Penerapan *Digital Signature* pada Dunia Internet

Nur Cahya Pribadi – NIM : 13505062

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if15062@students.if.itb.ac.id

Abstrak

Salah satu keuntungan berbisnis di dunia internet adalah dapat dilakukannya transaksi perdagangan dimana dan kapan saja tanpa harus adanya tatap muka atau fisik secara langsung. Dari segi keuntungan tersebut muncul permasalahan tersendiri, terutama yang berhubungan dengan autentikasi. Bagaimana penjual dapat yakin bahwa yang membeli produknya adalah orang yang sesungguhnya?Bagaimana penjual tahu bahwa yang kartu kredit yang digunakan adalah milik pembeli?Bagaimana penerima email tahu bahwa pesan yang diterimanya adalah benar-benar dari pengirim yang dimaksud dan juga dijamin kebenaran pesan yang terkirim?

Contoh diatas merupakan salah satu permasalahan di dunia internet yang dapat diselesaikan dengan *digital signature*. Masih ada banyak lagi permasalahan di dunia internet yang dapat diselesaikan dengan *digital signature* atau penggunaan *digital signature* untuk memperbaiki sistem *website*, misalnya di bidang *e-commerce*, *internet banking,* pengiriman pesan, dan lain sebagainya.

***Kata kunci**: Digital Signature,* Internet

1. Pendahuluan

Internet sudah sangat populer pada saat ini. Jangkauannya yang sangat luas dan bersifat global mempermudah menyebarkan informasi dan menjalin komunikasi antar penggunanya. Tidak sedikit pengguna internet memanfaatkan fasilitas ini untuk berjualan barang, berinteraksi sosial dengan pengguna lainnya, mempromosikan barang, dan lain sebagainya. Hal ini seakan-akan membuat diri sendiri dapat melakukan segala hal melalui internet.

Penerapan *digital signature* pada dunia internet sangat di butuhkan salah satu penyebabnya dikarenakan pengguna internet tidak dapat menjamin informasi yang didapatkan dari internet tersebut berasal dari orang yang dimaksud. Tidak sedikit orang yang memanfaatkan kekurangan tersebut untuk meraih keuntungan.

2. *Digital Signature*

Pada tahun 1976, Whitfield Diffie dan Martin Hellman adalah orang pertama yang menggambarkan gagasan skema *digital signature*. Tidak lama setelah itu Ronald Rivest, Adi Shamir dan Len Adleman menemukan algoritma RSA yang dapat digunakan untuk *digital signature*.

Pada tahun 1984, Shafi Goldwasser, Silvio Micalli, Ronald Rivest dan menjadi satu untuk menentukan kebutuhan keamanan dari skema digital signature.

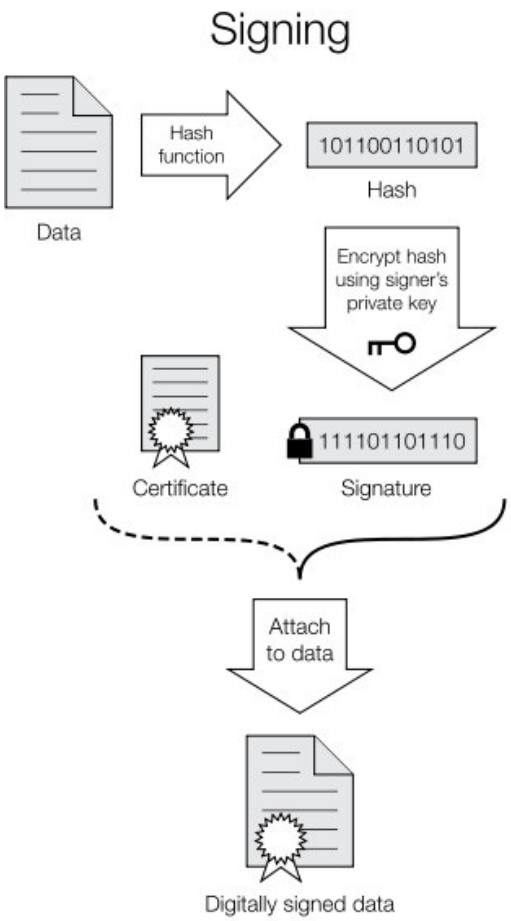
Digital signature adalah jenis kriptografi asimetrik. *Digital signature* ini digunakan untuk memastikan bahwa penerima menerima pesan yang diterima sungguh berasal dari pengirim yang dimaksudkan. *Digital signature* dapat disamakan dengan tanda tangan biasa, hanya saja untuk mengimplementasikannya lebih sulit. Kelebihan digital signature dibanding dengan tanda tangan sederhana adalah sulitnya untuk ditiru. Pesan yang telah ditandatangani dengan *digital signature* dapat direpresentasikan sebagai *bitstring*.

