**Digital Signature**

**Mata kuliah Kriptografi**

**Dosen : Tri Ismardiko Widyawan**



**Disusun oleh:**

**Ariel Terence Prasetyo (2015-81-021)**

**Raka Setiaji (2015-81-007)**

**FAKULTAS ILMU KOMPUTER JURUSAN TEKNIK INFORMATIKA**

**UNIVERSITAS ESA UNGGUL**

**2017**

**KATA PENGANTAR**

Puji syukur kita panjatkan kepada Tuhan Yang Maha Esa atas kehadirat-Nya yang telah memberikan rahmat dan kasih sayang-Nya kepada kita semua sehingga tugas makalah ini dapat terselesaikan dengan baik dan tepat pada waktunya.

Adapun tujuan dari pembuatan makalah ini adalah untuk memenuhi tugas yang diberikan oleh dosen Tri Ismardiko Widyawan pada bidang studi Kriptografi. Selain itu, makalah ini juga bertujuan untuk menambah wawasan tentang Digital Signature sehingga dapat memperluas pengetahuan di era ini.

Kami mengucapkan terima kasih kepada Bapak Tri Ismardiko Widyawan yang telah memberikan tugas untuk mengembangkan kreativitas pola pikir serta wawasan sesuai bidang studi. Kami juga mengucapkan terima kasih kepada semua pihak yang telah membagi sebagian pengetahuannya untuk berbagi.

Kami menyadari sekali bahwa makalah ini jauh dari kesempurnaan baik dari segi bentuk penyusunannya ataupun secara keseluruhannya. Apabila terdapat salah penulisan kami mohon maaf yang sebesar-besarnya.

Dengan demikian, kami ingin mengucapkan terima kasih untuk kesempatan yang diberikan dalam menyusun makalah ini. Semoga melalui makalah ini dapat memberikan manfaat yang baik untuk kita semua.

  Jakarta, Desember 2017

                                                                                             Ariel Terence

BAB I  
PENDAHULUAN

**1.1 Latar Belakang**

Perkembangan teknologi yang semakin pesat seiring berjalannya waktu membuat inovasi di berbagai aspek kehidupan manusia. Di masyarakat Indonesia baik dari sektor pekerjaan ataupun pendidikan tentunya tidak luput dari pengaruh teknologi. Banyaknya kasus penyalahgunaan identitas di Indonesia memunculkan suatu inovasi baru untuk lebih mengautitenfikasi identitas. Pengiriman dokumen baik berupa email ataupun surat langsung juga saat ini dibutuhkan keaslian pengirim yang harus terpercaya.

Banyaknya kasus yang terjadi seperti saat Kita menerima surat yang datang lewat tukang pos dan didalamnya mengatasnamakan siapapun. Karena memang tukang pos tidak berkepentingan dengan validitas isi surat tersebut. Tugas utama dia adalah mengantarkan surat ke alamat tujuan, tanpa memedulikan siapapun pengirimnya. Sudah menjadi tanggung jawab pengirim surat untuk menandai surat tersebut sehingga dapat dipercaya (trusted) bahwa memang pesan yang ditulis berasal darinya. Sedangkan di sisi penerima pesan, harus terdapat sebuah cara sehingga dia dapat mengetahui identitas pengirim pesan dan cukup yakin bahwa pesan tersebut memang ditulis oleh yang bersangkutan.

Banyaknya penipuan yang melalui kegiatan surat baik surat langsung maupun surat elektronik (E-Mail) butuh penanganan khusus dan perbaikan teknologi untuk mengantisipasi hal tersebut.

Dewasa ini aspek keamanan dalam segala hal mulai dipertimbangkan sebagai satu factor yang penting. Aspek keamanan mulai juga dihidupkan dalam dunia elektronik dan dunia maya. Kriptografi adalah salah satu langkah kemajuan pemikiran tentang keamanan yang dilakukan dalam bidang elektronik dan telekomunikasi. Digital signature atau tanda tanga elektronik menjadi salah satu implementasi krptografi dalam kehidupan sehari-hari teknologi Digital signature untuk memastikan keaslian dan keamanan dokumen. Sebuah platform yang dapat diterapkan atau digunakan oleh berbagai sistem yang sudah berjalan ataupun sistem yang akan dikembangkan. Sistem ini berfungsi untuk memberikan jaminan bahwa dokumen digital adalah otentik. Menambahkan sistem Digital signature proses transfer dokumen akan terjamin otentikasi dan kerahasiannya. Dengan demikian dapat menghindari kemungkinan terjadinya pemalsuan dokumen terkait.

