TIMOR CERDAS – Jurnal Teknologi Informasi, Manajemen Komputer dan Rekayasa Sistem Cerdas

Vol.1, No.1, Juni 2022

PENERAPAN KRIPTOGRAFI DENGAN METODE RSA PADA INTERNET BANKING
(STUDI KASUS: SECURITY TOKEN DAN SMART CARD)

Bonie Empy Giri
Program Studi Teknologi Informasi, Universitas Citra Bangsa, Kupang
Jl. Manafe No.17 Kel. Kayu Putih Kec. Oebobo Kupang-NTT
Email : angibonie@gmail.com

Abstrak

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 serta akan membahas tentang implementasi kriptografi yang di gunakan dalam penggunaan security token dan penerapan security token dalama penggunaan internet banking di Indonesia..

Kata Kunci - Kriptografi, RSA

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 di sampaikan 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 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.

A. Kriptografi

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita [bruce Schneier - Applied Cryptography]. Selain pengertian tersebut terdapat pula pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data [A. Menezes, P. van Oorschot and S. Vanstone - Handbook of Applied Cryptography]. Tidak semua aspek keamanan informasi ditangani oleh kriptografi.

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

•Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.

•Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

•Autentikasi, adalah 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 keaslian, isi datanya, waktu pengiriman, dan lain-lain.

•Non-repudiasi., atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman /terciptanya suatu informasi oleh yang mengirimkan atau 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 nformasi 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 dirahasiakan dinamakan plainteks yang secaraharafiah 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.

B. RSA (Rhivest Shamir Adleman)

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 mematenkannya.

II. 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 menjadifaktor 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.

Pada algoritma RSA terdapat 3 langkah utama yaitu key generation (pembangkitan kunci), enkripsi, dan dekripsi.

III. ANALISA DAN PEMBAHASAN

Kunci pada RSA mencakup dua buah kunci, yaitu public key dan private key. Public key digunakan untuk melakukan enkripsi, dan dapat diketahui oleh orang lain. Sedangkan private key tetap dirahasiakan dan digunakan untuk melakukan dekripsi.

Pembangkitan kunci atau key generation dari RSA adalah sebagai berikut :

1. Pilih dua buah bilangan prima sembarang a dan b. Jaga kerahasiaan a dan b ini.
2. Hitung n = a * b. Besaran n ini tidak perlu dirahasiakan.
3. Hitung m = (a-1) * (b-1). Sekali m telah dihitung, a dan b dapat dihapus untuk mencegah diketahuinya oleh pihak lain.
4. Pilih sebuah bilangan bulat untuk kunci publik, sebut namanya e, yang relative prima terhadap m (relatif prima berarti GCD(e, m) = 1) dengan syarat

$$e \neq (p-1),\ e \neq (q-1), \text{dan } e < n$$

5. Hitung kunci dekripsi, d, dengan kekongruenan $ed \equiv 1 \pmod m$.

Blok-blok plainteks dinyatakan dengan p1, p2, p3, ... (harus dipenuhi persyaratan bahwa nilai pi harus terletak dalam himpunan nilai 0, 1, 2, ..., n-1 untuk menjamin hasil perhitungan tidak berada di luar himpunan).

Pada langkah kelima pembangkitan kunci atau key generation, kekongruenan

$ed \equiv 1 \pmod m$ sama dengan $ed \bmod m = 1$. Sehingga dapat pula dikatakan bahwa $ed \equiv 1 \pmod m$ ekivalen dengan

$ed = 1 + km$.

Maka d dapat dihitung dengan cara yang sederhana dengan persamaan

Dengan mencoba nilai k = 1, 2, 3, ..., diperoleh nilai d yang bulat. Nilai itu yang akan dipakai sebagai kunci pribadi untuk dekripsi pesan.

