Kriptografi Dalam Sistem Uang Elektronik (Electronic Money System)

Ali Akbar

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jl. Ganesha No.10 Bandung, Indonesia

if13095@students.if.itb.ac.id

Abstrak

Sistem uang elektronik (*electornic money system / e-money*) merupakan suatu bentuk alat pembayaran tanpa uang fisik (*cashless money*). Bentuk dari uang elektronik bermacam-macam, diantaranya dompet elektronik (*e-purse*), kartu debit dan sebagainya. Pada sistem seperti ini, nilai uang tidak tersimpan secara fisik, tetapi hanya sebagai data elektronik. Oleh karena itu, pada sistem uang elektronik, keamanan data menjadi hal yang sangat penting. Tanpa didukung oleh keamanan yang kuat, dengan mudah seorang penjahat dapat memalsukan uang.

Keamananan (*security*) sebuah sistem dapat dibagi menjadi tiga aspek, yaitu aspek *people*, proses dan teknologi[6]. Pada aspek teknologi, keamanan data dapat didukung dengan menggunakan teknik-teknik kriptografi, seperti enkripsi/dekripsi (baik kunci simetris maupun asimetris), *hash*, *signature*, dan sebagainya. Makalah ini akan membahas keamanan data yang dibutuhkan oleh sistem uang elektronik, dan lebih spesifiknya, teknik-teknik kriptografi yang dapat dipakai dalam menjamin keamanan data sistem uang elektronik.

Kata kunci: sistem uang elektronik (*electronic money system / e-money*), kriptografi

1 Pendahuluan

Uang elektronik (disebut juga uang digital, atau dalam bahasa inggris: *electronic money, electronic cash, digital money, digital cash*) merupakan bentuk uang tanpa uang fisik (*cashless money*) yang menyimpan nilai uang dalam bentuk data digital. Uang elektronik pada saat ini semakin berkembang, karena lebih praktis dari uang konvensional (uang kertas) [12].

Uang elektronik terdiri dari 2, yaitu uang dan elektronik. Kata 'uang' dalam ilmu ekonomi modern dapat didefinisikan sebagai:

1. "alat tukar" (A.C. Pigou dalam bukunya, The Veil of Money [7]);
2. "sesuatu yang bisa diterima dalam pembayaran untuk mendapatkan barang-barang" (D.H.Robertson dalam bukunya, Money [7]);
3. "sesuatu yang tersedia dan secara umum diterima sebagai alat pembayaran bagi pembelian barang-barang dan jasa-jasa serta kekayaan berharga lainnya serta untuk pembayaran utang." (R.G. Thomas dalam bukunya, Our Modern Banking [7]).

Sedangkan kata 'elektronik' di sini berarti hanya menggunakan sistem komputer/sistem elektronik [8]. Jadi, uang elektronik dapat didefinisikan sebagai "alat pembayaran yang hanya dapat dipertukarkan dalam / menggunakan sistem elektronik".

Secara umum, uang memiliki fungsi sebagai perantara untuk pertukaran barang dengan barang, juga untuk menghidarkan perdagangan dengan cara barter. Fungsi uang ini juga berlaku untuk sistem uang elektronik. Dari fungsi-fungsi ini dapat diidentifikasi kebutuhan keamanan data nilai uang yang dikelola oleh sistem uang elektronik.

Fungsi asli uang :

1. Sebagai alat tukar (*medium of exchange*)

   Fungsi uang sebagai alat tukar umum atau *medium of exchange* sangat mempermudah pertukaran karena uang bersifat umum. Dengan uang orang yang akan melakukan pertukaran tidak perlu menukarkan dengan barang, tetapi cukup menggunakan uang sebagai alat tukar. Kesulitan-kesulitan pertukaran dengan cara barter dapat diatasi dengan pertukaran uang.

2. Sebagai satuan hitung (*unit of account*)

   Sebagai alat satuan hitung, uang dipakai untuk menunjukkan nilai berbagai macam barang/jasa yang diperjualbelikan, menunjukkan besarnya kekayaan, dan menghitung besar kecilnya pinjaman. Uang juga dipakai untuk menentukan harga barang/jasa (alat penunjuk harga). Sebagai alat satuan hitung, uang berperan untuk memperlancar pertukaran.

3. Sebagai penyimpan nilai

   Uang dapat berfungsi sebagai penyimpan nilai karena dapat digunakan untuk mengalihkan daya beli dari masa sekarang ke masa mendatang. Ketika seorang penjual saat ini menerima sejumlah uang sebagai pembayaran atas barang dan jasa yang dijualnya, maka ia dapat menyimpan uang tersebut untuk digunakan membeli barang dan jasa di masa mendatang.

Selain 3 fungsi utama tersebut, uang memiliki fungsi-fungsi turunan, yaitu sebagai berikut:

1. Sebagai alat pembayaran
2. Untuk menentukan harga
3. Sebagai alat pembayaran utang
4. Sebagai alat penimbun kekayaan
5. Sebagai alat pemindahan kekayaan (modal)
6. Sebagai alat untuk meningkatkan status sosial

Keamanan (*Security*)

Pada sistem uang elektronik, nilai uang disimpan dalam bentuk bit-bit data. Bit-bit data tersebut mengalir melalui jaringan komputer, diproses pada pemroses, disimpan pada basis data server, dan sebagainya. Seperti pada sistem uang konvensional, bit-bit data tersebut dapat diserang oleh orang yang tidak berhak, dan kemudian dimanipulasi, sehingga orang tersebut dapat menghasilkan uang palsu (berupa bit-bit data palsu). Sebuah sistem uang elektronik harus dapat melindungi keamanan data nilai uang yang dikelola, dengan memenuhi kriteria keamanan tertentu, sesuai dengan kebutuhan keamanan data nilai uang. Kriteria keamanan untuk sistem uang elektronik akan dibahas kemudian pada bagian 3.

Keamanan (*security*) dalam suatu sistem dapat dibagi menjadi tiga aspek, yaitu aspek *people*, aspek proses, dan aspek teknologi [6]. Aspek *people* membahas keamanan dari sisi manusia pelaksana sistem, misalnya bagaimana kesadarannya akan hal-hal yang berkatian dengan keamanan sistem, misalnya keamanan *password.* Aspek proses membahas keamanan dari sisi proses yang dilakukan. Maksudnya, setiap proses yang ada pada sistem tersebut dibuat sedemikian sehingga keamanan sistem tersebut dapat terjaga. Aspek proses ini harus muncul pada setiap SOP (*standard operation procedure*—prosedur operasi standar) yang ada. Aspek teknologi membahas keamanan dari sisi teknologi yang dapat diaplikasikan untuk mengamankan sistem tersebut.

Teknik-teknik kriptografi, seperti enkripsi / dekripsi, tandatangan digital, dsb. merupakan salah satu bagian penting aspek teknologi pada keamanan sistem uang elektronik. Teknik-teknik kriptografi dapat diaplikasikan pada sistem uang elektronik untuk melindungi data nilai uang yang dikelola oleh sistem uang elektronik tersebut. Bahasan ini termasuk pada bidang keilmuan yang berkaitan dengan kriptografi pada bidang finansial. Bidang keilmuan ini disebut dengan *financial cryptography* [10].