Skema dari *digital signature* terdiri dari 3 proses:

1. Proses pembangkitan kunci. Proses ini memilih kunci privat secara acak dari kumpulan kunci privat yang mungkin.

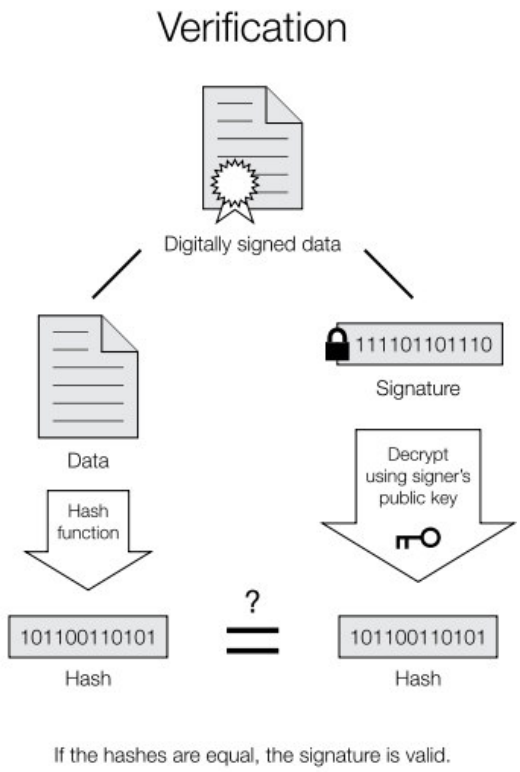
Hasil dari proses ini adalah kunci privat dan kunci publik yang sesuai.

2. Proses pemberian tanda tangan. Proses ini menerima isi pesan dan kunci privat, sehingga menghasilkan tanda tangan.



Gambar 1. Pemberian tanda tangan

3. Proses memverikasi tanda tangan. Proses ini memverikasi pesan yang telah terbubuhi tanda tangan. Proses memverikasi ini membutuhkan kunci publik.



Gambar 2. Verifikasi tanda tangan

3. Permasalahan

Ada beberapa permasalahan di dunia internet yang kerap dapat diatasi dengan *digital signature* yaitu :

1. Permasalahan pada *email*.
2. Permasalahan pada pengiriman paket.
3. Permasalahan identitas.

3.1 Permasalahan pada *Email*

Saat ini banyak email palsu yang menggunakan identitas seseorang, baik yang dihasilkan oleh program seperti worm ataupun sengaja dilakukan oleh pihak tertentu yang tidak bertanggung jawab. Dalam kondisi seperti ini penggunaan teknik otentifikasi pesan sangat diperlukan untuk memastikan bahwa email yang diterima dari pengirim valid.

Server email menerima pesan dan mengirimkannya ke alamat yang dituju seperti pengiriman surat yang tinggal dimasukkan ke kotak surat dan akan dikirimkan ke alamat yang dituju oleh tukang pos. Otentifikasi terhadap email pada umumnya hanya dilakukan terhadap alamat IP komputer pengirim, dan sepanjang alamat tersebut dianggap valid, maka siapapun dapat menulis email dari komputer tersebut.

