Penerapan algoritma RSA dan Rabin dalam Digital Signature

Gilang Laksana Laba / 13510028
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
gilang.laba@students.itb.ac.id

Abstract*— Makalah ini membahas tentang penggunaan kriptografi dalam digital signature. Digital signature adalah suatu metode untuk menjaga keaslian file digital dengan cara mengenkripsi data-data didalamnya. Terdapat banyak sekali skema algoritma yang dipakai utuk mengenkripsi digital signature. Secara garis besar, algoritma tersebut dibagi dua, yaitu skema yang membutuhkan pesan adli dan skema yang tidak membutuhkan pesan asli. Algoritma yang akan dibahas adalah algoritma RSA dan Rabin. Algoritma Rabin merupakan bentuk modifikasi algoritma RSA. Penulis juga akan membahas perbandingan kedua algoritma ini.

Kata Kunci : Kriptografi, Digital Signature, Enkripsi, RSA, Rabin

I. PENDAHULUAN

Dewasa ini, perkembangan teknologi terjadi begitu pesat. Terbukti dengan makin banyaknya penggunaan komputer untuk keperluan sehari-hari. Hal ini menyebabkan melesatnya pertumbuhan produksi software sebagai salah satu kebutuhan dasar penguna komputer.

Penggunaan file-file digital pun makin menjamur di masyrakat, bahkan file digital telah menggantikan fungsi dari file analog. Contohnya adalah lebih banyaknya pendistrisibusian lagu lewat file mp3 dibanding kaset biasa. Hal ini adalah sesuatu yang wajar mengingat fleksibilitas dan kemudahan yang ditawarkan produk digital.

Namun, hal ini juga menimbulkan beberapa masalah baru, salah satunya adalah menjaga keaslian file tersebut. Contoh kasus, yaitu banyaknya penggunaan software ilegal yang dilakukan oleh para pengguna komputer. Industri musik digital pun terhambat, karena orang-orang cukup mendownload atau meminta pada kerabat untuk mendapat lagu yang diinginkan. Tentunya ini sangat mengurangi profit dari pihak produsen. Solusi yang diharapkan bisa mengatasi masalah ini adalah penggunaan tanda tangan digital atau *digital signature*. Cara ini membuat file hanya bisa dibaca oleh orang-orang tertentu saja. *Digital signature* dibuat menggunakan kriptografi dengan metode enkripsi tertentu. Metode enkripsi dalam digital signature sangat bervariasi. Perbedaan ini terletak pada algoritmanya yang mempengaruhi kekuatan dari sandi yang dibuat dan lamanya waktu yang dibutuhkan untuk mengenkripsi dan mendekripsi file tersebut. RSA merupakan salah satu algoritma yang digunakan untuk digital signature dan algoritma Rabin merupakan bentuk modifikasi dari algoritma RSA.

II. DASAR TEORI

2.1 Kriptografi

2.1.1 Definisi Kriptografi

Kriptografi adalah ilmu yang menjaga kerahasiaan pesan dengan mengubahnya ke dalam bentuk sandi yang hanya bisa dimengerti oleh pengirim dan penerima pesan.Kriptografi sangat diperlukan pada era informasi seperti sekarang ini untuk menjaga kerahasiaan data-data yang penting. Aspek keamanan informasi sendiri kerahasiaan, keabsahan, integritas dan autentikasi data. Tujuan dasar kriptografi sendiri terbagi menjadi 4, yaitu:

1. Kerahasiaan : layanan yang membuat pesan data bisa dibaca oleh orang-orang yang tidak mempunyai hak untuk membaca pesan tersebut. Yang dapat mambaca hanyalah orang yang memiliki kunci dari data tersebut.

2. Integritas data : Sistem harus bisa melindungi file dari perubahan data yang dilakukan dengan tidak sah. Manipulasi yang dilakukan oleh orang yang tidak memiliki hak harus bisa dideteksi oleh sistem.

3. Autentikasi : Dua pihak yang berkomunikasi harus bisa memperkenalkan diri agar bisa melanjutkan komunikasi atau pertukaran pesan. Informasi yang harus sampai ke penerima adalah keaslian, isi data, waktu pengiriman dan lain-lain.

