APLIKASI RSA DALAM SMART CARD DAN SECURITY TOKEN

Adriano Milyardi / 13509010
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
Codezero91@yahoo.com

Abstrak

***Makalah ini membahas tentang salah satu penerapan dari teori bilangan yakni penerapannya di bidang kriptografi. Kriptografi adalah ilmu yang mempelajari cara menjaga kerahasiaan dari informasi. Salah satu metodenya bernama RSA. RSA memanfaatkan konsep bilangan prima dan aritmatika modulo. Penerapan dari RSA ini terbilang cukup banyak karena RSA merupakan salah satu algoritma kriptografi yang lumayan sulit untuk dipecahkan, terutama bila semakin besar bilangan non primanya. Contoh penerapannya adalah enkripsi dari secure connection, database, smart card dan lain-lain*. Pada makalah ini, akan dibahas bagaimana RSA diterapkan pada smart card dan security token.**

Kata kunci **– Kriptografi, RSA, Security Token dan Smart Card.**

I. PENDAHULUAN

Kerahasiaan dari pesan mungkin bukanlah menjadi masalah jika pesan tersebut hanya merupakan pesan "biasa" seperti daftar kontak di telepon genggam kita, atau list dari pekerjaan yang harus diselesaikan. Namun akan berbeda ceritanya jika pesan yang ingin disampaikan dari pengirim ke penerima adalah pesan yang berisi informasi yang sangat penting seperti PIN kartu kredit, data keuangan perusahaan dan lain-lain. Kebocoran informasi yang penting tersebut ke "pihak lain" dapat sangat merugikan baik bagi pengirim maupun penerima pesan.

Maka untuk menjaga agar informasi penting diterima oleh orang yang tepat, dibentuklah semacam sandi yang hanya bisa dimengerti oleh penerima yang seharusnya. Orang-orang zaman dulu menjaga kerahasiaan informasi ini dengan berbagai cara, mulai dengan menggunakan kata sandi pada pengantar pesan, menggunakan simbol-simbol, alat khusus seperti scytale dan lain lain.

Bagian penting dari keamanan informasi ini adalah kerumitan atau kesulitan untuk memecahkan sandi jika ada seseorang yang tidak berhak mencoba mencuri informasi tersebut. Alat seperti scytale dapat dengan mudah dipecahkan menggunakan metode coba-coba atau brute force, dan sandi rahasia pada pengantar pesan dapat dengan mudah diatasi dengan memaksa pengantar pesan membocorkan informasi. Sehingga untuk mengatasi masalah-masalah tersebut zaman sekarang digunakan teknik khusus yang membuat pemecahan sandi menjadi jauh lebih rumit bahkan hampir mustahil dipecahkan.

II. KRIPTOGRAFI

Kriptografi adalah salah satu ilmu yang merupakan aplikasi dalam ilmu komputer. Ilmu kriptografi bahkan dianggap sebagai seni dalam menjaga kerahasiaan pesan baik yang merupakan data maupun informasi dengan cara menyamarkannya menjadi suatu sandi dengan pola tertentu. Selain pengertian tersebut kriptografi dapat pula diartikan sebagai ilmu yang mempelajari teknik-teknik bidang matematika yang berhubungan dengan aspek-askpek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, dan autentikasi data. Namun tidak semua hal yang berhubungan dengan keamanan informasi apat ditangani oleh kriptografi.

Ada empat tujuan yang mendasar dari ilmu kriptografi yang juga merupakan aspek keamanan informasi yakni

- Kerahasiaan, merupakan layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah disandi
- Integritas data, berhubungan dengan penjagaan dari pengubahan data secara tidak sah. Untuk menjaga integritas dari data, maka sistem harus memiliki kemampuan untuk mendeteksi manipulasi data yang dilakukan oleh pihak-pihak yang tidak berhak, manipulasi tersebut dapat berupa penyisipan, penghapusan dan pensubstitusian data lain kedalam data yang sebenarnya.
- Autentikasi, berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keasliannya, isi datanya, waktu pengiriman dan keterangan lainnya.