2 Sistem Uang Elektronik

Sistem uang memiliki sejarah yang panjang [5], dan masing-masing sistem tersebut memiliki kelemahan serta kekurangan sehingga akhirnya sistem uang berikutnya muncul. Sebagian kelemahan sistem-sistem uang tersebut yang berada pada aspek keamanannya dapat juga berlaku pada sistem uang elektronik. Berikut ini adalah tahap-tahap sistem uang yang telah berkembang, beserta kelemahannya yang dapat berlaku juga pada sistem uang elektronik:

1. Tahap sebelum barter

   Pada masa ini masyarakat belum mengenal pertukaran karena setiap orang berusaha memenuhi kebutuhannnya dengan usaha sendiri. Apa yang diperolehnya itulah yang dimanfaatkan untuk memenuhi kebutuhannya.

   Pada masa ini tidak ada resiko keamanan yang berkaitan dengan alat pembayaran, karena tidak dikenal sama sekali pertukaran apapun. Resiko yang ada hanyalah resiko pencurian dan kehilangan barang yang sudah dipunyai. Kelemahan utama masa ini adalah keharusan setiap orang untuk memproduksi kebutuhan yang dibutuhkannya.

2. Tahap barter

   Tahap ini ditandai dengan sadarnya manusia akan tidak mungkinnya memproduksi sendiri seluruh kebutuhan untuk hidup. Karena itu, untuk memperoleh barang-barang yang tidak dapat dihasilkan sendiri, mereka mencari orang yang mau mempertukarkan barang yang dimilikinya dengan barang lain yang dibutuhkannya. Sistem barang ditukar dengan barang inilah yang disebut dengan barter.

   Sistem barter memiliki dua kelemahan utama, yaitu:

   1. Sulitnya menemukan orang yang mempunyai barang yang diinginkan dan juga mau menukarkan barang yang dimilikinya.
   2. Sulitnya memperoleh barang yang nilainya sama atau seimbang agar dapat dipertukarkan dengan barang lain

3. Tahap uang barang

   Kesulitan pada sistem barter mendorong manusia untuk mempermudah pertukaran, dengan menetapkan benda-benda tertentu sebagai alat tukar.

   Benda-benda yang ditetapkan sebagai alat pertukaran adalah benda-benda yang diterima oleh umum. Benda-benda yang dipilih bernilai tinggi (sukar diperoleh atau memiliki nilai magis dan mistik), atau benda-benda yang merupakan kebutuhan primer sehari-hari, misalnya garam yang digunakan oleh orang Romawi digunakan sebagai alat tukar.

   Meskipun alat tukar sudah ada, kesulitan dalam pertukaran tetap ada. Kesulitan-kesulitan itu antara lain sebagai berikut.

   1. Nilai yang dipertukarkan belum mempunyai pecahan
   2. Banyak jenis uang barang yang beredar, masing-masing hanya berlaku pada daerah yang sempit
   3. Sulit melakukan penyimpanan serta pengangkutan uang barang
   4. Mudah hancur atau tidak tahan lama

4. Tahap uang logam

   Pada tahap ini, logam dipilih sebagai bahan uang, menggantikan benda-benda tertentu pada tahap uang benda, karena logam memiliki sifat:

   1. Digemari umum
   2. Tahan lama dan tidak mudah rusak

3. Memiliki nilai tinggi

4. Mudah dipindah-pindahkan

5. Mudah dipecah-pecah dengan tidak mengurangi nilainya

Gambar 1. Satu Denarius, koin perak standar Romawi

Logam yang banyak dipakai karena paling memenuhi sifat-sifat tersebut adalah emas dan perak. Uang terbuat dari emas dan perak disebut dengan **uang logam**. Uang logam emas dan perak juga disebut sebagai Uang penuh (*full bodied money*), artinya nilai intrinsik (nilai bahan uang) sama dengan nilai nominalnya (nilai yang tercantum pada mata uang tersebut). Pada saat itu, setiap orang menempa uang, melebur, menjual, dan memakainya dan setiap orang mempunyai hak tidak terbatas dalam menyimpan uang logam.

Pada sistem uang logam emas dan perak ini, masalah keamanan utamanya adalah pengurangan berat uang logam emas dan perak. Dengan alat ukur yang ada pada saat itu, berat logam tidak dapat diukur secara presisi seperti sekarang. Hal inilah yang mendorong penemuan pengukuran berat yang cukup akurat oleh Archimides.

5. Tahap uang kertas

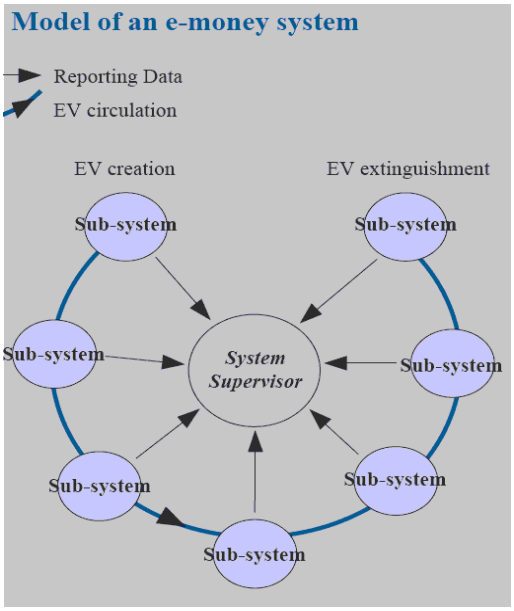
Sejalan dengan perkembangan perekonomian, maka perkembangan tukar-menukar yang harus dilayani dengan uang logam juga berkembang, sedangkan jumlah logam mulia (emas dan perak) terbatas. Penggunaan uang logam juga sulit dilakukan untuk transaksi dalam jumlah besar (sulit dalam pengangkutan dan penyimpanan). Sehingga lahirlah uang kertas.

Uang kertas mempunyai sebuah kelemahan keamanan yang cukup besar, yaitu masalah pemalsuan uang. Masalah ini disebabkan oleh sifatnya yang merupakan uang tanda, yaitu uang yang nilai nominalnya lebih besar dari nilai intrinsik uang tersebut. Untuk mencegah terjadinya pemalsuan, maka untuk mencetak uang kertas dipakailah teknik-teknik tertentu agar susah untuk ditiru, diantaranya dengan membubuhkan tanda air, menyelipkan benang pengaman, mencetak sebagian bagian uang dengan tinta timbul, dengan tinta yang bersinar di bawah sinar ultraviolet.

Sistem uang elektronik menyimpan nilai uang dalam bentuk bit-bit data. Uang tersebut menempati posisi yang sama dengan uang kertas, yaitu sebagai alat ganti pembayaran yang berupa uang tanda (nilai nominal lebih besar dari nilai intrinsik). Sistem uang elektronik harus dapat memenuhi fungsi yang sama dengan fungsi uang konvensional, yang telah dibahas pada bagian pendahuluan.