4. Non-repudiasi : Usaha untuk terjadinya gangguan dalam pengiriman atau pembuatan pesan.

Dalam kriptografi, pesan yang belum disamarkan disebut *plaintext* sedangkan pesan yang sudah berbentuk

sandi disebut *chipertext*. Dalam penggunaannya, *plaintext* diubah menjadi *chipertext* menuruti aturan tertentu. Chipertext ini lalu diberikan kepada penerima. Saat pengirimannya, penyadapan bukan menjadi masalah karena belum tentu penyadap mengerti isi dari *chipertext* ini. Setelah sampai di penerima, *chipertext* diubah lagi menjadi *plaintext* agar bisa dimengerti. Proses penyamaran dari plaintext ke chipertext ini disebut enkripsi (encrypt) sedangkan proses pembalikan dari chipertext ke dalam plaintext disebut dekripsi (decryption). Plaintext dilambangkan dengan P, chipertext dilambangkan dengan C. Fungsi enkripsi dituliskan dengan cara E(P)=C dan fungsi dekripsi dituliskan dengan cara D(C)=P.

2.1.2 Perkembangan kriptografi

Menurut sejarah, kriptografi sudah ada sejak 400 SM yang digunakan untuk keperluan perang. Kriptografi ini pertama kali digunakan oleh tentara sparta di Yunani. Metode kriptografi ini menggunakan daun papyrus dan batang pohon yang memiliki diameter tertentu. Daun papyrus dililitkan pada batang pohon tersebut, lalu pesan yang ingin dienkripsi dituliskan secara horizontal. Ketika daun papyrus dilepas dari batang, tulisan menjadi tidak bermakna ketika dibaca. Daun papyrus ini kemudian dikirim ke penerima. Penerima pesan harus memiliki batang pohon dengan diameter yang sama untuk bisa membaca pesan ini. Untuk membaca pesan yang disampaikan, penerima cukup melilitkan daun tersebut ke batang pohon yang dimiliki penerima. Kriptografi jenis ini disebut scytale.

Dapat kita lihat, enkripsi ini memiliki banyak kelemahan, salah satunya penerima dan pengirim harus memiliki batang dengan diameter yang sama.

Gambar 1. Scytale

Salah satu metode yang unik adalah kriptografi yang digunakan oleh Herodotus. Caranya adalah dengan mencukur habis rambut pada budaknya lalu pesan yang ingin disampaikan dituliskan pada kulit kepala budak tersebut. Rambut budak itu kemudian dibiarkan tumbuh dan setelah rambutnya menutupi pesan yang dituliskan, budak tersebut pergi ke tempat penerima pesan. Sampai disana rambut budak tadi dicukur lagi sampai habis agar penerima bisa membaca pesan. Selanjutnya yang menggunakan metode kriptografi adalah Julius Caesar, kaisar Romawi, dengan mengubah suatu karakter menjadi karakter lain. Huruf pada pesan asli diubah menjadi huruf ke-2 setelahnya. Contohnya dari A menjadi C. Sehingga ketika ingin menulis 'KRIPTOGRAFI', chipertextnya akan menjadi "MTKRVQITCHK". Pada metode yang telah dijelaskan, yang menjadi kekuatan pada kriptografi tersebut adalah kerahasiaan algoritmanya.

Pada zaman modern ini, kerahasiaan suatu algoritma tidak lagi menjadi kekuatan utama. Yang menjadi kekuatan utama adalah 'kunci' yang bisa merupakan bilangan bulat atau deretan karakter. Metode kriptografi dengan menggunakan kunci dibagi menjadi 2, yaitu algoritma simetris (private key) dan algoritma asimetris (public key). Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsi. Disebut juga private key karena kunci yang digunakan tidak boleh diketahui orang lain. Ini yang menjadi kelemahan algoritma simetris. Sedangkan algoritma asimetris adalah algoritma yang menggunakan kunci yang berbeda antara enkripsi dan dekripsi. Disebut juga public key karena kunci yang menjadi enkripsi boleh diketahui orang banyak. Kunci yang harus dijaga kerahasiannya adalah kunci untuk mendekripsi. Hal ini yang menjadi kelebihan algoritma asimetris. Kriptografi juga dibedakan lagi menjadi kriptografi yang mengenkripsi perblok dan yang mengenkripsi persatuan huruf. Penggunaan ini memiliki keuntungan dan kekurangan sendiri sehingga pengguna bebas menggunakan agoritma yang mana sesuai keadaan.

