VOL. II. NO. 1. MARET 2001 ISSN:1411-3201

JURNAL ILMIAH DASI

DATA EKONOMI, BISNIS DAN TEKNOLOGI INFORMASI

AKADEMI MANAJEMEN INFORMATIKA DAN KOMPUTER
"AMIKOM" YOGYAKARTA

KRIPTOGRAFI

Arief Setyanto

Jaringan komputer merupakan kemajuan yang telah di capai oleh bidang informatika yang menyediakan banyak peluang baru. Kemampuan komputer untuk saling bertukar data satu dengan yang lain telah menciptakan berbagai peluang bisnis gaya baru yang saat ini di beri label 'E' dari E-Commerce,E-Banking sampai banyak hal yang di beri label E di depannya menjadi laku. Suatu proses bisnis berlabel 'E' tadi hanya dapat terlaksana secara aman (secure) hanya jika di jamin dengan adanya mekanisme penyandian data yang memadai.

Perlu di ketahui disini bahwa protokol TCP/IP yang dipakai sebagai protokol standard saat ini tidak memiliki security sama sekali. Artinya jika anda mengirimkan text bertuliskan 'Ini Rahasia' kepada saya dan anda tahu persis alamat IP saya maka sebenarnya semua komputer yang berada satu jaringan dengan anda bisa membaca pesan itu. Bayangkan jika yang dikirim adalah nomor kartu kredit anda lewat internet, maka berarti anda memberi peluang semua orang yang terhubung dengan jaringan internet tersebut untuk mengetahui nomor kartu kredit anda. Pendek kata 'Tidak aman'.

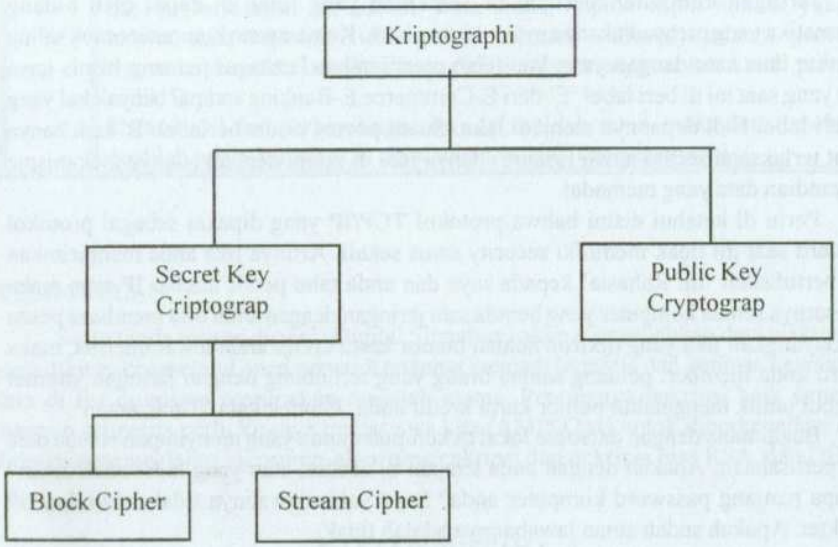
Bagaimana dengan database lokal di komputer anda yang menyimpan semua data aset perusahaan. Apakah dengan anda simpan di access, atau yang lain sudah aman? Berapa panjang password komputer anda? Saya yakin jawabnya tidak lebih dari 59 karakter. Apakah sudah aman jawabannya adalah tidak.

Agar semua menjadi aman perlu kiranya ditambahkan kunci rahasia untuk data data yang penting. Semakin rumit kunci tentunya semakin baik. Dengan demikian diharapkan anda tidak terancam kedudukannya hanya karena daftar gaji karyawan anda bocor, atau data data marketing anda tercecer sehingga pesaing anda dengan mudah mengambil pasar yang anda bidik. Dalam makalah ini akan dibahas bagaimana cara menyandikan data dengan beberapa algoritma penyandia

A. PENDAHULUAN

Penyandian data merupakan usaha untuk mengubah data asli yang biasa di kenal dengan *plain text* menjadi data yang tersandikan yang biasa disebut *chiper text*. Proses mengubah plain text menjadi chiper text disebut **Enkripsi.** Untuk melakukan enkripsi diperlukan **kunci** enkripsi.Chiper text harus bisa diubah kembali menjadi data aslinya atau plain text, proses ini disebut **dekripsi**.

