Analisis Implementasi dan Keamanan Digital Signature pada Kartu Kredit

Jimmy Karisma Ramadhan [1)]
1) Program Studi Teknik Informatika ITB, Bandung 40132, email: if14025@students.if.itb.ac.id

Abstract *– Dewasa ini penggunaan kartu kredit semakin meningkat tajam. Hal ini diperkuat pula dengan berbagai kemudahan dan fasilitas yang didapatkan dalam menggunakan kartu kredit. Pembelian barang secara online sangat marak digunakan dan dilakukan. Keadaan ini pula yang memicu banyaknya tindak kejahatan di dunia maya seperti mencuri / menggunakan kartu kredit orang lain tanpa sepengetahuan pemiliknya sehingga sang pemilik kartu kredit akan mengalami kerugian material akibat tindakan tersebut. Hal ini disebabkan di negara seperti Indonesia masih belum menerapkan teknologi pencatatan atau pendeteksian transaksi via kabel dengan baik, sehingga para carder (pencuri kartu kredit) semakin merajalela untuk melaksanakan aksinya.*

Sebenarnya ada beberapa cara untuk mengatasi masalah kurangnya atau sulitnya pendeteksian pencatatan atau recording dari wire transfer. Salah satunya adalah dengan menggunakan digital signature atau tanda tangan digital. Digital signature adalah tanda tangan secara elektronik yang digunakan oleh seseorang untuk mengotentikasi identitas pengirim pesan atau penandatangan sebuah dokumen. Menurut RUU Informasi dan Transaksi Elektronik, tanda tangan digital adalah informasi elektronik yang yang dilekatkan, memiliki hubungan langsung atau terasosiasi pada suatu informasi elektronik lain yang dibuat oleh penandatangan untuk menunjukkan identitas dan statusnya sebagai subyek hukum, termasuk dan tidak terbatas pada penggunaan infrastruktur kunci publik (tanda tangan digital), biometrik, kriptografi simetrik.

Dengan penerapan digital signature pada setiap bank atau PJK yang menyediakan pelayanan wire transfer maka diharapkan setiap transaksi melalui wire transfer dapat di lacak atau dideteksi. Dengan demikian maka tindak kejahatan melalui pencurian kartu kredit dapat diminimalisir dan diberantas. Namun masih terdapat celah-celah yang lebar bagi para carder untuk mencuri kartu kredit orang lain.

Dalam tugas makalah ini akan dikaji implementasi tanda tangan digital pada kartu kredit serta keamanannya.

Kata Kunci*: Kartu kredit, tanda tangan digital, keamanan.*

1. PENDAHULUAN

Pada era teknologi informasi seperti saat ini, transaksi elektronik semakin marak digunakan. Berbagai penawaran dan kemudahan ditawarkan oleh para penjual barang untuk menarik konsumen sebanyak-banyaknya. Beragam metode pembayaran pun ditawarkan untuk menunjang transaksi di dunia maya ini. Salah satu alat pembayaran yang cukup populer untuk transaksi elektronik adalah kartu kredit.

Penggunaan kartu kredit dewasa ini semakin canggih. Kartu kredit saat ini dilengkapi bermacam-macam fitur yang memudahkan para pelanggannya untuk bertransaksi baik secara konvensional ataupun transaksi elektronik. Namun seiring dengan semakin maraknya penggunaan kartu kredit sebagai alat pembayaran transaksi di internet, kejahatan di dunia ini pun semakin marak. Seringkali kita mendengar tentang pembobolan kartu kredit ataupun kejahatan lain yang melibatkan kartu kredit Kejahatan yang kebanyakan terjadi di dunia maya ini sulit untuk dilacak.