2.2 Digital Signature

Digital signature adalah identitas yang disatukan dengan suatu data sebagai identitas keaslian dari data tersebut. Tujuan dari adanya digital signature adalah menjaga keaslian file dan menghindari penggunaan data secara ilegal. Pembuatan digital signature ini menggunakan kriptografi dengan metode menggunakan public key. Tahapan penggunaan digital signature adalah sebagai berikut :

1. Pembuatan *pubilc key* dan *private key*.
Pembuatan key ini merupakan sesuatu yang sangat penting karena akan digunakan sebagai kunci untuk enkripsi dan dekripsi.

2. Pemberian digital signature.
Data yang ingin diberi signature diproses sesuai dengan algoritma yang digunakan. Langkah ini menggunakan private key. Signature yang dihasilkan kemudian digabungkan dengan data yang kita punya.

3. Verifikasi digital signature.
Langkah ini adalah untuk membaca data yang telah diberikan digital signature. Data yang ada diproses dengan algoritma pembalik dan public key yang sesuai. Jika valid, maka data bisa digunakan oleh user.

Terdapat bermacam-macam skema algoritma untuk pembuatan digital signature. Secara umum, skema algoritma ini dibagi menjadi 2 macam, yaitu:

1. Digital signature yang membutuhkan pesan asli, contoh : Skema DSA, ElGamal dan Schnorr,

2. Digital signature yang tidak membutuhkan pesan asli, contoh : skema RSA, Rabin dan Nyberg-Rueppel.

III. PEMBAHASAN

3.1. Algoritma RSA

Algortima pertama yang dipakai untuk dignital signature adalah RSA (Rivest – Shamir - Adleman). Langkah –langkah algoritma RSA dalam pembuatan digital signature adalah sebagai berikut :

1. Pembuatan public key dan private key
- Tentukan 2 buah bilangan prima secara acak. Sebut saja p dan q
- Hitung n = pq
- Hitung $\varphi = (p - 1)(q - 1)$
- Tentukan bilangan bulat $1 < e < \varphi$ yang relatif prima terhadap φ
- Hitung nila *d*, yaitu bilangan yang memenuhi $de \equiv 1 \mod \varphi$

Public key-nya adalah (e, n) dan *private key*-nya adalah d.

2. Pemberian signature
- Tentukan m yang memenuhi m<n, dengan m data yang diberikan signature
- Hitung $s = m^d \mod n$

S yang didapat merupakan *signature* dari m

3. Verifikasi
- Gunakan *public key* d untuk mendekripsi signature
- Hitung $m = s^e \mod n$

Contoh penggunaan algoritma RSA :

Suatu Perusahaan ingin memberikan suatu data kepada para karyawannya. Data ini bersifat penting sehingga hanya karyawan perusahaan tersebut yang boleh mengetahui isinya. Karyawan pun harus tau jika data yang diberikan telah diubah oleh pihak yang tidak berwenang. Data terebut berisi tulisan "TEST". Menurut tabel ASCII, huruf T kapital mempunyai biangan oktal 124, huruf E kapital mempunyai bilangan oktal 105 dan huruf S kapital mempunyai bilangan oktal 123. Dengan kata lain, saat mengirim data berisi tulisan TEST, perusahaan tersebut sebenarnya mengirim bilangan oktal 124-105-123-124.

