Studi dan Aplikasi Kriptografi pada Kehidupan Sehari-hari

Anggi Shena Permata / 13505117
Program studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknonogi Bandung
Jl. Ganesha10, Bandung
E-mail : if15117@students.if.itb.ac.id

Abstrak

Ketika kita bekerja dengan data bersama atau dalam komputer yang terhubung dalam jaringan umum, maka penting sekali untuk melindungi file data kita dari akses orang-orang yang tidak kita kehendaki. Salah satu metode melindungi file data dan membatasi akses terhadapnya adalah dengan menggunakan Kriptografi. Banyak sekali aplikasi dari Kriptografi ini yang telah digunakan pada masyarakat kita, khususnya perusahaan-perusahaan dan lembaga-lembaga yang sangat membutuhkan keamanan yang terjamin dalam proses pemindahan ataupun pengaksesan data. Makalah ini membahas tentang beberapa aplikasi Kriptografi dalam dunia kita saat ini, mulai dari yang sangat sederhana yang biasa diajarkan pada anak sekolah dasar melalui kegiatan Pramuka yaitu sistem sandi Vigenère sampai pada aplikasi Kriptografi yang lebih rumit yang biasa digunakan oleh perusahaan-perusahaan atau lembaga-lembaga yang sangat mementingkan keamanan dalam pemorosesan data-data yang mereka miliki. Sistem sandi Vigenère adalah sistem sandi substitusi multi-alfabet, yaitu sistem sandi Caesar tetapi dengan pergeseran alfabet yang berlainan disesuaikan dengan kata kuncinya. Yang dimaksud sistem sandi substitusi adalah menyandi dengan cara mengganti huruf-huruf pesan/teks aslinya dengan huruf-huruf sandi. Sistem sandi Caesar dan Viginère termasuk metode sistem sandi ini. Bahkan sistem sandi substitusi merupakan sistem sandi yang dipakai pula dalam kriptografi modern, dengan variasi-variasi yang terus berkembang.

Latar Belakang

Seiring dengan perkembangan jaman dan kemajuan teknologi yang sangat pesat, makin banyak juga orang dan computer yang terhubung dalam dunia maya yang biasa kita kenal dengan sebutan Internet. Tidak mau ketinggalan, perusahaan, lembaga-lembaga pemerintahan , lembaga-lembaga keuangan dan masih banyak lembaga lainnya yang juga turut berkecimpung dalam dunia maya ini. Banyak hal yang dapat dilakukan melalui internet untuk mempermudah hubungan antar lembaga tersebut. Salah satunya adalah penyampaian dan pemerolehan data dari pihak satu ke pihak lain ataupun penyampaian data yang dapat diakses oleh public. Dikarenakan hal tersebut, meka keamanan dalam proses pemindahan data amat sangat diperlukan. Kriptografi merupakan salah satu jawaban atas tutuntutan tersebut. Kriptografi adalah ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan ditransfer dari suatu tempat ke tempat lain, ada kemungkinan bahwa data tersebut dapat diambil atau bahkan dimodifikasi oleh pihak-pihak yang tidak diinginkan. Dalam hal tersebut, Kriptografi sangatlah berperan dalam menjadikan pesan-pesan yang dikirim tersebut menjadi pesan yang tidak dapat dimengerti oleh pihak lain. Kriprografi/penyandian termasuk metode pengamanan yang tangguh. Disebut tangguh karena, sekali data tersebut disandikan dengan algoritma sandi yang baik, data tersebut akan tetap aman kendati setiap orang dapat mengaksesnya secara bebas. Dan selama algoritma sandi tersebut tetap terjaga, data yang disandikan akan tetap aman.

I. Kriptografi

I.1. Pendahuluan

Dalam era masyarakat berbasis informasi, data base merupakan komponen yang sangat vital. Sehingga memerlukan pengamanan yang baik saat didistribusikan ataupun saat disimpan. Salah satu metode pengamanan data adalah dengan menerapkan kriptografi/penyandian.

Kriprografi /penyandian termasuk metode pengamanan yang tangguh. Disebut tangguh karena, sekali data tersebut disandikan dengan algoritma sandi yang baik, data tersebut akan tetap aman kendati setiap orang dapat mengaksesnya secara bebas. Dan selama algoritma sandi tersebut tetap terjaga, data yang disandikan akan tetap aman.

Konsep dari kriptografi adalah mengacak data (teks asli) dengan suatu metode tertentu (algoritma sandi) dan setelah menerapkan sebuah kunci rahasia maka akan menjadi kumpulan karakter yang tidak bermakna (teks sandi). Misalnya teks asli: pengalaman adalah guru yang terbaik. Setelah disandikan dengan algoritma sandi *xyz* dan dengan kunci *pqr* menjadi teks sandi: V5(tjg$gjbvBGd1297j?òè156a8U8A7£+Y.
Proses ini disebut penyandian dan proses sebaliknya disebut membuka sandi.