- Non-repudiasi, atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

Informasi yang bersifat rahasia tentu saja perlu disembunyikan agar tidak diketahui oleh merka yang tidak memiliki hak mengetahui informasi tersebut. Nomor PIN ATM atau kartu kredit, pesan yang bersifat rahasia dan hal lainnya tentu saja sangat penting agar informasi tersebut tidak diketahui oleh orang lain. Kriptografi dapat digunakan untuk menyembunyikan informasi rahasia tersebut dari pihak yang tidak berhak mengetahuinya.

Ide dari kriptografi adalah menyamarkan pesan, pesan yang disamarkan dapat dikembalikan lagi ke pesan aslinya sehingga dapat dibaca, namun hal tersebut hanya dapat dilakukan oleh orang yang berhak dan orang yang berhak tersebut memiliki metode atau sandi untuk mengembalikan isi pesan ke bentuk yang dapat dibaca. Pesan yang dirahsiakan dinamakan plainteks yang secara harafiah berarti teks jelas yang dapat dimengerti. Bentuk selanjutnya adalah chiperteks yang berarti teks yang sudah diberi sandi. Proses pengubahan dari bentuk plainteks ke bentuk chiperteks disebut dengan proses enkripsi dan proses mengembalikan informasi dari bentuk chiperteks ke bentuk plainteks disebut dekripsi.

Sebagai contoh, sebuah pesan rahasia (plainteks) berikut:

Kuliah di ITB itu susah dan stress

Disandikan menjadi chiperteks dengan suatu teknik kriptografi tertentu:

55,88,555,444,2,44 3,444 444,8,22 444,88,8 7777,88,7777,2,44 3,2,66 7777,8,777,33,7777,7777

Meskipun tidak bersifat rahasia lagi namun isi dari chiperteks sudah tidak dapat dimengerti maksudnya, hanya orang yang berhak yang dapat mengembalikan pesan yang tidak jelas tersebut ke bentuk yang dapat dibaca.

Proses menyamarkan informasi menggunakan pola tertentu. Proses tersebut dapat direalisakan dalam algoritma sandi. Algoritma sandi sendiri adalah algoritma yang berfungsi untuk melakukan tujuan kriptografis. Algoritma tersebut sebaiknya memiliki kekuatan dalam:

- Konfusi atau pembingungan , dari teks yang mudah dibaca sehingga sulit untuk disusun ulang secara langsung tanpa memanfaatkan algoritma dekripsinya.
- Difusi atau peleburan, dari teks yang mudah dibaca sehingga karakteristik dari teks tersebut hilang.

Sehingga dapat digunakan untuk mengamankan informasi. Pada implementasinya sebuah algoritma sandi harus memperhatikan kualitas layanan dari seluruh sistem dimana dia diimplementasikan. Algoritma sandi yang baik adalah algoritma sandi yang kekuatannya teretak pada kunci dan bukan pada kerahasiaan algoritma itu sendiri. Ada teknik tersendiri dalam menentukan kekuatan algoritma sandi yang dinamakan kriptanalisa.

Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara dua himpunan yaitu yang berisi elemen teks yang jelas /plainteks dan yang berisi elemen teks yang tersamarkan /chiperteks. Enkripsi dan dekripsi merupakan fungsi transformasi antara himpunan-himpunan tersebut. Apabila elemen-elemen plainteks dinotasikan dengan P, elemen-elemen chiperteks dinotasikan dengan C, sedang untuk proses enkripsi dinotasikan dengan E, dekripsi dengan notasi D.

Enkripsi : $E(P) = C$

Dekripsi : $D(C) = P$ atau $D(E(P)) = P$

Secara umum berdasarkan kesamaan kuncinya, algoritma sandi dibedakan menjadi :

- kunci-simetris/symetric-key, sering disebut juga algoritma sandi konvensional karena umumnya diterapkan pada algoritma sandi klasik
- kunci-asimetris/asymetric-key

Berdasarkan arah implementasi dan jamannya dibedakan menjadi :

- algoritma sandi klasik classic cryptography
- algoritma sandi modern modern cryptography

Berdasarkan kerahasiaan kuncinya dibedakan menjadi :

- algoritma sandi kunci rahasia secret-key
- algoritma sandi kunci publik publik-key

Pada skema kunci-simetris, digunakan sebuah kunci rahasia yang sama untuk melakukan proses enkripsi dan dekripsinya. Sedangkan pada sistem kunci-asimentris digunakan sepasang kunci yang berbeda, umumnya disebut kunci publik(public key) dan kunci pribadi (private key), digunakan untuk proses enkripsi dan proses dekripsinya. Bila elemen teks terang dienkripsi dengan menggunakan kunci pribadi maka elemen teks sandi yang dihasilkannya hanya bisa didekripsikan dengan menggunakan pasangan kunci pribadinya. Begitu juga sebaliknya, jika kunci pribadi digunakan untuk proses enkripsi maka proses dekripsi harus menggunakan kunci publik pasangannya.