Sistem uang elektronik, seperti sistem-sistem uang lainnya juga memiliki kelemahan dari sisi keamanannya. Motif utama penyerangan terhadap sistem uang elektronik adalah motif finansial. Dengan melakukan penyerangan terhadap sistem uang elektronik, seorang penyerang dapat dengan mudah memperoleh uang. Motif lainnya, selain motif finansial, seorang penyerang mungkin menyerang sistem uang elektronik dengan tujuan mengganggu sistem tersebut.

Sebelum membahas resiko-resiko apa saja yang terdapat pada sistem uang elektronik, model umum dari sistem uang elektronik perlu dideskripsikan terlebih dahulu.



Gambar 2. Model sebuah sistem *e-money* [4]

Gambar 2 Menggambarkan model umum sebuah sistem uang elektronik. Sebuah sistem elektronik terdiri atas subsistem-subsistem. Terdapat dua subsistem khusus, yaitu subsistem *EV Creation* (pembuatan *electronic value* / nilai uang elektronik) dan susbistem *EV Extinguishment* (penghancuran *electronic value* / nilai uang elektronik). Nilai uang bergerak dari subsistem *EV Creation*, melalui subsistem-subsistem lainnya, dan akhirnya berakhir pada *EV Extinguishment*. Pada pergerakan nilai uang antara subsistem satu ke subsistem lainnya, setiap subsistem yang terkait mengirimkan laporan ke *System Supervisor* (supervisor sistem). Supervisor sistem dapat mengatur jalannya subsistem-subsistem tersebut.

Sistem uang elektronik dapat dibagi menjadi dua kubu besar, yang masing-masing memiliki karakteristik yang berbeda, yaitu [2] [4]:

1. *Stored-value / card-based*

   Jenis sistem uang elektronik *stored value* (sering juga disebut sistem uang elektronik berbasis kartu atau *card-based e-money*) ini umumnya merupakan sistem pembayaran prabayar, dengan nilai uang yang dipunyai oleh pengguna disimpan pada sebuah alat elektronik yang dipegang oleh pengguna, misalnya pada *smart card*, *RFID card* atau teknologi lainnya. Nilai uang yang tersimpan ditambah atau dikurangi ketika pengguna memakai alat tersebut untuk melakukan pembayaran atau transaksi lain.

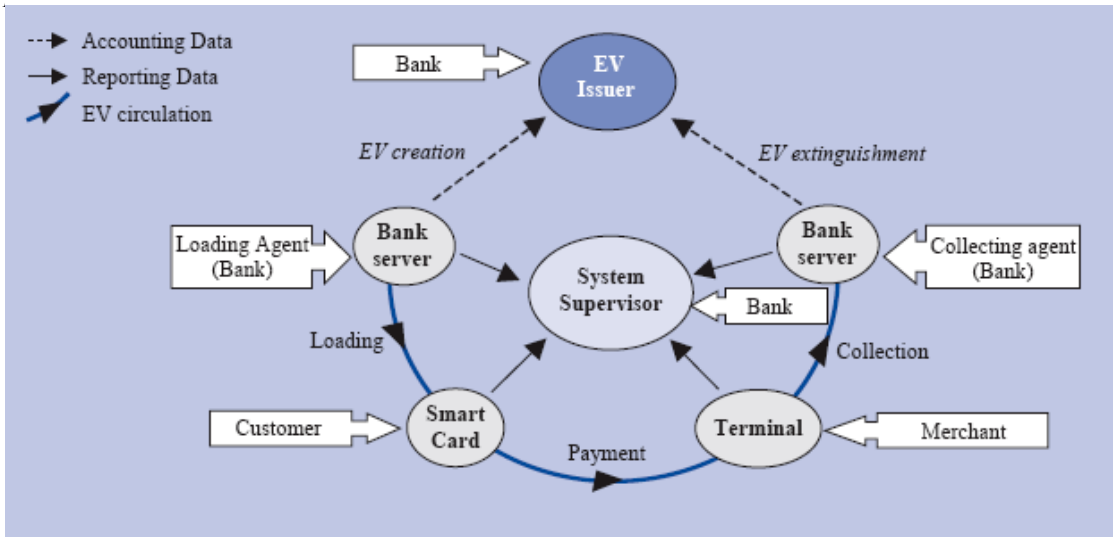
   Mengikuti model umum pada Gambar 3, sistem uang elektronik *stored value* dapat dimodelkan seperti pada Gambar 3. Subsistem yang ada pada sistem jenis ini biasanya mengandung empat fungsi, yaitu *loading agent,* pengguna (*customer*), penjual (*merchant*) dan *collecting agent*.

   Loading dan *collecting agent* biasanya berupa bank. *Loading agent* melakukan konversi dari nilai uang pada bentuk lain menjadi nilai uang elektronik pada sistem uang elektronik ini. *Collecting agent* bekerja sebaliknya, melakukan konversi dari uang pada sistem uang elektronik menjadi nilai uang dalam bentuk lain (misalnya uang kertas)

2. *Access / server-based*

   Pada sistem uang elektronik yang termasuk jenis *access* (sering juga disebut sistem uang elektronik berbasis server / *server-based electronic money system*) ini, nilai uang disimpan di basis data yang ada pada server. Pada setiap transaksi, server akan dihubungi, dan nilai uang yang tersimpan dalam basis data server akan dimodifikasi berdasarkan transaksi yang berlangsung.

   Sistem uang elektronik *access* dapat dimodelkan mengikuti model umum pada Gambar 2. Model tersebut dapat dilihat pada Gambar 4. Perbedaan antara jenis sistem uang *server-based* ini dengan sistem uang *card-based* dapat dengan jelas terlihat jika kita membandingkan antara model *server-based* pada Gambar 4 dengan model *card-based* pada Gambar 3. Pada *card-based*, pengguna dan penjual tidak menyimpan nilai uang elektronik. Nilai uang elektronik disimpan pada akun pengguna dan penjual pada basis data di server, yang diakses melalui jaringan komputer (misalnya melalui internet). Pada Gambar 4, akun tersebut digambarkan sebagai bulatan *Wallet*.



Gambar 3: Model sistem uang elektronik *stored value*

Kedua model dua jenis sistem uang elektronik ini akan menjadi acuan kebutuhan keamanan data serta teknik kriptografi pada bagian selanjutnya dari makalah ini.

