Pemanfaatan Kriptografi Sebagai Alat dalam Pembuatan *Certification Authority*

Rizkydaya Aditya Putra — 13506037
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
rizkydaya@students.itb.ac.id

***Abstrak*— Makalah ini membahas tentang studi pemanfaatan salah satu subbab dalam mata kuliah struktur diskrit. Subbab yang dimaksud merupakan salah satu dari subbab dari bab Teori Bilangan yaitu subbab Kriptografi. Kriptografi dalam bahasa Yunani berarti tersembunyi. Dalam masa modern ini, kriptografi dianggap sebagai cabang baik dari matematika dan ilmu computer serta berhubungan erat dangan teori infromasi. Kriptografi saat ini banyak digunakan dalam masyarakat maju, sebagai contoh dalam hal pembuatan otoritas sertifikat (*certification autthority*) yang mana hal tersebut sangat bergantung kepada kriptografi. Oleh karena itu, proses bagaimana suatu CA dapat terbentuk dan apa saja elemen-elemen yang terlibat amatlah penting untuk diketahui terutama bagi mereka yang berprofesi sebagai praktisi keamanan informasi.**

Kata Kunci*—kriptografi, certification authority (CA), sistem kripto simetris, sistem kripto asimetris.

I. PENDAHULUAN

Istilah yang sering kita dengar sehubungan dengan keamanan (*security*) adalah enkripsi, kriptografi, IKP, CA, SSL, *digital signature*, *firewall*, IDS, dan sebagainya. Penggunaan *Firewall* dan IDS bertujuan untuk mempertahankan jaringan dari serangan danpenyusupan. Sedangkan kriptografi digunakan untuk mengamankan data dari penyadapan.

Untuk menjaga suatu data agar tetap rahasia, tidak bisa dibaca oleh pihak-pihak yang tidak berkepentingan, dan agar tidak bisa dipalsukan, digunakan sistem khusus yang dapat mengacak data sedemikian rupa sehingga tidak bisa dibaca ataupun dipalsukan oleh pihak-pihak yang tidak berkepentingan. Sistem yang dipakai untuk mengacak data agar dapat ditransmisikan secara lebih aman disebut dengan sistem kripto, yaitu sistem pengacakan yang berbasiskan algoritma-algoritma kriptografi tertentu.

Tujuan dari penggunaan kriptografi adalah:

1. Mengamankan data dengan mengacak data sehingga sulit untuk dibaca (*Confidentiality*)
2. Meyakinkan tidak ada perubahan data (*Integrity*)
3. Memastikan identitas seseorang dengan digital signature (*Authentication*)

II. DASAR TEORI

A. Terminologi

Hingga zaman modern seperti saat ini, kriptografi semata-mata dianggap sebagai enkripsi, yaitu proses mengubah informasi yang tidak biasa dan tidak dapat dibaca menjadi suatu informasi yang jelas dan dapat dibaca. Sedangkan dekripsi adalah proses sebaliknya. Chipertext tersebut adalah suatu pasangan algoritma yang melakukan enkripsi dan membalikan dekripsi. Informasi detail dari chipertext dikontrol oleh algoritma tersebut, sengan kata lain dengan suatu kunci. Hal tersebut merupakan parameter rahasia untuk membaca pesan rahasia tersebut, dan biasanya hanya pengirim dan yang dikirim yang mengetahui kunci tersebut. Kunci tersebut amatlah penting karena tanpa kunci itu, pesan tersebut akan mudah terbongkar dan menjadi tidak berarti lagi. Berdasarkan sejarahnya, chipertext kadang kala digunakan langsung untuk mengenkripsi atau deskripsi tanpa prosedur tambahan seperti pengesahan dan pengecekan kepribadian.

