Kriptografi Dan Algoritma RSA

Wico Chandra (13509094)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
wicochandra@yahoo.com

Abstract

Dalam makalah ini dibahas mengenai kriptografi dan algoritma RSA. Kriptografi merupakan ilmu dan seni untuk menjaga kerahasian suatu informasi. Orang yang melakukan kegian di bidang kriptografi dinamakan kriptografer. Pesan kriptografi terdiri dari dua yaitu plainteks dan ciphertek. Plainteks merupakan pesan yang dapat dibaca dengan mudah dan sudah jelas, dan cipherteks adalah pesan yang isinya acak sehingga tidak dapat dibaca, pengacakan pesan tersebut menggunakan cara tertentu. Kriptografi terdiri dari dua yaitu simetri kriptografi dan asimetri kriptografi.

Saat ini algoritma kriptografi yang paling efektif adalah algoritma RSA, algoritma kriptografi ini sebenarnya sangat sederhana, yang diperlukan hanya dua bilangan prima. Yang menjadi kekuatan dari RSA ini adalah pencarian dua bilangan prima tersebut dari hasil kali kedua bilangan tersebut. Jika dua bilangan tersebut memiliki digit yang sedikit maka alogritma tersebut sangatlah lemah. Sang penemu menyarankan menggunakan bilangan prima dengan 100 digit. Sehingga tidak mungkin didapat karena membutuh waktu bermiliar tahun untuk mendapatkan kedua bilangan prima tersebut.

Index: Kriptografi. RSA, prima.

I. PENDAHULUAN

Dengan semakin berkembangnya sistem informasi dan komunikasi, kebutuhan manusia dalam melakukan komunikasi data pun semakin meningkat. Hal ini ditandai dengan berkembang pesatnya teknologi yangterkait di dalamnya, yaitu teknologi dan media transmisi. Tidak hanya melalui kabel, data pun dapat juga dikirim melalui media non-kabel (wireless) yang menggunakan udara sebagai medimerambatnya sinyal. Lewat sinyal yang merambat melalui udara, data dapat dikirimkan dari satu tempat ke tempat lain dengan mudah dan praktis. Namun, penggunaan media transmisi dalam pengiriman data memiliki permasalahan tersendiri yang perlu diperhatikan.

Penggunaan media transmisi memungkinkan pihak-pihak yang tidak memiliki kepentingan melihat bahkan mengubah isi data tersebut yang tentu saja membahayakan integritas data, terutama data yang bersifat sangat rahasia. Permasalahan ini pun meningkat seiring dengan semakin banyaknya data yang dikirimkan melalui media nonkabel. Dilihat dari karakteristiknya, media ini adalah yang paling rentan dengan pencurian data karena data dengan bebasnya merambat di udara sehingga siapapun dapat dengan mudah melihat isi data tersebut. Oleh karena itu, dibutuhkan suatu mekanisme yang dapat mengacak data (enkripsi) sehingga data tidak mudah dilihat dan diubah oleh pihak yang tidak memiliki kepentingan.

Kriptografi merupakan ilmu dan seni untuk menjaga kerahasiaan informasi dengan cara-cara tertentu. Teknik kriptografi biasa menggunakan matematika, tetapi teknik kriptografi dapat berupa gambar, pita kertas yang digulung, dan lain-lain. Menurut sejarah, kriptografi sudah lama digunakan oleh tentara Sparta di yunani pada permulaan tahun 400SM, sampai sekarang ini kriptografi digunakan untuk menyimpan rahasia seperti nomor PIN kartu kredit. Orang yang melakukan kegiatan di bidang kriptografi dinamankan kriptografer. Sedangkan orang yang melakukan analisis terhadap kriptografi dinamakan kriptanalis. Beda antara keduanya yaitu, jika kriptografi itu bertujuan untuk mengenkripsi dan dekripsi pesan dengan suatu kunci, sedangkan kriptanalisis bertujuan untuk mencari-cari kemungkinan plainteks yang terenkripsi tanpa menggunakan kunci.

kriyptografi sistem atau kriptositem adalah suatu fasilitas untuk mengkonversikan plaintext ke ciphertext dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan transformasi pencipheran tertentu disebut suatu kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi. Secara umum, kunci-kunci yang digunakan untuk proses pengenkripsian dan pendekripsian tidak perlu identik, tergantung pada sistem yang digunakan.