Berdasarkan latar belakang diatas , menarik untuk dibahas bagaimana sebenarnya proses kerja dari system Digital Signature tersebut, dan apakah sudah cukup untuk mengatasi kasus pemalsuan dokumen yang kerap terjadi di kalangan masyarakat.

**1.2 Identifikasi Masalah**

1. banyaknya kasus penipuan terkait pemalsuan pengirim dokumen

2. Efektifitas Teknologi Digital Signature

**1.3 Rumusan Masalah**

Bagaimana kerja digital signature dan efektifitas teknologi tersebut?

**1.4 Tujuan Penulisan**

Untuk mengetahui apa itu teknologi Digital Signature dan bagaimana cara kerja dari teknologi tersebut

**1.5 Manfaat Penulisan**

1. Secara Teoris

Memberikan pemahaman yang lebih baik dan memberikan pandangan untuk berinovasi terhadap penggunaan Digital Signature di berbagai bidang

2. Secara Praktis

Sebagai bahan masukan atau pertimbangan bagi masyarakat ataupun pihak pemerintah dan swasta mengenai pentingnya otentifikasi dokumen baik yang mereka kirim ataupun terima.

BAB II  
TINJAUAN PUSTAKA

**2.1. Pengenalan Kriptografi**

Menurut Sadikin (2012), kriptografi adalah ilmu yang bersandarkan pada teknik matematika yang berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Dalam kriptografi, pesan yang mempunyai makna disebut plaintext, dan pesan yang tidak bermakna lagi disebut ciphertext. Dua proses utama dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah transformasi plaintext menjadi ciphertext, sedangkan transformasi sebaliknya dari cipherteks menjadi plainteks semula disebut dekripsi. Baik enkripsi maupun dekripsi, proses keduanya melibatkan penggunaan kunci (key). Sistem kriptografi (yang terdiri atas algoritma kriptografi, kunci, plaintext, dan ciphertext) dapat digolongkan menjadi dua kelompok: sistem kriptografi simetri dan sistem kriptografi asimetris (kunci-publik). Kunci untuk enkripsi sama dengan kunci untuk dekripsi. Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu kunci tertentu yang sama untuk dipakai bersama, dan kunci ini harus sangat rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini disebut juga sebagai algoritma kunci rahasia (secret-key algorithm). Contoh algoritma kriptografi simetri diantaranya adalah DES, Blowfish, Twofish, Triple-DES, IDEA, AES, LOKI, GOST, dan lain-lain.

Kriptografi terbagi atas dua kategori yaitu kriptografi klasik dan kriptografi modern. Kriptografi klasik adalah sistem kriptografi yang menggunakan penyandian kunci simetris dan menggunakan metode subtitusi (pergantian huruf) atau transposisi (pertukaran tempat). Dan kriptografi modern adalah sistem kriptografi yang menggunakan penyandian kunci asimetris (Sadikin, 2012). Ada 4 (empat) aspek-aspek keamanan yang disediakan oleh kriptografi (Munir, 2006), yaitu:

1. Kerahasiaan Kerahasiaan (Confidentiality) merupakan layanan yang digunakan untuk menjaga isi pesan dari siapapun yang tidak berhak untuk membacanya. Didalam kriptografi, layanan ini umumnya direalisasikan dengan cara menyandikan pesan menjadi bentuk yang tidak dapat dimengerti.

2. Integritas Data Integritas data (integrity) merupakan layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan,dan pengsubsitusian data lain kedalam pesan yang sebenarnya.

3. Otentikasi Otentikasi (Authentication) merupakan layanan yang berhubungan dengan identifikasi. Baik mengidentifikasi benaran pihak-pihak yang berkomunikasi (user authentication dan entity authentication) maupun mengidentifikasi kebenaran sumber pesan (data origin authentication). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi juga harus diotentikasi asalnya. Otentikasi sumber pesan secara implisit juga memberikan kepastian integritas data, sebab jika pesan telah dimodifikasi berarti sumber pesan sudah tidak benar. Oleh karena itu, layanan integritas data selalu dikombinasikan dengan layanan otentikasi sumber pesan.