Dalam prakteknya kriptografi digunakan untuk melindungi kerahasiaan data dan menjamin integritas data.

melindungi kerahasiaan data

Kriptografi biasanya hanya diterapkan pada data-data yang dinilai penting dan sensitif, yang perlu dilindungi dari akses pihak-pihak yang tidak diinginkan dan dari potensi ancaman pencurian oleh pihak-pihak yang memperoleh akses terhadapnya. Secara prinsip, keamanan data yang disandi sangat tergantung dari terjaganya kerahasiaan kunci dan algoritma sandinya.

Dapat dikatakan bahwa kriptografi hanya mengubah masalah keamanan. Yaitu mengubah dari melindungi data rahasia (besar,kompleks dan banyak) menjadi melindungi algoritma sandi dan kunci (satu hal).

menjamin integritas data

Biasanya data-data dilindungi baik kerahasiaannya maupun integritasnya. Tetapi terkadang data tertentu tidak perlu dirahasiakan namun perlu dijaga integritasnya. Kriptografi dapat juga digunakan untuk menjamin integritas data yaitu agar data tidak dimanipulasi oleh pihak-pihak yang tidak diinginkan.

Kriptografi tidak menjamin keamanan 100 %, sebab tidak ada pengamanan yang sempurna. Perkembangan teknologi pengamanan selalu diimbangi dengan teknologi untuk membongkar keamanan yang diterapkan. Selain itu tingkat kesadaran individu yang bersentuhan dengan data-data yang diamankan tersebut, sangat menentukan lambat atau cepatnya sebuah pengamanan terbongkar.

I.2. Sejarah Kriptografi

Kriptografi mempunyai sejarah yang panjang, mulai dari kriptografi Caesar yang berkembang pada zaman sebelum Masehi sampai kriptografi modern yang digunakan dalam komunikasi antar komputer diabad 20.

Kata kriptografi sendiri berasal dari bahasa Yunani, yaitu kryptós yang berarti tersembunyi, dan gráphein yang berarti menulis. Jadi Kriptografi berarti penulisan rahasia. Ada dua cara yang paling dasar pada kriptografi klasik.

Yang pertama adalah transposisi. Transposisi adalah mengubah susunan huruf pada plaintext sehingga urutannya berubah. Contoh yang paling sederhana adalah mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik.

Cara kedua adalah cara substitusi yaitu setiap huruf pada plaintext akan digantikan dengan huruf lain berdasarkan suatu cara atau rumus tertentu. Ada dua macam substitusi yaitu polyalphabetic substitution cipher dan monoalphabetic substitution cipher. Pada polyalphabetic substitution cipher, enkripsi terhadap satu huruf yang sama bisa menghasilkan huruf yang berbeda sehingga lebih sulit untuk menemukan pola enkripsinya. Pada

monoalphabetic substitution cipher maka satu huruf tertentu pasti akan berubah menjadi huruf tertentu yang lain, sehingga pola enkripsinya lebih mudah diketahui, karena satu huruf

pada ciphertext pasti merepresentasikan satu huruf pada plaintext. Salah satu contoh cara substitusi adalah dengan dengan pergeseran huruf.

Pada masa itu, sekitar tahun 1500-an atau 1600-an, kriptografi klasik seperti ini dianggap sudah cukup aman, karena belum banyak orang yang bisa menulis atau membaca. Kriptografi dilakukan terhadap huruf-huruf yang membentuk plaintext, mengubahnya dalam huruf lain kemudian dikirimkan ke pada penerimanya. Penerima harus mengetahui cara menyamarkan berita agar bisa mendapatkan berita aslinya kembali.

Artikel tentang kriptografi klasik ini dibuat sebagai pengenalan terhadap kriptografi yang akan dipublikasikan pada artikel berikutnya yaitu kriptografi modern. Kriptografi modern banyak digunakan dalam pengiriman informasi melalui Internet. Kriptografi modern berkembang bersamaan dengan berkembangnya teknologi komputer dan teknologi jaringan. Seperti sudah dikatakan sebelumnya, pada kriptografi klasik, dua cara digunakan yaitu transposisi dan substitusi. Pada kriptografi modern, digunakan algoritma matematika yang juga pada akhirnya akan menyebabkan terjadinya transposisi dan substitusi pada plaintext sama seperti pada kriptografi klasik.. Hanya bedanya, transposisi dan substitusi huruf pada kriptografi modern dilakukan dengan bantuan komputer menggunakan algoritma matematika yang cukup rumit. Prinsip dasar dari kedua kriptografi sama yaitu melakukan transposisi dan substitusi pada huruf-huruf plaintextnya untuk menghasilkan suatu ciphertext.