Pada zaman modern ini, kriptografi sudah lazim dimanfaatkan dalam sistem pengamanan komputer, sebagai contoh dalam pengiriman data maupun untuk penyimpanan data di dalam disk storage. Data yang ditransmisikan melalui saluran telekomunikasi (sebagai contoh telepon) dapan direpresentasikan dalam bentuk

chiperteks. Di tempat penerima chiperteks dikembalikan lagi menjadi plainteks hanya oleh pihak yang berhak yang memegang kunci rahasia saja.

III. RSA (RIVEST-SHAMIR-ADLEMAN)

A. Sejarah

RSA adalah sebuah algoritma pada enkripsi public key. RSA merupakan salah satu algoritma pertama yang cocok untuk digital signature seperti halnya enkripsi dan salah satu yang paling maju dalam bidan kriptografi public key. RSA masih digunakan secara luas dalam protokol electronic commerence dan dipercaya dalam pengamanan dengan memanfaatkan kunci yang cukup panjang.

Pertama kali diperkenalkan oleh tiga orang peneliti dai MIT (Massachussets Institute of Technology), tiga orang peneliti tersebut adalah Ron Rivest, Adi Shamir, dan Len Adleman, pada tahun 1976. Pada tahun 1973 sebenarnya ada seorang matematikawan inggris bernama Clifford Cocks yang bekerja untuk GCHQ semacam badan pemerintah yang bergerak di bidang komunikasi di Inggris telah menjabarkan tentang sistem equivalen pada dokumen internal negara, namun baru terungkap pada tahun 1997 karena alasan *top-secret clssification*. Algoritma tersebut akhirnya dipatenkan oleh Massachusetts Institue of Technology pada tahun 1983 di Amerika Serikat sebagai U.S. Patent 4405829. Paten tersebut berlaku hingga 21 September 2000. Semenjak Algoritma RSA dipublikasikan sebagai aplikasi paten, regulasi di sebagian negara-negara lain tidak memungkinkan penggunaan paten. Hal ini menyebabkan hasil temuan Clifford Cocks dikenal oleh umum sehingga paten di Amerika Serikat tidak dapat dimatenkannya.

B. Dasar Teori

RSA memiliki dasar proses enripsi dan dekripsinya pada konsep bilangan prima dan aritmatika modulo. Kunci dekripsi dan enkripsi keduanya merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diketahui oleh umum sehingga kunci enkripsi biasa disebut juga dengan kunci publik, namun kunci untuk dekripsi bersifat rahasia. Kunci dekripsi dibangkitkan dari beberapa buah bilangan prima bersama-sama dengan kunci enkripsi. Untuk menemukan kunci dekripsi, orang tersebut harus memfaktorkan suatu bilangan non prima menjadi faktor primanya. Pada kenyataannya memfaktorkan bilangan non prima menjadi faktor primanya bukanlah pekerjaan yang mudah. Sampai saat ini belum ada algoritma yang benar-benar efektif untuk pemfaktoran tersebut. Semakin besar bilangan non primanya tentu saja semakin sulit pemfaktorannya. Semakin sulit pemfaktorannya, semakin kuat pula algoritma RSA-nya.

Sebagai contoh prosedur operasional pembangkitan kunci, dapat dilihat dari kasus dibawah ini. Misalnya ada seseorang bernama John berniat mengizinkan Alice temannya untuk mengirimkan kepadanya sebuah pesan pribadi (*private message*) melalui media transmisi yang tidak aman (*insecure*). John akan melakukan langkah-langkah berikut untuk membuat pasangan kunci *public key* dan *private key*:

1. Dipilih dua bilangan prima $p \neq q$ secara acak dan terpisah untuk tiap-tiap p dan q. Kemudian dihitung $N = p\,q$. N hasil perkalian dari p dikalikan dengan q.