Untuk menjaga keamanan pesan, direktur perusahaan tersebut memberikan digital signature. Berikut langkah yang dia lakukan :

1. Penentuan *private key* dan *public key*
- Untuk 2 bilangan prima acak, direktur itu memilih 73 dan 67
- n= 73 x 67= 4891
- $\varphi = (73 - 1) \times (67 - 1) = 4752$
- memilih 7 sebagai bilangan e
- Memilih 679 sebagai bilangan d karena memenuhi syarat $de \equiv 1 \mod \varphi$

Private key nya adalah 679 dan *public key*nya adalah 7. Kemudian direktur ini memberikan *public key* ke seluruh karyawannya. Saat ingin mengirimkan data, langkah yang dilakukan adalah

2. Pemberian signature
- Untuk huruf T, $S_T = 124^{679} \mod 4891 = 1669$
- Untuk huruf E, $S_E = 105^{679} \mod 4891 = 2048$
- Untuk huruf S, $S_s = 123^{679} \mod 4891 = 2713$

Direktur itu kemudian mengirimkan data berisi 1669-2048-2713-1669

Karyawan yang ingin membuka data dan memverifikasinya akan melakukan :

3. Verifikasi signature
- Untuk $m_1 = 1669^7 \mod 4891 = 124$
- Untuk $m_2 = 2048^7 \mod 4891 = 105$
- Untuk $m_3 = 2713^7 \mod 4891 = 123$

Karyawan perusahaan tersebut lalu akan merubah bilangan oktal tersebut ke huruf sesuai ASCII. Bila yang muncul adalah huruf tidak karuan, maka karyawan tahu kalo data tersebut telah diubah dalam pengirimannya. Jika yang keluar adalah tulisan "TEST" yang notabene bisa dimengerti karyawan, maka karyawan tahu bahwa data itu valid dan merupakan data yang dikirim oleh direktur.

Keamanan algoritma RSA dari penyerangan sangat tergantung pada penanganan masalah faktorisasi bilangan yang sangat besar. Membongkar algoritma RSA akan sangat mudah jika ditemukan metode faktorisasi yang sangat cepat. Pada zaman modern ini, bukan hal yang mustahil mendapatkan metode faktorisasi yang jauh lebih cepat dari sebelumnya, mengingat kemampuan komputasi komputer yang berkembang begitu cepat.

Pada tahun 2005, bilangan faktorisasi terbesar yang digunakan secara umum adalah 663 bit, sedangkan biasanya kunci RSA yang digunakan memiliki panjang antara 1024-2048 bit. Untuk memecahkan RSA dengan kunci 1024 bit, beberapa pakar yakin hal tersebut bisa dilakukan dalam waktu dekat ini. Untuk itu, untuk lebih menjamin keamanan data, mau tidak mau kita harus

menggunakan bilangan dengan 2048 bit. Tentu saja ini akan memakan waktu yang lama dalam mengenkripsinya. Semakin banyak data yang diproses suatu algoritma, makin banyak pula waktu yang dibutuhkan untuk menyelesaikannya. Hal ini yang membuat penggunaan algoritma RSA menurun. Pada tahun 1993, terbit algoritma Shor, yaitu algoritma yang menunjukkan bahwa sebuah komputer quantum dapat melakukan faktorisasi dalam waktu polinomial secara prinsip. Hal ini menyebabkan kemungkinan terbongkarnya algoritma RSA danalgoritma lain menajdi lebih besar. Namun perkembangan komputer quantum ini masih terhambat.

3.2 Algoritma Rabin

Algoritma Rabin merupakan bentuk modifikasi dari algoritma RSA. Langkah – langkah penggunaan algoritma Rabin dalam digital signature yaitu :

1. Pembuatan public key dan private key
   - Tentukan bilangan prima secara acak, sebut saja p dan q
   - Tentukan nilai n =pq

   N merupakan public key dan (p, q) merupakan private key

2. Pemberian signature
   - Hitung $c^2 = m \bmod n$. $m < n$, dengan m adalah data yang ingin diberikan signature

   C adalah data hasil pemberian signature

3. Verifikasi
   - Gunakan public key n
   - Hitung $m = c^2 \bmod n$

Keamanan algoritma Rabin sama seperti algoritma RSA dimana mengandalkan kesulitan pemfaktoran bilangan besar. Semakin N kecil, maka kode akan mudah untuk dipecahkan. Seperti algoritma RSA, jika ditemukan metode pemfaktoran bilangan besar, maka algoritma ini akan dengan mudah dipecahkan. Salah satu cara membobol algoritma ini adalah dengan *chosen chipertext attack*.

