA

INSTITUT TEKNOLOGI BANDUNG

2008

BASIS DARI KRIPTOGRAFI

Ketika Julius Caesar mengirimkan pesan pada para jendralnya, ia tidak mau mempercayai si pembawa pesan. Jadi ia mengganti tiap huruf a pada pesannya dengan d dan b dengan e dan begitu seterusnya tiap huruf diganti dengan tiga huruf setelahnya. Maka bahkan si pembawa pesan tidak tahu apa yang dibawanya.

1. Enkripsi dan Dekripsi

   Data yang dapat dibaca tanpa perlakuan ataupun perhitungan apapun disebut, *plaintext*, atau teks sederhana. Metode dalam mengubah teks sederhana dalam suatu aturan tertentu untuk menyembunyikan isinya disebut enkripsi. Mengenkripsi teks sederhana menjadi kode yang tidak dapat dibaca menghasilkan kode. Kita menggunakan enkripsi untuk menyembunyikan data dari orang-orang yang tidak diinginkan, bahkan pada orang yang dapat melihat pesan itu sekalipun. Proses dalam mengembalikan data yang telah terenkripsi menjadi teks sederhana disebut dekripsi.

2. Apa Itu Kriptografi?

   Kriptografi adalah ilmu yang menggunakan matematika untuk mengenkripsi dan dekripsi data. Kriptografi memungkinkan kita untuk mengirimkan data yang rahasia melalui jaringan tidak terjamin dan memastikan bahwa hanya orang yang diinginkanlah yang dapat membacanya.

   Sementara kriptografi adalah ilmu dalam menyembunyikan data maka kriptonalisis adalah ilmu dalam menganalisis kode dan memecahkan datanya. Kriptonalisis memanfaatkan suatu analisis metematika , kombinasi, kesabaran ,dan keberuntungan dalam memecahkan kode enkripsi.

   Kriptografi dan kriptonalisis adalah bagian dari kriptologi.

   a. Kriptografi yang Kuat

      Ada dua kiptografi di dunia ini yaitu kriptografi yang dapat menyembunyikan data dari keluarga, dan yang dapat menyembunyikan data dari pihak pemerintah. Makalah ini adala tentang yan terakhir.

      Kriptografi dapat menjadi lemah atau kuat berdasarkan wakru dan tenaga yang dibutuhkan dalam memecahkannya. Kriptografi kuat sanagt sulit untuk dipecahkan tanpa alat pamecah kode yang tepat. Seberapa sulit? Dengan seluruh kekuatan komputansi dan waktu yang tersedia bahkan tidak akan dapat memecahkan kode tersebut sampai kiamat.

      Orang akan berpikir kalau kriptogarfi tersebut dapat bertahan bakan dengan kriptonalisis yang paling baik sekalipun. Siapa yang tahu, bahkan kriptografi yang terkuat sekarangpun belum tentu dapat bertahan dengan kekuatan komputer dan komputansi besok(ilmu informasi terus berkembang).

   b. Bagaimana Kriptografi Bekerja?

      Algoritma kriptogafi, atau pengkodean adalah fungsi matematika yang digunakan dalam pengenkripsian dan dekripsian data. Algoritma kriptografi bekerja dengan kunci (baik huruf, angka, mauoun phrasa) untuk mengenkripsikan teks sederhana. Teks yang sama dapat menjadi kode yang berbeda dengan kunci yang berbeda. Kekuatan dari sebuah krpitografi tergantung pada rumitnya algoritma dan kerahasiaan dari kunci itu sendiri.

      Algoritma kriptografi, ditambah semua kunci dan protokol yang mungkin membentuk system kripto.

3. Kriptografi Umum

Kriptografi umum atau yang biasa disebut enkripsi kunci rahasia, adalah kriptografi yang menggunakan kunci yan g sama dalam mengenkripsi dan mendekripsi. DES(Data Encryption Standart) adalah contoh dari system kripto yang umum dan diguankan secara luas oleh kebanyakan instansi.

a. Pengkodean Caesar

Sebuah contoh dari kripogarfi yang sangat sederhana, yaitu denagn mengganti huruf dari teks dengan huruf lainnya. Dalam hal ini Julius Caesar mengganti setiap huruf dengan tiga huruf setelahnya. Sebagai contoh kata ”rahasia”, menjadi “udkdvld”. Jadi huruf alabet yang seharusnya berurut ABCDEFGHIJKLMNOPQRSTUVWZXYZ, menjadi DEFGHIJKLMNOPQRSTUVWXYZABC.

Tentu saja pengkodean seperti ini sangat lemah untuk zaman sekarang, tetapi berguna di zaman Julius Caesar dan juga menjelaskan bagaimana kriptografi yang sanagat sederhana itu.

b. Manajemen Kunci Dalam Kriptografi Umum

Kriptografi umum memiliki keuntungan, ia sangat cepat. Ia terutama berguna untuk data yang tidak akan keluar kemana-mana. Bagaimanapun, enkripsi umum saja sangat sangat sulit dalam menjaga kerahasiaan kunci ketika mendistribusikannya.

Untuk pengirim dan dan penerima dalam berkomunikasi secara rahasia dan aman mengguankan kode enkripsi, mereka harus menyepakati bahwa kunci enkripsi aalah rahasia dan tidak boleh diberitahukan pada orang lain siapapun itu.