I.2. Prinsip Kerja Kriptografi

Kriptografi adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi dapat memenuhi kebutuhan umum suatu transaksi:

1. Kerahasiaan (*confidentiality*) dijamin dengan melakukan enkripsi (penyandian).
2. Keutuhan (*integrity*) atas data-data pembayaran dilakukan dengan fungsi *hash* satu arah.
3. Jaminan atas identitas dan keabsahan (*authenticity*) pihak-pihak yang melakukan transaksi dilakukan dengan menggunakan *password* atau sertifikat digital. Sedangkan keotentikan data transaksi dapat dilakukan dengan tanda tangan digital.
4. Transaksi dapat dijadikan barang bukti yang tidak bisa disangkal (*non-repudiation*) dengan memanfaatkan tanda tangan digital dan sertifikat digital.

Pembakuan penulisan pada kriptografi dapat ditulis dalam bahasa matematika. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi. **Enkripsi** adalah proses mengubah suatu pesan asli (*plaintext*) menjadi suatu pesan dalam bahasa sandi (*ciphertext*).

$C = E(M)$

dimana

M = pesan asli
E = proses enkripsi
C = pesan dalam bahasa sandi (untuk ringkasnya disebut sandi)

Sedangkan **dekripsi** adalah proses mengubah pesan dalam suatu bahasa sandi menjadi pesan asli kembali.

$M = D(C)$
D = proses dekripsi

Umumnya, selain menggunakan fungsi tertentu dalam melakukan enkripsi dan dekripsi, seringkali fungsi itu diberi parameter tambahan yang disebut dengan istilah kunci.

Jenis-jenis serangan

Selain ada pihak yang ingin menjaga agar pesan tetap aman, ada juga ternyata pihak-pihak yang ingin mengetahui pesan rahasia tersebut secara tidak sah. Bahkan ada pihak-pihak yang ingin agar dapat mengubah isi pesan tersebut. Ilmu untuk mendapatkan pesan yang asli dari pesan yang telah disandikan tanpa memiliki kunci untuk membuka pesan rahasia tersebut disebut **kriptoanalisis.** Sedangkan usaha untuk membongkar suatu pesan sandi tanpa mendapatkan kunci dengan cara yang sah dikenal dengan istilah **serangan (*attack*).**

Di bawah ini dijelaskan beberapa macam penyerangan terhadap pesan yang sudah dienkripsi:

1. *Ciphertext only attack*, penyerang hanya mendapatkan pesan yang sudah tersandikan saja.
2. *Known plaintext attack*, dimana penyerang selain mendapatkan sandi, juga mendapatkan pesan asli. Terkadang disebut pula *clear-text attack*.
3. *Choosen plaintext attack*, sama dengan *known plaintext attack*, namun penyerang bahkan dapat memilih penggalan mana dari pesan asli yang akan disandikan.

Berdasarkan bagaimana cara dan posisi seseorang mendapatkan pesan-pesan dalam saluran komunikasi, penyerangan dapat dikategorikan menjadi:

1. *Sniffing*: secara harafiah berarti mengendus, tentunya dalam hal ini yang diendus adalah pesan (baik yang belum ataupun sudah dienkripsi) dalam suatu saluran komunikasi. Hal ini umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekam pembicaraan yang terjadi.
2. *Replay attack* [DHMM 96]: Jika seseorang bisa merekam pesan-pesan *handshake* (persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak.
3. *Spoofing* [DHMM 96]: Penyerang bisa menyamar menjadi pihak yang ditipu. Semua orang dibuat percaya bahwa penyerang adalah pihak yang di tipu. Penyerang berusaha meyakinkan pihak-pihak lain bahwa tak ada salah dengan komunikasi yang dilakukan, padahal komunikasi itu dilakukan dengan sang penipu/penyerang. Contohnya jika orang memasukkan PIN ke dalam mesin ATM palsu – yang benar-benar dibuat seperti ATM asli – tentu sang penipu bisa mendapatkan PIN-nya dan copy pita magentik kartu ATM milik sang nasabah. Pihak bank tidak tahu bahwa telah terjadi kejahatan.
4. *Man-in-the-middle* [Schn 96]: Jika *spoofing* terkadang hanya menipu satu pihak, maka dalam skenario ini, saat seseorang hendak berkomunikasi dengan pihak lain, sang penyerang di mata pihak pertama seolah-olah adalah pihak kedua yang sedang dihubungi, dan penyerang tersebut dapat pula menipu pihak kedua itu sehingga si penyerang seolah-olah adalah pihak pertama. penyerang dapat berkuasa penuh atas jalur komunikas ini, dan bisa membuat berita fitnah.