Dalam implementasi sebenarnya, nilai a dan b diharapkan sangat besar sekali (misalnya 100digit) agar pekerjaan memfaktorkan n menjadi faktor

primanya menjadi sangat sukar, sehingga lebih susah untuk ditembus.
Contoh penerapan algoritma RSA.
1. Menentukan bilangan acak a dan b
a = 13
b = 5
2. Hitung n dan m
n = 13 * 5 = 65
m = 12 * 4 = 48
3. Cari nilai e
GCD(e, 48) = 1
Misalnya,
e = 2 maka GCD(2, 48) = 2
e = 3 maka GCD(3, 48) = 3
e = 4 maka GCD(4, 48) = 4
e = 5 maka GCD(5, 48) = 1 , jadi digunakan e = 5
4. Lalu cari nilai d

Misalnya
k = 1 maka d = 9,8
k = 2 maka d = 19,4
k =3 maka d = 29, jadi digunakan d =29

Kita coba mengenkripsi pesan menggunakan angka-angka yang telah didapatkan. Misalkan pesan yang dikirim adalah angka 48.
E = 48 ^ 5 mod 65
= 254803968 mod 65
= 3
Setelah dilakukan enkripsi, didapat nilai sekarang adalah 3. Kemudian akan kita coba lakukan dekripsi pada nilai tersebut.
D = 3 ^ 29 mod 65
= 68630377364883 mod 65
= 48
Perhatikan bahwa nilai yang didapat sama dengan nilai awal, yaitu 48.
Kekuatan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan menjadi faktor primanya, dalam hal ini memfaktorkan n menjadi a dan b. Karena sekali n berhasil difaktorkan, maka menghitung nilai m adalah perkara mudah. Selanjutnya, walau nilai e diumumkan, perhitungan kunci d tidaklah mudah pula karena nilai m yang tidak diketahui.

4. Kemanan pada internet banking
Hal-hal yang menjadi ancamanan pada internet banking antara lain phising, keylogger, dan man in the middle. Phising adalah upaya untuk mencuri data pribadi seperti nama pengguna, sandi lewat, dan nomor rekening dengan cara meniru sebagai instansi terkait pada jalur komunikasi elektronik. Salah satu contoh phising adalah meniru sebuah situs milik bank tempat nasabah melakukan transaksi atau mengirim surat elektronik kepada nasabah dengan berpurapura sebagai bank terkait untuk meminta data pribadi yang diperlukan. Kegiatan yang pertama lebih sering disebut dengan website spoofing.

Keylogger adalah sebuah aplikasi yang berjalan secara tersembunyi pada sistem operasi sebuah komputer yang digunakan terutama untuk merekam aktivitas pengguna komputer tersebut. Dalam hal ini, aplikasi ini member ancaman yakni merekam nama pengguna serta sandi yang dimasukkan oleh nasabah pada situs internet banking. Para pemasang keylogger kemudian dapat mengambil rekaman tersebut dan menggunakannya untuk hal-hal yang tidak diinginkan.

Gambar 1. Model Internet Banking Bank BCA

Man In The Middle, adalah sebuah serangan di mana penyerang dapat membaca dan memodifikasi pesan-pesan yang dikirim oleh nasabah dengan sistem informasi bank atau sebaliknya Karena begitu banyaknya ancaman keamanan pada fasilitas internet banking maka sekarang bank-bank menambahkan lapisan keamanan yang lebih tinggi yakni berupa security token
5. Smart Cart
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

6. Security Token

Di dalam mengautentikasi seseorang ada 3 macam hal yangdigunakan untuk diidentifikasi dari orang tersebut.

1. Something that user knows, yakni sesuatu yang diketahui oleh pengguna seperti tanggal lahir, nama ibu, sandi lewat, PIN dan lain-lain.
2. Something that user has, yakni sesuatu yang dimiliki oleh pengguna seperti sidik jari, retina mata, dan lain-lain.
3. Something that user is, yakni siapa pengguna tersebut.

Security Token adalah sebuah objek fisik yang digunakan untuk autentikasi pada sebuah sistem. Alat ini biasanya didesain berukuran kecil sehingga dapat dibawa-bawa oleh nasabah dan kemudian dapat digunakan sewaktu-waktu untuk melakukan transaksi. Di dalam proses pengautentikasian, security token termasuk di dalam something that user has. Selain mengautentikasi nama dan sandi, bank juga perlu mengetahui tanda dari security token yang dimiliki oleh nasabah yakni data-data yang dimiliki oleh security token tersebut.

Bentuk-bentuk security token sangatlah bervariasi. Akan tetapi seperti yang disebutkan di atas, security token biasanya berukuran kecil sehingga dapat dibawa-bawa oleh
nasabah. Contoh bentuk-bentuk security token antara lain

1. Smart card
2. ID card
3. Papan bertombol
4. Handphone
5. Gantungan kunci
6. Pemancar Infrared/Bluetooth

Dengan adanya security token diharapkan keamanan pada sistem perbankan internet menjadi lebih kuat sehingga dapat melindungi kepentingan nasabah dan menumbuhkan kepercayaan nasabah pada bank.

