Aplikasi Kriptografi pada *Smart Card* di Indonesia

Riffa Rufaida / 13507007[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]riffa.rufaida@gmail.com

***Abstract*— Pemanfaatan kriptografi dalam kartu cerdas di Malaysia dapat mengurangi permasalahan yang terjadi pada jalur tol, dan juga dapat diaplikasikan pada aspek-aspek kehidupan lain dan memberi manfaat. Hal ini dapat dimanfaatkan oleh Indonesia untuk mengurasi masalah yang sama dan mendapatkan manfaatnya melalui kriptografi pada *smart card*.**

***Index Terms*— Cryptography, Smart card, Touch 'n Go**

I. PENDAHULUAN

Dalam kehidupan sehari-hari, tanpa disadari kita banyak bersentuhan dengan kriptografi. Salah satu aplikasi dari kriptografi yang banyak bersentuhan dalam kehidupan kita adalah kartu cerdas atau *smart card.* Sebuah kartu cerdas menyimpan kunci privat, sertifikat digital, dan informasi lainnya, selain itu juga menyimpan nomor kartu kredit dan informasi kontak personal. Sertifikat digital ditandatangani oleh CA (*Card Issuer*) untuk mensertifikasi kunci publik pemilik kartu.

Komputer server mengotentikasi kartu dengan cara mengirimkan nilai yang dikirim ke kartu. Kartu akan menandatangani string dengan kunci privat yang kemudian tanda tangan tersebut diverifikasi oleh mesin dengan kunci publik pemiliki kartu. Komputer server perlu menyimpan kunci publik CA (*Card Issuer*) untuk memvalidasi sertifikat digital.

Kartu cerdas ini dapat dimanfaatkan untuk beragam kepentingan, salah satunya jika kita berkaca ke negara tetangga, kartu cerdas **Touch 'n Go** dimanfaatkan sebagai sarana pembayaran tol secara elektronik. Mengingat kebutuhan akan jalur tol yang bebas hambatan, penggunaan kartu ini dapat mengurangi antrian yang terjadi pada loket pembayaran tol. Pada perkembangan selanjutnya, kartu cerdas ini juga dapat dikembangkan sebagai dompet elektronik dan menjadi alat pembayaran di banyak tempat. Hal yang telah dimanfaatkan di Malaysia ini dapat dikembangkan di Indonesia dengan terlebih dahulu menilai keamanan data dan informasi, cara kerja, dan diakhiri dengan usulan seperti apa kartu cerdas yang dapat diaplikasikan di Indonesia dengan berkaca pada Malaysia.

I.1 Kriptografi

Manusia dalam kehidupannya melakukan komunikasi satu sama lain. Secara umum, komunikasi berarti interaksi antara pengirim serta penerima yang melibatkan pesan yang disampaikan antara dua pihak tersebut.

Pesan sendiri memiliki makna yaitu data atau informasi yang dapat dibaca dan dimengerti maknanya. Pesan memiliki nama lain yaitu plainteks (*plaintext*) atau teks-jelas (*clearteks*). Pesan yang dipertukarkan dapat berupa teks, gambar, music, video, tabel, maupun beragam bentuk lainnya. Penyampaian pesan pun memiliki berbagai macam metode.

Isi pesan dapat memiliki berbagai tingkatan kepentingan sehingga muncul keadaan pengirim menginginkan pesan dapat dikirim secara aman, yaitu pihak lain tidak dapat membaca ataupun memanipulasi pesan. Hal ini diselesaikan dengan solusi berupa cipherteks (*ciphertext*) atau kriptogram (*cryptogram*), yang berarti pesan yang telah disandikan sehingga tidak bermakna lagi. Cipherteks menjadi solusi karena bertujuan agar pesan tidak dapat dibaca oleh pihak yang tidak berhak dan pada akhirnya dapat dikembalikan bentuknya menjadi plainteks semula.

Proses pembuatan cipherteks dari sebuah plainteks disebut dengan enkripsi, sedangkan proses sebaliknya disebut dengan dekripsi. Proses-proses ini akan mengenakan suatu fungsi yang telah dipilih kepada masing-masing teks untuk dapat menghasilkan teks yang lain.

Definisi kriptografi secara formal menurut Schneier adalah

"*art and science to keep message secure*".