Penyerang juga bisa mendapatkan kunci dengan cara yang lebih tradisional, yakni dengan melakukan penyiksaan, pemerasan, ancaman, atau bisa juga dengan menyogok seseorang yang memiliki kunci itu. Ini adalah cara yang paling ampuh untuk mendapat kunci.

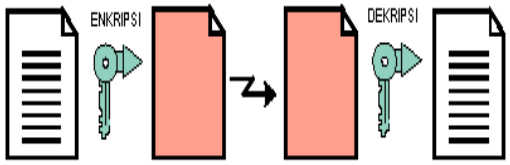
Jenis-jenis kunci

Kunci Simetris

Ini adalah jenis kriptografi yang paling umum dipergunakan. Kunci untuk membuat pesan yang disandikan sama dengan kunci untuk membuka pesan yang disandikan itu. Jadi pembuat pesan dan penerimanya harus memiliki kunci yang sama persis. Siapapun yang memiliki kunci tersebut, termasuk pihak-pihak yang tidak diinginkan, dapat membuat dan membongkar rahasia *ciphertext*. Problem yang paling jelas disini terkadang bukanlah masalah pengiriman *ciphertext*-nya, melainkan masalah bagaimana menyampaikan kunci simetris tersebut kepada

pihak yang diinginkan.

Contoh algoritma kunci simetris yang terkenal adalah DES (*Data Encryption Standard*) dan RC-4.

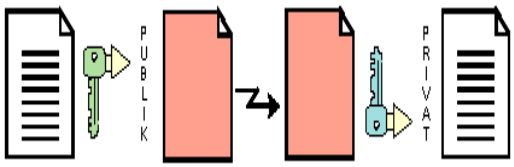


Gambar Kunci simetris

Kunci Asimetris

Pada pertengahan tahun 70-an Whitfield Diffie dan Martin Hellman menemukan teknik enkripsi asimetris yang merevolusi dunia kriptografi. Kunci asimetris adalah pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu, dalam hal ini kunci privat, untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya.

Dengan cara seperti ini, jika seorang pihak pertama mengirim pesan untuk pihak kedua, pihak pertapa tersebut dapat merasa yakin bahwa pesan tersebut hanya dapat dibaca oleh pihak yang bersangkutan, karena hanya dia yang bisa melakukan dekripsi dengan kunci privatnya. Tentunya si pihak pertama harus memiliki kunci publik milik pihak kedua untuk melakukan enkripsi. Pihak pertama bisa mendapatkannya dari pihak yang bersangkutan, ataupun dari pihak ketiga yang dipercaya.



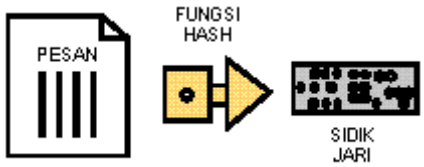
Gambar Penggunaan kunci asimetris

Teknik enkripsi asimetris ini jauh lebih lambat ketimbang enkripsi dengan kunci simetris. Oleh karena itu, biasanya bukanlah pesan itu sendiri yang disandikan dengan kunci asimetris, namun hanya kunci simetrislah yang disandikan dengan kunci asimetris. Sedangkan pesannya dikirim setelah disandikan dengan kunci simetris tadi. Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA (merupakan singkatan penemunya yakni Rivest, Shamir dan Adleman).

Fungsi Hash Satu Arah

Kini akan dibahas mengenai keutuhan pesan saat dikirimkan. Bagaimana jika seseorang sebagai pihak pertama mengirimkan surat pembayaran kepada pihak kedua sebesar 1 juta rupiah, namun di tengah jalan penyerang (yang ternyata berhasil membobol sandi entah dengan cara apa) membubuhkan angka 0 lagi dibelakangnya sehingga menjadi 10 juta rupiah? pesan tersebut seharusnya utuh, tidak diubah-ubah oleh siapapun, bahkan bukan hanya oleh penyerang, namun juga termasuk oleh pihak-pihak yang bersangkutan. Hal ini dapat dilakukan dengan fungsi *hash* satu arah (*one-way hash function*), yang terkadang disebut sidik jari (*fingerprint*), *hash*, *message integrity check,* atau *manipulation detection code*.