Permasalahan pelacakan transaksi ini muncul akibat tidak adanya pencatatan yang baik mengenai transaksi.Terdapat beberapa cara untuk mengatasi masalah kurangnya atau sulitnya pendeteksian pencatatan atau recording dari wire transfer. Salah satunya adalah dengan menggunakan *digital signature* atau tanda tangan digital. Tanda tangan digital adalah tanda tangan secara elektronik yang digunakan oleh seseorang untuk mengotentikasi identitas pengirim pesan atau penandatangan sebuah dokumen. Menurut RUU Informasi dan Transaksi Elektronik, tanda tangan digital adalah informasi elektronik yang yang dilekatkan, memiliki hubungan langsung atau terasosiasi pada suatu informasi elektronik lain yang dibuat oleh penandatangan untuk menunjukkan identitas dan statusnya sebagai subyek hukum, termasuk dan tidak terbatas pada penggunaan infrastruktur kunci publik (tanda tangan digital), biometrik, kriptografi simetrik.

Dengan penerapan digital signature pada setiap bank atau PJK yang menyediakan pelayanan wire transfer maka diharapkan setiap transaksi melalui wire transfer dapat di lacak atau dideteksi. Dengan demikian maka tindak kejahatan melalui pencurian kartu kredit dapat diminimalisir dan diberantas.

2. DASAR TEORI

2.1. Kriptografi

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan/kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi berasal dari bahasa yunani yang terdiri dari kata kryptos yang berarti tersembunyi dan grafo yang berarti tulis. Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut kriptografi juga merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data.

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

1. **Kerahasiaan pesan (*confidentiality/secrecy*)**
   Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.

2. **Otentikasi (*authentication*)**
   Otentikasi adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.

3. **Keaslian pesan (*data integrity*)**
   Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

4. **Nirpenyangkalan (*non-repudiation*).**
   Non-repudiasi atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

Poin kerahasiaan pesan (*confidentiality/secrecy*) dapat diselesaikan dengan menggunakan enkripsi dan deksripsi dari pesan. Sedangkan poin otentikasi, keaslian data, dan integritas data diselesaikan dengan Penandatanganan pesan dengan cata mengenkripsinya selalu memberikan dua fungsi yang berbeda yaitu kerahasiaan pesan dan otentikasi. Pada beberapa Dalam beberapa kasus, seringkali otentikasi yang menggunakan tanda-tangan digital atau lebih dikenal dengan istilah *Digital Siganture*.

2.2. Tanda Tangan Digital

Tanda-tangan mempunyai karakteristik sebagai berikut:

1. Tanda-tangan adalah bukti yang otentik.
2. Tanda tangan tidak dapat dilupakan.
3. Tanda-tangan tidak dapat dipindah untuk digunakan ulang.
4. Dokumen yang telah ditandatangani tidak dapat diubah.
5. Tanda-tangan tidak dapat disangkal(repudiation).

Fungsi tanda tangan pada dokumen kertas juga diterapkan untuk otentikasi pada data digital (pesan, dokumen elektronik). Tanda-tangan untuk data digital dinamakan tanda-tangan digital. Tanda-tangan digital bukanlah tulisan tanda-tangan yang di-digitisasi (di-*scan*).

Tanda-tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci. Tanda-tangan pada dokumen cetak selalu sama, apa pun isi dokumennya. Tanda-tangan digital selalu berbeda-beda antara satu isi dokumen dengan dokumen lain.

1. **Tanda tangan dengan cara melakukan enkripsi terhadap pesan**
   Tanda tangan dengan cara ini terbagi lagi menjadi dua yaitu penandatanganan pesan dengan algoritma kriptografi kunci simetri dan penandatanganan pesan dengan algoritma kriptografi kunci publik.

   Algoritma kunci simetri
   Dengan menggunakan algoritma kunci simetri sebenarnya sudah memberikan solusi untuk otentikasi pengirim dan keaslian pesan, namun algoritma simetri tidak menyediakan suatu mekanisme untuk mengatasi masalah penyangkalan, yaitu jika salah satu dari dua belah pihak menyangkal pesan. Harus terdapat orang ketiga yang dipercaya oleh pengirim/penerima.

   Algoritma kunci publik
   Jika algoritma kunci publik digunakan, maka enkripsi pesan dengan kunci publik tidak dapat digunakan untuk otentikasi, karena orang-orang yang berkepentingan memiliki kunci publik. Namun jika dikombinasikan dengan kunci privat maka otentikasi dan kerahasiaan pesan dapat dicapai sekaligus.