4. Anti Penyangkalan Anti Penyangkalan (non-repudiation) merupakan layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengiriman pesan menyangkal melakukan pengiriman atau penerimaan pesan menyangkal telah menerima pesan.

**2.2. Tanda Tangan Digital (Signature Digital)**

Tanda tangan digital adalah mekanisme otentikasi yang mengijinkan pemilik pesan membubuhkan sebuah sandi pada pesannya yang bertindak sebagai tanda tangan. Tanda tangan dibentuk dengan mengambil nilai hash dari pesan dan mengenkripsi nilai hash pesan tersebut dengan kunci privat pemilik pesan (Stallings, 2005). Prinsip yang digunakan dalam tanda tangan digital ini adalah dokumen yang dikirimkan harus ditandatangani oleh pengirim dan tanda tangan bisa diperiksa oleh penerima untuk memastikan keaslian dokumen yang dikirimkan. Fungsinya adalah untuk melakukan validasi terhadap data yang dikirim. Tanda tangan digital menggunakan algoritma yang disebut dengan istilah hashing algorithm. Fungsi tersebut akan menghasilkan sebuah kombinasi karakter yang yang unik yang disebut Message Digest. dengan cara ini pengirim bertanggungjawab terhadap isi dokumen dan dapat di cek keaslian dokumen oleh penerima. Keunikannya adalah jika di tengah perjalanan data mengalami modifikasi, penghapusan maupun di sadap diam-diam oleh hacker walaupun hanya 1 karakter saja, maka message digest yang berada pada si penerima akan berbeda dengan yang dikirimkan pada awalnya. Keunikan lainnya adalah message digest tersebut tidak bisa dikembalikan lagi ke dalam bentuk awal seperti sebelum disentuh dengan fungsi algoritma, sehingga disebutlah sebagai one-way hash (Sianturi, 2008). Fungsi utama dari tanda tangan digital pada pada aspek keamanan kriptografi adalah non-repudiation atau anti penyangkalan dimana apabila dokumen valid maka pengirim tidak bisa menyangkal bahwa keberadaan dokumen benar dikirim oleh pengirim yang bersangkutan. Suatu tanda tangan digital dapat digunakan di segala macam pesan, apakah itu terenkripsi maupun tidak, sehingga penerima dapat memastikan identitas pengirim itu dan pesan tiba secara utuh.

**2.3. Fungsi Hash**

Fungsi hash merupakan suatu fungsi yang menerima masukan berupa string yang panjangnya sembarang dan mengonversi masukan tersebut menjadi string yang mempunyai panjang tetap (fixed) dan umumnya menjadi lebih kecil dari panjang semula. Keluaran dari fungsi hash disebut juga nilai hash atau pesan-ringkas (message digest). Fungsi hash sering juga disebut fungsi satu arah (one way function), message digest, fingerprint, fungsi kompresi, dan message authentication code (MAC). Fungsi ini biasanya diperlukan bila kita menginginkan pengambilan sidik jari suatu pesan. Dinamakan fungsi kompresi karena biasanya masukan fungsi satu arah ini selalu lebih besar dari keluarannya, sehingga seolah-olah mengalami kompresi. Namun kompresi hasil fungsi ini tidak dapat dikembalikan ke asalnya sehingga disebut sebagai fungsi satu arah. Dinamakan sebagai message digest karena seolah-olah merupakan inti sari pesan mestinya merupakan ringkasan pesan yang masih dipahami maknanya, sedangkan disini justru sebaliknya, malahan dengan diketahuinya sidik jari ini, justru orang diharapkan tidak tahu pesan aslinya (Kurniawan, 2004).

Fungsi hash satu arah merupakan fungsi satu arah (one way function) yang dapat menghasilkan ciri (signature) dari data (berkas, stream). Perubahan satu bit saja akan mengubah keluaran hash secara drastis. Fungsi hash biasanya digunakan untuk menjamin integritas dan tanda tangan digital.