Saat pihak pertama hendak mengirimkan pesannya, dia harus membuat sidik jari dari pesan yang akan dikirim untuk pihak kedua. Pesan (yang besarnya dapat bervariasi) yang akan di-*hash* disebut *pre-image,* sedangkan outputnya yang memiliki ukurannya tetap, disebut *hash-value* (nilai *hash*). Kemudian, melalui saluran komunikasi yang aman, dia mengirimkan sidik jarinya kepada pihak kedua. Setelah pesan diterima, pihak kedua kemudian juga membuat sidik jari dari pesan yang telah diterimanya. Kemudian Badu membandingkan sidik jari yang dibuatnya dengan sidik jari yang diterimanya dari pihak pertama. Jika kedua sidik jari itu identik, maka pesan itu utuh tidak diubah-ubah sejak dibuatkan sidik jari yang diterima pihak kedua. Jika pesan pembayaran 1 juta rupiah itu diubah menjadi 10 juta rupiah, tentunya akan menghasilkan nilai *hash* yang berbeda.



Gambar Membuat sidik jari pesan

Fungsi *hash* untuk membuat sidik jari tersebut dapat diketahui oleh siapapun, tak terkecuali, sehingga siapapun dapat memeriksa keutuhan dokumen atau pesan tertentu. Tak ada algoritma rahasia dan umumnya tak ada pula kunci rahasia.

Jaminan dari keamanan sidik jari berangkat dari kenyataan bahwa hampir tidak ada dua pre-image yang memiliki *hash*-value yang sama. Inilah yang disebut dengan sifat *collision free* dari suatu fungsi *hash* yang baik. Selain itu, sangat sulit untuk membuat suatu pre-image jika hanya diketahui *hash*-valuenya saja.

Contoh algoritma fungsi *hash* satu arah adalah MD-5 dan SHA. *Message authentication code* (MAC) adalah salah satu variasi dari fungsi *hash* satu arah, hanya saja selain *pre-image,* sebuah kunci rahasia juga menjadi input bagi fungsi MAC.

II. Kriptografi dalam kehidupan sehari-hari

II.1. Kriptografi Sederhana

Metode Caesar

Di Amerika Serikat (AS) kriptografi telah mulai diperkenalkan sejak dini kepada anak-anak, dengan tujuan mencari kader-kader terbaik untuk dijadikan kriptografer atau kriptoanalis di instansi-instansi pemerintah AS. Tehnik pengenalan kriptografi bagi anak-anak ini berupa permainan sederhana tentang kriptografi.

Di Indonesia hal serupa pernah dilakukan dalam skala lebih kecil dan ringan, yaitu dalam kegiatan kepramukaan. Sehingga bila berbicara tentang kriptografi, anak-anak sekolah dasar (SD) pada tahun 70-an sampai dengan 90-an akan teringat dengan Pramuka. Kini kegiatan Pramuka sudah bukan merupakan kegiatan wajib bagi anak-anak SD sehingga tentu saja kriptografi semakin tidak dikenal.

Teknik kriptografi sederhana yang dapat diajarkan kepada anak-anak tingkat SD atau Pramuka Siaga / Penggalang kali ini adalah sistem kripto/sandi Caesar. Yaitu sistem sandi yang diciptakan oleh kaisar Romawi sekitar tahun 50-60 sebelum masehi, saat Julius Caesar mengirim pesan rahasia kepada tentaranya di medan perang. Karena diciptakan oleh Julius Caesar maka dinamailah sistem sandi ini dengan sistem sandi Caesar.

Sistem sandi Caesar ini dilakukan dengan menggeser deretan huruf (alfabet) tiga langkah kedepan guna mendapatkan alfabet baru yang digunakan untuk mengirimkan pesan rahasia.

Alfabet biasa :

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

Alfabet sistem sandi Caesar :

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

Sehingga A = D, B = E, C = F, … dst sampai Z = C

contoh :

pesan asli : **CARILAH COIN EMAS DI DALAM GUA**

pesan tersandi : **FDULODK FRLQ HPDV GL GDODP JXD**

Metode Vigenére

Teknik kriptografi berikut dapat diperkenalkan kepada para pemula, anak-anak Pramuka Penggalang ataupun sebagai permainan saat *boot champ* adalah sistem sandi Vigenère.

Sistem sandi ini pertama kali dipopulerkan oleh Blaise de Vigenère seorang diplomat Perancis pada abad 15, sehingga disebutlah metode ini dengan sistem sandi Vigenère

Sistem sandi Vigenère adalah sistem sandi substitusi multi-alfabet, yaitu sistem sandi Caesar tetapi dengan pergeseran alfabet yang berlainan disesuaikan dengan kata kuncinya.