2. **Tanda tangan dengan fungsi *hash***

diperlukan tetapi kerahasiaan pesan tidak. Maksudnya, pesan tidak perlu dienkripsikan karena yang dibutuhkan hanya otentikasi saja.

Hanya algoritma kunci publik yang cocok dan alami untuk pemberian tanda-tangan digital dengan menggunakan fungsi *hash*. Hal ini disebabkan karena skema tanda tangan digital berbasis sistem kunci publik dapat menyelesaikan masalah *non-repudiation*.

Proses pembubuhan tanda tangan digital adalah seperti berikut :

1. Pengirim pesan menghitung *message digest* (MD) diperoleh dengan mentransformasikan pesan *M* dengan menggunakan fungsi *hash* satu arah *H*.

$$MD = H(M)$$

2. Selanjutnya *message digest* (MD) dienkripsi dengan menggunakan algoritma kriptografi kunci publik dan menggunakan kunci privat (*SK*) si pengirim/ Hasil enkripsi inilah yang dinamakan dengan tanda tangan digital S.

3. Kemudian tanda tangan digital S dilekatkan ke pesan *M* dengan cara menyambungkan dengan tanda tangan digital *S*.

Proses verifikasi tanda tangan di tempat penerima adalah sebagai berikut :

1. Tanda tangan digital didekripsi dengan menggunakan kunci pubik (*PK*) pengirim pesan dan menghasilkan *message diggest* semula, MD, sebagai berikut :

2. Penerima kemudian mengubah pesan *M* menjadi *message digest MD2* menggunakan fungsi *hash* satu arah yang sama dengan fungsi *hash* yang digunakan pengirim.
3. Jika *MD2* = *MD* berarti tanda tangan yang diterima berasal dari pengirim yang benar.

2.3 Data Encryption Standard (DES)

Data Encryption Standard (DES) merupakan sebuah standar dalam sistem kriptografi dengan tipe dan mode algoritma simetri. Algoritma kriptografi yang digunakan pada DES – yang disebut sebagai Data Encryption Algorithm (DEA) – merupakan pemrosesan terhadap bit dalam bentuk block cipher (cipher blok). DES merupakan cipher blok dengan menggunakan blok 64-bit dan menggunakan kunci eksternal dengan panjang kunci sebesar 64 bit juga (sama dengan ukuran blok). Pada DES, proses enkripsi data (plaintext) menggunakan kunci internal atau upa-kunci (sub-key) sepanjang 56 bit yang dibangkitkan dari kunci eksternal.

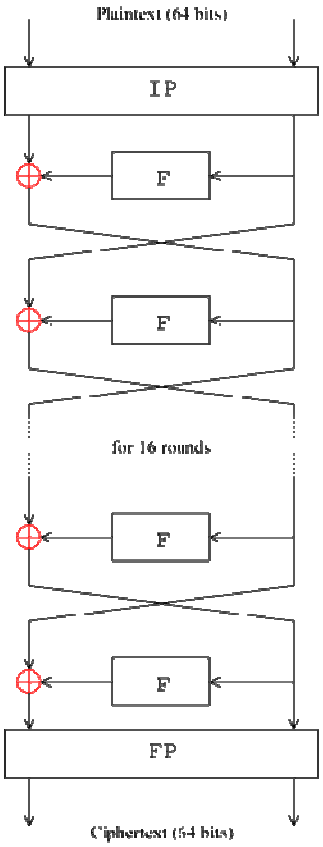
Berikut adalah skema global dari algoritma DES:

1. Blok plainteks dipermutasi dengan matriks permutasi awal (initial permutation).

2. Hasil permutasi awal kemudian di-*enchipering* sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda.

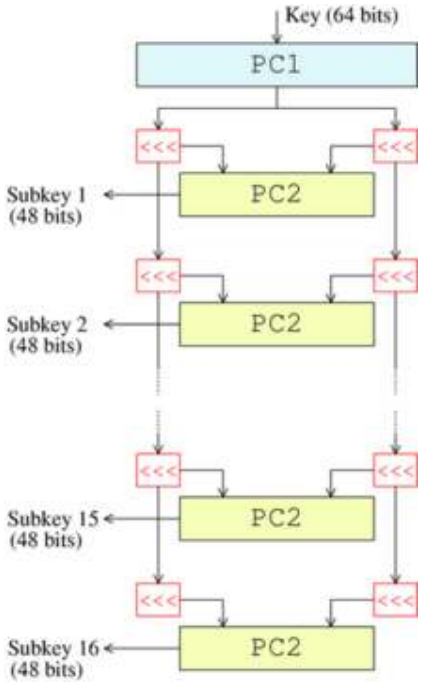
3. Hasil enkripsi kemudian dipermutasi dengan matriks permutasi balikan (invers initial permutation) menjadi blok cipherteks.

Pada proses enkripsi, setiap putarannya digunakan algoritma dengan model jaringan Feistel. Dengan demikian pada proses enciphering blok plaintext hasil permutasi awal akan dibagi menjadi dua bagian dengan ukuran masing-masing 32 bit. Di dalam jaringan Feistel inilah digunakan kunci internal terhadap fungsi transfromasi. Secara lengkap skema algoritma pada DES digambarkan pada gambar 2.1.



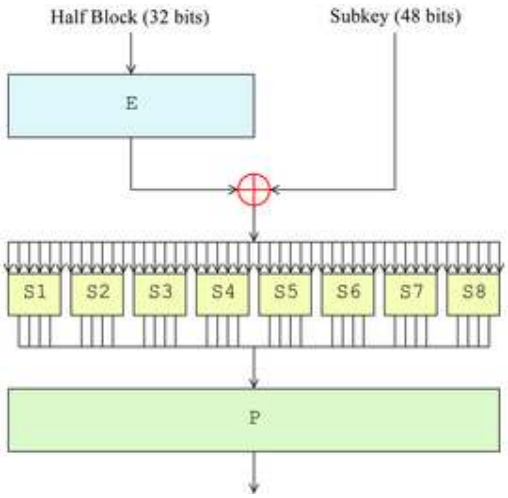
Gambar 2.1 Skema DES

Pada DES pembangkitan kunci dilakukan dengan menggunakan kunci eksternal yang diberikan sebelumnya. Proses pembangkitan kunci internal dilakukan dengan melakukan permutasi dan penggeseran bit ke kiri Keseluruhan pembangkitan kunci internal dilakukan seperti pada gambar 2.2.



Gambar 2.2 Diagram pembangkitan kunci internal pada DES

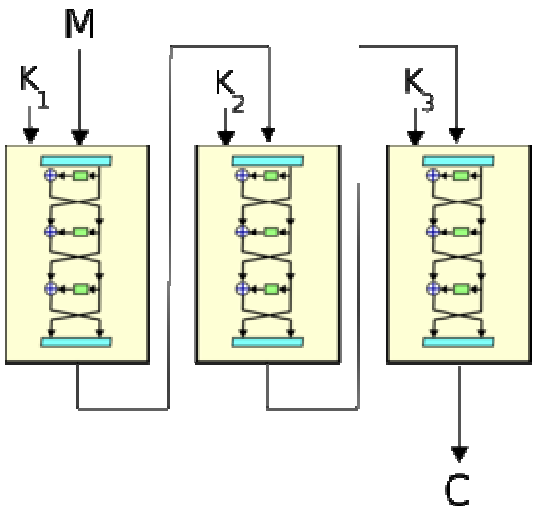
Pada fungsi tranformasi algoritma DES dilakukan fungsi ekpansi (E), fungsi XOR, subtitusi (S), dan permutasi (P) terhadap vektor-vektor bit dari setiap sub-blok. Fungsi transformasi digambarkan pada diagram komputasi berikut:



Gambar 2.3 Diagram komputasi fungsi DES

2.4 Triple DES

Triple DES dikenal juga dengan nama TDES, atau lebih standar lagi adalah TDEA (Triple Data Encryption Algorithm). TDES mengaplikasikan DES sebanyak 3 kali, dengan 3 buah kunci.