2. Dihitung M = (p-1)(q-1). Sekali M telah dihitung, a dan b dapat dihapus untuk mencegah agar tidak diketahui pihak lain.

3. Dipilih bilangan bulat (*integer*) antara satu dan M ($1 < e < M$) yang juga bersifat relatif prima terhadap M .

4. Bangkitkan kunci dekripsi, d, dengan kekongruenan $ed \equiv 1 (\text{mod } M)$. Lalu dilakukan enkripsi terhadap isi pesan dengan persamaan $c_i = p_i^e \text{ mod } N$, yang dalam hal ini pi 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.

5. Proses dekripsi dilakukan dengan menggunakan persamaan $p_i = c_i^d \text{ mod } N$, yang dalam hal ini d adalah kunci dekripsi.

bilangan prima dapat diuji probabilitasnya dengan menggunakan *Fermat's little theorem*- a^(n-1) mod n = 1 jika n adalah bilangan prima, diuji dengan beberapa nilai a menghasilkan kemungkinan yang tinggi bahwa n ialah bilangan prim. Untuk langkah 3 dan 4 dapat dihasilkan dengan algoritma *extended Euclidean*. Sedangkan langkah 4 dapat dihasilkan dengan menemukan integer x sehingga $d = (x(p\text{-}1)(q\text{-}1) + 1)/e$ menghasilkan bilangan bulat, kemudian menggunakan nilai dari $d \pmod{(p\text{-}1)(q\text{-}1)}$.

IV. SMART CARD

A. Deskripsi

Smart card adalah kartu berukuran kecil yang memiliki sirkuit terintegrasi. Secara umum ada dua jecis dari kartu dengan sirkuit terintegrasi. Memory card yang hanya memiliki komponen memori tetap dan mungkin logika keamanan yang sudah diatur sebelumnya. Mikroprosessor memiliki memori yang bisa berubah dan komponen mikroprosessor. Kartu itu sendiri terbuat dari plastik, biasanya *polyvinyl chloride*, tapi terkadang juga terbuat dari *acrylonitrile butadiene styrene* atau *polycarbonate*. Smart cards juga memungkinkan untuk menyediakan tingkat keamanan yang kuat untuk autentifikasi dari akses pada organisasi besar.

B. Sejarah

Pada tahun 1968 seorang ilmuwan roket dari Jerman bernama Helmut Grottup dan temannya Jurgen Dethloff menemukan kartu chip otomatis, dan mendapatkan paten pada tahun 1982, ketika bekerja di perusahaan Giesecke & Devirent di Jerman. Pertama kali digunakan secara masal, kartu tersebut dikenal sebagai *Télécarte* sebagai kartu telepon di Prancis.

Kemudian seorang penemu asal Prancis bernama Roland Moreno mematenkan konsep dari kartu memori pada tahun 1974. Pada tahun 1977, Michel Ugon dari Honeywell Bull menemukan kartu microprosessor. Pada 1978, Bull mematenkan Mikrokomputer Satu-chip yang dapat di program dan mendefinisikan arsitektur yang diperlukan untuk memrogram chip tersebut. Tiga tahun kemudian, Motorola menggunakan paten ini di "CP8". Pada masa itu, Bull sudah memiliki sebanyak 1200 paten yang berhubungan dengan smart card. Pada 2001, Bull menjual divisi CP8 dan hak patennya pada Schlumberg, yang kemudian menggabungkan departemen smart card internalnya dengan CP8 untuk membuat Axalto. Pada 2006, Axalto dan Gemplus yang ketika itu nomor satu dan dua dunia bergabung dan menjadi Gemalto.

Pemanfaatan kedua dari mikrochip terintegrasi adalah pada kartu debit Carte Bleue di Prancis pada tahun 1992. Para pelanggan memasukan kartu kepada sebuah terminal dan memasukan PIN, sebelum transaksi dijalankan. Hanya sedikit transaksi (seperti membayar biaya tol) yang diproses tanpa menggunakan PIN.

Peningkatan drastis dari pemakaian smart card sendiri dimulai pada sekitar tahun 1990, dengan pengenalan kartu SIM yang berbasis smart card yang pada akhirnya dimanfaatkan pada handphone dengan jaringan GSM di Eropa. Dengan mulai dikenalnya handphone di Eropa, pemanfaatan smart card pun semakin biasa pada berbagai peralatan elektronik.