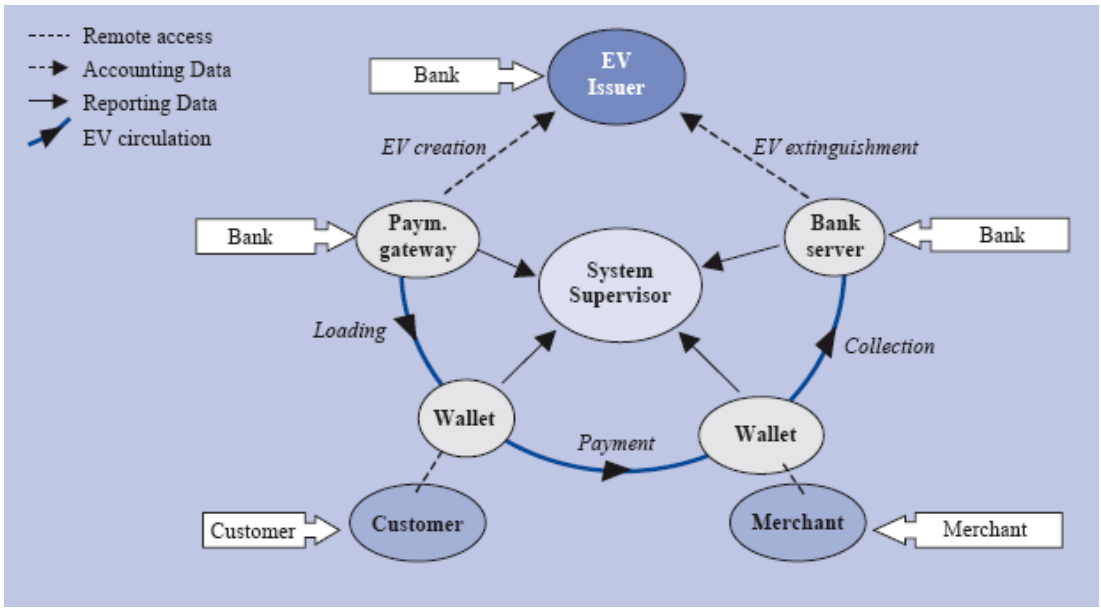
Proses perpindahan nilai uang dari satu subsistem ke subsistem lainnya disebut sebagai transaksi. Tabel 1 berisi transaksi-transaksi yang umum ditangani oleh suatu sistem uang elektronik. Transaksi terdiri atas operasi-operasi dasar berikut ini:

- Inisialisasi
- Pendebetan nilai uang elektronik
- Pengkreditan nilai uang elektronik
- Penutupan

Kompleksitas sistem sangat dipengaruhi oleh bagaimana setiap transaksi tersebut dijalankan.

Perbedaan Antar Sistem Uang Elektronik

Walaupun sistem uang elektronik yang ada mempunyai sifat-sifat umum, terdapat beberapa perbedaan besar terkait dengan desain dan implementasi sistem uang elektronik. Perbedaan desain dan implementasi, infrastuktur produk sistem uang elektronik, serta penanganan transaksi dapat mempengaruhi teknik kriptografi yang dapat dipakai. Karakteristik ini akan mempengaruhi seluruh rancangan sistem. Misalnya, dengan karakteristik nilai uang yang berbeda, proses transaksi *Loading* dapat sangat berbeda antara



Gambar 4. Model sistem uang elektronik jenis *access*

sistem uang elektronik berbasis kartu yang nilai uangnya hanya disimpan di kartu sebagai dompet elektronik (Lihat Gambar 5) dengan sistem yang mengaitkan nilai uang yang disimpan pada kartu sebagai dompet elektronik dengan akun yang disimpan pada server (Lihat Gambar 6). Perbedaan-perbadaan besar tersebut adalah sebagai berikut [2][3][4]:

Tabel 1. Transaksi pada sistem uang elektronik

Tipe Transaksi	Deskripsi Singkat
Loading	Memasukkan nilai uang elektronik ke dalam suatu *device* tertentu
Payment	Melakukan pembayaran untuk barang atau jasa dengan nilai uang yang tersimpan
Refund	Mengeluarkan seluruh nilai uang elektronik yang ada pada *device*
Cancellation of Payment	Melakukan pembatalan pembayaran suatu barang atau jasa
Collection	Mengeluarkan nilai uang elektronik yang didapatkan dari pembayran barang atau jasa

1. Desain dan Implementasi

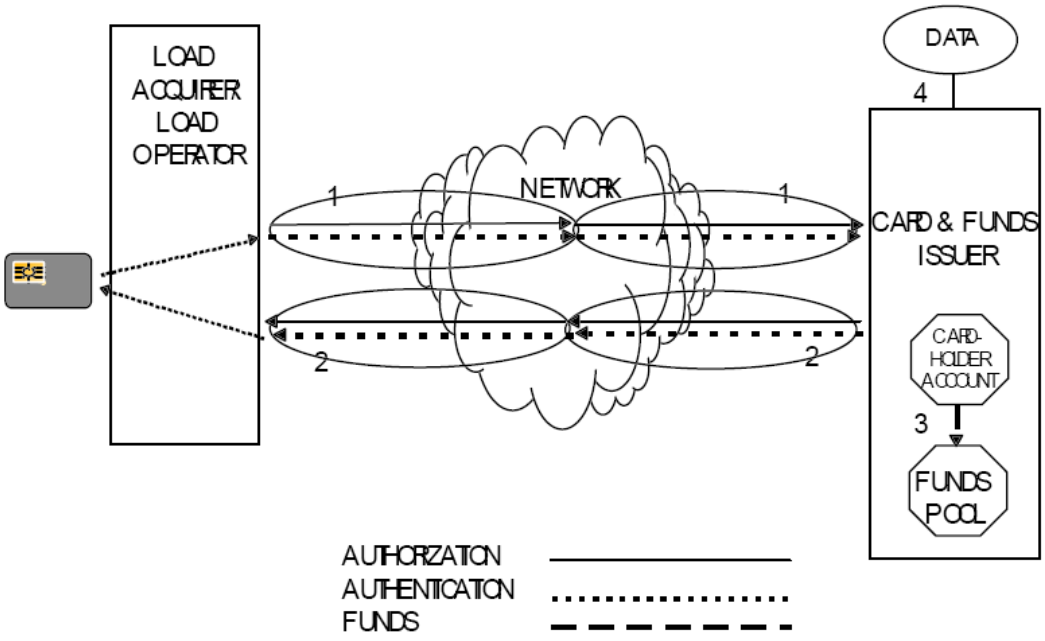
Bagian ini mencakup perbedaan-perbedaan yang cukup berpengaruh pada desain dan implementasi suatu sistem uang elektronik.