Yang menjadi pusat perhatian dari algoritma ini adalah bahwa algoritma ini terbilang kurang mangkus karena hasil enkripsi yang dilakukan menghasilkan 4 hasil sehingga penerima harus menentukan sendiri hasil mana yang paling benar. Dalam penggunaannya pun digunakan algoritma *chinese remainder theorem* yang membuat algoritma ini memakan waktu cukup lama.

3.3 Perbandingan antara algoritma RSA dan Rabin

Dari tingkat keamanan, kedua algoritma tersebut tidak jauh berbeda karena pada dasarnya rabin merupakan hasil modifikasi dari algoritma RSA. Kedua algoritma ini sama-sama mengandalkan sulitnya memfaktorkan bilangan berukuran besar (jika p dan q besar). Hasil enkripsi yang diberikan kedua algoritma ini terbilang cukup baik karena memiliki tingkat keamanan yang relatif tinggi.

Pada proses dekripsi, waktu yang dibutuhkan oleh kedua algoritma ini tidak berbeda jauh. Algoritma RSA melakukan dekripsi sedikit lebih lama dari algoritma Rabin. Namun, algoritma Rabin disebut kurang efektif karena terdapat 4 buah hasil dekripsi sehingga user harus menentukan lagi yang mana hasil yang sesuai. Namun, dalam penggunaan pada digital signature, hal itu tidak menjadi masalah karena yang melakukan dekrip adalah user yang memberikan signature pada data sehingga user dengan bebas menentukan hasil dekripsi mana yang akan ia gunakan.

Dilihat dari kerumitan pembuatan kunci,algoritma RSA memiliki kunci yang sedikit lebih rumit dari algoritma Rabin. Hal ini juga yang membuat algoritma Rabin lebih cepat dibanding RSA dalam pembuatan *key*. Namun perlu dicatat bahwa perbedaan waktu yang terjadi tidak terlalu signifikan. Komputer zaman sekarang menyebabkan lamanya waktu mengerjakan algoritma ini tidak berbeda jauh

IV. KESIMPULAN

1. Penggunaan kriptografi sangat banyak didunia ini, salah satunya untuk digital signature
2. Algoritma RSA dan algoritma Rabin bisa diaplikasikan untuk kriptografi pada Digital signature
3. Algoritma RSA dan Rabin mengandalkan kesulitan dari pemfaktoran bilangan besar
4. Algoritma RSA dan Rabin terbilang kurang efektif pada zaman sekarang ini
5. Dari segi kecepatan, algoritma Rabin sedikit lebih cepat dibandingkan algoritma RSA
6. Dari segi keamanan, kedua algoritma sama-sama mengandalkan sulitnya memfaktorkan bilangan besar
7. Dari segi kemangkusan, algoritma RSA relatif lebih mangkus dari algoritma Rabin
8. Penggunaan public key dan private key merupakan metode yang paling cocok digunakan pada zaman ini
9. Jumlah algoritma yang banyak membuat user dengan bebas memilih algoritma mana yang digunakan berdasarkan kemangkusan dan kecepatanya.

VI. REFERENSI

[1] http://en.wikipedia.org/wiki/Cryptography
[2] http://en.wikipedia.org/wiki/Encryption
[3] http://id.wikipedia.org/wiki/RSA
[4] http://en.wikipedia.org/wiki/Rabin_cryptosystem
[5] http://www.ta.trisakti.ac.id/ta/?q=node/1522

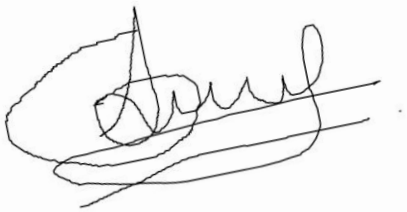
[6] http://ilmu-kriptografi.blogspot.com/2009/05/sejarah-kriptografi.html
[7] http://ae89crypt5.wordpress.com/2008/05/12/sejarah-kriptografi/
[8] http://ilmu-komputer.net/sejarah-kriptografi
[9] Munir, Rinaldi. "Matematika Diskrit", edisi ketiga. Bandung : Informatika, 2009.
[10] A. Menezes, P. van Oorschot, and S. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

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, 8 Desember 2011

Ttd



Gilang Laksana Laba / 13510028