Tanda Tangan Elektronik
sebagai Penjamin Integritas Data dan Otentifikasi
serta sebagai Kunci Enkripsi-Dekripsi

Rahmat Izwan Heroza – NIM : 13505008

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if15008@students.if.itb.ac.id

Abstrak

Salah satu masalah krusial mengenai Internet yang sampai hari ini masih menjadi perbincangan hangat adalah masalah keamanan, kenyamanan dan otorisasi dalam berinternet. Apakah bertransaksi via Internet bisa terjamin keamanannya? Bagaimana mencegah jika seseorang menggunakan kartu kredit yang bukan miliknya untuk belanja online misalnya? Diakuikah secara hukum administrasi yang dilakukan secara online? Bagaimana mencegah seseorang menggunakan identitas dan nama orang lain untuk publikasi di Internet? Bagaimana mengantisipasi ada kesamaan nama?

Makalah ini membahas tentang bagaimana kriptografi dapat menjamin integritas data dan otentifikasi terhadap suatu dokumen yang mana kedua hal ini menjadi amat sangat penting mengingat apabila terjadi penyimpangan/kesalahan terhadap dokumen yang bersifat sangat penting atau rahasia, hal ini akan sangat fatal. Pemalsuan dokumen dan dan perubahan dokumen dapat dicegah dengan adanya hal ini.

Makalah ini akan membahas salah satu cara yang dapat menjamin tercapainya kedua tujuan diatas, yaitu dengan menggunakan tanda tangan elektronik. Suatu tanda yang sangat unik. Tidak akan terjadi satu tanda tangan dimiliki oleh dua orang yang berbeda.

Disamping sebagai suatu cara yang menjamin tercapainya integritas data dan otentifikasi, tanda tangan elektronik juga dapat digunakan sebagai kunci enkripsi-dekripsi.

Suatu dokumen yang akan dikirim, di enkripsi dengan menggunakan tanda tangan pengirim sebagai kunci enkripsi. Di dalam dokumen yang dikirim, terdapat data yang memuat tanda tangan penerima yang nanti nya akan dipakai sebagai kunci dekripsi. Setelah dokumen di enkripsi, pihak lain yang tidak berwewenang, walaupun bisa men-download dokumen tersebut, tetapi tidak akan bisa membaca file yang sudah sudah di enkripsi dengan menggunakan tanda tangan elektronik tersebut. Jika si penerima sudah mennerima dokumen yang dikirim tadi, maka ia tinggal mendekripsi dengan menggunakan tanda tangan sebagai kunci dekripsi.sistem akan memeriksa apakah tanda tangan elektronik, dalam hal ini bertindak sebagai kunci dekripsi, valid..

Memang masih banyak kendala yang ditemui dalam pengembangan tanda-tangan digital ini, tapi cepat atau lambat, berbagai solusi tentu akan segera diatasi. Di beberapa negara, cyber law sudah diberlakukan, dan di Indonesia sendiri, cyber law sudah sampai pada tingkat pembahasan serius. Yang jelas, ketergantungan kita terhadap kertas dan berkas-berkas dokumen lambat-laun akan segera berkurang dan akan digantikan oleh realitas maya yang mulai merambat persis di depan mata kita.

1. Definisi

Ciphertext: Bentuk terenkripsi dari Plaintext.
Cryptanalysis: Ilmu atau seni mengembalikan ciphertext menjadi plaintext tanpa menggunakan kunci.
Cryptography: Ilmu untuk mengubah plaintext menjadi ciphertext.
Decryption: Proses mengkonversi kembali ciphertext menjadi plaintext.
Encryption: Proses mengkonversi plaintext menjadi ciphertext.
Key: Informasi rahasia yang hanya diketahui oleh pengirim dan penerima pesan dalam rangka mengamankan plaintext.
Plaintext: Informasi sumber yang hendak ingin diamankan..
Enigma: Sebuah mesin enkripsi yang gunakan pada saat perang dunia kedua.
Scytale: Alat enkripsi tertua yang menggunakan kayu berbentuk silinder sebagai kunci.
RSA: Suatu algoritma enkripsi yang paling modern saat ini.