Pada kenyataannya, kehidupan kita saat ini dikelilingi oleh kriptografi, dari penggunaan ATM, telepon genggam, komputer, maupun internet. Ini karena pengaplikasian kriptografi pada penggunaan peralatan tersebut.

Peralatan tersebut menggunakan kartu cerdas sebagai alat yang digunakan. Kartu tersebut menyimpan berbagai macam data penting yang privasi dan kerahasiaannya harus terjaga sehingga diperlukan pengaplikasian kriptografi dalam rangka meningkatkan keamanan pada alat tersebut. Oleh karena itu, tanpa disadari kehidupan sehari-hari manusia telah dikelilingi oleh kriptografi.

II. *SMART CARD*

Kartu cerdas, biasanya sebuah tipe dari kartu chip, adalah kartu plastic yang mengandung *embedded* chip

komputer, baik tipe memori ataupun mikroprosesor, yang menyimpan dan melakukan transaksi data. Data pada transaksi ini umumnya diasosiasikan dengan sebuah nilai, informasi, atau keduanya, dan disimpan dan diproses pada chip yang ada di dalam kartu. Data tersebut ditransaksikan melalui sebuah alat pembaca yang merupakan bagian dari sebuah sistem komputer. Sistem yang ditingkatkan dengan kartu cerdas banyak digunakan saat ini dalam aplikasi penting, termasuk pelayanan kesehatan, banking, hiburan, dan transportasi. Semua aplikasi dapat menikmati kelebihan dari fitur tambah serta keamanan yang disediakan oleh kartu cerdas. Pasar saat ini berisi teknologi tradisional oleh kartu yang *machine readable*, misalkan *barcode* dan *magnetic stripe*, mulai beralih ke kartu cerdas karena penghitungan *return on investment* yang dibuktikan oleh pengeluar kartu setiap tahunnya.

Pertama kali kartu cerdas digunakan di Eropa tiga puluh tahun lalu sebagai alat penyimpan nilai telepon untuk menghindari pencuri. Kartu cerdas terus berkembang hingga saat ini manusia menemukan cara pemanfaatan lain, salah satunya sebagai kartu untuk pembelian secara kredit dan untuk merekam data sebagai pengganti kertas.

Di Amerika, konsumen menggunakan kartu chip untuk segala hal, mulai dari mengunjungi perpustakaan hingga membeli sayuran dan menonton film, menjadikan kartu sebagai bagian tak terpisahkan dari hidup. Banyak industry pula yang menanamkan kelebihan dari kartu cerdas sebagai bagian dari produknya, seperti telepon genggam digital GSM dan decoder untuk TV satelit.

Kartu cerdas meningkatkan kenyamanan dan keamanan dari transaksi apapun. Kartu menyimpan identitas pengguna dan akun dalam penyimpanan yang tahan serangan. Sistem kartu cerdas telah terbukti lebih *reliable* dari kartu *machine-readable* lain, misalkan *barcode* atau *magnetic stripe*, melalui banyak penelitian yang menunjukkan peningkatan kemampuan hidup kartu dan alat pembacanya mampu memberikan biaya pengelolaan sistem yang jauh lebih kecil. Kartu cerdas turut menyediakan komponen penting sistem keamanan dalam aspek pertukaran data secara virtual dalam jaringan apapun. Kartu melindungi melawan berbagai macam ancaman keamanan, mulai dari penyimpanan sandi lewat yang tidak hari-hati hingga sistem *hack* yang canggih.

Biaya untuk mengelola reset sandi lewat pada organisasi sangat tinggi sehingga penggunaan kartu cerdas merupakan solusi yang efektif dari sisi biaya untuk lingkungan ini. Kartu multifungsi dapat digunakan pula untuk mengelola akses sistem jaringan dan menyimpan nilai serta data lainnya. Saat ini di seluruh belahan dunia, manusia menggunakan kartu cerdas untuk berbagai aktivitas sehari-hari, seperti :

a. Kartu SIM dan telekomunikasi
b. Program layanan *loyalty* dan penyimpanan nilai
c. Pengamanan konten digital dan asset fisik
d. *E-commerce*
e. Kartu cerdas yang dikeluarkan bank
f. Informasi layanan kesehatan
g. *Embedded medical device control*
h. Keamanan *enterprise* dan jaringan
i. Akses fisik

Dari penggunaan di atas, yang menjadi fokus makalah ini adalah penggunaan kartu cerdas sebagai alat pembayaran terutama transaksi transportasi dan pemanfaatan lainnya. Hal itu termasuk ke dalam fungsi kartu sebagai penyimpan nilai. Kartu cerdas akan berisi nilai yang dapat digunakan untuk melakukan pembayaran dan nilai tersebut akan berkurang dan dapat diisi kembali. Selain menyimpan nilai, kartu akan menyimpan identitas pemilik dan penggunaannya dapat dijadikan sebagai pengganti uang tunai. Kartu juga dapat menyimpan dan digunakan untuk melacak data.