BAB III  
PEMBAHASAN

**3.1 Sejarah Digital Signature**

Pada tahun 1976, Whitfield Diffie dan Martin Hellman pertama kali menggambarkan gagasan tentang skema tanda tangan digital, walaupun mereka hanya menduga bahwa skema semacam itu ada berdasarkan fungsi peralihan satu arah jalan jebakan. Segera setelah itu, Ronald Rivest, Adi Shamir, dan Len Adleman menemukan algoritma RSA, yang dapat digunakan untuk menghasilkan tanda tangan digital primitif (walaupun hanya sebagai bukti-konsep - - tanda tangan RSA "polos" tidak aman). Paket perangkat lunak pertama yang dipasarkan untuk menawarkan tanda tangan digital adalah Lotus Notes 1.0, dirilis pada tahun 1989, yang menggunakan algoritma RSA. Skema tanda tangan digital lainnya segera dikembangkan setelah RSA, tanda tangan Lamport yang paling awal, tanda tangan Merkle (juga dikenal sebagai "pohon Merkle" atau hanya "pohon Hash"), dan tanda tangan Rabin.

Sedangkan pada tahun 1984, Shafi Goldwasser, Silvio Micali, dan Ronald Rivest menjadi orang pertama yang secara ketat menentukan persyaratan keamanan skema tanda tangan digital. Mereka menggambarkan sebuah hirarki model serangan untuk skema tanda tangan, dan juga mempresentasikan skema tanda tangan GMR, yang pertama yang dapat terbukti mencegah pemalsuan eksistensial terhadap serangan pesan terpilih yang merupakan definisi keamanan yang berlaku saat ini untuk skema tanda tangan. Skema pertama yang tidak dibangun pada fungsi trapdoor melainkan pada keluarga fungsi dengan properti permutasi satu arah yang jauh lebih lemah disajikan oleh Moni Naor dan Moti Yung.

**3.2 Digital Signature**

Tanda tangan digital adalah tanda tangan elektronik yang dapat digunakan untuk mengotentikasi identitas pengirim pesan atau penandatangan dokumen, dan mungkin untuk memastikan bahwa konten asli dari pesan atau dokumen yang telah dikirim tidak berubah. Tanda tangan digital mudah diangkut dan tidak dapat ditiru oleh orang lain, juga bisa dicap secara otomatis di setiap waktu. Kemampuan untuk memastikan bahwa pesan asli yang ditandatangani tiba berarti pengirim tidak dapat menyangkalnya nanti.

**Keunggulan Digital Signature**

* Memberikan keaslian, integritas dan ketidaktaatan pada dokumen elektronik
* Untuk menggunakan Internet sebagai media yang aman dan aman untuk e-Governance dan e-Commerce

**Sifat – sifat yang dimiliki tanda tangan** **digital**

adalah sebagai berikut :

* Otentikasi

Otentik berarti tidak bisa bahkan sulit untuk ditiru oleh orang lain.Pesan dan tanda tangan pesan tersebut juga dapat menjadi barang bukti sehingga penanda tangan takbisa menyangkal bahwa dulu ia tidak pernah menandatanganinya . Meskipun pesan seringkali dapat mencakup informasi tentang entitas mengirim pesan, bahwa informasi mungkin tidak akurat. Tanda tangan digital dapat digunakan untuk otentikasi sumber pesan. Ketika kepemilikan kunci rahasia tanda tangan digital terikat kepada pengguna tertentu, tanda tangan yang sah menunjukkan bahwa pesan yang dikirim oleh pengguna tersebut. Pentingnya kepercayaan yang tinggi dalam otentisitas pengirim ini terutama jelas dalam konteks keuangan. Misalnya, kantor cabang bank mengirimkan instruksi ke kantor pusat meminta perubahan saldo account. Apabila kantor pusat tidak yakin bahwa pesan tersebut benar-benar dikirim dari sumber resmi, bertindak atas permintaan semacam itu bisa menjadi kesalahan besar.