2. Pendahuluan

Di dalam bidang teknologi informasi, apa yang sedang berkembang cepat selama 20 tahun terakhir, lebih luas dan lebih cepat daripada perkembangan teknologi informasi 150 tahun sebelumnya. Selalu ada perdebatan dalam upaya mempertemukan hak masyarakat untuk memperoleh dan mengakses informasi dengan hak negara untuk menjaga rahasia negara.

Untuk itulah diperlukan suatu sistem yang dapat mengamankan beberapa informasi yang dianggap perlu untuk dirahasiakan kepada public.

Kriptografi mempunyai sejarah yang panjang. Informasi yang lengkap mengenai sejarah kriptografi dapat ditemukan di dalam buku David Kahn yang berjudul *The Codebreakers*. Buku yang tebalnya 1000 halaman ini menulis secara rinci sejarah kriptografi mulai dari penggunaan kriptografi oleh Bangsa Mesir 4000 tahun yang lalu (berupa *hieroglyph* yang tidak standard pada priamid) hingga penggunaan kriptografi pada abad ke-20.

Secara historis ada empat kelompok orang yang berkontribusi terhadap perkembangan kriptografi, dimana mereka menggunakan kriptografi untuk menjamin kerahasiaan dalam komunikasi pesan penting, yaitu kalangan militer (termasuk intelijen dan mata-mata), kalangan diplomatik, penulis buku harian, dan pencinta (*lovers*). Di antara keempat kelompok ini, kalangan militer yang memberikan kontribusi paling penting penting karena pengiriman pesan di dalam suasana perang membutuhkan teknik enkripsi dan dekripsi yang rumit.

Sejarah kriptografi sebagian besar merupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (*transposition cipher*) dan algoritma substitusi (*substitution cipher*). *Cipher* transposisi mengubah susunan huruf-huruf di dalam pesan, sedangkan cipher substitusi mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain. Sejarah kriptografi klasik mencatat penggunaan *cipher* transposisi oleh tentara Sparta di Yunani pada permulaan tahun 400 SM. Mereka menggunakan alat yang namanya *scytale*.

(a) Sebuah *scytale*; (b) Pesan ditulis secara horizontal, baris per baris. Bila kertas dilepaskan, maka pesan yang terbentuk adalah cipherteks.

Scytale terdiri dari sebuah kertas panjang dari daun *papyrus* yang dililitkan pada sebuah silinder dari diameter tertentu (diameter silender menyatakan kunci penyandian). Pesan ditulis secara horizontal, baris per baris. Bila pita dilepaskan, maka huruf-huruf di dalamnya telah tersusun secara acak membentuk pesan rahasia. Untuk membaca pesan, penerima pesan harus melilitkan kembali melilitkan kembali kertas tersebut ke silinder yang diameternya sama dengan diameter silinder pengirim. Sedangkang algoritma substitusi paling awal dan paling sederhana adalah *Caesar cipher*, yang digunakan oleh raja Yunani kuno, Julius Caesar. Caranya adalah dengan mengganti setiap karakter di dalam alfabet dengan karakter yang terletak pada tiga posisi berikutnya di dalam susunan alfabet.

Kriptografi juga digunakan untuk tujuan keamanan. Kalangan gereja pada masa awal agama Kristen menggunakan kriptografi untuk menjaga tulisan relijius dari gangguan otoritas politik atau budaya yang dominan saat itu. Mungkin yang sangat terkenal adalah “Angka si Buruk Rupa (*Number of the Beast*) di dalam Kitab Perjanjian Baru. Angka “666” menyatakan cara kriptografik (yaitu dienkripsi) untuk menyembunyikan pesan berbahaya; para ahli percaya bahwa pesan tersebut mengacu pada Kerajaan Romawi.

Di India, kriptografi digunakan oleh pencinta (*lovers*) untuk berkomunikasi tanpa diketahui orang. Bukti ini ditemukan di dalam buku *Kama Sutra* yang merekomendasikan wanita seharusnya mempelajari seni memahami tulisan dengan *cipher*. Pada Abad ke-17, sejarah kriptografi mencatat korban ketika ratu Skotlandia, Queen Mary, dipancung setelah surat rahasianya dari balik penjara (surat terenkrpsi yang isinya rencana membunuh Ratu Elizabeth I) berhasil dipecahkan oleh seorang pemecah kode. Seperti yang telah disebutkan di atas bahwa kriptografi umum digunakan di kalangan militer.