Pesan yang dirahasiakan dianamakan *plainteks* (*plainteks* artinya teks jelas yang dapat dimengerti) sedangkan pesan yang telah dienkripsikan adalah *cipherteks* (*cipherteks*, artinya teks tersandi). Pesan yang telah disandikan dapat dikembalikan menjadi pesan yang dimengerti dengan metode penyandian atau memiliki kunci penyandian yang hanya diketahui oleh pesandi. Proses menyandikan plainteks menjadi cipherteks disebut *enkripsi* dan proses membalikan cipherteks menjadi plainteks dinamakan *dekripsi* [1].

Kriptografi banyak digunakan baik oleh kalangan diplomat, orang militer, pebisnis, dan mungkin cakupan yang lebih luas lagi karena sekarang sudah banyak berkembang komunikasi dan bahkan transaksi elektronik. Dalam hal ini kriptografi berguna untuk menghindari terjadinya hal-hal seperti interruption,

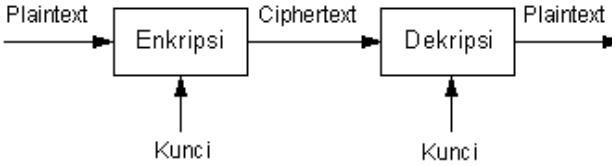
interception(penyadapan), fabrication, modification, dll. Ini beberapa manfaat dari kriptografi, misalnya pengamanan dalam transaksi di mesin ATM, transaksi dengan kartu kredit, percakapan telepon, bahkan pengaktifan peluru kendali. Enkripsi pada kartu kredit lebih sering menggunakan DES (Data Encryption Standard) maupun RSA. Dalam hal ini DES merupakan jenis algoritma kriptografi dalam stream cipher yang menggunakan kunci sepanjang 56 bit, input dan output sebanyak 128 bit. Di sini RSA merupakan salah satu bentuk algoritma public key yang paling dikenal, menggunakan suatu perhitungan matematis dengan mencari GCD (*Great Common Divisors*).

Sebagai contoh, sebuah pesan *plainteks* berikut

```
Uang disimpan di balik buku X
```

Disandikan menjadi cipherteks dengan suatu teknik kriptografi tertentu menjadi:

```
J&kloP(d$gkhtpuBn%6^k1p..t@
```



Gambar 1.1 Proses sederhana kriptografi

II. SEJARAH KRIPTOGRAFI

Berdasarkan sejarah, kriptografi sudah digunakan oleh orang Sparta pada permulaan 400SM. Sejarah kriptografi zaman dulu menggunakan alat yang bernama *scytale*, alat tersebut merupakan penyandian dengan menggunakkan daun papyrus yang dililitkan pada batang pohon yang mempunyai diameter tertentu. Pesan ditulis secara horizontal pada daun papyrus, selanjutnya setelah daun dilepas, maka yang akan terliahat pada daun papyrus hanyalah rangkaian huruf yang tak berarti (cipherteks). Selain menggunakan daun, ada juga menggunakan tattoo untuk mengirimkan pesan rahasia seperti yang digunakan oleh Herodotus.

Gambar 2.1 Gambar scytale

Kemudian ditemukan telegram Zimmermann yang membawa Amerika pada Perang Dunia I. Dahulu pada zaman Perang Dunia II, Jerman dan jepang menggunakan Kriptografi dalam keperluan militernya, yakni jerman dengan Enigma-nya dan jepang dengan Purple. Namun akhirnya, pemecahan algorima mesin sandi Jerman, Enigma, akhirnya menyebabkan berakhirnya Perang Dunia II [4].