Dalam bahasa sehari-hari, kode biasanya digunakan untuk mengartikan suatu metode enkripsi atau penyembunyian suatu makna. Tetapi, dalam kriptografi, kode memiliki arti spesifik lebih; berarti suatu pergantian dari suatu unit dari suatu informasi dengan kata kode (sebagai contoh, `apple pie` diganti dengan `attack at dawn`). Kode tidak digunakan lagi dalam kriptografi yang sesungguhnya-kecuali tidak sengaja seperti proses desain suatu unit (contoh '`Bronco Flight`' atau *Operation Overlord*)- sejak chipertext yang dipilih lebih praktis dan lebih aman dari biasanya, serta lebih mudah disesuaikan dengan computer.

Beberapa penggunaan kriptografi dan kriptologi dapat saling bertukar tempat dalam bahasa Inggris, ketika penggunaan kriptografi yang lain mengarah ke penggunaan dan praktek dari teknik kriptografik, dan kriptologi lebih mengarah ke subjek sebagai studi lapangan.

Kriptografi di Indonesia disebut persandian yaitu secara singkat dapat berarti seni melindungi data dan informasi

dari pihak-pihak yang tidak dikehendaki baik saat ditransmisikan maupun saat disimpan. Sedangkan ilmu persandiannya disebut kriptologi yaitu ilmu yang mempelajari tentang bagaimana tehnik melindungi data dan informasi tersebut beserta seluruh ikutannya.

B. Sistem Kriptografi Modern

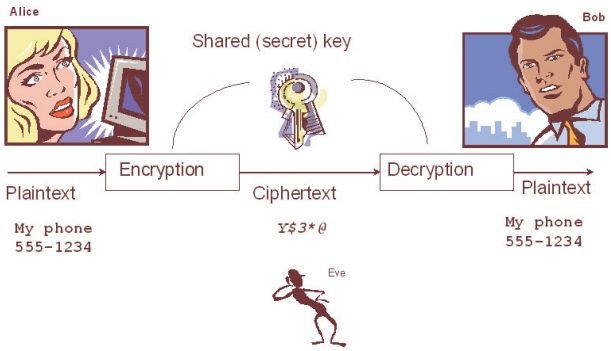
Untuk menjaga kerahasiaan data digunakan sistem kripto, yaitu sistem pengamanan yang dapat mengacak data sehingga seolah-olah data tersebut menjadi terkunci. Proses pengacakan data sehingga menjadi terkunci disebut dengan enkripsi. Selanjutnya agar data yang sudah terkunci ini dapat dibaca kembali, diperlukan kunci yang sesuai. Proses pengembalian informasi ini disebut dengan dekripsi.

Sistem kripto yang banyak digunakan ada dua macam, yaitu sistem kripto simetris (*symetric cryptosystem*) dan sistem kripto asimetris (*asymetric cryptosystem*). Contoh algoritma yang menggunakan sistem kripto simetris anatara lain adalah DES (*Data Encryption Standard*), Triple DES, IDEA, RC2, RC4, dan RC5. Sedangkan contoh algoritma yang menggunakan sistem kripto asimetris adalah RSA (Rivest Shamir Adleman) dan Diffie-Hellman.

Perbedaan kedua jenis sistem kripto ini terutama terletak pada penggunaan kunci. Pada sistem kripto simetris, kunci yang digunakan untuk enkripsi sama dengan kunci untuk dekripsi. Jadi kunci yang digunakan pada sistem kripto simetris hanya satu buah. Lain halnya dengan sistem kripto asimetris, yang juga dikenal dengan istilah sistem kripto kunci publik (*public key crypto system*). Pada sistem kripto kunci publik, kunci yang digunakan untuk enkripsi berbeda dengan kunci yang digunakan untuk dekripsi. Kunci yang digunakan pada sitem kripto asimetris ini ada dua buah, terdiri dari kunci publik dan kunci privat, yang keduanya terhubung secara matematis.

B.1. Sistem Kripto Simetris

Sistem kripto simetris melakukan proses enkripsi dan dekripsi dengan memakai kunci yang sama (seperti ilustrasi pada gambar berikut). Penggunaan kunci yang sama inilah yang menyebabkan sistem ini disebut dengan sistem kripto kunci simetris. Data asli (*plain text*) dienkripsi dengan menggunakan sebuah algoritma dan sebuah kunci. Data yang telah dienkripsi (*chipertext*) dikembalikan lagi ke aslinya (di-dekripsi) dengan menggunakan algoritma dan kunci yang sama. Pada sistem ini harus dijaga betul agar kunci (*key*) tidak jatuh ke pihak lain yang tidak berwenang. Inilah sebabnya nama sistemnya adalah sistem kripto kunci privat.