Surat yang kita terima dari tukang pos isinya dapat mengatasnamakan siapapun juga. Tukang pos tidak boleh membuka isi surat tersebut untuk memastikan keabsahan pengirimnya. Tukang pos hanya bertugas untuk mengantarkan surat tersebut sampai ke alamat tujuannya. Tugas pengirim suratlah untuk menandai bahwa surat yang dikirimnya tersebut dapat dipercaya dan benar-benar berasal darinya misalnya dengan memberi tanda tangan. Pihak penerima surat harus dapat memastikan keaslian surat tersebut dengan cara memastikan identitas pengirim surat dan pihak penerima harus yakin bahwa surat yang diterimanya benar-benar ditulis oleh pengirimnya. Salah satu cara yang digunakan untuk memastikan surat tersebut adalah dengan mengecek tanda tangan yang ada di dalam surat tersebut dan stempel yang menunjukkan keaslian pengirim surat. Tanda tangan digital atau yang lebih dikenal dengan *digital signature* mempunyai fungsi yang sama dengan tanda tangan analog yang ditulis di atas kertas. *Digital signature* harus unik sehingga dapat membedakan pengirim yang satu degan yang lainnya. *Digital signature* juga harus sulit untuk ditiru dan dipalsukan sehingga integritas dan keabsahan pesan dapat terjaga. Dengan demikian diharapkan pencatutan identitas ketika pesan atau email tersebut dikirim dapat dihindari. Tidak hanya pencatutan identitas yang diharapkan dapat dihindari dengan membubuhkan *digital signature*, tetapi juga pengubahan pesan oleh pihak yang tidak berhak. Hal ini disebabkan karena pengubahan pesan digital apalagi yang sudah dibubuhi *digital signature* lebih jauh sulit dibandingkan dengan mengubah pesan yang ditulis di atas kertas.

3.1.1 Penerapan *Digital Signature* pada Permasalahan *Email*

Untuk penerapan *digital signature* ini dapat diterapkan dalam beberapa platform :

1. Email client.
2. Aplikasi dari server email.
3. Aplikasi terpisah.

Pada ketiga penggunaan aplikasi *digital signature* diatas hampir memiliki kesamaan dalam penggunaan. Penggunaan *digital signature* ini tidak terlalu sulit. Kedua belah pihak yang akan berkomunikasi harus menyiapkan sepasang kunci, yaitu kunci privat dan kunci publik. Kunci privat hanya dipegang oleh pemiliknya sendiri. Sedangkan kunci publik dapat diberikan kepada siapapun yang memerlukannya. Ketika pengirim ingin mengirimkan pesan yang penting, maka pengirim dapat menggunakan fitur *sign* untuk memberikan tanda tangan pada pesan. Penerima pesan pun menerima pesan yang terkirim. Penerima pesan dapat menverifikasi untuk memastikan pesan yang terkirim tidak berubah atau benar-benar dikirim oleh orang yang dimaksud.

3.1.3 Analisis Penerapan *Digital Signature* pada Permasalahan Email

Dari segi kelebihan, penggunaan *digital signature* pada permasalahan email ini sangat bermanfaat. *Digital signature* merupakan tindakan yang tepat karena prosesnya sangat cepat(terkecuali menggunakan bilangan prima yang besar dalam pembangkitan kunci, karena membutuhkan komputasi yang lama). Tidak perlu mengubah atau menambah prosedur dari komponen luar sistem.

Jika dilihat di segi kekurangan, penggunaan *digital signature* memiliki kekurangan yaitu menambahkan beberapa bit sebagai tanda-tangan pada pesan, tetapi kekurangan tersebut tidak terlalu berarti.

3.2.1 Permasalahan pada Pengiriman Paket

Pengiriman paket pada jaringan masih kurang cukup aman dengan melakukan enkripsi terhadap isi dari paket tersebut. Dimana dengan enkripsi tersebut hacker hanya tidak mampu membaca data yang terdapat pada jaringan tersebut. Ada kasus lagi dimana isi dari paket tersebut diubah atau ada pengiriman paket yang tidak dikenal oleh orang yang tidak bertanggung jawab. Terlebih lagi pengubahan paket atau pengiriman paket yang tidak dikenal tersebut berisi virus atau *worm* yang berbahaya bagi komputer. Oleh karena itu penerima paket harus dijamin bahwa paket yang diterima tersebut tidak berubah dan

benar-benar berasal dari pengirim yang dimaksud.