7.Aplikasi RSA dalam Smart Cart 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 property 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 "kriptoalgoritma" 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 bias 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. 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 bias disimpulkan bahwa RSA kurang efektif untuk menangani pengamanan data yang berhubungan dengan jaringan yang luas.

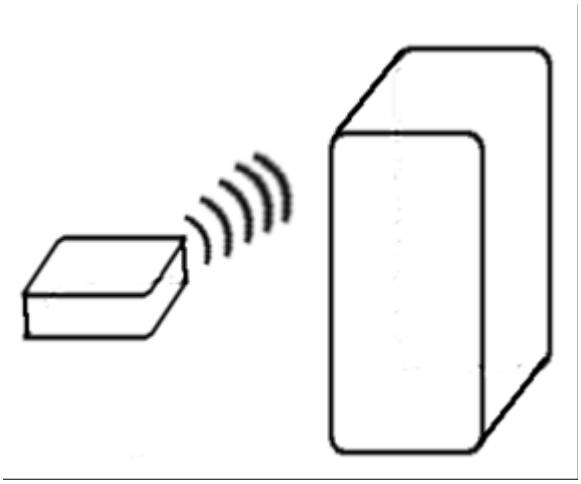
8. Implementasi kriptografi pada security token
Hal-hal yang menjadi fungsi jenis security token yang umum ada dan telah banyak dipatenkan : infrastruktur kunci publik, one time password, jalur komunikasi (communcation means)

8.1. Infrastruktur pada kunci public
Security token jenis ini berisi data identitas pengguna yang digunakan untuk penandatanganan
dijital. Dengan menggunakan infrastruktur kunci asimetrik, maka autentikasi yang dilakukan menjadi lebih aman.

Autentikasi pengguna ini berhasil dilakukan setelah pengguna menandatangani sejumlah data yang ditunjuk oleh protokol keamanannya (seperti SSL). Tandatangan dijital tersebut dihasilkan dari perhitungan yang dilakukan security token yang dilaksanakan setelah pengguna melakukan autentikasi pemegangan security token, seperti sandi lewat atau PIN (personal identification number).
Setelah autentikasi berhasil biasanya data mengenai pengguna seperti nama, alamat, tanggal kadaluarsa, diekstraksi oleh server masih menggunakan infrastruktur kunci publik untuk keperluan transaksi yang dilakukan oleh pengguna.

8.2. One time password
Ini disebut dengan OTP (One Time Password). Setelah suatu password dipakai, maka password yang sama tidak bisa lagi dipakai untuk kedua kalinya. Dengan cara ini tidak ada gunanya menyadap password yang dihasilkan token karena password tersebut tidak bisa dipakai lagi. Namun bila password tersebut di-intercept sehingga tidak pernah sampai ke server, maka password tersebut masih berharga karena di mata server, password itu belum pernah dipakai.

8.3. Communication Means
Security token jenis ini adalah security token yang dapat mentransmisikan datanya kepada server. Security token ini biasa diimplementasikan dalam bentuk RFID atau Bluetooth.



Gambar 3. Bluetooth Security Token
Ketika server mendeteksi keberadaan token, maka dengan segera server membangun sebuah jalur komunikasi aman dengan menggunakan pengenkripsian. Tujuannya adalah supaya data yang ditransmisikan tidak dicuri dengar oleh pihak lawan. Setelah jalur tersebut dibangun maka server akan mengautentikasi token berdasarkan data yang dimiliki oleh token tersebut. Selain itu token juga bisa digunakan dengan menggunakan jalur komunikasi lain seperti kabel data atau juga port USB (Universal Serial Bus)
Selain di atas, masih banyak lagi jenis-jenis security

token lainnya yang sedang dikembangkan.