Pada Perang Dunia ke II, Pemerintah Nazi Jerman membuat mesin enkripsi yang dinamakan *Enigma*. Mesin yang menggunakan beberapa buah *rotor* (roda berputar) ini melakukan enkripsi dengan cara yang sangat rumit. Namun *Enigma cipher* berhasil dipecahkan oleh pihak Sekutu dan keberhasilan memecahkan *Enigma* sering dikatakan sebagai faktor yang memperpendek perang dunia ke-2.

Kriptografi modern dipicu oleh perkembangan peralatan komputer digital. Dengan komputer digital, *cipher* yang lebih kompleks menjadi sangat mungkin untuk dapat dihasilkan. Tidak seperti kriptografi klasik yang mengenkripsi karakter per karakter (dengan menggunakan alfabet tradisionil), kriptografi modern beroperasi pada *string biner*. *Cipher* yang kompleks seperti DES (*Data Encryption Standard*) dan penemuan algoritma RSA adalah algoritma kriptografi modern yang paling dikenal di dalam sejarah kriptografi modern. Kriptografi modern tidak hanya berkaitan dengan teknik menjaga kerahasiaan pesan, tetapi juga melahirkan konsep seperti tanda-tangan digital dan sertifikat digital.

Dengan kata lain, kriptografi modern tidak hanya memberikan aspek keamanan *confidentiality*, tetapi juga aspek keamanan lain seperti otentikasi, integritas data, dan nirpenyangkalan.

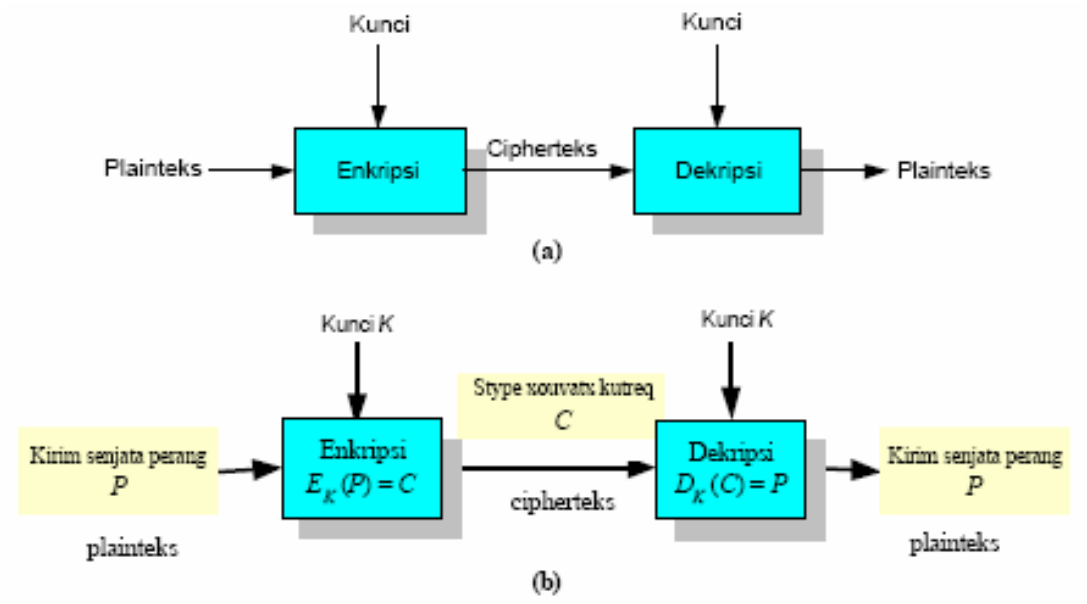
Secara garis besar, dalam kriptografi ada dua proses besar yang harus dilalui. Pertama adalah enkripsi dan yang kedua adalah dekripsi.

Agar plainteks yang kita punyai terkodekan ke dalam cipher text yang unik, maka kita memerlukan kunci yang unik pula.