Gambar 2.4 Skema Triple DES

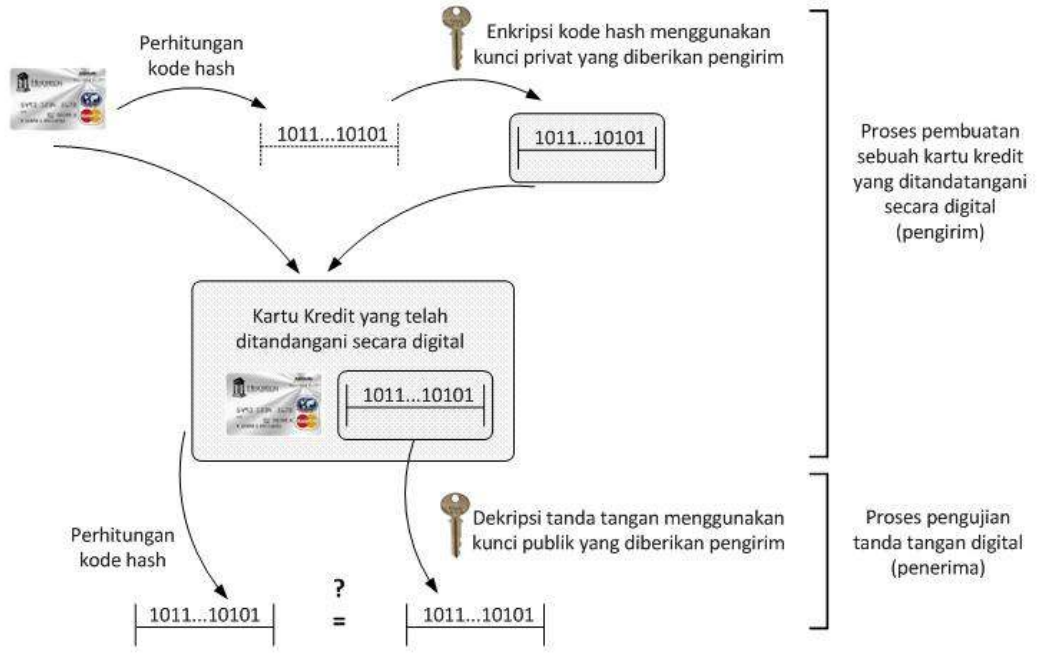
3. IMPLEMENTASI

Tujuan adanya implementasi tanda tangan digital pada kartu kredit adalah sebagai bukti otentik transaksi yang dilakukan oleh seorang nasabah itu valid atau tidak valid. Transaksi kartu kredit yang dibahas disini adalah aktivitas transaksi *online* pada dunia internet, dimana pengguna menggunakan *browser* untuk melakukan transaksi dan entri data-data penting seperti nomor kartu kredit dan lain sebagainya.

Implementasi tanda tangan digital pada kasus ini dilakukan dengan cara melakukan enkripsi dari data-data yang diperlukan pada saat melakukan transaksi dengan menggunakan kartu kredit seperti nama lengkap pemilik, alamat, waktu transaksi, nomor kartu kredit, nominal yang harus dibayarkan, dan lain sebagainya. Bukti transaksi dienkripsi dengan kunci yaitu tiga digit terakhir dari nomor kartu kredit. Agar menyulitkan para *hacker* maka diperlukan algoritma yang sangat tangguh dan sulit untuk membongkar kuncinya, contoh algoritma yang umum adalah penggunaan Triple DES untuk melakukan enkripsi dengan kunci adalah tiga digit terakhir dari nomor kartu kredit.

Hasil dari enkripsi ini berupa *message digest* yang nantinya akan dipakai untuk melakukan otentikasi keabsahan dari transaksi.

Dalam melakukan proses otentikasi digunakan kunci publik yang dimiliki oleh pihak-pihak yang berwenang saja misalnya pihak pemiliki jasa kartu kredit dan bank yang terkait dengan nasabah tersebut. Kunci publik didapat dari sertifikat digital yang ditandatangani oleh *card issuer*. Skema implementasi dapat dilihat pada gambar 3.1.