Banyak cara untuk melakukan penyandian data, dari model penyandian yang telah digunakan sejak jaman romawi sampai dengan yang paling mutakhir. Dari banyak metode tersebut secara garis besar akan kita bagi menjadi dua golongan besar yaitu penyandian dengan kunci rahasia (*secret key cryptography*) dan penyandian dengan kunci umum (*public key criptographi*). Untuk lebih jelasnya dapat dilihat pada gambar di bawah ini:

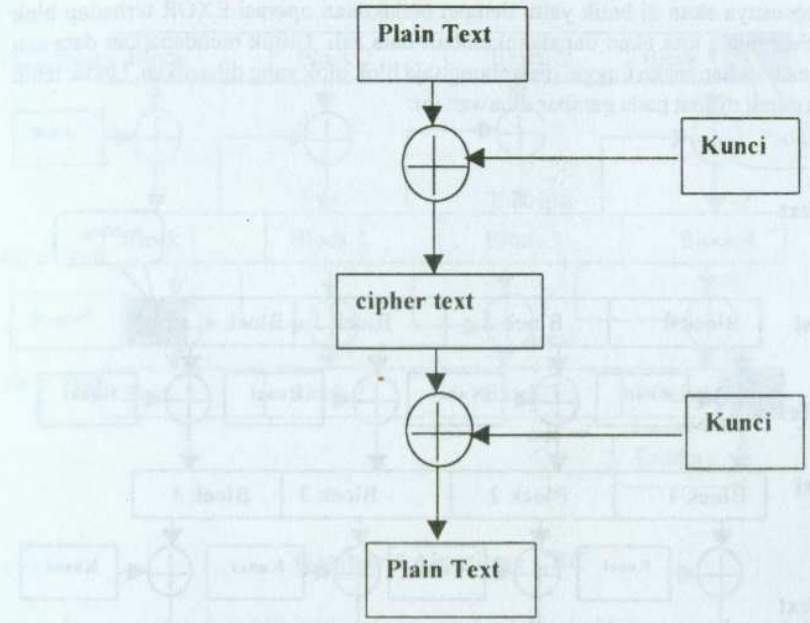


Gambar 1

Secret key cryptographi berkembang sejak zaman dahulu dan di pakai oleh angkatan bersenjarta romawi kuno sampai jerman pada perang dunia 2. Sedangkan public key cryptography berkemang baru 30 tahun terakhir menjawab tantangan perkembangan pertukaran data antar komputer melalui jaringan.

B. PENYANDIAN DENGAN KUNCI RAHASIA (*secret key cryptography*)

Penyandian dengan kunci rahasia mensyaratakan kunci untuk melakukan enkripsi dan melakukan dekripsi **harus sama**. Prosesnya seperti gambar dibawah ini:



Gambar 2

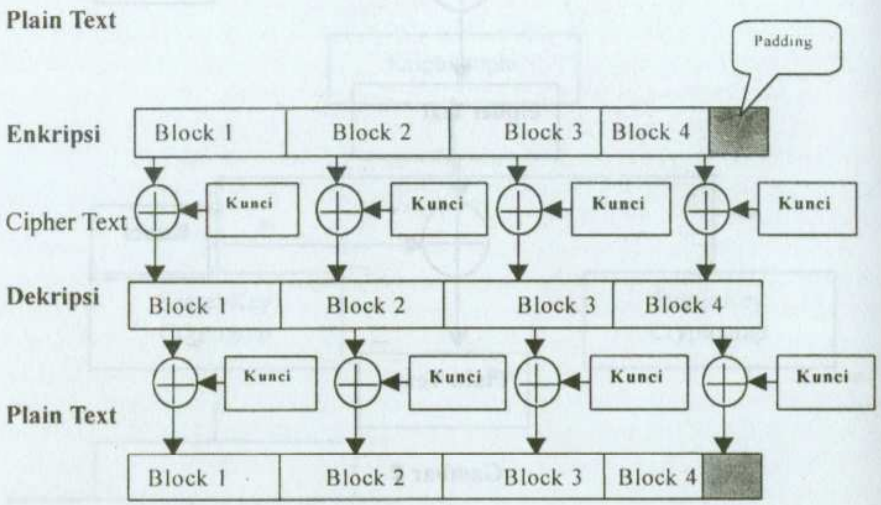
B.1 Block Cipher

Block cipher akan melakukan pembagian plain text menjadi block block text yang akan disandikan per block. Kunci yang disediakan dalam jumlah bit tertentu misalnya 64 bit. Data yang akan dienkripsi akan di bagi bagi menjadi blok yang panjangnya 64 bit juga. Jika kita memiliki data yang jumlah bitnya bukan kelipatan 64 bit misalnya 158 bit maka untuk membuat blok yang ketiga menjadi 64 bit ditambah dengan data yang acak sebanyak 34 bit agar blok ketiga menjadi 64 bit. Data yang ditambahkan merupakan sampah disebut ***padding***. Setelah kita mendapatkan blok blok yang berasal dari hasil pembagian data asli blok blok data tersebut kita enkripsi blok demi blok menjadi beberapa blok cipher text. Untuk melakukan enkripsi ini ada dua contoh algoritma yang ingin dipaparkan dibawah ini:

B.1.1 Electronic Code Block (EBC)

Algoritma EBC ini pertama akan membagi text menjadi blok blok data kemudian masing masing blok operasikan EXOR dengan kunci. Pada saat melakukan dekripsi

maka prosesnya akan di balik yaitu dengan melakukan operasi EXOR terhadap blok blok cipher maka kita akan dapatkankembali data asli. Untuk mendapatkan data asli secara keseluruhan maka tinggal disambung saja blok blok yang dihasilkan. Untuk lebih jelasnya dapat dilihat pada gambar dibawah ini:

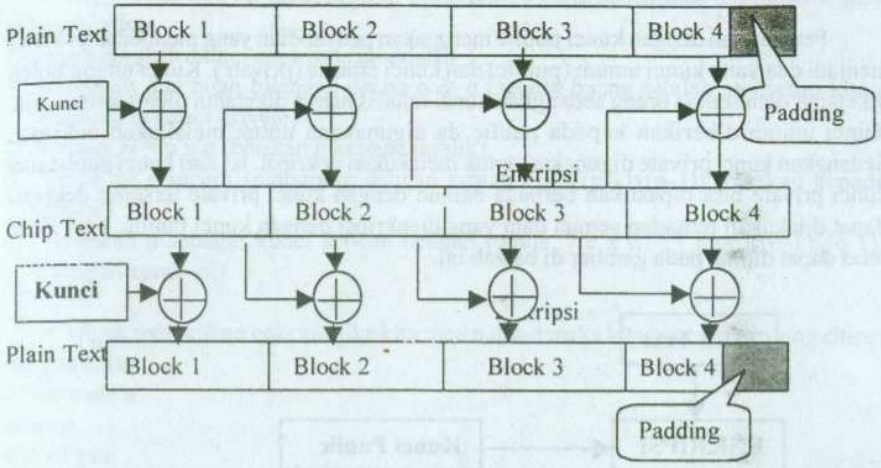


Gambar 3 Algoritma EBC

Kelemahan dari algoritma ini ialah kita tidak dapat mendeteksi jika ada keteputusan proses ekripsi maupun dekripsinya karena tidak ada kaitan antara blok yang pertama dengan blok yang kedua dan seterusnya. Oleh kerena itu jika yang di dekrip hanya sampai blok ketiga saja pada contoh diatas maka tidak akan terdeteksi.