Bagan 1 Sistem kripto kunci privat

Seorang *cracker* yang menyadap di jaringan masih bisa mendapatkan data asli asalkan ia berhasil menebak kunci yang digunakan. Tingkat kesulitan menebak kunci sesuai dengan panjangnya kunci yang digunakan.

Salah satu kesulitan sistem kripto kunci privat adalah dalam hal pertukaran kunci (*key exchange*). Dalam contoh di atas, bagaimana Bob tahu kunci yang akan digunakan oleh Alice? Jika kunci ini dikirimkan melalui saluran yang sama, maka penyadap dapat juga mengetahui kunci tersebut. Jadi, kunci harus dikirimkan dengan cara lain atau dengan jalur lain (*out of band communication*). Salah satu contoh pengiriman informasi melalui jalur lain adalah penggunaan fax, SMS, *token generator* (seperti yang digunakan dalam KeyBCA) atau bahkan bertemu secara fisik. Masalah *key exchange* ini merupakan salah satu masalah yang harus dipecahkan dalam sistem kripto kunci privat.

Masalah lain yang dihadapi oleh sistem kripto kunci privat adalah jumlah kunci yang meledak secara eksponensial. Untuk setiap pasangan pengguna dibutuhkan sebuah kunci rahasia. Sebagai contoh, Alice dan Bob memiliki sebuah kunci rahasia. Alice dengan Charlie (pengguna lain) memiliki sebuah kunci rahasia yang berbeda dengan kunci Alice-Bob. Demikian pula Bob dan Charlie memiliki kunci rahasia yang berbeda dengan kunci Alice-Bob dan Alice-Charlie. Secara matematis jumlah kunci yang dibutuhkan adalah n * (n-1) / 2.

Pada sistem kripto asimetris, kunci untuk proses enkripsi berbeda dengan kunci untuk proses dekripsi. Kedua kunci ini terhubungsecara matematis dengan rumus tertentu, sehingga data yang telah di-enkripsi oleh suatu kunci hanya dapat di-dekripsi dengan menggunakan kunci pasangannya. Ada persamaan matematik yang memungkinkan hal ini.

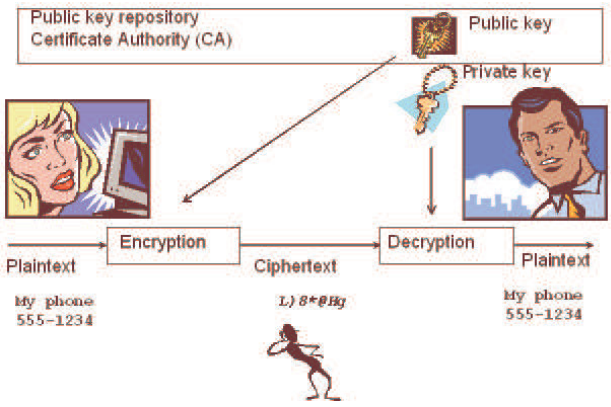
B.2. Sistem Kripto Asimetris

Pada sistem kripto asimetris, kunci untuk proses enkripsi berbeda dengan kunci untuk proses dekripsi. Kedua kunci ini terhubungsecara matematis dengan rumus tertentu, sehingga data yang telah di-enkripsi oleh suatu kunci hanya dapat di-dekripsi dengan menggunakan kunci

pasangannya. Ada persamaan matematik yang memungkinkan hal ini.

Setiap pengguna sistem ini mempunyai dua kunci, yaitu kunci publik dan kunci privat. Pengguna dapat menyebarkan kunci publik secara bebas, tetapi kunci privat harus dijaga kerahasiaannya.

Ilustrasi penggunaan sistem kripto asimetris ini dapat dilihat pada Gambar di bawah ini.