Sebagai contoh, kita akan mengganti huruf A dengan huruf D, B dengan E, dan seterusnya. Sehingga jika kita mempunyai plaintext ”ABU”,

maka kita akan segera memiliki ciphertext ”DEX”. Dengan kunci yang kita pakai adalah ”ganti dengan huruf ketiga berikutnya”.
Semakin kita memvariasikan kunci yang kita punya, maka pekerjaan cryptanalyst akan semakin susah. Adapun kunci enkripsi dan dekripsi bisa sama ataupun berbeda.

Ada banyak metode yang sudah lama dikenal untuk melakukan enkripsi-dekripsi. Dari metode yang paling tua seperti scytale sampai yang paling modern , RSA.



(a) skema enkripsi-dekripsi. (b) contoh ilustrasi enkripsi-dekripsi pesan

3. Tujuan Kriptografi

Kriptografi memiliki banyak sekali tujuan dan kegunaan, diantaranya adalah:

1. Kerahasiaan (*confidentiality*), adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak. Di dalam kriptografi, layanan ini direalisasikan dengan menyandikan pesan menjadi cipherteks. Misalnya pesan “Harap datang pukul 8” disandikan menjadi “TrxC#45motyptre!%”. Istilah lain yang senada dengan *confidentiality* adalah *secrecy* dan *privacy*. Lebih jauh mengenai metode penyandian akan dibahas di dalam bab-bab selanjutnya.
2. Integritas data (*data integrity*), adalah layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan: “Apakah pesan yang diterima masih asli atau tidak mengalami perubahan (modifikasi)?”. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam pesan yang sebenarnya. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (*digital signature*).

Pesan yang telah ditandatangani menyiratkan bahwa pesan yang dikirim adalah asli. Lebih jauh mengenai tanda-tangan digital akan dibahas di dalam Bab Tanda-tangan Digital.

3. Otentikasi (*authentication*), adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *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. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan: "Apakah pesan yang diterima benar-benar berasal dari pengirim yang benar?". 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 umber pesan. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (*digital signature*). Tanda-tangan digital menyatakan sumber pesan.

4. Nirpenyangkalan (*non-repudiation*), adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan. Sebagai contoh misalkan pengirim pesan memberi otoritas kepada penerima pesan untuk melakukan pembelian, namun kemudian ia menyangkal telah memberikan otoritas tersebut. Contoh lainnya, misalkan seorang pemilik emas mengajukan tawaran kepada toko mas bahwa ia akan menjual emasnya. Tetapi, tiba-tiba harga emas turun drastis, lalu ia membantah telah mengajukan tawaran menjual emas. Dalam hal ini, pihak toko emas perlu prosedur nirpenyangkalan untuk membuktikan bahwa pemilik emas telah melakukan kebohongan.

4. Tanda tangan elektronik

Salah satu masalah krusial mengenai Internet yang sampai hari ini masih menjadi perbincangan hangat adalah masalah keamanan, kenyamanan dan otorisasi dalam berinternet. Apakah bertransaksi via Internet bisa terjamin keamanannya? Bagaimana mencegah jika seseorang menggunakan kartu kredit yang bukan miliknya untuk belanja online misalnya? Diakuikah secara hukum administrasi yang dilakukan secara online? Bagaimana mencegah seseorang menggunakan identitas dan nama orang lain untuk publikasi di Internet? Bagaimana mengantisipasi ada kesamaan nama?

Tanda tangan elektronik digunakan dalam proses kriptografi yaitu pada segi integritas data dan otentifikasi.

Tanda tangan elektronik merupakan salah satu jurus otentikasi dunia tanpa kertas yang dikembangkan di AS dan bahkan kualitas legalnya sama dengan tanda tangan di atas kertas. Ini terjadi setelah Presiden Clinton 30 Juni 2000 menandatangani Undang-undang E-Sign (Electronic Signatures) dan secara efektif baru berlaku 1 Oktober 2000 lalu.

Pada tahap awal teknologi tanda tangan elektronik ini diharapkan bisa diadopsi perbankan dan institusi keuangan. Secara teori, e-signature akan memungkinkan mereka melakukan berbagai macam transaksi online yang lebih luas. Contohnya, beberapa bank memungkinkan untuk aplikasi pinjaman secara online tanpa harus meninggalkan meja komputer.