1. Kerangka penyimpanan dan transfer nilai uang

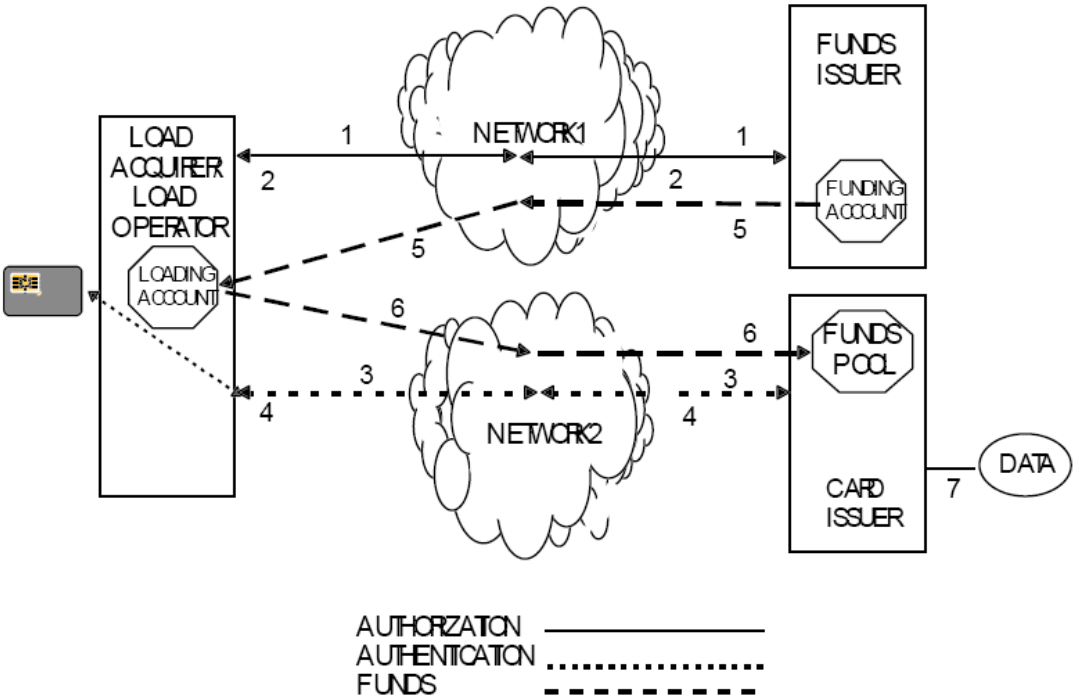
   Karakteristik-karakteristik di bawah ini merupakan karakteristik yang membentuk struktur fundamental dari sistem uang elektronik, dan mempengaruhi desain keamanan keseluruhan sistem.

   1. Representasi teknis nilai uang

      Nilai uang dapat disimpan dengan berbagai macam cara. Cara yang pertama adalah, nilai uang disimpan dan dimanipulasi sebagai nilai akun numerik, dengan transaksi yang dilakukan menjadi debet dan kredit terhadapnya. Alternatif lain adalah dengan menyimpan nilai uang sebagai token-token (kadang disebut koin, *notes*) elektronik yang memiliki nomor seri unik dan berasosiasi dengan nilai uang yang tetap, tidak dapat diubah.Pada model ini, transaksi dilakukan dengan melakukan pemindahan token tersebut.



Gambar 5. Transaksi Loading dengan nilai uang pada kartu [14]



Gambar 6. Transaksi Loading dengan nilai uang pada kartu terkait dengan akun [14]

Pendekatan ketiga adalah *hybrid* dari kedua pendekatan sebelumnya.

2. Transferability

Tingkat *transferability* pada implementasi sistem uang elektronik sangat berlainan, tergangung pada sistem uang yang bersangkutan.

2. Fitur implementasi

Berdasarkan kerangka penyimpanan dan transfer nilai uang, berikut ini karakteristik yang mendefinisikan satu atau lebih fitur utama dari sistem uang elektronik:

1. *Card-based* atau *server-based*

Hampir semua kasus dapat dipecahkan oleh keduanya. Sehingga, pemilihan antara kedua jenis sistem uang elektronik ini sepenuhnya tergantung pada yang melakukan perancangan serta implementasi sistem uang elektronik.

2. Struktur *EV issuer* (penerbit nilai uang elektronik)

Perbedaan struktur *issuer* (jumlah dan tipe *issuer*) mempengaruhi implementasi teknis dari sistem. Sistem dengan hanya satu *issuer* tidak harus berurusan dengan interbank settlement, dan macam-macam hal lainnya. Pada sistem dengan banyak *issuer,* diperlukan cara untuk mengidentifikasi *issuer.*

3. Online authorisation

Sebagian sistem uang elektronik yang bekerja secara online (tersambung dengan server pusat) dapat melakukan otorisasi dengan melakukan pengecekan ke server.

3. Fitur tambahan

Karakteristik berikut ini adalah fitur tambahan, yang mungkin opsional pada suatu sistem uang elektronik, tetapi berpengaruh terhadap desain keamanan sistem uang elektronik secara keseluruhan.

1. Koleksi informasi

   Setiap transaksi yang terjadi pada sistem uang elektronik menghasilkan informasi, yaitu informasi finansial dan informasi yang terkait dengan keamanan. Informasi-informasi ini dapat disimpan, secara permanen atau temporer, pada setiap alat (*device*) yang ada, termasuk alat yang dibawa pelanggan, terminal untuk penjual, atau pada server di pusat. Jumlah, pembuatan serta waktu dari penyimpanan koleksi informasi bergantung pada struktur finansial dari sistem uang elektronik tersebut, biaya menyimpan informasi. Jika terjadi masalah, misalnya terjadi penyerangan terhadap sistem uang elektronik, koleksi informasi ini dapat berguna untuk misalnya, melacak letak penyerang.

2. Kemampuan reload / isi ulang.

   Kemampuan isi ulang dapat bervariasi, dari segi cara dan metoda isi ulang.

3. Satu / lebih mata uang

   Sebagian besar sistem uang elektronik menyimpan nominal uang elektroniknya dalam besaran mata uang lokal. Tetapi tidak menutup kemungkinan suatu sistem uang elektronik mampu melakukan pertukaran uang menjadi besaran uang asing.

2. Infrastruktur produk

   Proses pengembangan dan implementasi infrastruktur dari sistem uang elektronik dapat membuat kelemahan *security*. Berikut ini adalah hal-hal yang memiliki pengaruh besar pada proses pengembangan dan implementasi infrastruktur sistem uang elektronik:

   1. Pengembangan dan produksi

      Untuk produk sistem uang elektronik yang berbasis karu (*card based electronic money system*), alat-alat yang dipakai harus didesain, diuji, diproduksi dan dipersiapkan sebelum dapat dipakai. Kartu diproduksi berdasarkan standar kartu internasional, operating system pada chip kartu juga diproduksi oleh produsen kartu. Aplikasi sistem uang elektronik dapat didesain oleh developer lain.

      Selama pembuatan kartu, aplikasi dan sistem operasi kartu diset secara fisik pada chip kartu. Setelah dilakukan pengetesan terhadap kartu, inisialisasi dilakukan dengan membubuhkan nomor seri dan kunci-kunci kriptografi.

      Untuk produk sistem uang elektronik yang berbasis server, perangkat lunak yang mendukungnya harus didesain, diimplementasikan dan kemudian diuji.

   2. Distribusi

      Pada sistem yang berbasis kartu, kartu dapat didistribusikan ke pelanggan melalui berbagai macam jalur distribusi.

   3. Operasi sistem dan jaringan

      Sistem uang elektronik dapat memiliki satu atau lebih sistem komputer dan basis data sentral yang menyediakan fungsi seperti pengaturan kunci kriptografi, kliring, dan pengawasan data dari resiko kejahatan.