Yang dimaksud sistem sandi substitusi adalah menyandi dengan cara mengganti huruf-huruf pesan/teks aslinya dengan huruf-huruf sandi. Sistem sandi Caesar dan Viginère termasuk metode sistem sandi ini. Bahkan sistem sandi substitusi merupakan sistem sandi yang dipakai pula dalam kriptografi modern, dengan variasi-variasi yang terus berkembang.

contoh :

kata kunci : **MERAPI**

pesan asli : **SUKSES ADALAH PERMAINAN PIKIRAN**

alfabet biasa :

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

alfabet sistem sandi Vigenère dengan kata kunci **MERAPI** :

M N O P Q R S T U V W X Y Z A B C D E F G H I J K L

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 D

R S T U V W X Y Z A B C D E F G H I J K L M N O P Q

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

P Q R S T U V W X Y Z A B C D E F G H I J K L M N O

I J K L M N O P Q R S T U V W X Y Z A B C D E F G H

sehingga

S dengan pergeseran M = E; U dengan pergeseran E = Y; K dengan pergeseran R = B; S dengan pergeseran A = S; E dengan pergeseran P = T; S dengan pergeseran I = A; A dengan pergeseran M = M; D dengan pergeseran E = H; dsb….. sampai N dengan pergeseran A = N

pesan tersandi : **EYBSTA MHRLPP BIIMPQZEE PXSUVRN**

Permainan menemukan pesan tersandi dengan sistem sandi Vigenère sangat menarik dan menantang untuk dilakukan.

II.2. Password

Password biasanya diterjemahkan dengan kata sandi. Walaupun penerjemahan ini tidak salah tetapi lebih tepat bila disebut kata kunci (la chiave), karena password lebih sering digunakan sebagai kunci untuk memasuki sebuah sistem.

Pada jaman dahulu password diilustrasikan dengan sebuah tempat yang dijaga oleh pengawal dimana kepada setiap orang yang hendak memasuki tempat tersebut pengawal selalu menanyakan kata kuncinya. Password saat ini digunakan untuk mengontrol akses masuk menuju sebuah sistem misalnya decoder TV kabel, mesin ATM, telepon seluler, komputer, dan lain-lain. Dalam interaksi dengan komputer, password lebih sering lagi dipakai misalnya untuk login e-mail, surfing internet, memasuki network, mengakses file di server, mengedit web site, transfer bank atau membaca koran on-line.

Selain untuk mengontrol akses masuk, password juga dipakai untuk mengklasifikasikan pengguna (*user*) dalam sebuah sistem untuk masuk sampai pada tingkat keamanan tertentu. Pengklasifikasian password biasanya adalah untuk operator, guest/member, service atau administrator.

Sebuah password selalu diberi nama/identitas, sehingga password hanya akan berfungsi dengan username (pemilik). Username dapat berupa nama biasa atau deretan angka tertentu (PIN, personal identity number atau serial number dari sebuah hardware), kartu magnetik atau biometrik. Seringkali PIN atau biometrik disamakan dengan password, padahal karakteristik PIN dan biometrik berbeda dengan password karena PIN dan biometrik merupakan identitas yang biasanya tetap. Sedangkan password harus dapat diubah-ubah sesuai kebutuhan.

Password akan efektif dan handal bila dikelola dengan baik :

1. Membuat password dengan karakter acak misalnya g2rFt5Ru. Jangan membuat password yang mudah diterka dengan kata-kata yang berpusat pada diri pengguna, misalnya nama anjing kesayangan, tanggal lahir, nama pacar/orang tua/anak, alamat rumah, nama sekolah, dan lain-lain.

2. Menggunakan satu password hanya untuk satu keperluan. Jangan menggunakan satu password untuk berbagai keperluan dengan alasan agar tidak bingung dan menghindari kesalahan memasukkan password milik sistem yang lain.

3. Melakukan perubahan password secara berkala untuk menghindari analisis dan diketahuinya password oleh pihak lain.

4. Menyimpan / menyembunyikan password, baik secara fisik maupun secara kriptografis untuk menghindari mudahnya pihak lain mendapatkannya.

5. Tidak memberikan password kepada orang lain (yang dipercaya misalnya saudara dan lain-lain) untuk menghindari tercecernya password yang akan merugikan pemiliknya.

II.3. USB Flashdisk sandi

USB Flashdisk sangat ideal untuk membawa data dengan jumlah bit yang besar. Namun karena ukurannya kecil, flashdisk sangat mudah untuk hilang, yang mana data didalamnya bisa saja jatuh kepada orang lain yang menemukannya.

Untuk mengatasi agar data yang jatuh ke tangan orang lain itu tetap terjaga kerahasiannya, saat ini terdapat flashdisk yang dapat memproteksi data didalamnya dengan aplikasi sandi. Diantaranya adalah : ***CryptoStick***^{TM} dari Research Triangle Software Inc, ***MicroDriver*** dan ***BioDrive*** dari Kanguru

CryptoStick^{TM}

CryptoStick^{TM} menggunakan algoritma Blowfish untuk menyandi data/file didalam flashdisk. Flashdisk ini dilengkapi pula dengan program yang dapat menyembunyikan web brousing history dan melindunginya dari pengecekan situs apa yang telah dikunjungi. Suatu hal yang sangat berguna bila sedang menggunakan PC yang bukan milik sendiri.