III. KRIPTOGRAFI

1. Kriptografi Sistem

Suatu kriptosistem terdiri dari sebuah algoritma, seluruh kemungkinan plainteks, ciperteks, dan kunci-kunci. Secara umum kriptosystem dapat digolongkan menjadi dua, yaitu:

1. Kriptosistem simetri

Dalam symmetric cryptosystem ini, kunci yang digunakan untuk proses enkripsi dan dekripsi pada prinsipnya identik, tetapi satu buah kunci dapat pula diturunkan dari kunci yang lainnya. Kunci-kunci ini harus dirahasiakan. Oleh karena itulah sistem ini sering disebut sebagai secret-key ciphersystem. Jumlah kunci yang dibutuhkan umumnya adalah :

$$C_2^n = \frac{n.(n-1)}{2}$$

n adalah banyak pengguna.

2. Kriptosistem Asimetri

Dalam assymmetric cryptosystem ini digunakan dua buah kunci. Satu kunci yang disebut kunci publik (public key) dapat dipublikasikan, sedang kunci yang lain yang disebut kunci privat (private key) harus dirahasiakan. Proses menggunakan sistem ini dapat diterangkan secara sederhana sebagai berikut : bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca surat tersebut, ia perlu mendekripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut, karena adanya mekanisme ini. Contoh sistem ini antara lain RSA Scheme dan Merkle-Hellman Scheme.

Kriptosistem yang bai harus memiliki karakteristik sebagai berikut:

- Kerahasiaan kunci adalah keamanan system bukan pada algoritma.,
- Harus memiliki ruang kunci yang besar,
- Kriptosistem yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh test statistic yang dilakukuan terhadapnya, dan
- Kriptosistem yang baik mampu menahan seluruh serangan yang telah diketahui sebelumnya.

2. Protokol Kriptografi

Protokol kriptografi adalah suatu protocol yang menggunakan kroptografi. Protokol ini melibatkan sejumlah algoritma kriptografi, namun secara umum tujuan hanya untuk kerahasian. Protokol sebenarnya digunakan untuk mengabtraksikan proses penyelesaian suatu tugas dari mekanisme yang digunakan.

Penyerangan terhadap kriptografi dilalkukan dapat dengan tujuan memperoleh algoritma kriptografi yang digunakan dalam protocol, teknik kriptografi yang digunakan untuk mengimplementasikan algoritma dan protocol, dan protocol itu sendiri. Seseorang dapat menjadi penyerang pasif, seseorang yang menyadap sebagian atau seluruh protocol tapi tidak mengubah protocol tersebut melainkan hanya untuk memperoleh

informasi, penyerang aktif, seseorang yang mengubah protocol dengan tujuan untuk kecurangan.

3. Penyerangan Kriptografi

Tujuan penyerangan kriptografi adalah untuk mengetahui beberapa plaintext yang sesuai dengan ciphertext yang ada dan berusaha menentukan kunci yang memetakan satu dengan yang lainnya. Plaintext ini dapat diketahui karena ia merupakan standar atau karena pendugaan. Jika suatu teks diduga berada di dalam suatu pesan, posisinya mungkin tidak diketahui, tetapi suatu pesan lazimnya cukup pendek sehingga memungkinkan cryptanalyst menduga plaintext yang diketahui dalam setiap posisi yang mungkin dan melakukan penyerangan pada setiap kasus secara paralel.

Suatu algoritma enkripsi yang kuat tidak hanya mampu bertahan terhadap serangan plaintext yang dikenal tetapi juga mampu bertahan terhadap adaptive chosen plaintext. Dalam penyerangan ini, cryptanalyst berkesempatan memilih plaintext yang digunakan dan dapat melakukannya secara berulang kali, memilih plaintext untuk tahap N+1 setelah menganalisis hasil tahap N.

