Jurnal Antarabangsa (Teknologi Maklumat) 2(2002): 83-104

Tanda Tangan Digital untuk Keselamatan Mesej Mel Elektronik

NOOR HAYATI HASHIM, KHAIRUDDIN OMAR, MD. JAN NORDIN & ZULKARNAIN MD. ALI

ABSTRAK

Kepentingan keselamatan mesej mel elektronik timbul akibat dari pertambahan penggunaan perkhidmatan mel elektronik di seluruh dunia. Oleh itu perlunya teknologi yang memastikan keselamatan terhadap mesej yang dihantar. Kertas ini memuatkan kajian kesusasteraan tanda tangan digital dan penggunaannya. Ia memperkatakan tentang pengenalan tanda tangan digital meliputi kriptografi dan sistem kripto kunci awam, komponen-komponen, faedah penggunaan, proses, bentuk serangan, dan protokol. Perbandingan sistem kripto RSA dan LUC dan pemilihan sistem kripto LUC untuk penggunaan tanda tangan digital juga turut dbincangkan.

ABSTRACT

The importance of electronic mail messages' security rises for the increasingly utilization of this service all over the world. Therefore, transferring messages needs a technology for security measure. This paper studied about digital signature that covers areas on cryptography, public key cryptosystems, digital signature components, usages, attacks and protocols. Comparison between RSA and LUC cryptosystems is discussed and algorithm based on Lucas function has been chosen to produce digital signature.

PENDAHULUAN

Dewasa ini, mel elektronik digunakan dengan meluas sebagai satu cara berkomunikasi untuk perniagaan dan mungkin menjadi popular seperti penggunaan telefon. Oleh kerana itu, mel elektronik tidak mungkin terpinggir dari digunakan sebagai mod untuk berkomunikasi secara bertulis dalam kehidupan sehari-hari kerana kemajuan aplikasi dan perkembangannya.

Tidak dinafikan cara kita berkomunikasi melalui perubahan yang besar samada dalam situasi dunia korporat hinggalah kepada ikatan dalam sesuatu kekeluargaan. Dalam kerajaan dan perniagaan, mel elektronik menukar cara

sesuatu organisasi berinteraksi dengan pelanggan, cara bagaimana media memberi reaksi kepada pemerhati dan pendengar serta cara bagaimana pekerja berinteraksi dengan ketua dan rakan setugas.

Hari ini, banyak organisasi berminat menggantikan sistem berasaskan kertas dengan sistem elektronik yang diautomasi. Satu daripada penghalang kepada kemajuan transaksi komersial secara elektronik ialah kerisauan terhadap risiko pemalsuan yang dilakukan melalui rangkaian yang tidak selamat. Kerisauan ini membawa kepada keperluan cara untuk menggantikan tanda tangan tulisan tangan dengan tanda tangan digital.

Dalam persekitaran perniagaan secara tradisi, tanda tangan tulisan tangan digunakan secara meluas sama ada untuk menandatangan dokumen atau untuk mengenalpasti seseorang. Tanda tangan digital merupakan alternatif untuk persekitaran elektronik yang juga boleh digunakan untuk mengenal pasti dan mengesahkan asalan sesuatu maklumat. Tanda tangan digital juga berkeupayaan untuk menentusah sesuatu maklumat tidak dipinda selepas ianya ditanda tangan.

Teknologi tanda tangan digital membawakan ciri-ciri sulit, keselamatan, dan keyakinan kepada transaksi yang menggunakan Internet dan sistem komunikasi elektronik yang lain. Sama seperti tanda tangan dan cop materai, tanda tangan digital memberikan rasa yakin terhadap sesuatu transaksi. Ia mengesahkan siapakah pengirim mesej dan memastikan mesej atau dokumen yang dihantar adalah sulit di samping mengesahkan bahawa dokumen yang dihantar tidak diubah sepanjang laluan penghantaran.

Pada masa ini, kira-kira 25 negara bertindak atau mencadangkan akta berhubung dengan penggunaan tanda tangan digital dan mengharapkan tanda tangan digital dapat menggalakkan perkembangan perdagangan elektronik (Roberts 1997). Tanda tangan digital juga dapat memainkan peranan utama dalam perdagangan elektronik dari segi membantu memastikan dokumen elektronik tidak dipinda dan tidak dipalsukan.

Tanda tangan digital merupakan teknologi yang penting untuk merealisasikan penggantian tanda tangan tulisan tangan pada mel biasa kepada tanda tangan pada mel elektronik.

Pengenalan Kepada Tanda Tangan Digital

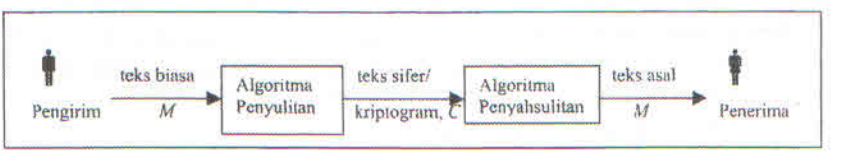
Tanda tangan digital merupakan sumbangan yang bermakna dari kriptografi kunci awam. Ia adalah satu ciri tersendiri bagi seorang pengguna atau proses yang digunakan untuk menandatangan mesej (Denning 1983). Tanda tangan digital merupakan transformasi sebenar ke atas mesej elektronik menggunakan kriptografi kunci awam.

Perbezaan nyata antara tanda tangan tulisan tangan dengan tanda tangan digital ialah tanda tangan digital hendaklah sebagai fungsi kepada dokumen yang ditanda tangan dan bukannya sebagai pemalar. Tanda tangan digital

adalah fungsi kepada dokumen kerana dokumen yang berlainan menghasilkan tanda tangan digital yang berlainan. Ia juga mestilah fungsi kepada keseluruhan dokumen iaitu perubahan satu bit pada dokumen asal menghasilkan tanda tangan yang berbeza (Nechvatal 1991).

KRIPTOGRAFI DAN SISTEM KRIPTO KUNCI AWAM

Kriptografi adalah sains dan seni menyimpan maklumat dalam bentuk yang boleh dilihat oleh orang yang dimaksudkan dan tidak pada orang lain untuk tujuan memastikan maklumat adalah selamat. Kriptografi terdiri daripada dua proses transformasi data iaitu penyulitan dan penyahsulitan. Proses menukar mesej daripada bentuk yang difahami ke bentuk yang tidak difahami dikenali sebagai penyulitan. Proses kebalikannya pula, iaitu menukar daripada bentuk yang tidak difahami ke bentuk mesej asal yang difahami adalah dikenali sebagai penyahsulitan. Mesej asal yang lazimnya ditulis sebagai *M*, dipanggil teks asal, dan hasil penyulitan dikenali pula sebagai teks sifer atau kriptogram yang lazimnya ditulis sebagai *C*. Teks asal boleh jadi sebagai rentetan bit, fail teks, satu peta bit, satu rentetan suara yang telah didigitkan, imej video digital atau apa-apa jua. Sistem komputer hanya mengenali teks asal *M*, sebagai data perduaan. Sistem yang digunakan untuk proses penyulitan dan penyahsulitan dikenali sebagai sistem kripto. Rajah 1 menunjukkan komponen asas sistem kripto.