* Integritas

Dalam skenario banyak, pengirim dan penerima pesan mungkin memiliki kebutuhan untuk keyakinan bahwa pesan belum diubah selama transmisi. Meskipun menyembunyikan enkripsi isi pesan, dimungkinkan untuk mengubah sebuah pesan terenkripsi tanpa memahaminya. (Algoritma enkripsi Beberapa, yang dikenal sebagai nonmalleable yang, mencegah hal ini, tetapi yang lain tidak.) Namun, jika pesan secara digital ditandatangani, setiap perubahan dalam pesan setelah tanda tangan akan membatalkan tanda tangannya. Selain itu, tidak ada cara yang efisien untuk memodifikasi pesan dan tanda tangan untuk menghasilkan pesan baru dengan tanda tangan yang sah, karena ini masih dianggap layak oleh sebagian besar komputasi fungsi hash kriptografi (lihat resistensi tabrakan ).

* Non-repudiation

Non-repudiation , atau lebih khusus non-repudiation asal, merupakan aspek penting dari tanda tangan digital. Dengan properti ini suatu entitas yang telah menandatangani beberapa informasi tidak dapat di lain waktu menyangkal memiliki menandatanganinya. Demikian pula, akses ke kunci publik hanya tidak memungkinkan pihak penipuan untuk palsu tanda tangan valid.

**Cara kerja dari digital signature**

Dimulai dari pencetus pesan menggunakan tombol tanda tangan (Kunci Pribadi) untuk menandatangani pesan dan mengirim pesan dan tanda tangan digital ke penerima. Penerima menggunakan kunci verifikasi (Kunci Publik) untuk memverifikasi asal pesan dan pesan tersebut tidak dirusak saat dalam perjalanan.

Tanda tangan digital menggunakan tipe Asymmetric Cryptography. Skema biasanya terdiri dari tiga Algoritma yakni:

1. A key generation algorithm, yang memilih kunci pribadi secara seragam secara acak dari sekumpulan kunci pribadi yang mungkin. Algoritma mengeluarkan kunci privat dan kunci publik yang sesuai.
2. A signing algorithm, yang mana jika diberi pesan dan kunci privat, menghasilkan tanda tangan.
3. A signature verifying algorithm, yang mana ketika diberi pesan, kunci publik dan tanda tangan, akan menerima atau menolak klaim pesan tersebut atas keasliannya.

Cara kerja Digital Signature dengan memanfaatkan dua buah kunci, yaitu kunci publik dan kunci privat. Kunci publik digunakan untuk mengenkripsi data, sedangkan kunci privat digunakan untuk mendekripsi data. Pertama, dokumen di-hash dan menghasilkan Message Digest. Kemudian, Message Digest dienkripsi oleh kunci publik menjadi Digital Signature. Untuk membuka Digital Signature tersebut diperlukan kunci privat. Bila data telah diubah oleh pihak luar, maka Digital Signature juga ikut berubah sehingga kunci privat yang ada tidak akan bisa membukanya. Ini merupakan salah satu syarat keaman jaringan, yaitu Authenticity. Artinya adalah, keaslian data dapat terjamin dari perubahan-perubahan yang dilakukan pihak luar. Dengan cara yang sama, pengirim data tidak dapat menyangkal data yang telah dikirimkannya. Bila Digital Signature cocok dengan kunci privat yang dipegang oleh penerima data, maka dapat dipastikan bahwa pengirim adalah pemegang kunci privat yang sama. Ini berarti Digital Signature memenuhi salah satu syarat keamanan jaringan, yaitu Nonrepudiation atau non-penyangkalan.

**Penggunaan Tanda Tangan Digital**

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. Tanda tangan digital harus unik sehingga dapat membedakanpengirim yang satu degan yang lainnya. Tanda tangan digital 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 Untuk keperluan yang penting ini, tersedia alat bantu yang dapat diperoleh secara cumacuma, yakni Pretty Good Privacy (PGP) dan Gnu Privacy Guard atau GPG. Tentu saja masih terdapat penyedia layanan tanda tangan digital lainnya, namun PGP dan GPG lebih dikenal luas. GPG adalah produk Open Source yang dapat diperoleh secara gratis tanpa harus membayar lisensi. Penggunaaan PGP di luar

Amerika Serikat harus menggunakan versi internasional. Sedangkan GPG sendiri karena dikembangkan di luar wilayah hukum Amerika Serikat, maka bebas digunakan oleh siapapun. Restriksi ini berkaitan dengan aturan ekspor produk enkripsi yang berkait dengan pemakaian kunci sandi untuk pemakaian tanda tangan digital ini [DIR04]. Penggunaan tanda tangan digital ini tidak terlalu sulit. Kedua belah pihak yang akan berkomunikasi harus menyiapkan sepasang kunci, yaitu kunci privat (private key) dan kunci publik (public key). Kunci privat hanya dipegang oleh pemiliknya sendiri. Sedangkan kunci publik dapat diberikan kepada siapapun yang memerlukannya.