Bagan 2 Kripto kunci publik

Alice ingin mengirimkan pesan rahasia kepada Bob. Enkripsi dilakukan oleh Alice dengan menggunakan kunci publik milik Bob. Kunci ini dapat diambil dari suatu tempat penyimpanan kunci *public*. Kemudian Alice mengirimkan pesan terenkripsi tersebut kepada Bob. Hanya Bob yang dapat membaca (dekripsi) pesan Alice dengan menggunakan kunci privat milik Bob. Bahkan Alice pun sudah tidak dapat lagi membuka pesan yang dia kirimkan.

Seperti yang telah dikatakan di atas, Bob tidak diperkenankan untuk memberikan kunci privatnya kepada Alice. Kunci privat ini harus disimpan dengan aman oleh Bob. Dengan demikian seorang *cracker* yang menyadap di jaringan, walaupun berhasil menebak kunci untuk enkripsi, tetapi ia tidak dapat membaca informasinya, sebab kunci untuk mendapatkan *plaintext* pesan yang dikirim Alice, tidak dimiliki oleh *cracker* tersebut (disimpan dengan aman oleh Bob).

Karena algoritmanya yang lebih kompleks (misalnya algoritma RSA), komputasi yang diperlukan untuk sistem kripto asimetris jauh lebih besar dibandingkan dengan sistem kripto simetris. Oleh karena itu, biasanya data yang dikomunikasikan tetap dienkrip dengan menggunakan sistem kripto simetris. Kunci simetris yang digunakan adalah kunci sesi (*session key*), bersifat unik untuk setiap sesi komunikasi yang dilakukan. Kunci sesi itu merupakan kunci simetris yang digunakan untuk komunikasi data pada jangka waktu tertentu. Di pihak lain, sistem kripto asimetris digunakan pada awal sesi komunikasi untuk pengiriman kunci sesi yang diperlukan. Pada umumnya, kunci sesi diganti-ganti terus jika transaksi data berlangsung dalam jangka waktu lama. Penggantian ini diperlukan untuk menghindari kemungkinan penyerang mencari kunci yang sesuai, karena kunci simetris lebih cepat untuk ditebak dibandingkan dengan kunci asimetris.

Pada sistem kripto asimetris, kunci privat tidak boleh jatuh ke tangan orang lain, sedangkan kunci publik harus disebarkan , tetapi harus ada jaminan bahwa kunci publik tersebut adalah benar-benar dimiliki oleh pemilik yang sah. Oleh karena itu kunci publik harus diberi sertifikat oleh suatu badan yang berwenang. Sertifikat adalah file data yang berisi kunci publik yang disertai dengan identitas pemilik. Sertifikat dibuat dan disahkan oleh badan khusus yang bernama *Certification Authority* (CA). Penyelenggara CA yang secara defacto diakui di dunia adalah Verisign. Namun dimungkinkan adanya penyelenggara CA yang lain.

B.3. Hash Function

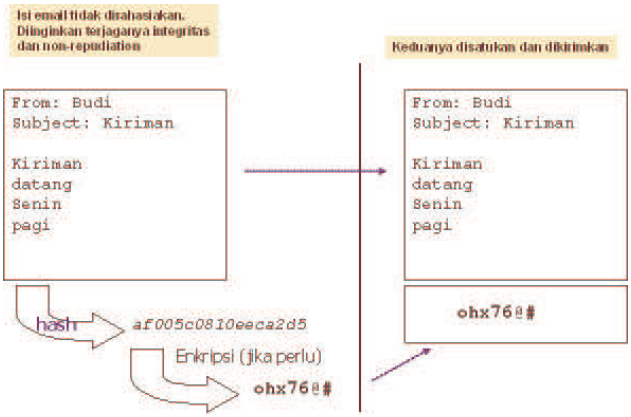
Selain untuk enkripsi ada kegunaan lain dari sistem kripto, yaitu untuk menjamin integritas data dan digital signature. Algoritma kripto digunakan untuk menghasilkan ciri atau tanda dari sederetan data, yaitu sebuah "*message digest*". Fungsi yang dapat mengimplementasikan hal ini dikenal dengan nama Hash function. Fungsi ini memiliki sifat berlangsung satu arah, artinya keluarannya tidak dapat diubah kembali menjadi data aslinya. Satu sifat lain yang juga diinginkan dari sebuah hash function adalah perubahan data satu bit saja akan mengubah keluaran hash secara drastis, yang disebut *avalanche effect*.