V. SECURITY TOKEN

Sebuah security token mungkin berupa sebuah alat (berupa benda) yang digunakan oleh seorang pemakai yang memiliki hak untuk memberikan autentikasi. Selain berupa benda dengan bentuk fisik, dapat juga berupa sorftware tokens.

Security tokens digunakan untuk membuktikan identitas seseorang secara elektronik. Token dirancang sebagai pengamanan ganda selain kata sandi yang dimiliki oleh seseorang. Dapat diibaratkan bahwa token befungsi sebagai kunci elektrik yang digunakan untuk mengakses sesuatu.

Token biasanya berukuran cukup kecil untuk dibawa dalam saku atau dompet bahkan digunakan sebagai gantungan kunci. Beberapa ada yang menyimpan data penting yang sudah didekripsi, seperti *digital signature*, *data medis*, dan lain-lain. Bentuk dari token sendiri pun bermacam-macam, ada yang didesain tahan bantingan, ada yang membutuhkan PIN untuk mengaksesnya, ada yang didesain dengan menggabungkan konektor USB, bluetooth, wireless dan lai-lain.

Secara umum ada sekitar 4 jenis token:

1. Dengan sandi lewat yang statik
2. Sandi lewat dinamis yang sinkron
3. Sandi lewat asinkron
4. Challenge response

Pada makalah ini akan lebih difokuskan pada Token dengan sandi lewat dinamis yang sinkron.

Security token yang paling sederhana tidak memerlukan koneksi apapun ke komputer. Pengguna tinggal memasukan PIN pada tombol-tombol yang ada pada token tersebut. Token lain yang lebih canggih mungkin akan memanfaatkan teknologi wireless seperti bluetooth misalnya. Token-token seperti ini akan mentransfer data kunci pada klien lokal atau ke akses point terdekat.

Token juga ada yang memanfaatkan smart card, dimana salah satu keunggulannya adalah biayanya yang murah meskipun dengan mengorbankan umur token itu sendir Kelemahan ini disebabkan karena dengan memanfaatkan smart card, maka akan sering terjadi gesekan dengan alat untuk membaca smart card ketika akan dimasukan.

Varian lain dari token yang memanfaatkan smart card adalah token USB yang berbasiskan smart card. Token ini memiliki chip smart card didalamnya dan menghasilkan fungsionalitas dari usb token maupun smart card. Alat ini memungkinkan solusi dari pengamanan yang luas dan menghasilkan kemampuan dan tingkat keamanan yang sama dengan smart card traditional tanpa memerlukan alat penerima masukan yang khusus.

VI. APLIKASI RSA DALAM SMART CARD DAN SECURITY TOKEN

Aplikasi RSA dalam Smart Card terutama dalam Cryptographic Smart Card. Cryptographic Smart Card bisanya digunakan dalam single sign-on. Single sign-on atau biasa disingkat sebagai SSO adalah sebuah properti dari kontrol akses sistem perangkat lunak yang independen namun banyak dan berhubungan. Dengan sifatnya yang seperti ini, seorang pemakai melakukan log in sekali dan mendapatkan akses ke semua bagian dari sistem tanpa perlu melakukan log-in kembali disetiap bagiannya.

Smart Card yang paling canggih memiliki alat kriptographic khusus yang memanfaatkan algoritma antara lain RSA dan DSA. Cryptographic Smart Card yang sekarang dapat menghasilkan pasangan kunci secara on board, untuk menghindari resiko memiliki lebih dari satu salinan kunci (karena secara desain biasanya tidak ada cara utnuk mengambil private key dari sebuah smart card). Smart card yang demikian biasanya secara umum digunakan untuk digital signature dan identifikasi.

Cara paling umum untuk mengakses fungsi dari cryptographic smart card pada komputer dengan

memanfaatkan library PKCS#11 yang disediakan oleh vendor. Pada Microsoft Windows CSP API juga sudah bisa dimanfaatkan.

Algoritma kriptografi yang paling luas digunakan adalah Triple DES dan RSA (terkecuali "kripto algoritma" pada GSM). Set kunci biasanya di-load (DES) atau dibuat (RSA) pada kartu ketika tahap personalisasi. Beberapa dari smart card ini juga dibuat untuk mendukung standard NIST dari Personal Identity Verivication atau biasa disingkat dengan PIV.