      Untuk komunikasi, seperti pada transaksi yang online atau transaksi *collection* yang dilakukan oleh penjual, banyak sekali metode yang dapat digunakan. Beberapa produk memakai koneksi telepon standar, atau jaringan komputer yang terbuka, seperti Internet sebagai media komunikasi antara pelanggan, penjual, *issuer*, dan *acquirer*.

3. Pemrosesan transaksi

   Transaksi pada sistem uang elektronik dilakukan dengan melakukan pertukaran

pesan-pesan elektronik dengan suatu protokol tertentu. Pesan tersebut dapat ditransmisikan melalui kontak elektrik langsung, seperti antara *smart card* dengan *smart card reader*, atau melalui transmisi nirkabel, ataupun melalui jalur-jalur telekomunikasi seperti Internet.

1. Pengisian (*Loading*)

2. Pembelian atau pembayaran lain (*Payment*)

3. Deposit, c*ollection,* dan kliring

Berikut ini adalah resiko-resiko penyerangan terhadap sistem uang elektronik:

1. Duplikasi alat / *device*

   Penyerangan terhadap sistem uang elektronik dapat berupa pembuatan alat baru yang dapat bekerja seolah-olah alat tersebut asli, sehingga dapat diterima oleh alat-alat yang sudah ada. Misalnya pada sistem uang elektronik yang berbasis kartu, penyerangan dapat dilakukan dengan cara memalsukan kartu, dengan membuat kartu baru yang dapat bekerja seperti kartu asli, tetapi menyimpan nilai nominal uang elektronik yang tidak benar (tanpa melakukan transaksi pengisian kartu dan membayar kepada *issuer* sistem uang elektronik).

2. Pengubahan atau duplikasi data atau perangkat lunak

   Tujuan penyerangan dapat berupa pengubahan data yang disimpan pada alat uang elektronik yang asli. Misalnya, penambahan dilakukan terhadap jumlah nominal uang yang tersimpan pada alat tersebut (misalnya alatnya adalah kartu yang dipegang oleh pengguna), tanpa merusak kartu tersebut, sehingga pemilik kartu tersebut dapat melakukan transaksi dengan kartu yang tampak asli bagi terminal (Lihat Gambar 3 sebagai referensi model sistem uang elektronik berbasis kartu). Modifikasi lain misalnya dengan mengubah fungsi internal yang ditanam pada kartu, sehingga misalnya pada transaksi pembayaran, nilai uang yang disimpan pada kartu tidak berkurang.

   Pengubahan data dan fungsi pada alat dapat dilakukan dengan mengeksploitasi kelemahan keamanan pada sistem.

3. Pengubahan pesan

   Penyerang dapat mencoba untuk mengganti data atau proses pada suatu alat dengan menyadap saluran komunikasi, dan melakukan manipulasi terhadap pesan-pesan yang melewati saluran komunikasi tersebut.

4. Pencurian

   Cara penyerangan yang paling sederhana adalah dengan mencuri *device* milik pelanggan maupun terminal milik penjual dan menggunakan nilai uang elektronik yang tersimpan di dalamnya secara ilegal.

5. Penyangkalan

   Pada sistem uang elektronik, resiko lain yang cukup besar adalah penyangkalan yang dilakukan oleh pengguna. Pengguna menyangkal telah melakukan suatu transaksi. Keadaan ini dapat menimbulkan kerugian di sisi penjual maupun dari sisi institusi yang mengeluarkan produk sistem uang elektronik ini.

6. Malfungsi

   Sistem uang elektronik dapat terkena dampak dari malfungsi terhadap bagian dari sistem uang elektronik tersebut. Malfungsi dapat diakibatkan oleh gangguan fisik maupun gangguan elektronik terhadap alat-alat yang mendukung sistem uang elektronik tersebut.

3 Kebutuhan Keamanan Data

European Central Bank berdasarkan Common Criteria mendefinisikan 24 tujuan dan kebutuhan keamanan data yang harus dipenuhi

Tabel 2. Contoh pengukuran keamanan untuk sistem uang elektronik

	Prevention	Detection	Containment	Organisational
Creation of transactions	Payment transactions are digitally signed using the key unique to the card. Transactions are authorised online. Devices are mutually authenticated.	Transaction sequence numbers are verified. Shadow-balance accounts are maintained. Unusual payment patterns are detected.		
Alteration of application, operating system software and static data (maximum amount, etc.)	Applications and operating system software are stored in physically protected memory areas (ROM) and are logically protected through scrambling or encryption.	Software checksums show evidence of alteration.		
Alteration of electronic value balance	Balance can only be modified upon the instruction of an authorised device.	Shadow-balance accounts are maintained.		
Alteration of messages				
Modification of messages	Challenge-response mechanisms are used to initiate the transaction. The message exchange is controlled by the transaction protocol and by the use of derived session keys. Message integrity is verified by a hash algorithm or a Message Authentication Code (MAC). Messages are authenticated by MAC or electronic signatures.	Electronic signatures are verified. Transaction sequence numbers are verified. Transaction time-stamps are verified.		

oleh sistem uang elektronik [2]. Kebutuhan keamanan data yang paling prinsip adalah:

1. *Confidentiality*

   Semua hal yang dikelola oleh sistem uang elektronik harus terjaga kerahasiaannya

2. *Integrity*

   Integritas dari data nilai uang elektronik harus terjaga. Misalnya, pada setiap transaksi, jumlah total nilai uang yang didebit dari sebuah susbistem harus sama dengan jumlah uang yang dikredit pada transaksi yang sama.

3. *Authentication*

   Otentikasi dilaksanakan pada setiap transaksi. Masing-masing bagian yang terlibat suatu transaksi harus saling mengotentikasi satu sama lain.

4. *Non-repudiation*

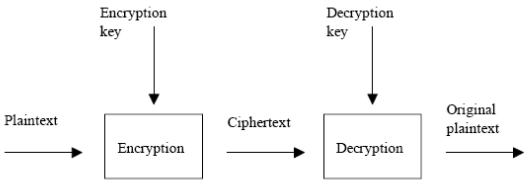
   Sistem uang elektronik harus dapat mencegah terjadinya penyangkalan yang dilakukan oleh pengguna maupun penjual (*merchant*).

Prinsip tersebut dapat berlaku untuk setiap bagian dari sistem uang elektronik, dari ujung ke ujung. Kemudian, untuk mengukur tingkat kemananan suatu sistem uang elektronik, dapat digunakan ukuran seperti pada Tabel 2.

4 Teknik Kriptografi

Pada bagian ini, prinsip-prinsip general dari teknik-teknik kriptografi yang paling penting dibahas. Teknik-teknik yang dibahas meliputi enkripsi dan dekripsi, fungsi hash satu-arah, protokol *challenge-response* dengan bilangan acak, tandatangan digital dan pengelolaan kunci.