Contoh hash function adalah MD5 dan SHA.

- Contoh MD5:

```
unix$ md5sum /bin/login
af005c0810eeca2d50f2904d87d9ba1
c /bin/login
```

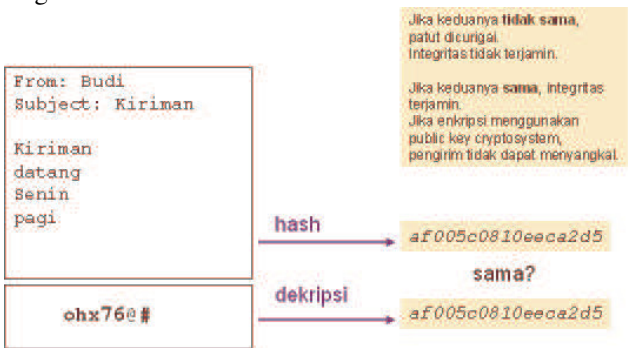
Gambar berikut memberikan ilustrasi penggunaan hash pada sisi pengirim.



Bagan 3 Hash function pada sisi pengirim

Sebelum dikirim, terlebih dahulu dibuat hash function dari isi pesan e-mail. Kemudian keluaran hash dienkripsi jika diperlukan. Keluaran ini dikenal dengan istilah "*digital signature*". Setelah itu pesan e-mail (*plain text*) dan *signature*-nya dikirim oleh pengirim melalui jaringan

(TCP/IP), dan diterima oleh penerima. Penerima akan melakukan proses *checking*, seperti yang diilustrasikan pada gambar berikut ini.



Bagan 4 Hash function pada sisi penerima

Informasi yang diterima berupa pesan e-mail (plain text) dan *signature*-nya. Kemudian hash function dilakukan terhadap isi pesan e-mail, dan dekripsi dilakukan terhadap *signature*-nya. Apabila keluaran hash dan hasil dekripsi sama maka penerima mendapatkan jaminan bahwa pengirim terjaga integritasnya Apabila keduanya tidak sama maka, integritas pengirim perlu dicurigai.

Apabila enkripsi menggunakan sistem kripto kunci publik, maka pengirim tidak dapat menyangkal bahwa ia telah mengirim email/ pesan.

Contoh penggunaan hash adalah:

- Hasil hash dienkripsi untuk menjamin keamanannya (integritas)
- Ukuran hasil hash yang lebih kecil dibandingkan ukuran pesan asalnya membutuhkan waktu enkripsi yang lebih singkat (dibandingkan jika mengenkripsi seluruh pesan)
- *Digital signature*
- Pesan juga dapat dienkripsi jika diinginkan kerahasiaan

III. Analisis dan Perancangan

A. Perancangan Infrastruktur Kunci Publik

Infrastruktur Kunci Publik (IKP) adalah implementasi terhadap sistem yang menggunakan sistem kripto kunci publik. *Certification Authority* (CA) adalah salah satu komponen utama dari IKP yang berfungsi sebagai pembuat sertifikat. Sertifikat yang dikeluarkan oleh CA dapat digunakan untuk menjamin keaslian kunci publik milik suatu entity pengguna sistem kripto kunci publik. Keberadaan CA sangat penting untuk menjaga integritas dalam *e-government* maupun *e-commerce*.

Secara umum, IKP terdiri atas:

- kebijakan (*policy*) untuk kemanan yang mendefinisikan bagaimana sistem kripto diimplementasikan dan dioperasikan.
- perangkat lunak (*software*) untuk membuat, menyimpan, dan mengelola kunci
- prosedur yang mengatur bagaimana kunci dan sertifikat dibuat, disimpan, didistribusikan, dan dipakai.