B.1.1 Cipher Block Chaining(CBC)

Untuk memperbaiki kelemahan pada algoritma EBC disuluakn algoritma CBC yang mengkaitkan antara hasil enkripsi blok pertama dengan enkripsi blok berikutnya.



Gambar 4 Algoritma CBC

Dengan cara diatas jika diketahui terutus salah satu blok saja pada saat dekripsi maka tidak dapat didapatkan text aslinya dan bisa terdeteksi.

B.1 Stream Cipher

Stream chiper merupakan metode penyandian data bit per bit, text akan dibaca bit –perbit kemudian dilakukan operasi EXOR dengan kunci. Operasi ini biasanya dilakukan jika data akan di kirimkan melalui media komunikasi serial. Pada metode ini idealnya setiap jumlah bit kunci sebanyak jumlah bit data. Ada beberapa algoritma yang dikenal untuk metode stream cipher ini namun pada dasarnya semuanya melakukan enkripsi dengan cara :

Ci=Mi Ki

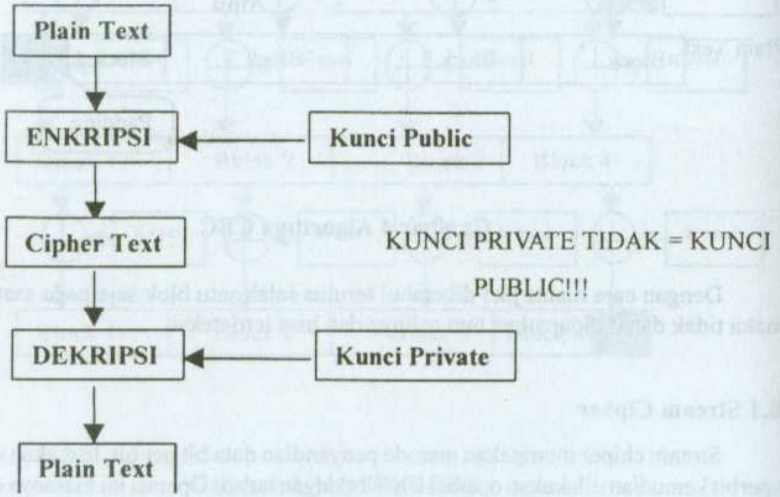
Dimana

Ci = bit ke i dari cipher text
Mi = bit ke i dari Plain text
Ki =bit ke i dari kunci

Beberapa algoritma yang menjadi varian metode ini hanya berbeda pada cara mencari kunci ke i yang diusahakan acak.

C. PENYANDIAN KUNCI UMUM (*Public key Cryptography*)

Penyandian dengan kunci public merupakan penyandian yang menbedakan kunci menjadi dua yaitu kunci umum (public) dan kunci rahasia (private). Kunci umum boleh diketahui oleh semua orang sedangkan kunci rahasis hanya diketahui oleh seorang saja. Kunci umum diberikan kepada public da digunakana untuk melakukan enkripsi. Sedangkan kunci private digunakan untuk melakukan dekripsi. Isi dari kunci public dan kunci private bisa dipastikan berbeda namun dengan kunci private tersebut dekripsi dapat dilakukan terhadap semua data yang dienkripsi dengan kunci public. agar lebih jelas dapat dilihat pada gambar di bawah ini.



GAMBAR 5 Public Key Cryptography

Dari gambar diatas dapat dilihat bahwa pemilik kunci private dapat melakukan dekripsi terhadap semua cipher text yang menggunakan kunci public tetapi pemilik kunci public tidak dapat melakukan dekripsi terhadap cipher text. jadi kunci public hanya bisa digunakan untuk melakukan enkripsi sedangkan kunci private hanya dapat digunakan untuk melakukan Dekripsi. Sampai sejauh ini ide ini sepertinya mustahil tapi ini bisa terjadi dengan sedikit matematika. Ada beberapa contoh cryptography yang menggunakan metode ini yang terkenal diantaranya adalah RSA (Ron Rivest, Adi Shamir, and Leonard Adleman) yang ditemukan pada tahun 1978 yang akan dijadikan contoh pada pembahasan ini.