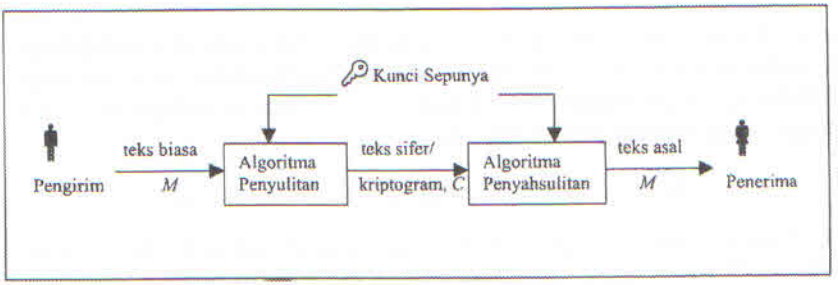


RAJAH 1. Komponen Asas Sistem Kripto

Menurut Massey (1996), dua matlamat utama kriptografi adalah pertama, untuk kerahsiaan iaitu penafian capaian kepada maklumat oleh individu yang tidak diberi kebenaran dan kedua, untuk pengesahan. Bagi pengesahan, ia dikategorikan kepada pengesahan mesej dan pengesahan identiti pengirim. Pengesahan mesej yang berada dalam perjalanan tidak diubahsuai sama ada secara sengaja atau tidak sengaja dan dengan ini keutuhan mesej adalah terjamin (Diffie 1988).

Sistem kripto terdiri dari algoritma, teks biasa, teks sifer, dan termasuk kunci yang mungkin (Schneier 1996). Sistem kripto kunci rahsia atau simetri dan sistem kripto kunci awam atau asimetri merupakan dua contoh sistem kripto. Rajah 2 menunjukkan sistem kripto kunci rahsia.

Keselamatan sistem kripto kunci rahsia bergantung kepada pengirim dan penerima memiliki suatu kunci rahsia sepunya yang tidak diketahui oleh orang lain. Kunci yang sama digunakan untuk melakukan proses penyulitan



RAJAH 2. Sistem Kripto Kunci Rahsia

dan penyahsulitan. Pengirim dan penerima mesej hendaklah terlebih dahulu mempersetujui kunci rahsia yang digunakan.

Konsep sistem kripto kunci awam diperkenalkan oleh Diffie dan Hellman pada tahun 1976. Keselamatan sistem kripto kunci awam bergantung kepada pengirim dan penerima memiliki suatu maklumat yang dipercayai oleh keduanya yang juga diketahui oleh orang lain (Massey 1996).

Sistem kripto kunci awam menggunakan pasangan kunci awam dan kunci persendirian (K, K^{-1}) yang berkaitan secara matematik. Namun demikian kunci persendirian tidak boleh diterbitkan daripada kunci awam. Kunci awam, K perlu dihebahkan tetapi kunci persendirian, K^{-1} hanya diketahui oleh pemiliknya sahaja. Sistem kripto kunci awam bergantung kepada prosedur matematik untuk menghasilkan kunci awam dan kunci persendirian.

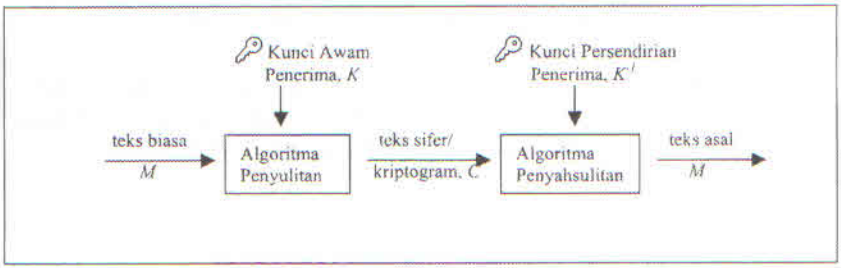
Sistem kripto kunci awam boleh beroperasi dalam dua mod iaitu mod penyulitan dan mod pengesahan. Rajah 3(a) menunjukkan sistem kripto kunci awam untuk mod penyulitan manakala Rajah 3(b) menunjukkan sistem kripto kunci awam untuk mod pengesahan.

Dalam mod penyulitan, pengirim mesej menggunakan kunci awam penerima mesej untuk menyulitkan mesej dan hanya pemilik kunci persendirian yang berkaitan (penerima mesej), boleh menyahsulitkan teks sifer berkenaan. Sebaliknya dalam mod pengesahan, pengirim mesej menggunakan kunci persendiriannya untuk menyulitkan mesej dan penerima mesej boleh menyahsulitkan teks sifer berkenaan menggunakan kunci awam pengirim mesej.

Hari ini terdapat banyak aplikasi baru kriptografi kunci awam. Kebanyakan aplikasi baru ini bersandarkan kepada tanda tangan digital (Omura 1990).

KONSEP ASAS TANDA TANGAN DIGITAL

Konsep tanda tangan digital mula diperkenalkan oleh Diffie dan Helman pada tahun 1976 menerusi kertas bertajuk *New Directions in Cryptography* (Piper 1991). Tanda tangan digital merupakan fungsi cincang (rumusan matematik) ke atas maklumat dan menghasilkan apa yang dikenali sebagai



(a)

(b)

RAJAH 3. (a) Sistem Kripto Kunci Awam - Mod Penyulitan.
(b) Sistem Kripto Kunci Awam - Mod Pengesahan.

mesej diges dan disulitkan menggunakan kunci asimetri atau tak simetri. Tanda tangan digital juga sepatutnya boleh menghalang jenis-jenis penipuan seperti pemalsuan tanda tangan oleh penerima (atau oleh pihak ketiga) dan menafikan menghantar mesej oleh pengirim.

Tanda tangan digital dapat mengenalpasti identiti pengirim secara berkesan kerana hanya kunci persendirian pengirim sahaja yang boleh menghasilkan tanda tangan tersebut. Ia juga dapat membuktikan integriti kandungan mesej yang ditanda tangan kerana mesej diges yang disulitkan adalah berhubung kait secara sistematik dengan kandungan mesej asal, tetapi jika sebaliknya maka tanda tangan tersebut adalah tidak sah. Tanda tangan digital juga tidak boleh ditiru dari satu mesej kepada mesej yang lain kerana mesej diges yang dihasilkan adalah tidak sama. Sebarang perubahan kepada mesej selepas ditanda tangan juga menjadikan sesuatu tanda tangan tidak sah.

Andaikan A hendak menandatangan mesej M yang dihantar kepada B. Mula-mula A menukar mesej M menggunakan fungsi cincang, $h(\ )$. Hasil dari fungsi cincang adalah satu nilai khusus untuk mesej tersebut. Hasil fungsi cincang $h(M)$ dipanggil mesej diges dan boleh dianggap sebagai cap jari mesej tersebut. A kemudian menghasilkan tanda tangan, iaitu menyulitkan $h(M)$ dengan menggunakan kunci persendiriannya, $D_A(h(M))$:

$$S = D_A(h(M)) \qquad (1.0)$$

S merupakan tanda tangan yang dihasilkan dari proses transformasi. A kemudian menghantar M dan S kepada B.

Untuk mengesahkan M dihantar oleh A, B mendapatkan kunci awam A, E_A dan mengira mesej diges $h(M)$ bagi mesej M yang dihantar. B kemudian menyahsulit tanda tangan, iaitu mengira $E_A(S)$, dan membandingkan hasil dengan $h(M)$. Jika B mendapati bahawa:

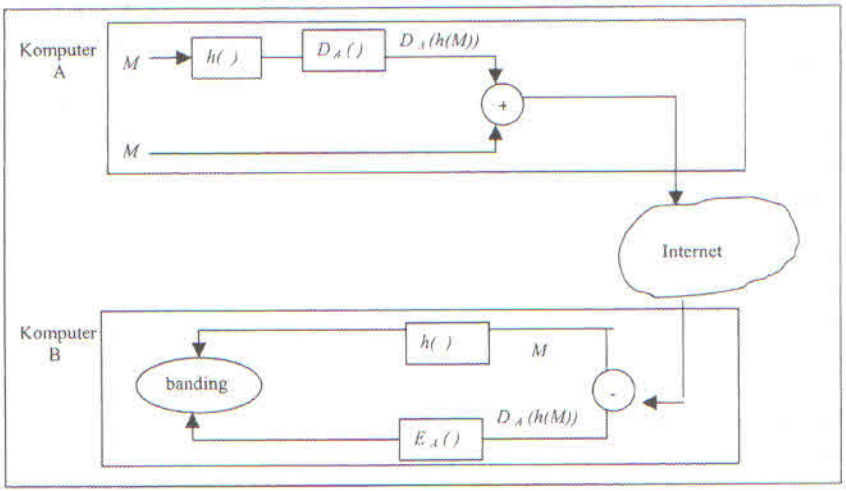
$$E_A(S) = h(M) \tag{1.1}$$

maka tanda tangan A adalah sah dan jika sebaliknya, S bukanlah tanda tangan A.