**Otentikasi tanda tangan**

Untuk melakukan verifikasi tanda tangan, pesan beserta tanda tangannya harus dimasukkan ke dalam aplikasi. Pesan tanpa tanda tangan akan diubah menjadi message digest kembali dengan menggunakan fungsi HAVAL dan diubah ke dalam BigInteger kemudian tanda tangan yang diberikan ke pesan tersebut didekripsi dengan algoritma RSA dan dibandingkan dengan hasil message digest dalam bentuk BigInteger tersebut. Apabila hasil dekripsi tersebut sama dengan message digest berarti pesan tersebut telah lulus otentikasi.

**Implementasi Skema Tanda Tangan Digital**

Implementasi akan dilakukan untuk menguji skema tanda tangan digital yang telah dibuat dengan menggunakan kombinasi algoritma kriptografi kunci publik RSA dan fungsi hash HAVAL. Implementasi dilakukan dengan menggunakan bahasa pemrograman C# dan diuji pada lingkungan Windows.

Spesifikasi Implementasi

Aplikasi diberi nama “RSA-HAVAL Digital Signature” ini memiliki spesifikasi sebagai berikut:

 Dapat melakukan pembangkitan kunci publik dan privat secara acak dan menyimpannya dalam file eksternal

 Dapat menandatangani dokumen teks

 Dapat melakukan otentikasi terhadap dokumen yang telah ditandatangani

Berikut ini daftar nama kelas yang telah diimplementasikan untuk membangun aplikasi tersebut:

 BigInteger : kelas BigInteger dan operasinya

 GenAlgo: kelas untuk membangkitkan kunci publik dan kunci privat

 RSA: kelas yang mengimplementasikan algoritma RSA

 Haval: kelas yang mengimplementasikan algoritma fungsi hash HAVAL

 AuthSignature: merupakan kelas interface untuk melakukan otentikasi dokumen

 DigitalSignature: merupakan kelas interface utama dari aplikasi

 KeyGen: merupakan kelas interface untuk pembangkitan kunci acak

 GiveSignature: merupakan kelas interface untuk memberikan tanda tangan KeyGen akan secara otomatis membangkitkan kunci publik dan privat beserta nilai n yang kemudian kedua kunci tersebut disimpan ke dalam file eksternal terpisah dengan ekstensi .pukey (kunci publik) dan .pikey (kunci privat). Algoritma RSA sendiri membutuhkan parameter yang cukup besar sehingga tidak memungkinkan untuk menggunakan integer. Oleh karena itu, aplikasi ini menggunakan kelas BigInteger yang telah ada dikembangkan untuk C#.

**Hambatan Aplikasi Digital Signature**

Ada masalah dalam pendistribusian kunci publiknya. Katakanlah Budi hendak mengirim kunci publiknya (PbA) kepada Ita. Tapi saat kunci itu dikirim lewat jaringan publik, Maling mencuri kunci PbA. Kemudian Maling menyerahkan kunci publiknya (PbM) kepada Ita, sambil mengatakan bahwa kunci itu adalah kunci publik milik Budi. Ita, karena tidak pernah memegang kunci publik Budi yang asli, percaya saja saat menerima PbM. Saat Budi hendak mengirim dokumen yang telah ditandatanganinya dengan kunci privatnya (PvA) kepada Ita, sekali lagi Maling mencurinya. Tanda tangan Budi pada dokumen itu lalu dihapus, dan kemudian Maling membubuhkan tanda tangannya dengan kunci privatnya (PvM). Maling mengirim dokumen itu ke Ita sambil mengatakan bahwa dokumen ini berasal dari budi dan ditandatangani oleh Ita. Ita kemudian memeriksa tanda tangan itu, dan mendapatkan bahwa tanda tangan itu sah dari Budi. Tentu saja kelihatan sah, karena Ita memeriksanya dengan kunci public PbM, bukan dengan PbA.