Sedangkan pada Security token, RSA diterapkan pada komputer user yang menghasilkan kode untuk autentifikasi pada interval yang sudah ditentukan (biasanya 30 atau 60 detik) menggunakan sebuah built-in clock dan kunci random yang ada berasal dari pabrik. Untuk setiap token memiliki kunci yang berbeda, dan dimasukan kedalam Server RSA SecurID ketika token dibeli. Kode tersebut biasanya panjangnya sampai 128 bits.

Ketika sistem RSA SecurID memasukan sebuah strong layer security pada suatu jaringan kerja, mungkin dapat terjadi kendala jika clock autentifikasi pada server tidak lagi sinkron dengan clock yang ada pada token. Tapi biasanya kendala semacam ini dapat diperbaiki secara otomatis tanpa menganggu pengguna.

Meskipun RSA menyediakan proteksi terhadap penyerangan password yang bekelanjutan, RSA mungkin bisa dikatakan gagal dalam menyediakan proteksi yang layak terhadap serangan bertipe *man in the middle*. Tipe serangan seperti ini memiliki tipe serangan dimana si penyerang dapat memanipulasi autentifikasi dari aliran data antara user dan server, si penyerang kemudian dapat mengirimkan informasi autentifikasi dari server untuk dirinya sendiri dan pada akhirnya secara efektif dapat seakan-akan menjadi user yang seharusnya. Jika si penyerang dapat memblokir akses dari user yang seharusnya dari melakukan autentifikasi dengan server sampai kode selanjutnya yang dimasukan valid, si penyerang akan bisa melakukan log-in pada server.

Kelemahan fatal lainnya adalah dimana RSA tidak bisa menangani penyerangan dengan tipe *Man in the Browser*. Bentuk penyerangannya secara garis besar berhubungan erat dengan *Man in the Middle* , berupa sebuah virus trojan yang menginfeksi sebuah web browser dan memiliki kemampuan untuk mengubah halaman web, mengubah data transaksi atau memasukan transaksi fiktif, dan semuanya itu dapat seakan-akan tidak terlihat oleh user maupun aplikasi penyedia.

VII. KESIMPULAN

Algoritma RSA secara garis besar banyak dimanfaatkan secara luas untuk pengamanan data-data penting. Umumnya RSA dipakai untuk pengamanan data pada smart card, Security token dan autentifikasi ketika user akan melakukan log-in. Kekuatan utama dari algoritma RSA adalah lamanya waktu yang dibutuhkan jika seseorang yang tidak berhak ingin memecahkan algoritma tersebut untuk mengambil suatu data atau autentifikasi. RSA sulit ditembus oleh serangan terus menerus, terutama yang menggunakan metode brute force, dimana si penyerang berusaha menggunakan semua kombinasi dari kata lewat yang mungkin.

Namun demikian ternyata RSA sendiri memiliki kelemahan ketika harus menghadapi tipe penyerangan dengan metode Man in the Middle dan Man in the Browser. Karena tipe penyerangan ini tidak secara frontal memecahkan sandi lewat untuk mencapai target, namun memanipulasi data setelah autentifikasi pertama kali terjadi. Karena tipe penyerangan ini cenderung digunakan untuk data yang berhubungan dengan network, maka bisa disimpulkan bahwa RSA kurang efektif untuk menangani pengamanan data yang berhubungan dengan jaringan yang luas.

REFERENSI

[1] Munir, Rinaldi. Ditktat Kuliah IF 2091 Struktur Diskrit . Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, Hal V-21 – V-27

[2] http://en.wikipedia.org/wiki/SecurID
Tanggal akses: 14 Desember 2010

[3] http://en.wikipedia.org/wiki/Man_in_the_Browser
Tanggal akses: 14 Desember 2010

[4] http://en.wikipedia.org/wiki/Smart_card
Tanggal akses: 14 Desember 2010

[5] http://en.wikipedia.org/wiki/Security_token
Tanggal akses: 14 Desember 2010

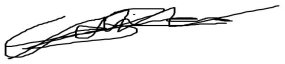
.

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, 14 Desember 2010

ttd



Adriano Milyardi / 13509010