Yang dimaksud cryptanalytic attacks adalah usaha-usaha yang dilakukan seseorang untuk memperoleh informasi ataupun data yang telah dienkripsi. Secara ringkas terdapat tujuh macam basic cryptanalytic attacks berdasarkan tingkat kesulitannya bagi penyerang, dimulai dari yang paling sulit adalah :

- *Ciphertext-only* attack, seorang cryptanalyst memiliki cipherteks dari sejumlah pesan yang seluruhnya telah dienkripsi mengunakan algoritma yang sama,
- *Known-plaintext* attack, cryptanalyst memiliki akses tidak hanya ke chperteks sejumlah pesan, tai ia juga memiliki plain teks pesan-pesan tersebut.
- Chosen-plaintext attack. cryptanalyst tidak hanya memiliki akses atas ciphertext dan plaintext untuk beberapa pesan, tetapi ia juga dapat memilih plaintext yang dienkripsi.
- Adaptive-chosen-plaintext attack. Penyerangan tipe ini merupakan suatu kasus khusus chosen-plaintext attack. Cryptanalyst tidak hanya dapat memilih plaintext yang dienkripsi, ia pun memiliki kemampuan untuk memodifikasi pilihan berdasarkan hasil enkripsi sebelumnya. Dalam chosen-plaintext attack, cryptanalyst mungkin hanya dapat memiliki plaintext dalam suatu blok besar untuk dienkripsi; dalam adaptive-chosen-plaintext attack ini ia dapat memilih blok plaintext yang lebih kecil dan kemudian memilih yang lain berdasarkan hasil yang pertama, proses ini dapat dilakukannya terus menerus hingga ia dapat memperoleh seluruh informasi.
- Chosen-ciphertext attack. Pada tipe ini, cryptanalyst dapat memilih ciphertext yang berbeda untuk didekripsi dan memiliki akses atas plaintext yang didekripsi.
- Chosen-key attack. Cryptanalyst pada tipe penyerangan ini memiliki pengetahuan tentang hubungan antara kunci-kunci yang berbeda.
- Rubber-hose cryptanalysis. Pada tipe penyerangan ini, cryptanalyst mengancam, memeras, atau bahkan memaksa seseorang hingga mereka memberikan kuncinya.

III. ALGORITMA RSA

Algoritma RSA diperkenalkan oleh tiga peneliti dari MIT (*Masschussets Institute of Technology*), yaitu Ron Rivest, Adi Shamir, dan Len Adleman, pada tahun 1976. RSA merupakan teknik kriptografi dengan memanfaatkan 2 bilangan prima. Dari kedua bilangan prima tersebut dapat diperoleh sebuah *Public Key* (digunakan untuk mengenkripsi sebua plainteks) dan sebuah *Private Key* (digunakan untuk mengdekripsi cipherteks). Algoritma RSA merupakan teknik kriptografi yang paling efektif sampai saat ini, hal ini disebabkan karena butuh waktu yang sangat lama untuk mendapatkan *Private Key*.

Untuk mendapatkan private key orang tersebut harus mendapatkan dua bilangan prima yang hasil kalinya adalah Public key. Semakin sulit pemfaktorannya maka semakin kuat Algoritma RSA tersebut.

Sebenarnya Algoritma RSA sangat sederhana, terdiri dari tiga tahap yaitu pembangkitan pasangan kunci, Enkripsi, dan dekripsi.

1. Pembangkin pasangan kunci

Langkah-langkah melakukan pembangkit pasangan kunci adalah sebagai berikut:

- Pilih dua bilangan prima sembarang, sebut *a* dan *b*. jaga kerahasian *a* dan *b* ini.
- Hitung $n = a.b$. nilai dari n tidak perlu dirahasiakan.
- Hitung $m = (a - 1)(b - 1)$. Sekali *m* telah dihitung, *a* dan *b* dapat dihapus untuk mencegah diketahui oleh orang lain.
- Pilih sebuah bilanganbulat untuk kunci public, sebut namanya *e*, yang relative prima terhadap *m*.
- Hitung kunci dekripsi, *d*, dengan kekongruenan $ed = 1 \pmod m$.