Apabila kunci itu merupakan sesuatu yang nyata maka mereka harus memastika agar pergiriman kunci berlangsung aman dan tidak ada seorang pun yang tahu, menggunakan sarana yang sangat aman dan terpercaya, atau lebih baik lagi yang sangat tidak umum digunakan agar kunci senantiasa aman. Karena siapapun yang dapat mensabotase dan mencuri kunci dalam pengirimannya dapat dengan mudah mengetahui data rahasia tersebut. Bahkan dapat mengubah dan mengirimkan kembali data yang telah dienkripsi dengan kunci tersebut. Jadi masalah utama dari kriptografi umum sejak dulu kala adalah bagaimana mendistribusikan kunci tanpa dapat di sabotase oleh pihak ketiga.

4. Kriptografi Kunci Pulblik

Masalkah distribusi kunci dapat diselesaikan dengan kriptografi kunci publik, yang konsepnya diperkenalkan oleh Whitfileld Diffie dan Martin Hellman in 1975.

Kriptografi kunci publik menggunakan sepasang kunci untuk proses enkripsi, yang satu bernama kunci publik untuk menenkripsi data, dan satu lagi bermana kunci rahasia untuk mendekripsikannya. Kita mendistribusikan kunci publik dan menyimpan kunci rahasianya. Semua orang yang memiliki kopi dari kunci publik dapat mengenkripsi data yang hanya kita dapat baca. Bahkan orang yang belum pernah kita temui. Adalah hal yang tidak mungkin untuk mencari kunci rahasia dari kunci publik. Setiap orang yang memiliki kunci publik dapat menenkripsi tetapi tidak dapat mendekripsinya.

Keuntungan utama dari sistem ini adalah memungkinkan orang tanpa perjanjian apapun untuk bertukar informasi secara aman. Kebutuhan dari pengirim dan penerima untuk mendistribusikan kunci secara aman dihilangkan, semua komunikasi hanya menggunakan kunci publik, kunci rahasia tidak pernah terlibat, ataupun didistribusikan.

Karena dalam kriptografi konfensional hanya aman apabila kunci aman maka pendristribusian kunci hanya pada orang yang dapat menjaganya, seperti pemerintah ataupun bank besar. Kriptografi publik merupakan salah satu kriptografi kuat yang mampu bertahan pada orang dewasa umum.

5. Kunci

Kunci adalah suatu nilai atau prosedur atau fungsi yang dapat beerja dengan algoritma kriptografi untuk menghasilkan kode tertentu, kunci biasanya bernilai/ukuran sangat besar. Ukuran kunci diukur dalam bits, apabila suatu kunci berukuran 1024 bit kunci itu pastilah sangat luar biasa besar. Dalam kriptografi publik ssemakin besar kunci maka semakin aman datanya.

Bagaimanapun, ukuran kunci publik dan ukuran kunci rahasia sama sekali tidak berhubungan. Ukuran 80 bit untuk kunci rahasia sebanding dengan 1024 bit kunci publik, dan 128 bit kunci rahasia sebanding dengan 3000 bit kunci publik. Lagi, semakin besar kunci maka senakin aman data, tetapi setiap jeni s kriptografi memiliki perbandingan yang bebeda.

Ketika kunci publik dan kunci rahasia bertautan(memiliki keterkaitan), adalah sangat sulit untuk mengekstrak kunci rahasia dengan hanya manggunakan kunci publik, walaupun itu mungkin saja dengan cukup waktu dan tenaga. Hal ini membuat sangat penting untuk memilih kunci dengan ukuran yang tepat, cukup besar untuk menjaga kerahasiannya dan cukup kecil untuk dapat diproses secara cepat. Terakhir kita harus mampu memperkirakan orang yang mencoba menyadap informasi dari kita, seberapa hebat mereka, seberapa banyak waktu mereka, dan seberapa baik alat yang mereka miliki.

Kunci yang besar akan secara kriptologi aman untuk waktu yang lebih lama, kalau yang ingin dienkripsikan adalah data yang harus terjaga selama beberapa tahun maka ukuran kunci haruslah sangat besar(juga tergantung pada orang yagm berupaya mendekripsikannya), tentu saja siapa yang tahu erapa lama waktu untuk mendekripsikan kode tersebut dengan komputer esok hari. Pernah ada zaman dimana kunci 56 bit merupakan kunci yang tak mungkin terpecahkan.

6. Tanda pengenal digital

Keuntungan utama dari kriptografi kunci publik ialah memungkinkan adanya penggunaan tanda pengenal digital. Tanda pengenal digital memungkinkan si penerima untuk memastikan kebenaran dan keaslian dari informasi yang disampaikan. Hal ini juga menyebabkan si pengirim tidak dapat menyangkal bahwa ia tidak sebenarnya tidak mengirim informasi tersebut.

Tanda pengenal digital memiliki kegunaan yang sama dengan tanda tangan. Bagaimanapun tanda tangan sangat mudah untuk dipalsukan. Tanda pengenal digital lebih baik dari tanda tangan dan hampir mustahil untuk ditiru, dan ini juga memastikan identitas dari si pengirim.

Beberapa orang memilih untuk menggunakan tanda pengenal digital dari pada menggunakan enkripsi, sebagai contoh kita mungkin tidak begitu peduli jika seseorang tahu kita pnya satu miliar dalam tabungan, tapi kita pasti ingin memastikan kalau yang menghubungi kita adalah benar-benar petugas bank.

Dasar dari penggunaan tanda pengenal digital ialah kebalikan dari kriptografi kunci publik, yaitu kita menenkripsi dengan kunci rahasia dan mendekripsi dengan kunci publik jadi tiap yang memiliki kunci dapat melihat data yang telah tertanda olehkita.

DAFTAR PUSTAKA

Khan, David. *Intoductoin to kriptography*, www.indocisc.com

Bsmbenek, John C.A. , *Defeating Encryptios:Security Is More Than Just a Good Crypto*. Coordinated Sience Lab. Univercity od Illinois