Selain itu, CryptoBuddy^{TM} menyediakan software berupa program aplikasi untuk membuka pesan tersandi yang disandi dengan CryptoStick. Hal ini memungkinkan seseorang mengirimkan file tersandi kepada temannya yang tidak mempunyai CryptoStick.

Keistimewaan flashdisk CryptoStick diantaranya adalah :

- High speed USB 2.0 flash memory kompatibel dengan USB 1.1

- Plug and play hardware dan software dan dapat bekerja baik dalam OS Windows
- Tidak memerlukan install software tambahan.
- Dapat menyimpan dan menyandi segala bentuk file / data.
- Mengkompres dan menyandi secara simultan.
- Kemampuan kompresinya sampai 3 kali.
- Private Internet browsing
- Tidak meninggalkan jejak dalam komputer yang digunakan.
- Fully licensed version of eTrust® Pest Patrol® Anti-Spyware
- Designnya yang bagus.
- Casing dari aluminum yang kuat. dan
- 1 tahun garansi

MicroDrive AES

Kanguru MicroDrive AES (Advanced Encryption Standard) adalah USB flashdisk untuk membatasi akses dan melindungi data / informasi rahasia dengan mengacak data/file serta mengamankan PC. Dapat digunakan pula untuk mengunci PC hanya dengan cara mengeluarkan usb flashdisk-nya.

Kanguru MicroDrive AES dibundel dengan program aplikasi sandi Kanguru Lock yang dapat bekerja dalam semua OS. Program aplikasi ini secara virtual membuat disk protected dengan 256 Bit AES encryption dalam KanguruMicro Drive-nya, dan kemudian melindunginya dengan password.

BioDrive

Kanguru BioDrive adalah flashdisk yang dilengkapi dengan pembaca sidik jari untuk melindungi data dan membatasi aksesnya. Saat biometric protection digunakan, BioDrive akan menyandi data dan kemudian menyembunyikan data partisinya. Untuk dapat menggunakan data-data tersebut cukup log in dengan sidik jari.

Keistimewaan Kanguru BioDrive diantaranya :

- Mampu menyimpan sampai 5 sidik jari.
- Write Protection Switch
- Dapat digunakan dalam berbagai user level, sehingga tidak harus Admin.
- Tidak memerlukan software tambahan.
- High Speed USB2.0 Interface
- Top grade fingerprint sensor-508 DPI
- Kompatibel dengan Windows 98/ME/2000/XP

Contoh program aplikasi sandi lain yang dipasarkan secara bebas diantaranya adalah : ***DESlock+ 3.2.4*** dari Data Encryption System, ***Namo FileLock 3.10*** dari SJ Namo Interactive dan ***T3 Basic Security*** dari Trilogy Total Technology.

DESlock+ 3.2.4

DESlock hardware dengan model koneksi USB, bentuknya menyerupai flash memory, disebut juga DESkey USB token. DESkey mempunyai kapasitas menyimpan 64 kunci dalam satu password. Pilihan algoritma yang disediakan yaitu 3DES, AES dan BlowFish.

Mengoperasikan DESkey sangatlah sederhana, tidak memerlukan perangkat tambahan lainnya hanya plug in, log on dan siap bekerja.

Keistimewaan yang dipunyai DESlock+ diantaranya :

- Email Encryption
- Folder Encryption
- File Encryption
- Mountable Encrypted Files (Volumes)
- Compressed Encrypted Archives
- Clipboard & Text Encryption
- Secure File Deletion
- Multiple, Shared Encryption Keys

Namo FileLock

Mengoperasikan aplikasi ini sangat mudah yakni hanya dengan cara drag and drop kedalam area sandinya. Algoritma yang digunakan adalah SEED 128 bit. Sayangnya Namo FileLock tidak memiliki versi hardware.

Keistimewaan yang dipunyai Namo FileLock diantaranya :

- Access Control and Data Encryption
- Powerful Backup Feature
- Rapid Processing
- User-Friendly Interface

T3 Basic Security

T3 lebih pas digunakan untuk notebook atau laptop. T3 memiliki versi hardware dengan koneksi USB yang bentuknya mirip dengan flash memory. T3 menggunakan algoritma CAST 128 bit sebagai standar sandinya.