Asalan mesej boleh dipastikan dari kenyataan bahawa S adalah bergantung kepada mesej. Katakan tanda tangan A iaitu S disalin dan dihantar dengan mesej W, pengesahan tanda tangan akan mendedahkan bahawa:

$$E_A(S) \neq h(W) \tag{1.2}$$

Kegunaan lain ialah untuk mengesahkan bahawa kandungan mesej M tidak dipinda. Pindaan kandungan mesej akan menyebabkan fungsi cincang menghasilkan satu nilai baru bagi $h(M)$. Oleh itu, apabila $E_A(S) \neq h(M)$ berlaku, mungkin penipuan telah terjadi atau disebabkan oleh ralat semasa transmisi. Rajah 4 merupakan gambaran proses yang terdapat pada komputer A dan B.



RAJAH 4. Gambaran Proses Penghasilan dan Penghantaran Mesej Beserta Tanda Tangan Digital.

KOMPONEN TANDA TANGAN DIGITAL

Sistem kripto moden mempunyai dua komponen utama. Komponen pertama adalah algoritma, iaitu satu set prosedur yang ditentukan manakala komponen kedua adalah kunci (Williams 1980). Tanda tangan digital berasaskan kriptografi kunci awam yang mana melibatkan pasangan kunci yang dikenali sebagai kunci awam dan kunci persendirian.

Sebagai tambahan kepada pasangan kunci serta komunikasi elektronik, tanda tangan digital melibatkan dua proses, iaitu penjanaan dan menentusah tanda tangan. Berkaitan dengan kedua-dua proses ini pula adalah algoritma fungsi cincang dan algoritma tanda tangan yang merupakan persamaan matematik yang kompleks.

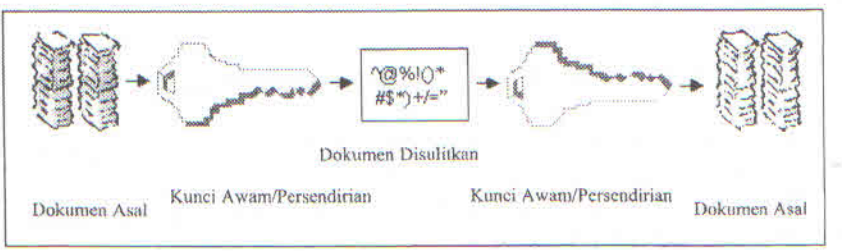
Algoritma fungsi cincang bertindak terhadap kod binari mesej elektronik yang asal dan menghasilkan apa yang dirujuk sebagai mesej diges, iaitu rentetan digit 128 bit atau 160 bit yang unik kepada mesej asal. Algoritma tanda tangan dilaksanakan ke atas mesej diges. Rentetan digit yang terhasil adalah merupakan tanda tangan digital.

PASANGAN KUNCI

Proses penyulitan dan penyahsulitan data menggunakan pasangan kunci yang dikenali sebagai kunci awam dan kunci persendirian. Kunci awam boleh diketahui umum sementara kunci persendirian dipunyai oleh seseorang individu dan hanya diketahui oleh individu tersebut sahaja. Kunci awam dan kunci persendirian merupakan pasangan kunci yang saling berkait. Perkaitan pasangan kunci ini adalah seperti berikut:

(i) Data disulitkan dengan kunci awam boleh dinyahsulitkan hanya dengan kunci persendirian yang sejajar.
(ii) Data disulitkan dengan kunci persendirian boleh dinyahsulitkan hanya dengan kunci awam yang sejajar.

Rajah 5 menunjukkan pasangan kunci awam dan kunci persendirian. Kunci awam dan kunci persendirian berkait secara matematik, maka untuk mendapatkan kunci persendirian adalah sukar jika hanya diberikan kunci



RAJAH 5. Pasangan Kunci Awam dan Kunci Persendirian

awam. Bagaimanapun mendapatkan kunci persendirian adalah mungkin jika diberikan masa dan komputer yang berkuasa tinggi.

ALGORITMA FUNGSI CINCANG

Fungsi cincang merupakan algoritma matematik yang menjana satu nombor besar sebagai perwakilan sesuatu mesej. Terdapat 3 ciri penting fungsi cincang (Tanenbaum 1996) iaitu:

(i) Diberikan mesej, adalah mudah untuk mengira mesej diges.
(ii) Diberikan mesej diges, adalah mustahil untuk mendapatkan mesej.
(iii) Tidak mungkin dua mesej yang berbeza mempunyai mesej diges yang sama.

Fungsi cincang boleh digunakan untuk mengatasi dua masalah di atas iaitu kelajuan proses menandatangan mesej yang panjang dan pautan blok-blok yang ditanda tangan (Wilson 1995).

Penggunaan fungsi cincang untuk kriptografi adalah dengan tanda tangan digital dan untuk tujuan integriti data. Fungsi cincang yang digabungkan dengan algoritma kunci awam boleh digunakan untuk mengimplementasikan tanda tangan digital. Apabila fungsi cincang digunakan untuk menentukan sama ada mesej asal dipinda ianya dikenali sebagai *modification detection codes (MDC)*. Berkaitan dengan fungsi cincang yang digunakan untuk pengesahan identiti serta identiti data dikenali sebagai *message authentication codes (MAC)* (Menezes et al. 1996). Terdapat beberapa fungsi cincang yang digunakan dalam kriptografi seperti MD2, MD4, MD5, dan *Secure Hash Algorithm* (SHA).

ALGORITMA TANDA TANGAN

Algoritma tanda tangan merupakan fungsi matematik yang digunakan dalam proses penyulitan dan penyahsulitan. Algoritma tanda tangan bekerja bersama-sama dengan kunci untuk menyulit teks asal. Teks asal yang sama menghasilkan teks sifer yang berlainan jika disulitkan dengan kunci yang lain. Keselamatan data yang disulitkan bergantung pada dua perkara iaitu algoritma tanda tangan dan kerahsiaan kunci yang digunakan (Noor Hayati 2002; Noor Hayati et al. 2002).

CIRI-CIRI DAN KEPERLUAN PADA TANDA TANGAN DIGITAL

Tanda tangan digital adalah setanding dengan tanda tangan tulisan tangan. Ia mempunyai ciri-ciri berikut (Stallings 1998):

(i) Boleh menentusah pengarang, masa, dan tarikh tanda tangan dihasilkan.
(ii) Boleh mengesahkan kandungan pada masa ditanda tangan.