Enkripsi dan Dekripsi



Gambar 7. Enkripsi dan Dekripsi

Fungsi enkripsi dan dekripsi dapat membantu untuk mencapai kebutuhan *Confidentiality*. Pengirim dan penerima informasi dapat menggunakan metode eknripsi dan dekripsi tertentu untuk memastikan pesan di antara mereka tidak dapat dibaca oleh orang lain. Proses enkripsi dan dekripsi (lihat Gambar 7) dilakukan dengan menggunakan fungsi matematis yang disebut algoritma, dengan masukan kunci.

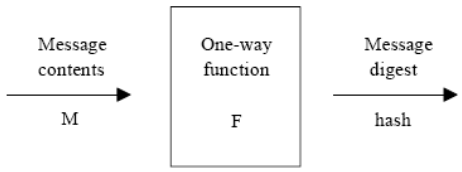
Sebuah algoritma disebut simetris jika kunci untuk enkripsi sama dengan kunci dekripsi. Pemakaian algoritma ini bergantung pada keamanan kunci pada pengirim dan penerima. DES (Data Encryption Standard) merupakan salah satu contoh algoritma simetris.

Jenis lain algoritma adalah algoritma asimetris. Algoritma ini tidak menggunakan kunci yang sama sebagai kunci enkripsi dan kunci dekripsi, tetapi memakai sepasang kunci yang berbeda tetapi terkait secara matematis. Satu kunci disimpan oleh pembuat pasangan kunci (disebut kunci privat) dan kunci lainnya dipublikasikan (disebut kunci publik). Sebuah pesan yang dienkripsi oleh salah satu kunci hanya dapat dibuka oleh pasangannya, tidak dapat dibuka oleh pasangan kunci lain yang berbeda. RSA (Rivest Shamir Adleman) merupakan salah satu algoritma asimetris yang banyak dipakai.

Algoritma asimetris dapat dipakai juga sebagai cara otentikasi. Jika sebuah pesan dienkripsi dengan menggunakan kunci privat pengirim, maka pesan tersebut hanya dapat didekripsi oleh kunci publik pengirim tersebut. Sehingga, pesan tersebut dapat dipercaya dikirim oleh pengirim tersebut.

Umumnya, algoritma simetris dapat dieksekusi secara lebih cepat daripada algoritma asimetris karena kekompleksan perhitungan matematis yang digunakan pada algoritma asimetris.

Fungsi hash satu-arah

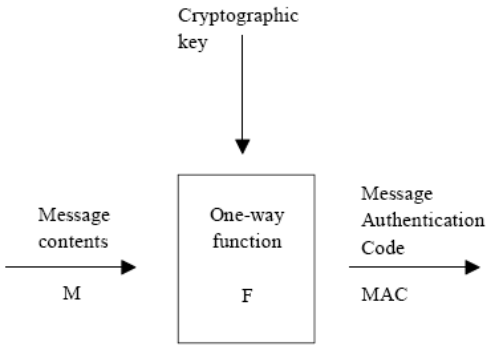


Gambar 8. Fungsi hash satu-arah

Fungsi hash satu-arah (Lihat Gambar 8) adalah cara bagi penerima untuk dapat mengecek apakah isi dari pesan benar-benar tidak diubah di tengah perjalanan. Pengirim pesan memasukkan pesan ke dalam fungsi hash satu-arah untuk mengasilkan *message digest*. Penerima pesan mengulangi proses ini terhadap pesan yang diterimanya, kemudian membandingkan hasil *message digest* yang didapatkan dengan *message digest* yang dikirimkan juga oleh pengirim.

Karakteristik terpenting pada fungsi hash adalah fungsi ini hanya dapat dihitung satu arah dan tidak dapat dibalikkan. Fungsi hash juga tidak boleh menghasilkan *message digest* yang sama terhadap dua pesan yang berbeda. Fungsi hash yang banyak dipakai diantaranya Message Digest 5 (MD5) dan Secure Hash Algorithm (SHA).

Dengan mengkombinasikan fungsi hash dengan memakai kunci kriptografi, maka orang yang dapat memverifikasi pesan dapat dibatasi. Proses ini adalah proses yang lebih kompleks (Lihat Gambar 9, proses ini digambarkan secara sederhana dari luar sistem). Hasil fungsi tersebut disebut Message Authentication Code (MAC).



Gambar 9. Message Authentication Code (MAC)

Protokol *Challenge-Response*

Protokol ini digunakan untuk memastikan keaslian dua pihak yang berkomunikasi, sehingga dapat melanjutkan komunikasi antara keduanya. Satu pihak akan memastikan keaslian pihak lain dengan cara membuat bilangan acak yang dikirimkan sebagai *challenge* (tantangan) kepada pihak lainnya. Proses yang harus dilakukan oleh pihak yang mendapatkan *challenge* telah disepakati sebelumnya, termasuk penyertaan kunci privat. Untuk dapat menghasilkan *response* (jawaban) yang sesuai, pihak lain tersebut harus mengetahui langkah proses dan mempunyai kunci privat yang sesuai. Dengan begitu, pihak yang melakukan *challenge* dapat mengasumsikan pihak lainnya asli jika hasil yang didapatkan sesuai/cocok.

Pemakaian bilangan acak digunakan untuk mempersulit penyerang sehingga penyerang tidak dapat mempergunakan pasangan *challenge* dan *response* yang sudah pernah dipakai pada masa lalu untuk memperdaya protokol *challenge-response* ini.

Tandatangan Digital

Tandatangan digital adalah sebuah string data yang dapat memastikan keaslian pengirim dan isi dari pesan. Algoritma kunci publik digunakan untuk mengenkripsi sebagian dari pesan atau *message digest* dari pesan. Setiap penerima yang memiliki kunci publik dari pengirim dapat mendekripsinya dan memastikan identitas pengirim.

Salah satu penggunaan tandatangan digital adalah dengan membuat masing-masing pihak menandatangan pesan yang dikirimkannya, sehingga dapat mencegah penyangkalan pengiriman pesan oleh salah satu pihak.

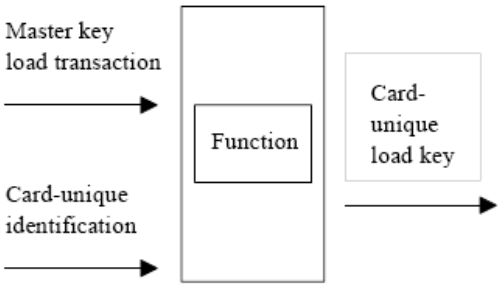
Teknik-teknik serta algoritma tandatangan digital bermacam-maca, diantaranya memakai teori matematika mengenai pemfaktoran, ataupun masalah logaritma diskret [11].

Manajemen Kunci

Sistem uang elektronik yang memakai kriptografi kunci simetris dalam melakukan enkripsi, dekripsi dan otentikasi lemah terhadap penyerang. Penyerang hanya perlu mencari tahu kunci tunggal tersebut untuk dapat memanipulasi aspek manapun dari

sistem. Karena itu, perancang sistem harus mengikuti prinsip manajemen kunci.