Yang sangat diharapkan sekarang terutama berkaitan dengan perluasan hukum yang mengatur tanda tangan elektronik ini termasuk standar teknologinya. Seperti biasanya munculnya teknologi baru selalu diawali dengan berbagai pendekatan yang tidak standar. Ada yang menyebutkan paket informasi seperti data dalam kartu ATM dan nomor PIN sudah bisa dianggap sebagai tanda tangan digital. Jika komputer bank bisa membuktikan tanda tangan digital sesuai (nomor PIN cocok dengan data kartu ATM), maka mesin ATM ini akan mengeluarkan sejumlah uang secara otomatis.

Ketika kita berbicara tentang tanda tangan elektronik, maka kita harus juga membicarakan siapa yang akan menjamin kebenaran tanda tangan elektronik itu. Hal ini karena keterpercayaan atas identitas pemilik tanda tangan elektronik, barulah terbangun apabila ada pihak lain yang melakukan verifikasi terhadap kebenaran identitas pemilik tanda tangan elektronik tersebut. Konsep tentang pihak ketiga yang dipercaya untuk melakukan verifikasi terhadap pemilik tanda tangan sudah berkembang dengan makin dikenalnya Public Key Infrastructure (PKI). Namun, konsep ini tidak hanya berlaku untuk PKI, karena di dunia nyata pun, hal ini sudah berlaku, misalnya pembuatan KTP.

Konsep ini didukung oleh satu entitas yang memiliki tanda tangan elektronik, satu entitas yang melakukan verifikasi terhadap identitas pemilik tanda tangan elektronik, satu entitas yang menghubungkan pemilik tanda tangan elektronik dengan yang memverifikasinya, serta pihak yang berhubungan dengan pemilik tanda tangan elektronik. Pada PKI, entitas yang melakukan verifikasi disebut Certification Authority (CA), sedangkan dalam UNCITRAL 2001, sesuai dengan pasal 9 dan definisinya, fungsi tersebut diemban oleh Certification Service Provider (CSP), dimana seperti halnya CA, menjelmakan hasil verifikasi dalam bentuk sertifikat (digital). Apabila pasal 9 ini dibedah, maka kita akan merasakan 'jiwa' CA dalam nama 'baru' tersebut.

Tanda tangan digital ini bagaimanapun masih bekerja dalam lingkungan tertutup, hanya satu orang yang dibutuhkan untuk memberikan otorisasi. Tentu tidak demikian apabila menyangkut sebuah kontrak, paling tidak ada dua pihak yang harus memberikan tanda tangan.

Pada dasarnya tanda tangan elektronik ini memiliki tujuan yang sama dengan tanda tangan di atas kertas biasa. Majalah PC Magazine melihat cara elektronik bisa lebih baik, dengan menggunakan teknik biometrik, seperti pengenalan tanda tangan dinamik, tidak mungkin lagi dipalsukan.

Untuk cara terakhir ini penandatanganan dilakukan di atas tablet yang peka dengan tekanan. Piranti lunak akan mencatat bentuk karakter, kecepatan tulisan, tekanan pena, sampai waktu. Seluruh catatan ini secara unik mengidentifikasi seseorang yang tidak bisa ditiru maupun dicuri. Dua perusahaan yang menawarkan verifikasi tanda tangan dinamik adalah Communication Intellegence Corp (www.cic.com) dan Cyber-Sign (www.cybersign.com).

Tandatangan digital ini akan memicu penggunaan teknik pengesahan secara elektronik di bidang komersil. Teknik ini juga akan meningkatkan efisiensi dan penghematan biaya yang berarti bagi perusahaan-perusahaan, karena tidak perlu lagi menyimpan berkas-berkas kertas.

Namun, perusahaan yang terbiasa mengadakan proses perjanjian di atas kertas, harus menyelesaikan beberapa masalah sebelum e-signature dapat digunakan pada bisnis sehari-hari, kata Daniel Greenwood, direktur E-Commerce Architecture Project MIT. Selain membutuhkan infrastruktur yang dapat diandalkan agar dapat menunjang tandatangan digital ini, perusahaan-perusahaan juga dihadapkan pada masalah perbedaan di antara vendor, kerumitan teknologi, dan biaya pengadaan teknologi tersebut.