A.1. Komponen-Komponen pada IKP

Komponen-komponen pada IKP yang dirancang terdiri atas:

a. *Certification Authority* (CA)
   CA adalah *entity* berupa institusi ataupun perorangan yang bertugas mengeluarkan sertifikat, yang mengesahkan pasangan kunci publik dengan identitas pemilik kunci tersebut.
b. *Registration Authority* (RA)
   RA adalah *entity* yang berfungsi sebagai jembatan penghubung antara CA dengan *subscriber* yang memesan sertifikat. Melalui RA, seorang *subscriber* dapat membuat certificate request, mengimpor sertifikat CA, mengimpor sertifikat yang sudah dipesan, ataupun mengambil sertifikat *subscriber* lainnya
c. Kebijakan keamanan (*security policy*)
   Kebijakan keamanan merupakan dokumen tertulis yang bersifat legal, berisi langkah-langkah kebijakan organisasi dalam mengamankan sistem informasinya, serta proses dan prinsip-prinsip kriptografi yang dipakai.
d. Sistem distribusi sertifikat
   Sertifikat harus disimpan di suatu tempat khusus yang bisa diakses oleh semua orang, sehingga sewaktu-waktu bisa diambil oleh orang yang membutuhkan. Tempat tersebut bisa saja berupa direktori pada RA

A.2. Penggunaan Sertifikat

Sertifikat yang diterbitkan oleh suatu CA dapat digunakan untuk:

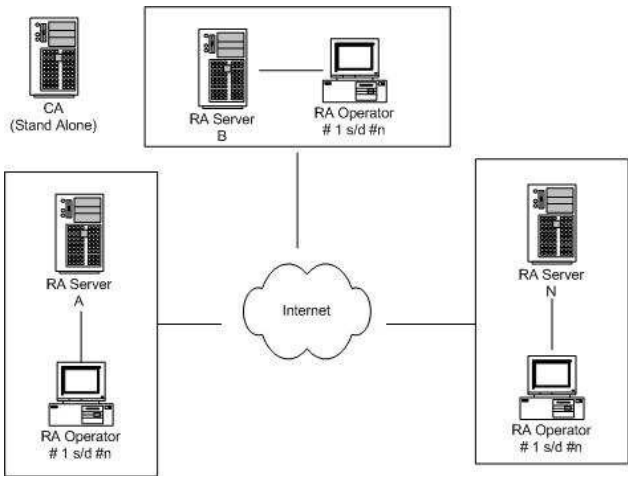
a. otentikasi pada protokol SSL
b. enkripsi pada protokol S/MIME
c. pemberian tanda tangan digital pada pesan email
d. dan lain-lain

B. Penggunaan OpenCA

Perangkat lunak OpenCA merupakan perangkat lunak CA yang bersifat *open source*. OpenCA dikembangkan oleh OpenCA *group*, dan pada dasarnya merupakan integrasi antara penggunaan perangkat lunak OpenSSL, Apache, serta OpenLDAP. Semuanya juga merupakan produk *open source*.

B.1. Struktur OpenCA

Struktur OpenCA meggunakan mekanisme CA-RA yang berlapis, dengan memisahkan fungsi dari CA dan RA (*Registration Authority*). CA bisa membawahi lebih dari satu buah RA. Struktur ini dapat dilihat pada gambar di bawah ini.



Bagan 5 Struktur OpenCA

Komputer yang menjadi server CA merupakan komputer *stand-alone* yang tidak dihubungkan dengan jaringan di luar. File-file yang perlu ditransfer ke komputer lain dapat dipindahkan dengan menggunakan fasilitas *removable* media. Cara ini digunakan untuk menghindarkan serangan (*intrusion*) yang biasanya dilakukan melalui jaringan. Perangkat lunak untuk manajemen CA dipasang hanya pada komputer ini. Kunci private CA juga hanya ditempatkan pada komputer ini, dan dilindungi dengan enkripsi 3DES.