II. 1 **Touch 'n Go** *Smart Card*

Salah satu pengaplikasian kartu cerdas adalah **Touch 'n Go** atau **TnG** *smart card* di negara tetangga, yaitu Malaysia. Kartu ini merupakan kartu cerdas yang digunakan oleh jalan bebas hambatan sebagai sistem pembayaran elektronik. Kartu cerdas ini berukuran sebesar kartu kredit, terbuat dari plastic, dan memiliki teknologi microchip MIFARE dari Philips di dalamnya. Sistem **TnG** didesain untuk memroses hingga 800 kendaraan perjam untuk menghilangkan antrian pada loket tol. Kartu ini jika digunakan dengan alat Smart**TAG** dapat memroses hingga 1.200 kendaraan perjam.

Teknologi ini diluncurkan pada tanggal 18 Maret 1997 di Malaysia dan berisi nilai dengan mata uang Ringgit Malaysia yang dapat diisi. Kartu ini akan tetap aktif selama masih diisi dengan nilai uang atau digunakan minimal satu kali dalam satu tahun.

Kartu cerdas **TnG** memiliki 4 tipe, yaitu :

a. Kartu *Prepaid*
1. Kartu standar
   Penggunaan seperti kartu *top up.*

b. Kartu *Postpaid*
1. Kartu Fleet Xs
   Penggunaan utama untuk pembayaran biaya tol. Detail dari nama perusahaan, nomor registrasi kendaraan, dan kelas kendaraan tertulis pada kartu. Operator dapat memonitor rekaman tol atau pergerakan kendaraan pada jalan tol pada *e-statement* yang tersedia dalam satu hingga dua hari setelah transaksi.
2. Kartu Biz Xs
   Kartu sama dengan kartu standar tetapi penggunaan dikhususkan untuk pengguna korporasi.

c. Kartu *Auto-reload*
1. Kartu Zing
   Kartu standar yang memiliki dihubungkan ke Visa, MasterCard atau American Express yang dikeluarkan oleh bank yang berpartisipasi di Malaysia. Setiap waktu nilai pada kartu berada di bawah RM50, mekanisme pengisian otomatis akan dijalankan dan kartu ditambahkan nilai sebesar RM100. Jumlah ini akan dikenakan ke tagihan kartu kredit beserta biaya RM2 sebagai biaya *auto-reload*.

d. Kartu *Multi-purpose*
1. MyKad

Kartu identitas penduduk Malaysia yang dapat digunakan sebagai dompet elektronik.

Kartu TnG digunakan tidak hanya dalam pembayaran biaya tol, tetapi layanan parker, transportasi umum, taman rekreasi, dan pembayaran tanpa uang tunai pada outlet retail.

Penggunaan kartu ini dimulai dengan pengguna jalan tol menyentuhkan kartu ke alat pembaca pada loket masuk tol, dan menyentuhkannya lagi saat loket keluar. Biaya tol yaitu nilai yang akan dikurangi pada kartu tergantung kepada jarak yang ditempuh. Nilai pada kartu harus bernilai lebih dari RM2 agar sistem dapat berfungsi.

Kartu cerdas memiliki alat ekstensi yaitu SmartTAG atau TAG On Board Unit (OBU) yang membuat pengguna dapat memasukkan kartu ke alat pembaca di dalam kendaraan sehingga tidak perlu memberhentikan kendaraan pada loket tol. Pembayaran dilakukan secara otomatis saat unit TAG membaca kartu TnG.

Pada pelaksanaannya, kartu TnG memiliki kritik yang masuk dari penduduk Malaysia, kritik ini terkait dengan penggunaan kartu, misalkan adanya biaya yang harus dibayarkan pada saat dilakukan pengisian ataupun penggantian kartu.