2. Enkripsi

Langkah-langkah melakukan enkripsi adalah sebagai berikut:

- Nyatakan pesan menjadi: blok-blok plainteks: *p1, p2, p3,…* (harus dipenuhi persyaratan bahwa nilai *p*, harus terletak dalam himpunan nilai $0,1,2,\ldots,(n-1)$ untuk menjamin hasil perhitungan tidak berada di luar himpunan).
- Hitung blok cipherteks *c*, untuk blok plain teks *p*, dengan persamaan

$$c_i = p_i^{\,e} \bmod n$$

dalam hal ini, *e* adalah kunci public (*public*

key)

3. Dekripsi

Proses dekripsi dilakukan dengan menggunakan persamaan

$$p_i = {c_i}^d \ mod \ n$$

dalam hal ini, *d* adalah kunci privat (*privat key*).

Perhatikan Langkah ker-5 pada proses pembangkitan pasangan kunci. Kekonguenan *ed = 1 (mod m)* sama dengan *ed mod m = 1*. Dengan menggunakan pernyataan *a = b (mod m)* ekivalen dengan *a = b +km* maka *d* dapat dicari dengan rumus

$$d = \frac{1 + km}{e}$$

Dalam implementasinya, nilai *a* dan *b* disarankan memiliki nilai yang sangat besar (100 angka). Agar tidak mudah mendapatkan factor bilangan prima dari *n.*

Seperti yang telah dijelaskan di atas, kekuatan algoritma RSA itu bergantung pada tingkat kesulitan memfaktor *n* menjadi 2 bilangan prima. Dengan menggunakan komputer, pencarian factor bilangan prima menjadi mudah, oleh karena itu sang penemu menyarankan untuk memilih dua buah bilangan prima yang jumlah digitnya minimal 100 sehingga hasil perkalian kedua bilangan prima tersebut memiliki digit 200. Untuk mencari factor bilangan prima dari 200 digit tersebut dibutuhkan waktu 4 miliar tahun dengan kecepatan computer 1 mililidetik.

IV. APLIKASI ALGORITMA RSA

Salah satu aplikasi dari algoritma RSA adalah Tanda tangan digital. Tanda tangan digita adalah satu tandantangan elektronik yang dapat digunakan untuk membuktikan keaslian identitas pengirim dari suatu pesan atau penandatangan dari suatu dokumen, dan untuk memastikan isi yang asli dari pesan atau dokumen itu sudah dikirim tanpa perubahan. Tanda tangan digital dengan mudah dapat dipindahkan, tidak bisa ditiru oleh orang lain, dan dapat secara otomatis dilakukan time-stamp. Kemampuan itu untuk memastikan bahwa pesan asli yang tiba di pengirim tidak bisa dengan mudah diganti. Suatu tanda tangan digital dapat digunakan di segala macam pesan, apakah itu terenkripsi atau tidak, sehingga penerima dapat memastikan identitas pengirim itu dan pesan tiba secara utuh. Suatu sertifikat digital berisi tanda tangan digital dari sertifikat yang mengeluarkan otoritas sehingga siapapun dapat memverifikasi bahwa sertifikat itu adalah nyata.