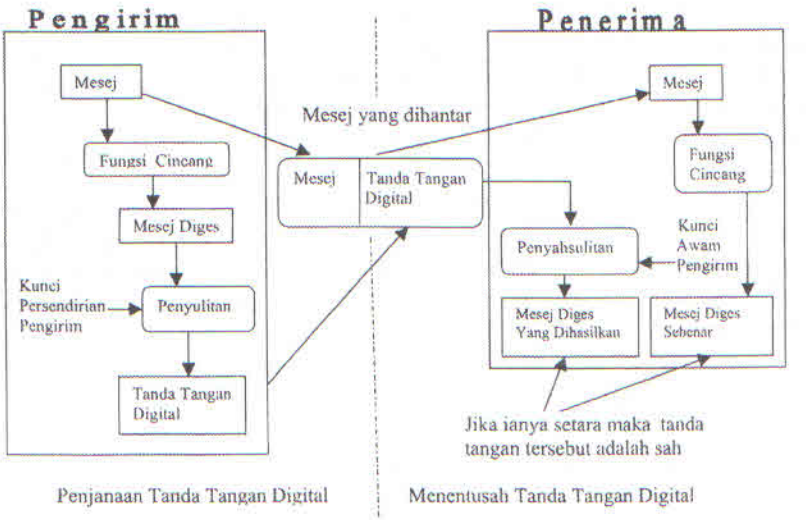
(iii) Tanda tangan tersebut boleh ditentusahkan oleh pihak ketiga, untuk menyelesaikan sebarang pertikaian (Stallings 1998)

Berdasarkan kepada ciri-ciri ini, dapat dirumuskan keperluan-keperluan yang perlu ada pada tanda tangan digital, iaitu:

(i) Tanda tangan tersebut merupakan corak bit yang bergantung kepada mesej yang ditanda tangan.
(ii) Tanda tangan tersebut menggunakan maklumat unik untuk seseorang pengirim bagi mengelakkan pemalsuan dan penafian.
(iii) Mudah untuk menghasilkan tanda tangan digital.
(iv) Mudah untuk mengenalpasti dan menentusah tanda tangan digital.
(v) Tidak munasabah untuk memalsukan tanda tangan digital, sama ada dengan membentuk mesej baru untuk tanda tangan digital yang ada atau membentuk tanda tangan digital palsu untuk mesej yang ada.
(vi) Adalah praktikal untuk menyimpan salinan tanda tangan digital dalam storan (Stallings 1998).

Pada kebiasaannya tanda tangan digital dipersembahkan sebagai satu rentetan bit. Ianya sama ada ditambah kepada mesej yang sedia ada atau mesej yang ada merupakan sebahagian dari tanda tangan digital tersebut (Piper 1991).

Penggunaan tanda tangan digital melibatkan dua proses, satu dilaksanakan oleh penandatangan iaitu penjanaan tanda tangan digital, manakala proses satu lagi dilaksanakan oleh penerima tanda tangan digital iaitu menentusah tanda tangan digital. Rajah 6 menunjukkan skema tanda tangan digital.



RAJAH 6. Skema Tanda Tangan Digital.

Skema tanda tangan digital merupakan kaedah penandatangan menandatangani dokumen elektronik yang boleh disimpan oleh penerima sebagai bukti bahawa dokumen ditanda tangan oleh pemilik asal (Yen & Laih 1995) dengan ciri-ciri berikut:

(i) Penjanaan tanda tangan digital menggunakan fungsi cincang untuk memampatkan mesej yang dikenali sebagai mesej diges. Mesej diges dan kunci persendirian dijadikan input kepada proses penyulitan.
(ii) Menentusah tanda tangan digital melibatkan dua proses iaitu penghasilan mesej diges daripada teks asal dan penyahsulitan tanda tangan digital menggunakan kunci awam. Jika didapati hasil proses penyahsulitan adalah setara dengan mesej diges maka tanda tangan digital adalah sah.

Untuk menjadikan tanda tangan digital berguna sebagai amalan, tanda tangan digital mestilah:

(i) Mudah untuk penandatangan melakukan pengiraan (fungsi menghasilkan tanda tangan mudah diaplikasi).
(ii) Mudah untuk ditentusah oleh sesiapa sahaja (fungsi menentusah tanda tangan mudah diaplikasi).
(iii) mempunyai jangkahayat yang munasabah, iaitu selamat dari pemalsuan sehingga tanda tangan tidak diperlukan untuk tujuan asalnya (Menezes et al. 1996)

Faedah-Faedah Hasil Penggunaan Tanda Tangan Digital

Komunikasi secara elektronik dan saluran komunikasi yang lain perlu kepada ciri-ciri keselamatan seperti kerahsiaan, pengesahan, integriti, dan tiada penafian/*non-repudiation*. Keperluan bagi masyarakat yang mana kebanyakan maklumat disimpan dan dihantar dalam bentuk elektronik ialah suatu kaedah untuk memastikan keselamatan maklumat tanpa mengira media yang digunakan untuk menyimpan atau membawa maklumat tersebut. Satu daripada alat asas yang digunakan dalam keselamatan maklumat ialah tanda tangan.

Tanda tangan digital merupakan satu daripada beberapa aplikasi kriptografi kunci awam. Proses menghasilkan dan menentusah tanda tangan digital menyempurnakan kesan keperluan tanda tangan tulisan tangan untuk tujuan undang-undang. Tanda tangan digital memenuhi lima kriteria tanda tangan tulisan tangan:

(i) Tanda tangan tidak boleh ditiru atau dipalsukan.
(ii) Tanda tangan adalah tulen.
(iii) Tanda tangan tidak diguna semula.
(iv) Dokumen yang ditanda tangan tidak dipinda.
(v) Tanda tangan tidak boleh dinafikan (Scheiner 1995), (Noor Hayati 2002), dan (Noor Hayati et al. 2002).

Tanda tangan digital mempunyai kebaikan yang bermakna berbanding dengan tanda tangan tulisan tangan. Kebaikan tanda tangan digital dapat dilihat pada keupayaan tanda tangan digital itu iaitu ia boleh meningkatkan kelajuan transaksi, dan meluaskan jangkauan komunikasi secara geografi, (American Bar Association 1997), (Noor Hayati 2002), dan (Noor Hayati et al. 2002).

Tanda tangan digital membekalkan satu set keupayaan keselamatan yang sukar diimplementasikan dengan cara lain. Tanda tangan digital direka bentuk untuk membekalkan jaminan-jaminan seperti integriti data, pengesahan pengirim, pengesahan mesej, tidak boleh menafikan menghantar mesej dan memberi kesan di sisi undang-undang dibeberapa negara yang Malaysia adalah satu daripada negara tersebut, (Noor Hayati 2002), dan (Noor Hayati et al. 2002).

Serangan Ke Atas Tanda Tangan Digital

Cabang kepada bidang kriptologi, iaitu kriptanalisis merupakan sains dalam mendapatkan semula teks asal sesuatu mesej dari teks sifer tanpa mencapai kepada kunci. Usaha-usaha dalam kriptanalisis dikenali sebagai serangan (Schneier 1996). Terdapat dua serangan asas terhadap skema tanda tangan digital kunci awam:

(i) Serangan kunci: serangan bentuk ini musuh hanya mengetahui kunci awam penandatangan.

(ii) Serangan mesej: musuh berkeupayaan memeriksa tanda tangan yang sejajar sama ada dengan mesej yang diketahui atau mesej yang dipilih. Serangan mesej terbahagi kepada tiga kelas:

   (a) Serangan mesej yang diketahui.
   Musuh mempunyai tanda tangan dan padanan mesej yang mana diketahuinya tetapi bukan merupakan pilihannya.

   (b) Serangan mesej pilihan.
   Musuh memperoleh tanda tangan yang sah dari satu senarai mesej terpilih sebelum cuba memecahkan skema tanda tangan. Serangan ini tidak diubahsuai dalam erti bahawa mesej dipilih sebelum tanda tangan dilihat. Serangan mesej pilihan terhadap skema tanda tangan adalah bersamaan dengan serangan teks sifer pilihan terhadap skema penyulitan kunci awam.

   (c) Serangan mesej pilihan yang diubahsuai.
   Musuh dibenarkan menggunakan penandatangan sebagai petunjuk; musuh mungkin meminta tanda tangan mesej yang bergantung kepada kunci awam penandatangan dan musuh mungkin meminta tanda tangan mesej yang mana bergantung terhadap tanda tangan atau mesej yang didapati terdahulu (Menezes et al. 1996).

PROTOKOL TANDA TANGAN DIGITAL

Protokol merupakan satu siri langkah yang direka bentuk untuk menyelesaikan sesuatu tugas dan melibatkan dua atau lebih pihak. Dewasa ini terdapat beberapa jenis protokol yang digunakan. Satu contoh protokol tanda tangan digital ialah *Kriptografi Kunci Awam* dan *Fungsi Cincang Satu Hala*. Rajah 7 di bawah menunjukkan protokol menandatangan dokumen dengan kriptografi kunci awam dan fungsi cincang satu hala (Schneier 1996).