Meskipun mendapat beberapa kritik dari warganya, penggunaan kartu TnG dengan tujuan menghindari penumpukan pada loket tol dapat dikatakan telah berhasil. Hal ini terbukti dari fakta dari situs TnG bahwa saat ini terdapat lebih dari 7,2 juta pengguna kartu TnG, pengguna MyKad dengan fasilitas TnG sebanyak lebih dari 13 juta pengguna dari penduduk Malaysia sebesar 19 juta penduduk. Pengguna SmartTAG berkisar di angka 1,2 juta orang. Tingkat *throughput* pada jalur TnG di loket tol besarnya 3 kali lebih cepat dari jalur loket pembayaran tunai, sedangkan penggunaan SmartTAG memiliki *throughput* hingga 4 kali lebih cepat dari jalur pembayaran tunai. Rata-rata transaksi yang dilakukan perhari dengan menggunakan kartu TnG adalah lebih dari 2 juta transaksi.

III. ANALISIS

Pada bagian ini akan berisi cara kerja aplikasi kriptografi pada kartu cerdas, penggunaan pada TnG, dan analisis tingkat keamanan data dan informasi yang tersimpan pada chip, serta analisis pemanfaatan kartu cerdas di Indonesia saat ini juga kartu cerdas seperti apa yang cocok untuk diaplikasikan di Indonesia dengan berkaca pada Malaysia.

III. 1 Cara Kerja

III. 1. 1 Cara Kerja *Smart Card*

Kartu cerdas memiliki beragam tipe dan didefinisikan berdasarkan dua hal, yaitu bagaimana data ditulis dan dibaca, serta tipe chip yang ditanamkan pada kartu dan kemampuannya. Pembangunan kartu dibuat dari beberapa lapisan yang terdiri atas materi yang berbeda-beda. Lapisan kartu akan dicetak lalu dilaminasi, dipotong sesuai bentuknya dan kemudian ditanamkan chip, dan dimasukkan data pada kartu.

III. 1. 1. 1 Kartu cerdas *contact*

Ini merupakan jenis kartu cerdas paling umum. Hubungan elektrik berada di luar kartu dan terhubung dengan pembaca kartu saat kartu dimasukkan. Penghubung ini terikat dengan chip pada kartu.

III. 1. 1. 2 Kartu cerdas *contactless*

Kartu cerdas ini menggunakan frekuensi radio (RFID) antara kartu dan alat pembaca tanpa kontak fisik melalui pemasukan kartu. Kartu hanya perlu dilewatkan ke alat pembaca untuk membaca kartu.

III. 1. 1. 3 Sistem Operasi

Dua tipe utama dari sistem operasi kartu cerdas adalah *fixed file structure* serta *dynamic application system.* Tipe pemilihan ini akan bergantung kepada penggunaan kartu cerdas itu sendiri. Perbedaan lain ada pada kemampuan enkripsi dari sistem operasi dan chip. Tipe enkripsi yang ada adalah *symmetric key* dan *asymmetric key*. Algoritma enkripsi telah ditanamkan ke perangkat keras maupun *library* perangkat lunak pada arsitektur chip.

III. 1. 1. 3. 1 *Fixed File Structure OS*

Kartu berlaku sebagai tempat penyimpanan sekaligus sistem komputasi yang aman. File dan hak akses ditentukan terlebih dahulu oleh pihak yang mengeluarkan kartu. Hal tersebut seperti ini ideal untuk tipe kartu yang fungsi maupun strukturnya tidak akan berubah dalam waktu lama. Tipe kartu dengan sistem operasi seperti ini merupakan tipe kartu yang paling umum.

III. 1. 1. 3. 2 *Dynamic Application Card OS*

Tipe ini membuat pengembang mampu membangun, mengetes, dan memiliki aplikasi yang berbeda pada kartu secara aman. Aplikasi dan sistem operasi terpisah sehingga dapat dilakukan *update*. Ini dimiliki pada kartu yang lingkungan dan pengembangannya bersifat dinamik, sebagai contoh yaitu kartu SIM untuk telepon genggam.

III. 1. 1. 4 Pembaca *(Readers)* dan Terminal

Proses mengambil informasi yang ada dalam kartu cerdas maupun proses melakukan transaksi dilakukan dengan *readers* dan terminal. Pembaca (*readers*) terhubung dengan komputer untuk kebutuhan pemrosesan. Terminal merupakan alat pemrosesan yang *self-contained* sehingga tidak perlu dihubungkan dengan komputer. Pembaca dan terminal ini keduanya digunakan untuk membaca maupun menulis ke kartu cerdas.