Komponen-komponen dari suatu tanda tangan digital terdiri atas :

1. Kunci Publik. Semua orang mendapatkannya yang akan diguanakan pada system verifikasi
2. Nama dan alamat e-mail. Ini meyimpan informasi kontak untuk mengidentifikasi pengguna,
3. Tanggal jatuh tempo kunci publik: Bagian ini digunakan untuk menetapkan suatu umur simpan dan untuk memastikan bahwa dalam hal penyalahgunaan yang diperpanjang suatu tandatangan pada akhirnya tandatangan itu diatur ulang
4. Nama dari perusahaan: Bagian ini mengidentifikasi perusahaan yang tandatangan menjadi anggota juga.
5. Nomor urut dari Digital ID: Bagian ini adalah nomor yang unik yang digabung pada tandatangan untuk pertimbangan identifikasi iklan perkerjaan mengikuti jalur khusus.
6. Tanda tangan digital dari CA (Sertifikasi Authority): Ini adalah suatu tandatangan yang dikeluarkan oleh otoritas yang mengeluarkan sertifikat.

Berikut adalah proses pemeriksaan tanda tangan digital:

1. Pengguna A mengirimkan dokumen yang ditandatangani Pengguna B.
2. Untuk memverifikasi tanda tangan pada dokumen, aplikasi pengguna B pertama menggunakan kunci publik otoritas sertifikat untuk memeriksa tanda tangan pada sertifikat pengguna A
3. Kesuksesan dari dekripsi sertifikat membuktikan bahwa otoritas sertifikat telah dibuat.
4. Setelah sertifikat tersebut adalah de-dienkripsi, perangkat lunak pengguna B dapat memeriksa apakah pengguna A adalah dalam performa yang baik dengan otoritas sertifikat dan bahwa semua informasi sertifikat mengenai identitas pengguna A belum diubah
5. Pengguna perangkat lunak B kemudian mengambil kunci publik Seorang pengguna dari sertifikat dan menggunakannya untuk memeriksa tanda tangan pengguna A. Jika kunci publik Seorang pengguna de-mengenkripsi tanda tangan berhasil, maka user B adalah meyakinkan bahwa tanda tangan itu dibuat menggunakan kunci pribadi pengguna A, untuk otoritas sertifikat telah disertifikasi kunci publik yang cocok.
6. Jika tanda tangan ditemukan valid, maka kita tahu bahwa penyusup tidak mencoba untuk mengubah isi ditandatangan [6].

V. KESIMPULAN

Dari penjelasan diatas dapat diambil kesimpulan bahwa sampai saat ini, algoritma RSA adalah yang paling efektif dalam penyembunyian informasi. Algoritma RSA menjadi sangat efektif karena untuk mendapatkan factor bilangan prima dari bilangan yang berdigit 200 lebih sangat membutuhkan waktu yang sangat lama.

Algoritma RSA juga digunakan pada tanda tangan digital yang sampai sekarang ini banyak digunakan oleh orang-orang terutuma seseorang yang bekerja pada perusahan besar

VI. ACKNOWLEDGMENT

Saya ucapkan terima kasih kepada Tuhan Yang Maha Esa atas berkatnya sehingga saya diberi kesempatan menulis makalah yang berjudul *Kriptografi dan Algoritma RSA* ini. Saya juga berterima kasih kepada dosen IF2091 atas pengajarannya yang sangat membantu dalam proses penulisan makalah ini. Tidak lupa juga kepada orang tua saya yang sudah mendidik dan meyekolah kan saya hingga mengijak ke tingkat perguruan tinggi. Begitu juga kepada teman-teman saya yang telah membantu dalam menyusun makalah ini sehingga dapat selesai dengan tepat waktu.

REFERENCES

[1] Rinaldi Munir, *Matematika Distrit.* Bandung: Informatika, 2005.
[2] Kenneth H. Rosen. *Discrete Mathematics and Its Application*. New York:McGraw Hills, 2007.
[3] http://ae89crypt5.blogspot.com/2010/05/pengantar-kriptografi.html 11 Desember 2010
[4] http://ae89crypt5.wordpress.com/2008/05/12/sejarah-kriptografi/ 11 Desember 2010
[5] http://tedi.heriyanto.net/papers/p_kripto.html 10 Desember 2010
[6] http://www.windowsecurity.com/articles/Digital_Signatures.html 12 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, 12 Desember 2010

Wico Chandra
(13509094)