Seiring dengan meluasnya penggunaan e-signature, dunia bisnis juga dihadapkan pada masalah keamanan data, termasuk memastikan bahwa tidak ada pihak ketiga yang terlibat dan data-data tertentu hanya dapat diakses oleh pihak yang bersangkutan, dan perjanjian tersebut langsung dikirim ke alamat yang dituju, kata Sara Greenberg, seorang pengacara dari Testa, Hurwitz & Thibeault LLP di Boston.

Jerry Archer, dari Fidelity Personal Investments and Brokerage Group, mengatakan bahwa perusahaanya harus mengeluarkan 2 milyar dollar AS untuk memfasilitasi 15 juta pelanggannya dengan tandatangan digital. Saat ini, perusahaan tersebut menggunakan user ID dan password 6 digit untuk sistem keamanannya.

“Dengan sistem tersebut, seseorang mungkin dapat menemukan password-nya dan masuk ke sistem kami, sedangkan sistem idetikikasi suara, ada kemungkinan 2 di antara 10.000 orang bersuara sama dapat mengaksesnya,” kata Jerry.

Memang masih banyak kendala yang ditemui dalam pengembangan tanda-tangan digital ini, tapi cepat atau lambat, berbagai solusi tentu akan segera diatasi. Di beberapa negara, cyber law

sudah diberlakukan, dan di Indonesia sendiri, cyber law sudah sampai pada tingkat pembahasan serius. Yang jelas, ketergantungan kita terhadap kertas dan berkas-berkas dokumen lambat-laun akan segera berkurang dan akan digantikan oleh realitas maya yang mulai merambat persis di depan mata kita.

4.1 Otentifikasi dan integritas data oleh tanda tangan elektronik

Dalam setiap transaksi bisnis, kedua pihak memerlukan jaminan identitas masing-masing. Kadang-kadang, authentication semudah menyediakan sebuah password. Dalam sebuah intranet, authentication dapat dilakukan dengan berbagai cara, menggunakan teknologi enkripsi yang juga digunakan untuk authentication. Teknologi ini termasuk Mekanisme Public-key Sederhana (Simple Public-key Mechanism / SPKM) yang dikembangkan Entrust Technologies, S-HTTP (Secure Hyper Text Transport Protocol) yang dikembangkan Enterprise Integration Technologies, dan SSL (Secure Sockets Layer) yang dikembangkan Netscape Communication Corporation. Tiap protokol authentication ini menggunakan algoritma RSA.

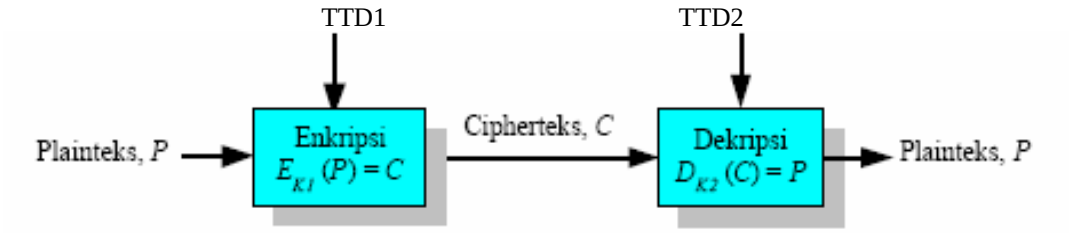
Authentication memerlukan, diantara yang lain, sebuah tanda tangan digital. Proses dimulai dengan summary matematis yang disebut "hash" yang berlaku sebagi "sidik jari" pesan. Isi pesan tak dapat diubah tanpa mengubah code hash. Kode hash ini kemudian di-enkrip dengan private-key si pengirim dan dilampirkan pada pesan tersebut. Ketika pesan telah dterima, kode hash yang dilampirkan dibandingkan dengan kode hash yang lain atau dikalkulasi summary oleh si penerima. Jika cocok, kemudian si penerima tahu bahwa pesan tidak berubah dan integritasnya tidak berubah. Si penerima juga tahu bahwa pesan datang dari si pengirim, karena hanya si pengirim yang mempunyai private-key yang meng-enkripsi koda hash.

DSS (Digital Signal Standard) adalah sebuah standar pemerintah AS yang menyediakan jaminan integritas data dan authentication asli data. DSS juga melayani sebagaimana sebuah tanda tangan yang terikat secara legal untuk transaksi elektronik.