Server RA menggunakan antarmuka yang berbasis web, dan hanya bisa diakses oleh operator-operator RA yang mempunyai sertifikat khusus untuk *client authentication*. Dengan cara ini (penggunaan antarmuka RA) maka operator RA dapat melakukan proses penyetujuan pada *certificate request* dari *subscriber*. Proses ini akan menghasilkan CSR yang ditandatangani oleh operator RA tersebut. Pada operator RA ini juga dijalankan fungsi servis direktori yang menyediakan jasa penempatan sertifikat pada direktori di servis.

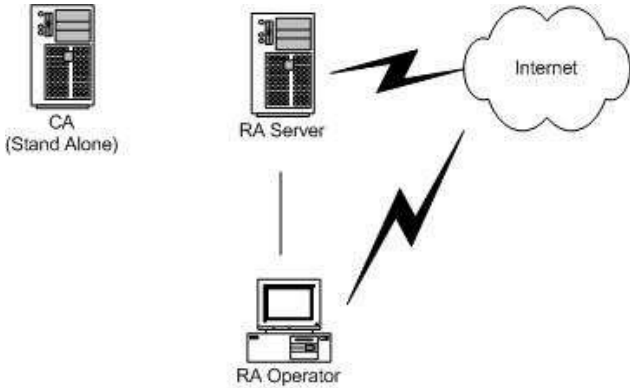
B.2. Pemanfaatan Karakteristik OpenCA

Karakteristik dan kemampuan OpenCA terkait pembuatan CA adalah:

a. Pembuatan, penandatanganan, pencabutan, serta verifikasi sertifikat X.509, menggunakan algoritma pasangan kunci RSA, dan algoritma digest menggunakan SHA-1, MD5, MD2, MDC-2
b. Jenis sertifikat yang dapat dibuat adalah sertifikat CA dan sertifikat untuk *subscriber (user certificate & server certificate)*
c. Penyimpanan kunci private menggunakan format PKCS #8 (terenkripsi DES).
d. Database yang digunakan untuk penyimpanan sertifikat adalah database DBM, yang merupakan jenis database standar pada sistem UNIX (termasuk Linux)
e. Menggunakan struktur CA_RA
f. Pada server RA sertifikat dapat dipublikasikan dengan menggunakan servis web dan servis direktori LDAP.
g. Dalam proses registrasi *subscriber*, operator RA dapat menandatangani CSR (Certificate Signing Request) dalam rangka menjaga keaslian dan keutuhan CSR tersebut.
h. Setelah sertifikat selesai dibuat dan telah tiba pada server RA, maka Operator RA dapat memberitahukan kepada pemilik sertifikat baru melalui email

C. Metode Penerbitan Sertifikat

Pada bagian ini akan dijelaskan langkah-langkah yang diperlukan untuk penerbitan sertifikat. Topologi dari sistem arsitektur penerbitan CA dapat dilihat pada gambar di bawah ini.



Bagan 6 Topologi CA yang digunakan

C.1. Inisialisasi CA

Sebelum CA melakukan tugasnya, maka CA harus diinisialisasi terlebih dahulu. Inisialisasi CA ini dilakukan dengan tujuan memberikan sertifikat serta kunci privat kepada server CA, sertifikat kepada RA Operator, dan sertifikat untuk server RA. Sertifikat-sertifikat yang dibuat pada proses ini adalah sertifikat yang digunakan untuk keperluan internal (bukan *subscriber*), dan dibuat langsung oleh CA (atau Operator CA). Keperluan internal yang dimaksud dapat dijelaskan sebagai berikut:

- sertifikat yang dibuat untuk CA hanya dibuat untuk menandatangani bakal sertifikat atau disebut *Certificate Signing Request* (CSR) dari RA,
- sertifikat yang dibuat untuk RA Operator digunakan oleh RA Operator untuk menandatangani sertifikat sebelum diajukan ke CA, tanpa tanda tangan dari RA Operator, CA akan menolak untuk mensyahkan sertifikat yang diajukan ke CA,
- sedangkan sertifikat yang dibuat untuk server RA digunakan agar web server RA dapat diakses dengan protokol HTTPS. Seperti disebutkan di atas, proses inisialisasi CA dilakukan oleh CA