**Solusi**

Untuk mengatasi masalah sekuriti pendistribusian kunci publik, maka kunci publik itu,direkatkan‟ pada suatu sertifikat digital. Sertifikat digital selain berisi kunci publik juga berisi informasi lengkap mengenai jati diri pemilik kunci tersebut, sebagaimana layaknya KTP, seperti nomor seri, nama pemilik, kode negara/perusahaan, masa berlaku dsb. Sama halnya dengan KTP, sertifikat digital juga ditandatangani secara digital oleh lembaga yang mengeluarkannya, yakni otoritas sertifikat (OS) atau certificate authority (CA). Dengan menggunakan kunci public dari suatu sertifikat digital, pemeriksa tanda tangan dapat merasa yakin bahwa kunci publik itu memang berkorelasi dengan seseorang yang namanya tercantum dalam sertifikat digital itu. Kini Internet tools versi terbaru dari Microsoft dan Netscape sudah menyediakan fasilitas bagi penggunaan sertifikat digital user. Dengan Outlook Express dari Microsoft Internet Explorer 4.0 misalnya, kita bisa memesan suat sertifikat digital melalui menu Tools Options Security, lalu mengklik [Get Digital ID …] . Sedangkan pada Netscape Comm unicator 4.0, hal s erupa dil akuk an den gan menekan tombol Security pada toolbar, lalu mengklik Certificate Yours, lantas mengkli k tom bol [ Get A C ertificate…] .

Sertifikat yang didapatkan itu kemudian disimpan di hard disk, dan diproteksi dengan password. Patut dicatat bahwa teknologi kunci publik dan sertifikat digital pada kedua produk ini juga dipergunakan untuk melakukan proses merahasiakan/menyandikan data, sehingga tidak ada pihak ketiga yang bisa membaca data yang sedang dikirimkan.

Sebenarnya perkakas terbaik yang digunakan untuk membuat tanda tangan digital adalah smart card.Di dalam smart card tersimpan kunci privat dan sertifikat digital, namun yang bisa dikeluarkan dari smart card hanya sertifikat digital saja (untuk keperluan verifikasi tanda tangan). Sedangkan kunci privat tidak bisa diintip oleh apapun dari luar smartcard hanya dipakai untuk proses penandatanganan yang di lakukan di dalam smartcard.

**Tingkat Kegagalan .**

Tetapi sayangnya ada satu hal yang terlupa, bahwa pada dunia komputasi manipulasi terhadap program dan sabotase terhadap komputer pengguna bukanlah hal yang sulit dilakukan. Seseorang bisa saja menyabotase komputer orang lain untuk menandatangani dokumen tanpa sepengetahuan orang yang bersangkutan. Dengan kata lain, tanda-tangan digital hanya memberikan otentikasi antara dokumen dengan komputer, tetapi tidak memberikan otentikasi keterkaitan antara komputer dengan pemilik kunci privat yang sah. Jika seseorang berada di pengadilan dan ditanya tentang tanda-tangan digital miliknya pada sebuah dokumen, dia dapat saja mengatakan bahwa ia tidak pernah menandatangani dokumen tersebut, dan ketika saksi ahli dihadirkan ia akan menjelaskan bahwa mungkin saja dokumen diberi tandatangan digital tanpa sepengetahuan si pemilik kunci privat .

BAB IV  
PENUTUP

**5.1 Kesimpulan**

Kesimpulan dari teknologi digital signature yaitu bahwasanya teknologi digital signature sangat membantu dalam otentifikasi dokumen sehingga dapat menjamin keasliannya dan mampu mengurangi resiko pembajakan ataupun penipuan

**5.2 Saran**

Untuk lebih memudahkan masyarakat dan meningkatkan kesadaran masyarakat akan pentingnya kegunaan digital signature perlu diadakannya sosialisasi dan evaluasi selalu apakah dengan adanya penerapan digital signature mampu diterapkan secara efisien dan maksimal.