3.2.2 Penerapan *Digital Signature* pada Permasalahan Pengiriman Paket

Untuk mengatasi masalah ini maka diperlukan sebuah autentifikasi pada paket sehingga penerima paket dapat mengecek apakah paket tersebut benar-benar dikirim yang dimaksud dan tidak terdapat pada kontennya.

Untuk penerapan digital signature untuk permasalahan ini dapat diilustrasikan dengan contoh kasus dibawah ini :

Client melakukan *request* kepada server. Setelah menerima *request* dari client, server melakukan pembangkitan kunci, kunci privat maupun kunci publik. Kemudian kunci publik yang telah tercipta dikirimkan bersamaan dengan Ack ke client. Yang mana kunci publik tersebut digunakan untuk memverifikasi paket yang akan dikirimkan selanjutnya. Kemudian server melakukan tanda-tangan dengan parameter isi pesan dan kunci privat kepada paket yang sudah siap akan dikirim. Hal ini membuat penambahan bit pada paket yang dikirim. Kemudian paket dikirimkan ke client. Client yang menerima paket tersebut kemudian memverifikasi isi pesan tersebut dengan menggunakan kunci publik. Dari situ client dapat memastikan bahwa pesan yang dikirim benar-benar dari server yang dimaksud dan tanpa ada perubahan dari isi paket.

3.2.3 Analisis Penerapan *Digital Signature* pada Permasalahan Pengiriman Paket

Dari segi kelebihan, penggunaan *digital signature* pada permasalahan pengiriman paket sangat menjamin dari otentikasi paket. Penerima benar-benar dijamin bahwa pengirim paket tersebut berasal dari pengirim yang dimaksud.

Kekurangan penerapan digital signature ini adalah harus menggunakan bilangan prima yang kecil untuk membangkitkan kunci, karena dengan bilangan prima kecil mempercepat komputasi pembangkitan kunci. Kalau dengan bilangan prima yang besar maka komputasi memerlukan waktu yang lama, dan delay pada pengiriman paket sangatlah penting dalam jaringan. Jika pada permasalahan email, penambahan berapa bit menjadi tidak terlalu berarti, lain halnya dengan pengiriman paket, karena pengiriman paket tidak hanya sekali, tetapi berkali-kali.

3.3.1 Permasalahan pada Identitas

Setiap layanan online, baik itu gratis atau dipungut bayaran, selalu memiliki sejumlah persyaratan di antaranya meminta data pribadi calon pengguna. Hal ini erat kaitannya dengan proses otorisasi, meskipun juga ada "agenda tersembunyi" perusahaan penyedia layanan yang ingin mendapatkan database para konsumennya sebagai target promosi berikutnya.

Soal otorisasi memang merupakan salah satu perbincangan hangat di kalangan komunitas cyber dewasa ini karena menyangkut aspek keamanan dan kenyamanan berinternet juga. Contoh sederhana: misalkan sesorang punya *account* di sejumlah layanan *email* berbasis web, mengelola website pribadi, *chatting*, *mailing list*, belanja hingga main game online. Pasti orang tersebut diminta memasukkan identitas pribadi, setidaknya harus memiliki ID dan password. Karena untuk itu masing-masing layanan meminta jumlah karakter yang berbeda, akibatnya Anda harus memasukkan 10 ID dan 10 password untuk 10 layanan yang berbeda.

Bayangkan orang itu harus mengingat begitu banyak ID dan password, yang sering membuat dia bingung karena kata atau kode rahasia yang dimasukkan itu kadang bisa saling tertukar atau salah kombinasi.

Ketika dia meminta agar administratornya mengirimkan lagi password yang tersimpan di database mereka (dengan memanfaatkan fasilitas "*forget password*"), dia belum tentu sukses mendapatkannya karena data-data tersebut pasti dikirimkan ke email yang dia masukkan ketika mendaftar. Masalahnya, dia juga lupa ID dan password untuk membuka email itu.