Kunci-kunci untuk tanda tangan digital telah di-file-kan dalam sebuah direktori public-key, terbuat dari "sertifikat-sertifikat" untuk setiap pengguna. Sertifikat-sertifikat ini seperti kartu-kartu tanda tangan dalam sebuah bank dan digunakan untuk mengecek identitas-identitas. Sebuah CA (Certification Authority) yang dipercaya, mengatur dan mendistrubusikan sertifikat-sertifikat ini, sebagai tambahan dalam untuk mendistribusikan kunci-kunci elektronik.

4.2 Tanda tangan digital sebagai kunci enkripsi-dekripsi

Tanda tangan digital berfungsi juga sebagai password untuk proses enkripsi dokumen. Dokumen yang dikirimkan hanya bisa diakses oleh orang yang dituju lewat tanda tangan digital. Artinya, walaupun suatu dokumen bisa didownload oleh orang lain, tetapi tidak akan bisa dibaca tanpa adanya tanda tangan digital dari orang yang berwenang membukanya.



4.3 Ruu tanda tangan elektronik

Indonesia adalah negara hukum. Suatu sistem harus memiliki landasan hukum yang dapat mengokohkan kedudukannya di mata hukum.

Dikatakan Cahyana, pelanggaran hukum dalam transaksi elektronik dan perbuatan hukum di dunia maya lainnya merupakan fenomena yang sangat mengkawatirkan, mengingat berbagai hal yang bersifat tindakan *carding, hacking, crcking, phising, viruses, cybersquating,* pornografi,

perjudian (online gambling), transnasional *crime* yang memanfaatkan IT sebagai *"tools"* penyebaran informasi destruktif, seperti cara pembuatan dan penggunaan bom, telah menjadi bagian dari aktivitas pelaku kejahatan Internet."Dengan berbagai kejahatan internet saat ini, maka pemerintah memandang RUU Informasi dan Transaksi Elektronik adalah sebagai instrument yang mutlak diperlukan bagi negara Indonesia. Karena saat ini Indonesia merupakan salah satu negara yang telah menggunakan dan memanfaatkan tekhnologi informasi secara luas dan efisien, namun belum mempunyai Undang-Undang Cyber," ujar Ir. Cahyana Ahmadjayadi, MH kepada wartawan usai Sosialisasi RUU Informasi dan Transaksi Elektronika yang diselenggarakan Depkominfo kerjasama dengan Pansus RUU ITE DPR-RI dan Mabes Polri, di hotel Saphir Yogyakarta,

Diantara pasal-pasal yang melegitimasi tanda tangan elektronik adalah sebagai berikut,

Pasal 1,

(5). Tanda tangan elektronik adalah informasi elektronik yang dilekatkan, memiliki hubungan langsung atau terasosiasi pada suatu informasi elektronik lain yang ditujukan oleh pihak yang bersangkutan untuk menunjukkan identitas dan status subyek hukum.

6) Penandatangan adalah subyek hukum yang terasosiasikan dengan tanda tangan elektronik.

Pasal 2,

Pemanfaatan teknologi informasi dan transaksi elektronik dilaksanakan berdasarkan asas kepastian hukum, manfaat, hati-hati, itikad baik, dan netral teknologi.

Pasal 4,

(1) Informasi elektronik memiliki kekuatan hukum sebagai alat bukti yang sah.

(2) Bentuk tertulis (print out) dari informasi elektronik merupakan alat bukti dan memiliki akibat hukum yang sah.

(3) Informasi elektronik dinyatakan sah apabila menggunakan sistem elektronik yang dapat dipertanggungjawabkan sesuai dengan perkembangan teknologi informasi.

Pasal 5,

Pemanfaatan teknologi informasi dan sistem elektronik dilindungi berdasarkan undang-undang ini.

Pasal 7,

Setiap orang yang menyatakan suatu hak, memperkuat hak yang telah ada, atau menolak hak orang lain berdasarkan atas keberadaan suatu informasi elektronik harus menunjukkan bahwa informasi elektronik tersebut terjamin keutuhannya, dapat dipertanggungjawabkan, dapat diakses, dan dapat ditampilkan sehingga dapat menerangkan suatu keadaan.

Pasal 11,

Tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi ketentuan dalam undang-undang ini.