Algoritma kunci awam tidak efisien untuk menandatangan dokumen yang panjang. Untuk menjimatkan masa, protokol tanda tangan digital sering diimplementasi dengan fungsi cincang satu hala.

Andaikan *A* adalah pengirim mesej, *B* adalah penerima mesej, *M* adalah mesej asal, *D* adalah hasil fungsi cincang satu hala mesej asal iaitu teks cincang, *S* adalah hasil penyulitan *D*, S_{-1} adalah hasil penyahsulitan *S*, *K* adalah kunci awam untuk *A* dan K_{-1} adalah kunci persendirian untuk *A*. Protokol menandatangan dokumen dengan kriptografi kunci awam dan fungsi cincang satu hala adalah seperti berikut:

(i) *A* menghasilkan teks cincang, *D*.

(ii) *A* menyulitkan *D* menggunakan K_{-1} dan menghasilkan *S*, dengan yang demikian menandatangan mesej tersebut.

(iii) *A* menghantar *M* bersama-sama *S* kepada *B*.

(iv) *B* menghasilkan *D* dari *M*. *B* kemudian menggunakan algoritma tanda tangan digital serta menyahsulitkan *S* dan menghasilkan S_{-1} menggunakan *K*. Jika *D* sama dengan S_{-1}, maka tanda tangan adalah sah.

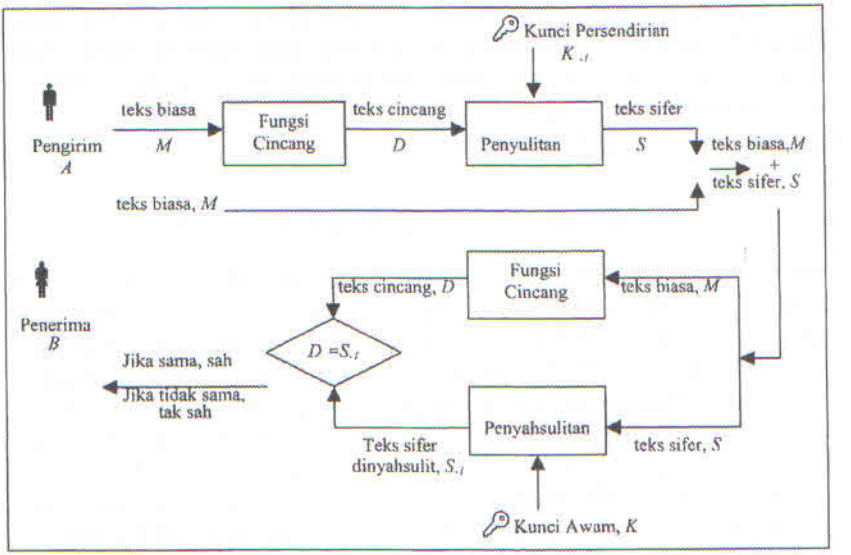
Protokol ini mempunyai beberapa kebaikan, antaranya ialah tanda tangan boleh disimpan berasingan dari dokumen asal serta keperluan storan untuk dokumen dan tanda tangan yang kecil.

Protokol-protokol lain yang sering digunakan ialah *Sistem Kripto Simetri dan Penimbangtara*, *Kriptografi Kunci Awam*, dan *Penanda Masa*, (Schneier 1996), (Noor Hayati 2002), (Noor Hayati et al. 2002).

Protokol juga mempunyai beberapa ciri lain seperti ia mesti diwujudkan terlebih dahulu, saling dipersetujui, tidak mengelirukan, dan mesti lengkap (Schneier 1996; Pfleeger 1989; Noor Hayati 2002; Noor Hayati 2002).

APLIKASI TANDA TANGAN DIGITAL

Aplikasi tanda tangan digital pertama bermula di Sandia iaitu selepas artikel pertama Diffie dan Helman pada tahun 1976 diterbitkan (Omura 1990). Pada masa kini penggunaan tanda tangan digital adalah secara meluas dan piawaian di peringkat negara dan antara bangsa banyak dicadangkan. Satu daripada contoh penggunaannya adalah dalam mel elektronik dan pertukaran data atau *Electronic Data Interchange (EDI)* iaitu kontrak dan tempahan pembelian



RAJAH 7. Protokol Menandatangan Dokumen dengan Kriptografi Kunci Awam dan Fungsi Cincang Satu Hala.

boleh ditanda tangan dan dihantar secara elektronik (Omura 1990). Tanda tangan digital penting dalam urus niaga bank secara elektronik (Denning 1983).

Tanda tangan digital digunakan dalam sistem mel elektronik untuk mengesahkan kandungan dan identiti pengirim sesuatu mesej. Pihak pengirim menjana satu mesej dan menandatangan mesej menggunakan kunci persendirian. Mesej asal dan tanda tangan digital yang dihasilkan dihantar kepada pihak penerima. Pihak penerima membuat pengesahan mesej, pihak penerima yakin bahawa mesej ditanda tangan oleh pihak pengirim. Pihak penerima juga yakin bahawa mesej tidak dipinda selepas ditanda tangan oleh pihak pengirim.

Selain daripada itu tanda tangan digital digunakan juga di dalam Kawalan Capaian iaitu kebolehan meningkatkan tahap keselamatannya dalam sistem kawalan capaian dan pengesahan dalam rangkaian (Jackson & Hruska 1992; Noor Hayati 2002; Noor Hayati et al. 2002). Sistem seperti ini mula digunakan di Sandia National Laboratories pada tahun 1979.

Tanda tangan digital juga digunakan untuk menentusah perisian, (Omura 1990), dan mengesan virus, (Jackson & Hruska 1992; Norhayati 2002; Norhayati et al. 2002).

Pengesan Larangan Ujian Nuklear juga menggunakan tanda tangan digital, (Denning 1983; Schneier 1996; Norhayati 2002; Norhayati et al. 2002).

Tanda tangan digital juga digunakan untuk sistem radar pesawat udara untuk keperluan mengenalpasti pesawat udara yang kelihatan pada skrin radar. Dengan tanda tangan digital setiap pesawat udara berkeupayaan menandatangan sebarang isyarat yang diterima dan menghantarnya semula (Omura 1990; Norhayati 2002; Norhayati et al. 2002).

SISTEM KRIPTO *RIVEST SHAMIR ADLEMAN* (RSA)

Sistem kripto RSA merupakan hasil usaha Rivest, Shamir, dan Adleman pada tahun 1978 (Wilson 1995). Sistem kripto RSA digunakan dengan meluasnya pada hari ini. Sistem RSA dikatakan sebagai sistem kripto kunci awam yang terbaik (Schneier 1996). Tahap kekuatan sistem RSA berdasarkan kepada kepayahan memfaktorkan nombor integer yang besar (Denning 1983; Rivest et al. 1978). RSA dipatenkan di Amerika Syarikat dan tempohnya telah berakhir pada tahun 2000.

Sistem kripto RSA banyak diimplementasikan pada perkakasan seperti cip dan kad pintar. Perbandingan antara RSA dan DES menunjukkan kelajuan perlaksanaan dalam perkakasan adalah 1000 kali lebih perlahan manakala perlaksanaan dalam perisian adalah 100 kali lebih perlahan. Serangan terhadap implementasi RSA melibatkan serangan ke atas protokol dan bukannya ke atas algoritma asas RSA. Antara serangan ke atas protokol RSA ialah serangan teks sifer pilihan, serangan modulus sepunya, dan serangan terhadap penggunaan eksponen penyulitan yang kecil (Schneier 1996).