3.3.2 Penerapan *Digital Signature* pada Permasalahan Identitas

Solusi yang tepat adalah membuat web portal identitas. Misalkan dibuat suatu web portal identitas yang dimana penggunanya dapat memasukkan informasi tentang dirinya. Dari informasi yang dikirimkan tersebut ditambahkan tanda-tangan. Dan pengguna portal tersebut

diberikan sebuah kunci, lebih tepatnya kunci privat dari pembangkitan kunci. Pengguna itu harus benar-benar mengingat kunci privat tersebut, karena dengan menggunakan kunci privat tersebut pengguna dapat melakukan register pada beberapa website.

Ketika pengguna ingin melakukan register ke suatu website, pengguna cukup harus memasukkan ID dan kunci privat yang diberikan oleh web portal identitas. Kunci privat itu hanya memverifikasi bahwa ID tersebut benar-benar merupakan milik pengguna.

Hal ini merupakan solusi bagi pengguna internet yang tidak mau direpotkan dengan menyimpan berbagai macam ID dan password, serta cocok sekali dengan pengguna internet yang serin merasa jenuh dengan mengisikan data-data pribadi lagi.

3.3.3 Analisis Penerapan *Digital Signature* pada Permasalahan Identitas

Kelebihan penggunaan *digital signature* pada kasus ini adalah membuat praktis setiap orang untuk melakukan register. Dilihat setiap hari pengguna internet semakin bertambah dan sudah semakin banyak web aplikasi yang membutuhkan identitas personal. Maka cara ini sangat berguna. Serta penggunaan dari *digital signature* lebih aman daripada menggunakan *password*, serta isi dari informasi lebih terjaga.

Kekurangan dari penerapan ini adalah membutuhkan prosedur dari sistem luar. Misalkan web A yang menggunakan fasilitas dari web portal identttitas ini haru mengikuti aturan dari web portal tersebut. Jadi tidak semua web yang dapat menggunakan *digital signature* tersebut sebagai pendaftaran, tetapi web-web yang sebelumnya sudah bekerjasama dengan web portal identitas tersebut.

4. Kesimpulan

Kesimpulan yang dapat diambil penerapan *digital signature* pada dunia internet ini adalah:

1. *Digital Signature* sangat bermanfaat diterapkan di dunia internet untuk kemudahan dan keamanan bagi pengguna internet. .

2. Ada permasalahan yang dapat terjadi di internet yaitu :
   - Permasalahan email
   - Permasalahan pengiriman paket
   - Permasalahan identitas

3. Kelebihan penerapan *digital signature* pada masalah email adalah penerima dijamin bahwa pesan yang diterima dari benar dari pengirim yang dimaksud. Kekurangannya adalah penambahan bit pada pesan.

4. Kelebihan penerapan *digital signature* pada masalah pengiriman adalah keamanan dan otentifikasi dari paket benar-benar terjaga.Sedangkan kekurangannya adalah butuh komputasi yang cepat dan penambahan bit pada pesan.

5. Kelebihan penerapan *digital signature* pada masalah identitkas adalah membuat pengguna internet lebih praktis dalam melakukan register pada web aplikasi.Sedangkan kekurangannya adalah masih membutuhkan prosedur dari web portal identitas untuk menerapkan sistem tersebut.

DAFTAR PUSTAKA

[1] Munir, Rinaldi. (2004). Bahan Kuliah IF3058 Kriptografi. Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung.

[2]Wordpress. *http://yurindra.wordpress.com/e-commerce/implementasi-digital-signature-dalam-proses-autenfitikasi/*. Tanggal akses: 20 Mei 2009 pukul 21:00.

[3] The gadget. *http://thegadget.wordpress.com/2002/09/10/78467145-48/*. Tanggal akses: 21 mei 2009 pukul 08:00.

[4] Indoskripsi. *http://one.indoskripsi.com/node/1662*. Tanggal akses: 21 mei 2009 pukul 10:00.