9. Security Token Untuk Keperluan Internet Banking.
Seluruh token yang digunakan dalam fasilitas internet banking adalah token yang termasuk ke dalam jenis token yang dapat membangkitan one-time password. Sebagai contoh, penulis mengambil penyedia layanan internet banking yakni Bank BCA dan Bank Mandiri. Untuk layanan yang diberikan Bank BCA, tokennya diberi nama KeyBCA sedangkan Bank Mandiri diberi nama PIN Mandiri.
Kedua jenis token yang digunakan oleh kedua bank adalah token yang dikeluarkan oleh Vasco, sebuah perusahaan yang bergerak dibidang keamanan data di internet, yakni jenis DP250, DP250i, serta DP300 dengan menggunakan server Velis Authenticator (Server VA). Cara kerja token ini adalahdengan membangkitkan one-time password berdasarkan waktu.
Jenis aplikasi yang terdapat pada token jenis ini adalah
1.Aplikasi Response Only (RO), aplikasi ini memiliki 2 variable yaitu, seed value dan current time untuk membangkitkan sandi atau PIN.
2.Aplikasi Challenge Response (C/R), aplikasi ini memiliki 3 variable yaitu, seed value yakni nilai yang diinisialisasi pada awal perilisan token, dan current time (waktu pada saat token digunakan) dan challenge yaitu berupa angka dengan digit tertentu yang digenerate oleh server VA yang harus di input ke dalam token, untuk membangkitkan sandi atau PIN. Biasanya untuk Bank Mandiri, challenge code yang digunakan adalah rekening penerima transfer (jika menggunakan transfer) atau nomor tertentu milik recipient.
3.Aplikasi Digital Signature, aplikasi ini mirip dengan C/R, hanya saja challenge yang disediakan lebih dari 1 challenge (max 8) yang dapat diinputkan kedalam token, dan challenge ini tidak berasal dari server VA, bisa berupa angka dari mana saja. fungsi dari aplikasi ini salah satunya adalah untuk transfer uang antar rekening
field/challenge yang digunakan olek BCA/Mandiri adalah 3 buah. Field : nomor rekening pengirim, nomor rekening tujuan, dan nominal tranfer. Ketiga nilai ini akan dikomputasikan oleh token menjadi sebuah nilai lagi yang nantinya akan menjadi seed untuk sandi.
Seperti yang terlihat pada gambar 10, situs Internet Banking, membangkitkan nilai yakni challenge code yang akan dimasukkan ke dalam token. Dari challenge code ini kemudian dibangkitkan kunci konfirmasi yang digunakan oleh server untuk mengautentikasi.
Karena token ini bekerja berdasarkan waktu, maka sewaktuwaktu jika token kehabisan baterai atau karena suatu hal jam internal yang ada di dalam token tidak sinkron maka nasabah pemegang token diharuskan untuk segera menghubungi costumer service.

IV. PENUTUP

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.
Oleh kerena itu fasilitas Internet Banking, nasabah dapat dengan mudah melakukan transaksi perbankan dengan menggunakan internet. Fasilitas ini sudah banyak disediakan oleh bank-bank di Indonesia seperti Bank Mandiri dan BCA. Akan tetapi fasilitas ini rawan serangan keamanan seperti phising, keylogger, dan man in the middle. Oleh karena itu dengan menggunakan implementasi kriptografi berupa security token, maka kerahasiaan dan kepentingan nasabah dapat dilindungi dengan baik untuk meningkatkan kepercayaan nasabah terhadap bank.

11. 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: 30 july 2011

[3]Http://en.wikipedia.org/wiki/Man_in_the_Browser Tanggal akses: 30 july 2011
[4]http://en.wikipedia.org/wiki/Smart_card Tanggal akses: 30 july 2011
[5]http://en.wikipedia.org/wiki/Security_token Tanggal akses: 30 july 2011

[6]Agam, Leedor et.al. Security Token. World Intellectual Property Organization. 2004. Patent no. PCT/II.2004/000628

[7] De Cock, Deni et.al. Threat Modelling For Security Tokens In Web Applications. COSIC Research Group, Katholieke Universiteit Leuven. Belgium, 2004.

[8]Internet Banking Mandiri. http://ib.bankmandiri.co.id Terakhir di akses 30 july 2011

[9] Munir, Rinaldi. Bahan Kuliah IF5054 Kriptografi. Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung. 2006. Bandung

[10] Rollier, Alain et. al. Security Token And Method For Authenticating Of A User With The Security Token. World Intellectual Property Organization. 2006. Patent no. PCT/CH2006/000715

[11] Vasco. Strong User Authentication.