Sistem RSA beroperasi menggunakan matematik mod n. n merupakan hasil darab dua nombor perdana iaitu p dan q. Sistem RSA melibatkan sepasang kunci untuk penyulitan dan penyahsulitan. e adalah kunci awam untuk penyulitan dan d pula merupakan kunci persendirian untuk penyahsulitan. Pertalian antara kedua-dua kunci ini diberikan oleh persamaan $e \cdot d ? 1 \bmod (p-1) \cdot (q-1)$. Penyulitan mesej teks asal, M kepada mesej teks sifer, C diberikan oleh $C = M^e \bmod n$. Penyahsulitan mesej teks sifer, C kepada mesej teks asal, M diberikan oleh $M = C^d \bmod n$. Oleh kerana fungsi penyulitan dan penyahsulitan adalah fungsi kebalikan antara satu sama lain, sistem kripto RSA boleh digunakan untuk kerahsiaan dan pengesahan (Denning 1983).

SISTEM KRIPTO LUC

Sistem kripto LUC merupakan sistem kunci awam yang dibangunkan oleh sekumpulan penyelidik yang berpangkalan di New Zealand dan merupakan satu sistem alternatif kepada sistem kripto RSA (Smith & Lennon 1993). Struktur keseluruhan LUC adalah sama seperti RSA yang berasaskan masalah matematik yang sama seperti RSA, LUC menggunakan pengiraan fungsi Lucas sebagai ganti kepada eksponen pada RSA. Oleh kerana fungsi Lucas adalah kompleks secara matematiknya maka ia menghasilkan sifer yang baik.

Satu skema tanda tangan digital berasaskan fungsi Lucas telah dicadangkan oleh Smith dan Lennon yang bebas dari serangan berulang-ulang (Yen & Laih 1995). Ini yang menjadikan skema tanda tangan digital LUC sebagai alternatif kepada sistem RSA. Sistem LUC menggunakan fungsi yang diterangkan oleh Lucas pada tahun 1878 dan keselamatan LUC bergantung kepada kepayahan untuk memfaktorkan hasil dua nombor perdana (Denning 1983; Rivest et al. 1978).

LUC berasaskan kepada integer-integer besar di dalam jujukan Lucas. Fungsi Lucas merupakan dua siri jujukan integer-integer V_n dan U_n yang ditakrifkan oleh

$$V_n = V_n(P,Q) = a^n + b^n \tag{1.3}$$

$$U_n = U_n(P,Q) = (a^n - b^n) / (a - b). \tag{1.4}$$

untuk sebarang integer n, P, dan Q, dengan a dan b adalah punca kepada persamaan:

$x^2 - Px + Q = 0$ (dengan yang demikian $P = a+b$ manakala $Q = ab$).

Sistem kripto LUC akan hanya menggunakan jujukan daripada siri V_n dan Q bernilai 1 sahaja.

Jujukan Lucas $V_n = V_n(P,Q)$ untuk integer n = 0, 1, 2, 3 dan seterusnya adalah seperti berikut:

$V_0 = 2$	untuk $n = 0$
$V_1 = P$	untuk $n = 1$
$V_{n+1} = PV_n - QV_{n-1}$	untuk n = 1, 2, 3 dan seterusnya.

Jujukan Lucas memenuhi persamaan-persamaan berikut dengan D adalah *discriminant* untuk persamaan $x^2 - Px + Q$, iaitu $D = P^2 - 4Q = (a-b)^2$.

$$(i)\ U_{2n} = U_n V_n \text{ dan } V_{2n} = V_n^2 \tag{1.6}$$

$$(ii)\ V_n = DU_n^2 + 4Q_n \tag{1.7}$$

$$(iii)\ U_{m+n} = U_m U_{n+1} - QU_{m-1} U_n \tag{1.8}$$

$$(iv)\ 2Q_n V_{n-m} = V_m V_n - DU_m U_n \tag{1.9}$$

$$(v)\ V_{nk}(P,Q) = V_n(V_k(P,Q), Q^k) \tag{2.0}$$

Untuk sebarang nombor N, maka $V_n(P \bmod N, Q \bmod N) \stackrel{?}{=} U_n(P,Q) \bmod N$ dan ini sentiasa benar apabila n adalah 0 atau 1. Seterusnya bagi n bernilai 2 atau lebih, maka $U_n(P,Q) \bmod N \stackrel{?}{=} (P \bmod N)(U_{n-1}(P,Q) \bmod N) - (Q \bmod N)(U_{n-2}(P,Q) \bmod N)$.

LUC boleh digunakan untuk tujuan penyulitan, tanda tangan dan pertukaran data. Sistem kripto LUC juga telah dibuktikan adalah lebih kuat dari sistem kripto RSA dan memerlukan usaha-usaha pengiraan bersamaan dengan sistem kripto RSA. Sistem kripto LUC tidak terjejas kepada serangan-serangan terhadap sistem kripto yang berasaskan kepada eksponen kerana fungsi Lucas yang digunakan tidak mempunyai ciri berdaya darab (Smith & Lennon 1993). Bagaimanapun kriptanalisis menunjukkan bahawa sistem kripto LUC juga boleh diserang menggunakan teknik pemalsuan mesej pilihan (Bleichenbacher et al. 1996).

PERBANDINGAN ANTARA RSA DAN LUC

RSA dan LUC, kedua-duanya merupakan sistem kripto kunci awam. Sistem kripto hari ini terbahagi kepada sama ada penyelesaian masalah pemfaktoran integer, masalah log diskret atau *Elliptic Curve Discrete Logarithm*. Kedua-dua sistem kripto RSA dan LUC tergolong dalam penyelesaian masalah pemfaktoran integer. Smith dan Lennon (1993) mendapati secara kriptografi sistem LUC memerlukan usaha-usaha pengiraan yang hampir sama dengan sistem RSA. Keselamatan LUC dan RSA bergantung kepada masalah matematik untuk memfaktorkan hasil dua nombor perdana. Jadual 1 menunjukkan perbandingan secara umum antara sistem LUC dan sistem RSA.

JADUAL 1. Perbandingan Umum Bagi RSA Dan LUC.

	RSA	LUC
Penjanaan Kunci	Cari nombor perdana p & q $N = pq$ Kira kunci persendirian d	Cari nombor perdana p & q $N = pq$ Kira kunci persendirian $d1$, $d2$, $d3$ & $d4$
Penyulitan	$C = M^e \bmod N$	$C = V_e(M,1) \bmod N$
Penyahsulitan	- $M = C^d \bmod N$	Pilih antara $d1$, $d2$, $d3$ & $d4$ $M = V_{dx}(C,1) \bmod N$
Kelajuan Relatif (bilangan darab)	3	4
Kemungkinan hanya serangan kunci terhadap tanda tangan digital	Ya	Tidak
Kebarangkalian relatif bahawa mesej secara rawak akan mengunjur ruangan penyulitan yang maksimum	Rendah	Tinggi

Analisis perbandingan daripada segi pelaksanaan sistem kripto RSA dan sistem kripto LUC dijalankan oleh Siti Jauyah (1999). Analisis pelaksanaan melihat keupayaan kedua-dua sistem dalam menjalankan operasi penyulitan, penyahsulitan, penjanaan, dan pengesahbetulan tanda tangan digital.

Perbandingan algoritma penghasilan kunci, penyulitan dan penyahsulitan untuk sistem RSA dan LUC dapat dilihat pada Jadual 2.

Pengkaji mendapati sistem kripto LUC adalah setanding dengan RSA seperti yang didakwa oleh Smith dan Lennon (1993) iaitu algoritma LUC adalah selamat daripada RSA berdasarkan kepada fungsi Lucas yang digunakan dalam LUC tidak berdaya darab.