T3 Basic Security mempunyai keistimewaan :

T3 Security Key :

- Langsung melindungi seluruh akses secara fisik kedalam PC setelah T3 Key ini dicabut.
- Mengunci PC saat tidak digunakan
- Mencegah pihak yang tidak berhak mengakses PC dan data

T3 Data Vault (Data Encryption Module) :

- Menyimpan data rahasia dalam hidden data vault yang hanya dapat diakses melalui T3 Security key holder
- Menyandi data rahasia menggunakan CAST 128 bit yang sangat baik.
- Dapat digunakan untuk single atau multiple private data vaults
- Hanya dapat diakses oleh T3 key dan security password
- Tidak ada batas besarnya file

T3 Parental Control Module

- Melindungi website dari akses yang tidak dikehendaki
- Dapat membuat sendiri, daftar website yang diperbolehkan melakukan akses.
- Memberikan kekuasaan untuk mengizinkan atau tidak sebuah URL kepada user.

T3 Audit Trail Module

- Dapat menciptakan log file sendiri sebagai referensi.
- Menyediakan sarana untuk mengecek PC dari akses pihak yang tidak dikehendaki.

II.4. Si Kartu Pintar

Salah satu eksportir jasa TI terbesar India, Tata Consultancy Services (TCS) merencanakan untuk mengembangkan kartu-pintarnya sendiri berdasarkan aplikasi kriptografi untuk mempercepat pengadopsian public key infrastructure (PKI) di negara tersebut.

Kartu tersebut dapat menyimpan aplikasi-aplikasi, seperti tanda tangan digital dan informasi-informasi pribadi lainnya, sehingga para pemiliknya bisa mengakses berbagai layanan yang diberikan berbagai institusi swasta maupun pemerintah dengan aman.

TCS pun berusaha agar bisa menekan harga kartu-pintar ini, mengingat harga kartu yang begitu tinggi bagi kebanyakan penduduk India merupakan salah satu faktor penghambat dalam kemajuan layanan digital di negara tersebut. Penerapan PKI di negeri india sangat lambat, karena tingginya biaya untuk membuat kartu. Sekarang ini misalnya, kartu-kartu pintar yang beredar berharga sekitar 700 sampai 2.500 rupee (125 ribu sampai 440 ribu rupiah).

III. Kesimpulan

Ketika kita bekerja dengan data bersama atau dalam komputer yang terhubung dalam jaringan umum, maka penting sekali untuk melindungi file data kita dari akses orang-orang yang tidak kita kehendaki. Salah satu metode melindungi file data dan membatasi akses terhadapnya adalah dengan menggunakan Kriptografi. Berbagai macam aplikasi Kriptografi yang telah digunakan dalam pengamanan data. Mulai dari yang sederhana dan mudah dipelajari sampai yang cukup rumit. Beberapa aplikasi tersebut adalah :

■ **Kriptografi sederhana Metode Caesar** Sistem sandi Caesar ini dilakukan dengan menggeser deretan huruf (alfabet) tiga langkah kedepan guna mendapatkan alfabet baru yang digunakan untuk mengirimkan pesan rahasia.

■ **Kriptografi sederhana Metode Vigenère** sistem sandi Caesar tetapi dengan pergeseran alfabet yang berlainan disesuaikan dengan kata kuncinya.

■ **Password** kunci untuk memasuki sebuah system

■ **USB Flashdisk Sandi** Untuk mengatasi agar data yang jatuh ke tangan orang lain tetap terjaga kerahasiannya. Beberapa diantaranya adalah :

- **CryptoStick™**

- **MicroDrive AES**

- **BioDrive**

- **DESlock+ 3.2.4**

- **Namo FileLock**

- **T3 Basic Security**

Dengan kelebihan dan kekurangan masing-masing.

■ **Aplikasi Kartu Pintar dari TCS** Kartu yang dapat menyimpan aplikasi-aplikasi, seperti tanda tangan digital dan informasi-informasi pribadi lainnya, sehingga pemiliknya bisa mengakses berbagai layanan yang diberikan berbagai institusi swasta maupun pemerintah dengan aman.

Daftar Pustaka

1. http://hadiwibowo.wordpress.com/tag/kriptografi
Tanggal akses : 26 Desember 2006, pukul 12:15

2. http://www.ebizzasia.com/0109-2003/asia,0109.htm/
Tanggal akses : 27 Desember 2006, pukul 14:30

3. http://hadiwibowo.wordpress.com/tag/aplikasi
Tanggal akses : 26 Desember 2006, pukul 12:15

4. http://hadiwibowo.wordpress.com/2006/09/20/mengamankan-data-dengan-kriptografi/
Tanggal akses : 26 Desember 2006, pukul 12:15

5. http://www.cryptography.com/
Tanggal akses : 27 Desember 2006, pukul 14:30

6. http://www.ilmukomputer.com/
Tanggal akses : 27 Desember 2006, pukul 14:15