Gambar 3.1 Skema implementasi tanda tangan digital pada kartu kredit

4. ANALISIS

Analisis penggunaan tanda tangan digital dalam kartu kredit mencakup keamanan dan kehandalan dari algoritma-algoritma yang dilakukan.

1. **Penggunaan Triple DES**
   Penggunaan Triple DES dalam enkripsi sebenarnya sudah sangat banyak dipakai dalam teknologi transaksi secara *online*. Pada tahun 2005, serangan yang terbaik pada TDES membutuhkan 2^{32} known plaintexts, 2^{113} steps, 2^{90} single DES encryptions, dan 2^{88} memory. Tentu saja hal ini tidak praktis. Serangan ini dapat diparalelisasikan jauh dari praktek, dan dibutuhkan milyaran dolar budget dan tahun untuk mencoba serangan tersebut, dan juga kegunaannya terbatas.

   Memang Triple DES ini cukup handal, namun pemrosesan penggunaan Triple DES memakan waktu yang lama. Hal ini mungkin akan menjadi kendala karena saat ini bukan hanya kehandalan yang dibutuhkan, tetapi kecepatan dalam pemrosesan data juga penting.

2. **Penggunaan kunci**
   Penggunaan tiga digit terakhir dari nomor kartu digunakan sebagai kunci privat dalam proses enkripsi cukup rawan. Sewajarnya memang tiga digit terakhir ini dijaga kerahasiaannya selayaknya PIN pada ATM. Karena memang program tidak akan mengenali siapa orang yang memasukkan data transaksi pada situs belanja, apakah benar pemiliki kartu kredit atau pencuri. Namun jika tiga digit terakhir dari kartu kredit ini dapat dijaga kerahasiaannya maka keamanan dalam melakukan transaksi dapat dijamin.

3. **Faktor lain**
   Faktor lain yang perlu dipertimbangkan adalah masalah keamanan fisik dan bentuk-bentuk pencurian. Memang hal ini akan berada di luar kendali pengguna dan pembuat sistem, namun hal keamanan fisik ini juga perlu diperhatikan. Keamanan fisik yang dimaksud disini adalah ancaman keamanan seperti pencurian kartu kredit secara langsung, penyadapan data, dan lain-lain. Selain itu juga terdapat berbagai cara yang dilakukan oleh para pencuri seperti *phishing* (membuat situs palsu). Tidak ada algoritma apapun yang mampu melawan ancaman yang seperti ini selain dari kewaspadaan dari pengguna kartu kredit yang akan membelanjakan uangnya.

5. KESIMPULAN

1. Penggunaan tanda tangan digital dalam kartu kredit sangat diperlukan untuk proses otentikasi terhadap keabsahan dari transaksi.

2. Algoritma untuk melakukan enkripsi data dari transaksi harus sangat tangguh, selain sulit untuk dibobol juga harus memiliki kecepatan proses yang tinggi.

3. Penggunaan Triple DES memang akan sangat menyulitkan bagi para pembobol karena biaya dan waktu yang dibutuhkan sangat besar. Namun algoritma ini sudah tidak cocok lagi untuk saat ini karena tidak dapat memproses data secara cepat dan membutuhkan biaya besar.

4. Faktor keamanan yang lain seperti pencurian dan lain sebagainya juga harus diperhatikan karena tidak ada algoritma apapun yang mampu mencegah hal seperti ini.

DAFTAR REFERENSI

[1] Munir, Rinaldi. (2006). Bahan Kuliah IF5054 Kriptografi. Program Studi Teknik Informatika. Institut Teknologi Bandung.

[2] Ramayanti, Desy, "Aplikasi Digital Sinature sebagai Autentikasi pada Kartu Tanda Penduduk (KTP)", 2007, Institut Teknologi Bandung.

[3] Schneier Bruce, (1996), Applied Cryptography Second Edition: Protocols, Algorthms, and Source Code in C (cloth), John Wiley Sons, Inc.

[4] http://www.geocities.com/amwibowo/resource/hukum_ttd/hukum_ttd.html

[5] http://members.tripod.com/~tipon/dai071.htm