Prinsip dari manajemen kunci adalah sebuah kunci kriptografi hanya ditujukan untuk sebuah fungsi pula. Sebuah transaksi load dilindungi oleh sebuah kunci load yang khusus, transaksi pembelian dilindungi oleh kunci yang lain, dsb. Lebih jauh lagi, kunci harus unik untuk setiap kartu ataupun terminal pembayaran (dalam kasus *card-based*), sehingga kartu ataupun terminal yang tertembus oleh penyerang hanya akan berdampak pada level terminal tersebut saja. Kunci spesifik tersebut dibuat menggunakan proses yang disebut dengan penurunan kunci (*key derivation*), seperti pada Gambar 10. Proses ini biasanya dilakukan pada proses pembuatan kartu dan dapat dilakukan untuk semua kunci yang spesifik kartu (kunci load kartu, kunci pembelian kartu, dsb.



Gambar 10. Key Derivation

Penerapan Kriptografi Dalam Sistem Uang Elektronik

Untuk mengaplikasikan kriptografi dalam mengimplementasikan sebuah sistem uang elektronik yang aman bukan hanya memerlukan pertimbangan algoritma yang akan dipakai tetapi juga pertimbangan yang berkaitan dengan manajemen kunci dan penyimpanan kunci. Walaupun topik-topik tersebut didekripsikan terpisah pada pembahasan di atas, tetapi topik tersebut sangat terkait satu sama lain

Pemakaian Algoritma dan Fungsi

Prinsip kriptografi dan dasar-dasar pembangun kriptografi yang dijelaskan pada bagian sebelumnya dapat digunakan untuk mencapai tujuan keamanan seperti *confidentiality*, *integrity, authentication*, serta *non repudiation*.

Confidentiality dapat didapatkan secara mudah dengan menggunakan DES sebagai metoda enkripsi. Walaupun dengan menggunakan algoritma asimetris hasil yang sama juga dapat didapatkan, tetapi karena algoritma asimetris memerlukan proses yang lebih intensif, maka algoritma simetris lebih didahulukan.

Beberapa pemerintah negara di dunia membatasi penggunaan algoritma-algoritma kriptografi, bahkan juga membatasi ekspor algoritma tersebut (dalam bentuk perangkat keras maupun perangkat lunak) ke negara lain. Hal ini dilakukan agar tidak ada yang menyalahgunakan algoritma kriptografi tersebut untuk tujuan buruk. Oleh karena itu, untuk mengimplementasikan algori-tma-algoritma kriptografi tertentu, masalah legal harus juga diperhitungkan.

Masalah lain yang harus diperhitungkan adalah keterbatasan kemampuan prosesin subsistem. Misalnya pada sistem uang elektronik yang berbasiskan kartu, jika kartu yang dipakai tidak mendukung pemrosesan yang memakan resource banyak, dan dalam kartu tersebut tidak disertakan modul enkripsi yang dibutuhkan, maka pemilihan algoritma kriptografi juga harus disesuaikan dengan kemampuan kartu tersebut.

Untuk mencapai kebutuhan keamanan yaitu integritas data, dan otentikasi (termasuk nirpenyangkalan / *non-repudiation*), DES, triple-DES dan algoritma kunci publik seperti RSA dapat digunakan, dengan digabungkan dengan protkol *challenge-response*, konsep MAC dan digital signature.

David Chaum menemukan sebuah skema penandatanganan, yang disebut sebagai *blind signature* (tandatangan buta) yang banyak dipakai pada aplikasi sistem uang elektronik. Keterangan lebih lanjut mengenai *blind signature* dapat dilihat di [13].

Algoritma-algoritma dan teknik-teknik tersebut dapat diaplikasikan tidak hanya pada komunikasi tetapi juga pada penyimpanan data. Misalnya pada sistem yang menyimpan data pada basis data server, data disimpan dengan terenkripsi pada media penyimpanannya. Juga pada kartu, data yang penting disimpan dalam bentuk terenkripsi.

Pengelolaan Kunci

Pengelolaan kunci sangat bergantung pada pengalaman desainer sistem uang elektronik.

Prinsip pengelolaan kunci yang baik berdasar pada pembuatan tambahan penghalang bagi penyerang sistem uang elektronik. Dengan adanya penghalang tambahan tersebut, diharapkan penyerang dapat tidak berhasil menyerang atau setidaknya memperlambat penyerangan-nya sehingga dapat digagalkan.

Halangan yang dapat ditambahkan misalnya dengan melakukan penggantian kunci secara berkala, misalnya satu minggu sekali. Semua kunci yang berkaitan dengan kriptografi diganti. Sehingga, penyerang yang menyerang dengan menggunakan brute-force attack tidak dapat menyelesaikan serangannya.

Kesimpulan

Untuk mendukung sistem uang elektronik, yang menyimpan nilai uang yang ada padanya dalam bentuk bit-bit data, dibutuhkan keamanan data yang kuat. Dari sisi teknologi, keamanan data tersebut dapat didukung oleh kemajuan yang didapat pada bidang kriptografi. Kriptografi dapat diaplikasikan untuk melindungi data uang elektronik dari *creation* sampai *extinguishment*.

Daftar Referensi

[1] R. Munir. “Bahan Kuliah IF5054 Kriptografi”. Departemen Teknik Informatika. Institut Teknologi Bandung. 2004

[2] European Central Bank. ”Electronic Money System Security Objectives According to The Common Criteria Methodology”. European Central Bank, Germany. 2003.

[3] Poirier, S. ”Principles for a free, powerful and stable monetary system for the digital era”. http://spoirier.lautre.net/money.htm Diakses: Desember 2006

[4] Bank for International Settlements. (1996). ”Security of Electronic Money”. http://www.bis.org/publ/cpss18.pdf Diakses: Desember 2006

[5] Davies, Glyn. “History of Money from Ancient Times to the Present Day”. http://www.exeter.ac.uk/~RDavies/arian/llyfr.html Diakses: Desember 2006

[6] Website Sharing Vision. http://www.sharingvision.biz/ Diakses: Desember 2006

[7] Wikipedia Indonesia. “Uang”. http://id.wikipedia.org/wiki/Uang Diakses: Desember 2006

[8] Oxford University. “Pocket Oxford Dictionary”. Oxford University Press. 1994.

[9] Sheptun, Alla. “Philosophy Of Money”. http://www.bu.edu/wcp/Papers/Econ/EconShep.htm Diakses: Desember 2006

[10] Website International Financial Cryptography Association http://www.ifca.ai/ Diakses: Desember 2006

[11] Schneier, B. “Applied Cryptography”. New York, 1996.

[12] Website ContactlessNews, “Contactless News: Technology, Smart Cards, Readers, Programmers, Government, and Software” http://www.contactlessnews.com/ Diakses: Desember 2006

[13] European patent application on "Electronic voting process using fair blind signatures", http://ep.espacenet.com/details/bibliographicData?NR=1721408&CC=EP&KC=A2&DB=ep.espacenet.com&locale=en_EP Diakses: Desember 2006

[14] CEPSCO, “Common Electronic Purse Specification”, CEPSCO, 2000.