Hasil eksperimen yang dijalankan oleh pengkaji dengan melihat kepada jalanan proses penyulitan menggunakan saiz modulus N, 256 bit sehingga 2048 bit menunjukkan kelajuan proses kedua-dua sistem RSA dan LUC adalah setara. Eksperimen juga menunjukkan kelajuan proses penyahsulitan bagi LUC adalah perlahan berbanding RSA. Pengkaji mengatakan terjadinya begini kerana dalam sistem LUC, bagi setiap blok teks sifer yang dibaca

JADUAL 2 : Perbandingan Algoritma RSA Dan LUC.

	RSA	LUC
Penjanaan Kunci	Pilih p, q p dan q adalah nombor perdana	Pilih p, q p dan $q$nombor perdana
	Kirakan $n = p$ X q Kirakan $\phi(n) = (p\text{-}1)(q\text{-}1)$	Kirakan $n = p$ X q Kirakan S(n) = $(p\text{-}1)(q\text{-}1)$ $(p+1)(q+1)$ S(n) – fungsi euler totient
	$\phi(n)$ – fungsi euler totient Pilih integer e gcd($?(n)$,e)=1; $1 < e < \phi(n)$	Pilih integer e gcd(S(n),e)=1
	gcd – pembahagi sepunya terbesar	gcd – pembahagi sepunya terbesar
	Kirakan d $d = e^{-1} \bmod \phi(n)$ Kunci awam = $\{e,n\}$ Kunci Persendirian = $\{d\}$	Kirakan $d1$, $d2$, $d3$, & $d4$ $d1 = e^{-1} \bmod (\text{lcm}((p\text{-}1),(q\text{-}1)))$ $d2 = e^{-1} \bmod (\text{lcm}((p\text{-}1),(q+1)))$ $d3 = e^{-1} \bmod (\text{lcm}((p+1),(q\text{-}1)))$ $d4 = e^{-1} \bmod (\text{lcm}((p+1),(q+1)))$
	Kunci awam = {e,n} kunci Persendirian = {d}	Kunci Awam = {e,n} Kunci Persendirian = $\{d1,d2,d3,d4\}$
Penyulitan	Teks biasa : $M < n$ Teks sifer : $C = M^e \pmod n$	Teks biasa : $M < n$ Teks sifer : $C = V_e(M,1) \pmod n$ V_e : jujukan Lucas
Penyahsulitan	Teks biasa : C Teks sifer : $M = C^d \pmod n$	Teks biasa : C Teks sifer : $M = V_e(C,1) \pmod n$ V_e : jujukan Lucas

perlu ditentukan pula kunci persendirian yang berpadanan. Sistem LUC mempunyai empat kemungkinan kunci persendirian berbanding hanya satu kunci sahaja bagi sistem RSA. Proses penjanaan tanda tangan digital pula memberi hasil seperti proses penyahsulitan dan proses menentusah tanda tangan digital pula memberi hasil seperti proses penyulitan.

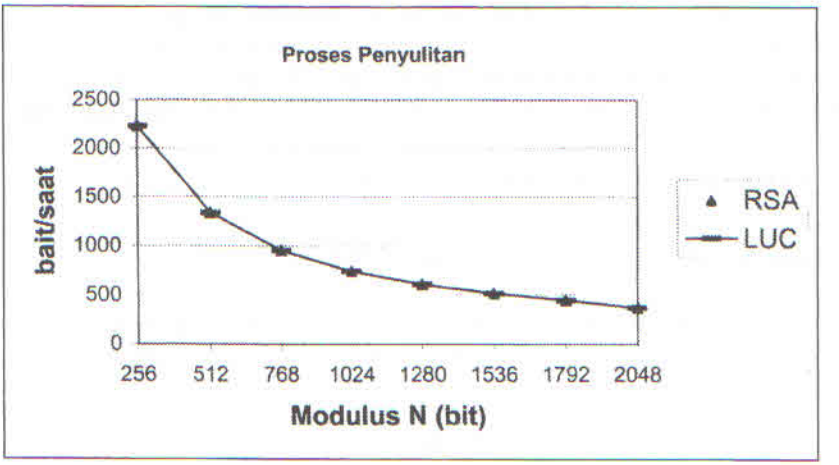
Data kajian adalah merupakan masa yang diambil untuk proses-proses penyulitan, penyahsulitan, penjanaan tanda tangan digital dan pengesahbetulan tanda tangan digital bagi setiap saiz kunci yang berlainan (256 – 2048 bit). Teks asal untuk ujian adalah bersaiz 6685 bait. Proses-proses penyulitan, penyahsulitan, penjanaan tanda tangan digital dan pengesahbetulan tanda tangan digital dilakukan dengan menggunakan mesin Pentium 166 MHz, 32 MB RAM. Atur cara ditulis dalam bahasa C dan dikompil dengan pengkompil C++ versi 3.1. Hasil kajian kelajuan proses penyulitan teks asal menggunakan saiz modulus *N*, 256 bit sehingga 2048 bit dapat dilihat pada Jadual 3 dan digambarkan secara graf pada Rajah 8. Hasil kajian kelajuan proses penyahsulitan teks asal menggunakan saiz modulus N, 256 bit sehingga 2048 bit dapat dilihat pada Jadual 4 dan digambarkan secara graf pada Rajah 9.

JADUAL 3. Kelajuan Proses Penyulitan Bagi RSA Dan LUC.

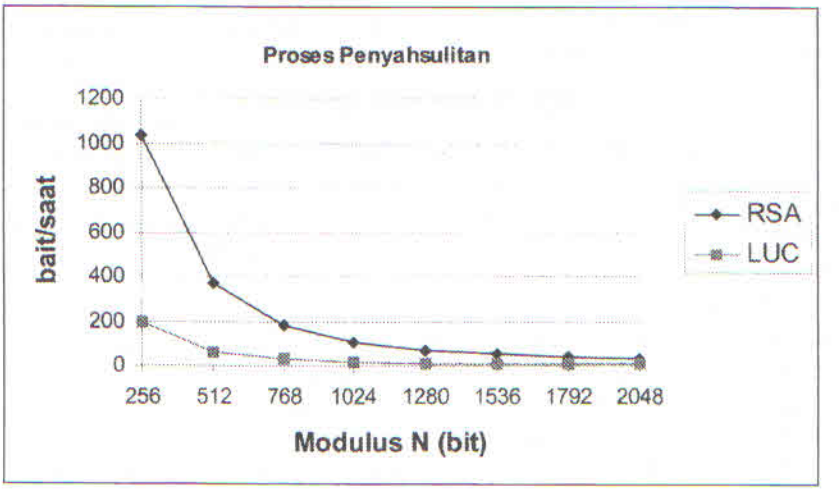
Saiz Modulus (bit)	Kelajuan (bait/saat)	
	RSA	LUC
256	2228.3	2228.3
512	1337.0	1337.0
768	955.0	955.0
1024	742.7	742.7
1280	607.7	607.7
1536	514.2	514.2
1792	445.6	445.6
2048	371.3	371.3

JADUAL 4. Kelajuan Proses Penyahsulitan Bagi RSA Dan LUC.

Saiz Modulus (bit)	Kelajuan (bait/saat)	
	RSA	LUC
256	1034.5	199.5
512	371.3	58.6
768	180.6	27.0
1024	107.8	15.5
1280	71.1	9.9
1536	49.8	7.0
1792	37.4	5.2
2048	28.0	3.9



RAJAH 8. Saiz Modulus *N* Melawan Kelajuan Proses Penyulitan.



RAJAH 9 : Saiz Modulus *N* Melawan Kelajuan Proses Penyahsulitan.

Siti Jauyah (1999) juga menjalankan perbandingan dari segi keselamatan terhadap algoritma RSA dan LUC. Perbandingan ini dibuat dengan cara melaksanakan kajian mengenai kaedah untuk memecah atau menyerang sistem kripto (kriptanalisis). Kriptanalisis yang dijalankan adalah terhadap protokol perlaksanaan. Dua serangan terhadap protokol perlaksanaan yang dilaporkan adalah serangan teks sifer pilihan (Schneier 1996) dan serangan pemalsuan mesej pilihan (Bleichenbacher et al. 1996).