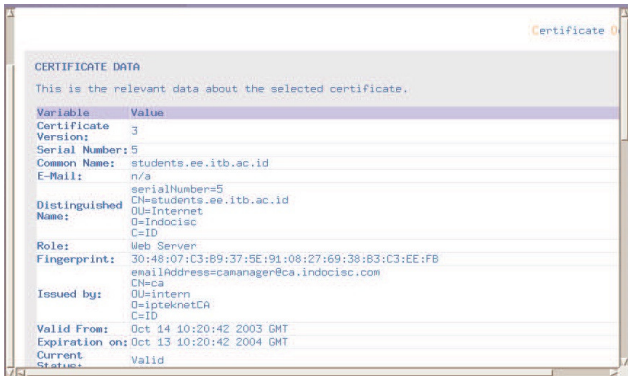
(Operator CA) sendiri, dan dilakukan pada (komputer CA). Jadi, pada proses ini akan dilakukan 3 macam proses, yaitu:

- Pembuatan sertifikat untuk CA
- Pembuatan sertifikat untuk RA Operator
- Pembuatan Sertifikat untuk RA server

C.2. Proses Pembuatan Sertifikat untuk CA

Proses pembuatan sertifikat CA pada sistem diawali dengan pembuatan pasangan kunci (*privat* dan *public*) milik CA. Setelah itu dilanjutkan dengan pembuatan sertifikat yang ditandatangani oleh CA sendiri atau oleh Root CA (dalam kasus ini, server sistem CA adalah Root CA). Root CA bisa dari penyelenggara CA yang sudah diakui di dunia Internasional, seperti Verisign. Setelah langkah-langkah tersebut selesai diproses, maka akan langsung terbentuk suatu CA yang baru dan terautentikasi.

Berikut ini adalah contoh tampilan CA yang telah berhasil dibuat oleh sistem:



Bagan 7 Contoh dari CA yang telah dibuat

IV. KESIMPULAN

Kriptografi merupakan salah satu dari media komunikasi dan informasi kuno yang masih dimanfaatkan hingga saat ini. Kriptografi di Indonesia disebut persandian yaitu secara singkat dapat berarti seni melindungi data dan informasi dari pihak-pihak yang tidak dikehendaki baik saat ditransmisikan maupun saat disimpan. Sedangkan ilmu persandiannya disebut kriptologi yaitu ilmu yang mempelajari tentang bagaimana tehnik melindungi data dan informasi tersebut beserta seluruh elemennya.

Pembuatan *Certification Authority* (CA) mengimplementasikan metode-metode kriptografi terutama sistem kripto simetris, sistem kripto asimetris, dan fungsi hash. Sedangkan infrastruktur yang digunakan adalah infrastruktur kunci publik (IKP) dan alat bantu yang dapat digunakan adalah aplikasi OpenCA.

REFERENSI

[1] Mollin, Richard, "*An Introduction to Cryptography, Second Edition (Discrete Mathematics and Its Applications)*", Chapman & Hall/CRC, 2006, pp.9-13.

[2] Munir, Rinaldi, "*Matematika Diskrit*", ITB, 2003, pp.V-21 s.d V-25.

[3] Rahardjo, Budi, "*Panduan Menulis dan Mempresentasikan Karya Ilmiah: Thesis, Tugas Akhir, dan Makalah*", ITB, 2005.

[4] Rahardjo, Budi, "*Slide Kuliah Kriptografi Keamanan Informasi*", ITB, 2010.

[5] Robshaw, Matthew, "*Algebraic Aspects of the Advanced Encryption Standard (Advances in Information Security)*", Springer-Verlag, 2005, pp.21-23.

[6] http://en.wikipedia.org/wiki/Cryptography/, tanggal akses 13 Desember 2010, pukul 16.20 WIB.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 17 Desember 2010
ttd

Rizkydaya Aditya Putra (13506037)