Algoritma RSA ini menyediakan kunci public yang merupakan perkalian 2 buah bilangan prima.

Langkah langkah dalam algoritma ini adalah

1. Tentukan dua buah bilangan prima p & q (segera buang setelah mensetup kunci publik dan kunci private)
2. Hitung N = p x q (berikan n kepada publik)
3. Tentukan e secara sembarang dengan syarat $1<e<((p-1)x(q-1))$ (berikan kepada publik)
4. Tentukan d sebagai kunci private dengan rumus $e \times d = 1 \bmod ((p-1)x(q-1))$ (simpan kunci ini)

Untuk melakukan enkripsi jika kita tahu n dan e maka kita bisa menghitung chiper dengan cara:

$C=M^e \bmod n$

dimana

C = chiper

M = data

n,e=kunci public yang diberikan

Sedangkan untuk melakukan dekripsi maka akan dipergunakan kunci private d dengan cara:

$M=C^d \bmod n$

dimana

C = chiper

M = data

d=kunci private

Contoh

1. di pilih p=11 dan Q=3
2. N=11x3 =33
3. $1<e<(11-1)(3-1) \Rightarrow 1<e<20$ dan kelipatan pembagi terbesar (e,20)=1 misal dipilih e=3
4. Hitung d dimana $3 \times d = 1 \bmod 20 = 1$
   d=7 karena $3 \times 7 = 21 \bmod 20 = 1$

Misalnya ada seseorang yang melakukan enkripsi dengan kunci publik e=3 dengan data M=5

$C=5^3 \bmod 33$

C = 26

Maka dengan kunci private dapat dihitung Message asli M

$M=26^7 \bmod 33$

$M=5$

Dengan public key cryptography ini dijamin orang orang yang tahu kunci public tidak dapat melihat data asli. jadi data dijamin hanya dapat dibaca oleh penerima yang memiliki legalitas untuk membaca dengan kunci private.

D. PENUTUP

Kriptografi adalah sebuah cabang informatika yang memegang peran kunci di dalam era perdagangan melalui internet. Dengan kriptography faktor keamanan data baik yang berada di komputer lokal anda maupun data data yang dikirimkan melelui jaringan akan aman. Aplikasi secret key kriptografi biasanya lebih berguna untuk mengamankan data data pada komputer lokal anda. Sedangkan public key kriptography sangat berguna untuk mengamankan pertukaran data.

Disamping kriptografi, aspek lain yang perlu diperhatikan pada komunikasi data adalah kompresi data dan koreksi error atau yang lebih dikenal dengan (*error correcting code*).

Kriptografi di masa yang akan datang akan selalu dituntut untuk menemukan cara cara baru, algoritma algoritma baru karena setiap saat harus menjamin keamanan data. Keamana data ini menjadi sangat krusial karena setiap saat orang juga berlomba untuk memecahkan kode kode text rahasia dengan berbagai cara.Salah satu contoh kasus adalah terbongkarnya DES (*Data Encryption Standard*) dalam waktu 30 jam yang jelas membuat orang harus mencari metode baru untuk melakukan enkripsi. Kiranya akan menjadi topik riset yang sangat menarik di masa yang kana datang.

DAFTAR PUSTAKA

1. A menezes, P. van Orschoot, S. Vanstoone, **Handbook Of Cryptography,** CRC Press,1996
2. Francis Litterio, **The Mathematical Guts of RSA Encryption,** http://world.std.com/~franl/crypto/rsa-guts.html, 1999
3. Volker Muller,DR.,**Materi Kuliah Komunikasi Informasi**,UGM,2000