Serangan teks sifer pilihan merupakan percubaan untuk mendapatkan teks asal berdasarkan teks sifer yang diperoleh manakala serangan pemalsuan mesej pilihan adalah untuk meniru tanda tangan digital terhadap mesej atau dokumen pilihan. Jadual 5 menunjukkan dapatan dari kajian yang dijalankan.

JADUAL 5 : Perbandingan Jenis Serangan Terhadap RSA dan LUC.

Jenis Serangan	RSA	LUC
Serangan Teks Sifer Pilihan	Algoritma serangan dikenalpasti	Belum terdapat sebarang Kaedah
Serangan Pemalsuan Mesej Pilihan	Algoritma serangan dikenalpasti	Algoritma serangan dikenalpasti

KESIMPULAN

Tanda tangan digital merupakan teknologi yang mampu menyediakan khidmat-khidmat keselamatan. Khidmat-khidmat keselamatan yang dapat disediakan dengan penggunaan tanda tangan digital ialah kesahihan asalan mesej, integriti kandungan, kerahsiaan kandungan, ketidakbolehnafian asalan serta dilindungi undang-undang.

Sistem kripto LUC merupakan sistem kripto kunci awam yang digunakan untuk penjanaan pasangan kunci awam dan kunci persendirian, penjanaan tanda tangan digital, dan menentusah tanda tangan digital. Sistem Kripto LUC didapati masih selamat daripada serangan teks sifer pilihan dan serangan terhadap kunci adalah sukar kerana terdapat empat kemungkinan kunci persendirian.

Algoritma sistem kripto LUC digunakan untuk membina prototaip sistem keselamatan dalam aplikasi mel elektronik. Teknologi tanda tangan digital digunakan dalam prototaip yang dibina sebagai cara untuk melindungi integriti mesej dan mengesahkan asalan mesej. Sistem ini dapat meningkatkan tahap keselamatan mel elektronik.

Dengan keupayaan menjana dan menentusah tanda tangan digital, maka dengan ini mampu digunakan sebagai membekalkan pengguna dengan fungsi yang dapat memastikan mel yang dihantar dan diterima mempunyai tanda tangan digital. Tanda tangan digital yang boleh dijana dan ditentusah membolehkan pengguna menentukan kebenaran mesej yang dihantar dan kesahihan identiti pengirim.

Adalah diharapkan dengan kajian yang berkaitan dengan tanda tangan digital ini mengalakkan penggunaan tanda tangan digital sebagai teknologi yang memungkinkan pejabat elektronik yang kurang menggunakan kertas *(paperless electronic office)* menjadi kenyataan. Di samping itu teknologi tanda tangan digital ini dapat meningkatkan kesedaran dan menambahkan

pengetahuan pengguna tentang kewujudan Akta Tanda tangan Digital 1997 di Malaysia. Akta ini merupakan satu-satunya akta dari beberapa akta yang terdapat dalam Undang-undang Siber yang dikuatkuasakan penggunaannya. Akta ini dapat melindungi sesiapa sahaja di Malaysia yang menggunakan tanda tangan digital.

Akhir sekali diharapkan kajian ini dapat mencetuskan kajian-kajian mengenai keselamatan yang berkaitan dengan dunia elektronik bagi kegunaan pada masa hadapan dan melangkah bersama dengan kemajuan teknologi maklumat.

RUJUKAN

American Bar Association, Section of Science and Technology, Information Security Committee. Digital signature guidelines tutorial (atas talian) http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html [10 Mac 1997].

Bleichenbacher, D., Bosma, W. & Lenstra, A.K. 1996. Some remarks on Lucas-Based cryptosystem, *Proc. Crypto '95, Lecture Notes in Comp. Sci. Eds: G. Goos, J. Hartmanis, J. Van Leeuwen 963, Springer-Verlag*: hal. 386-396.

Denning, D. E. 1983. *Cryptography and data security*. Massachusetts: Addison Wesley.

Diffie, W. & Hellman, M. E. 1976. New directions in cryptography: *IEEE Transactions on Information Theory*, 22(6): hal. 644-654 .

Diffie, W. 1988. The first ten years of public-key cryptography, *Proceedings of the IEEE, 76*: hal. 560-577. (Simmons, G.J. "Contemporary Cryptology: The Science of Information Integrity", IEEE PRESS, 1991).

Jackson, K. M. dan Hruska, J. 1992. *Computer security reference book*, Florida : CRC Press.

Massey, J. L. 1996. Cryptography: Fundamental and applications, *Journal of Cryptology*, 9(1): hal. 167-173.

Menezes, A., van Oorschot, P. & Vanstone, S. 1996. *Handbook of applied cryptography*. California. CRC Press.

Nechvatal, J. 1991. Public–Key cryptography, NIST Special Publication 800-2, Security Technology Group, National Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersbury, MD 20899.

Noor Hayati H. 2002. Penjanaan Tanda Tangan Digital untuk Keselamatan Mesej Mel Elektronik. *Tesis Sarjana, Jabatan Sains dan Pengurusan Sistem, Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia* (tidak terbit).

Noor Hayati, H., Khairuddin, O., Md Jan, N., & Zulkarnain, M. A. 2002. Tanda Tangan Digital untuk Keselamatan Mesej Mel Elektronik. Siri Laporan Teknik *Fakulti Teknologi dan Sains Maklumat*, /Mac 2002/LT8. (tidak terbit).

Omura, J. K. 1990. Novel applications of cryptography in digital communications, *IEEE Communications Magazine*, 28(5): hal. 21-29.

Pfleeger, C. P. 1989. *Security in computing*. Englewood Cliffs, New Jersey : Prentice Hall.

Piper, F. 1991. Digital signatures, *Proceedings of the IFIP TC11 Seventh International Conference on Information Security (IFIP/Sec '91)*: hal. 67-76.

Rivest, L., Shamir, A. & Adleman, L. 1978. A method for obtaining digital signature and public key cryptosystems, *Communications of the ACM*, 21(2): hal. 120-126.

Roberts, P. 1997. Electronic/Digital signature position paper (atas talian) http://www.state.tn.us/finance/oir/prd/edsignat.html (29 Ogos 2000).

Schneier, B. 1995. *E-Mail security : how to keep your electronic messages private*. New York : John Wiley & Sons.

Schneier, B. 1996. *Applied cryptography, second edition : protocols, algorithm, and source code in C*. New York : John Wiley.

Siti Jauyah S. 1999. Sistem kripto LUC untuk pengesahan aplikasi TELNET. Tesis Sarjana, (tidak terbit).

Smith, P. dan Lennon, M. 1993. LUC : A new public key system, Proceedings, *Ninth International Conference on Information Security*, IFIP/Sec.

Stallings, W. 1998. *Cryptography and network security : principles and practice*. Upper Saddle River, New Jersey : Prentice Hall.

Tanenbaum A. S. 1996. *Computer networks*. New Jersey : Prentice Hall.

William H. C. 1980. *Computationally "hard" problems as a source for cryptosystems*. AAAS Selected Symposium Series, California, USA : West View Press, Inc.

Wilson S. B. 1995. Digital signature and public-key cryptography, *Proceeding of IMA conference on cryptography and coding, January 1995*.

Yen, S. M. dan Laih C. S. 1995. Fast algorithms for LUC digital signature computation, *IEE Proc. Compu. Digit Tech.*, 142(2): hal. 165-169.

Noor Hayati Hashim, Khairuddin Omar,
Md. Jan Nordin & Zulkarnain Md. Ali
Fakulti Teknologi dan Sains Maklumat
Universiti Kebangsaan Malaysia
43600 UKM, Bangi, Selangor D.E, Malaysia.
ko@ftsm.ukm.my; jan@ftsm.ukm.my; zma@ftsm.ukm.my