Pasal 12,

Teknik, metode, sarana, atau proses pembuatan tanda tangan elektronik memiliki kedudukan hukum yang sah selama memenuhi persyaratan yang ditetapkan dalam undang-undang ini.

Pasal 14,

(1) Setiap orang yang terlibat dalam tanda tangan elektronik berkewajiban memberikan pengamanan atas tanda tangan elektronik yang digunakannya.

(2) Pelanggaran ketentuan sebagaimana dimaksud dalam ayat (1) berakibat tanda tangan elektronik dimaksud tidak dapat digunakan sebagai alat bukti.

Pasal 28,

(1) Penggunaan setiap informasi melalui media elektronik yang menyangkut data tentang hak pribadi seseorang harus dilakukan atas persetujuan pemilik data tersebut.

Pasal 45,

Undang-undang ini berlaku di seluruh wilayah Negara Kesatuan Republik Indonesia dan untuk setiap orang di luar Indonesia yang melakukan tindak pidana sebagaimana diatur dalam undang-undang ini yang akibatnya dirasakan di Indonesia.

5. Kesimpulan

Kesimpulan yang dapat dimbil dari studi dan implementasi AES dengan empat mode operasi *block cipher* ini ini adalah:

1. Kriptografi sangat berperan dalam kehidupan kita. Terutama dalam menjaga informasi agar terjaga kerahasiannya, integritas data, otentifikasi, dan nirpenyangkalan terhadap pihak-pihak yang terkait. Misalnya pihak pengirim yang menyangkal telah mengirim informasi atau pihak penerima yang menyangkal telah menerima informasi yag telah dikirim.

2. Tanda tangan elektronik menjamin tercapainya fungsi otentifikasi dan integritas data yang dejanjikan oleh proses kriptografi.

3. Tanda tangan elektronik juga dapat digunakan sebagai kunci enkripsi-dekripsi yang sangat terjamin.

4. Seperti diketahui, fakta menunjukkan bahwa masyarakat pada umumnya dan perbankan khususnya telah melakukan kegiatan transaksi yang seluruhnya menggunakan teknologi informasi sebagai alat (tools). Berdasarkan data transasksi elektronik melalui perbankan di Indonesia, tahun 2005 di Bank Indonesia jumlah transaksi mencapai 1,017 milliar (39,9 juta pemegang kartu) dengan nilai transaksi mencapai Rp.1.183,7 triliun yang dikelola oleh 107 penyelenggara. Sehingga Undang Undang Informasi dan Transaksi Elektronik dapat dikatakan sangat penting artinya dalam rangka mengantisipasi kejahatan internet dan juga sebagai alat legitimasi yang berkekuatan hukum.
5. Memang masih banyak kendala yang ditemui dalam pengembangan tanda-tangan digital ini, tapi cepat atau lambat, berbagai solusi tentu akan segera diatasi. Di beberapa negara, cyber law sudah diberlakukan, dan di Indonesia sendiri, cyber law sudah sampai pada tingkat pembahasan serius. Yang jelas, ketergantungan kita terhadap kertas dan berkas-berkas dokumen lambat-laun akan segera berkurang dan akan digantikan oleh realitas maya yang mulai merambat persis di depan mata kita.

DAFTAR PUSTAKA

[1] *Oliver Pell. Cryptologyl. http://www.cryptology.ic.ac.uk*. Tanggal akses: 24 Desember 2006 pukul 09:00.

[2] *Budi Putra. Tanda Tangan Elektronik. http://thegadget.wordpress.com*. Tanggal akses: 31 Desember 2006 pukul 21:00.

[3] *Portal Canggih Layanan Online di Kota Bremen. http://www.pempropsu.go.id*. Tanggal akses: 31 Desember 2006 pukul 21:00.

[4] Pengantar Kriptografi. *http://www.kur2003.if.itb.ac.id*. Tanggal akses: 24 Desember 2006 pukul 09:00.

[5] *Arnoldus Trio.Kolaborasi Persandian dan Komunikasi. http://www.tni.mil.id*. Tanggal akses: 24 Desember 2006 pukul 09:00.

[6] *Freak Einstein.http://www.kriptonesia.com* Tanggal akses: 24 Desember 2006 pukul 09:00.