III. 1. 1. 4. 1 Pembaca (*Readers*)

a. *Contact*
   Pembaca tipe ini membutuhkan koneksi fisik ke kartu dengan cara memasukkan kartu ke dalam pemaca. Tipe ini lebih aman dan transfer data yang lebih cepat. Tipe ini paling umum digunakan pada aplikasi identifikasi dan penyimpanan nilai.
b. *Contactless*
   Pembaca tipe ini bekerja dengan frekunsi radio yang berkomunikasi saat kartu mendekati pembaca. Tipe

ini umum digunakan untuk pembayaran, control akses fisik, dan aplikasi transportasi.

c. *Interface*
Pembaca didefinisikan oleh metode hubungannya ke komputer. Metode ini di antaranya berupa port USB, infrared, keyboard, dan sebagainya.

d. *Reader & terminal to Card Communication*
Seluruh kartu dan pembaca mengikuti standar ISO 7916-3 dan memiliki kumpulan komando yang memungkinkan dilakukannya komunikasi dengan kartu CPU. Kumpulan komando ini disebut APDU (*Application Protocol Data Units*) dapat dieksekusi pada *low level* atau dituliskan ke API untuk pengguna mengirim komando dari aplikasi ke pembaca. Pembaca berkomunikasi dengan kartu dimana diberikan respon atas permintaan.

III. 1. 1. 4. 2 Terminal

Terminal lebih mirip dengan alat yang memiliki komputer di dalamnya, dengan sistem operasi dan alat pengembangan. Terminal biasanya spesifik terhadap use case, misalkan keamanan dan informasi kesehatan. Hubungan ke terminal dilakukan melalui TCP-IP atau jaringan GSM.

III. 1. 2 Cara Kerja **Touch 'n Go**

Kartu cerdas TnG pada penggunaan awalnya merupakan kartu cerdas untuk sistem pembayaran elektronik untuk jalur bebas hambatan. Berdasarkan tujuan ini, kartu cerdas TnG adalah kartu cerdas *contactless* yang berisi nilai yang dapat diisi ulang.

Cara kerja kartu TnG adalah dengan mendekatkan kartu ke terminal yang akan membaca nilai kartu pada saat loket masuk tol, dan kemudian mendekatkan kartu kembali pada saat berada di loket keluar untuk mengurasi nilainya dari kartu. Terminal akan merekam keseluruhan transaksi sehingga bisa dilihat kembali.

Perkembangan berikutnya adalah munculnya penggunaan SmartTAG untuk mempercepat laju pembayaran dan membuat pengendara tidak perlu berhenti pada lajur tol. Unit SmartTAG menggunakan sinar infra merah yang tidak berbahaya bagi manusia untuk membaca nilai kartu dan mengurangi nilainya.

Setelah sukses diaplikasikan pada jalur bebas hambatan, kartu TnG dikembangkan lebih jauh sebagai alat pembayaran di berbagai *merchant* dan menjadi uang elektronik. Kartu ini pun diaplikasikan pada kartu identitas penduduk Malaysia. Perkembangan ini membuat adanya beragam informasi sensitive yang terdapat pada kartu cerdas TnG.

Pada perlindungan informasi maupun data pada kartu, secara umum kartu TnG mengaplikasikan algoritma kriptografi. Informasi mendetail mengenai spesifikasi cara kerja TnG tidak ditemukan tetapi secara garis besar kartu TnG bekerja seperti kartu cerdas pada umumnya.

III. 2 Keamanan Data dan Informasi

III. 2. 1 *Smart Card*

Kartu cerdas menimbulkan masalah keamanan tersendiri karena orang dapat melakukan pengaksesan data pada beragam aplikasi yang lebih luas dari sebelumnya. Keamanan pada dasarnya merupakan perlindungan terhadap informasi agar tidak jatuh ke pihak yang tidak berhak. Aspek yang dijaga pada keamanan informasi, termasuk pada kartu cerdas :

a. Integritas Data
Fungsi ini memastikan karakter dari dokumen dan transaksi. Karakter dari keduanya diperiksa dan dikondirmasi untuk isi dan otorisasi. Integritas data diperoleh dengan kriptografi elektronik yang memberikan identifikasi unik pada data seperti sidik jari. Setiap percobaan untuk merubah identitas ini akan memicu perubahan dan menandai usaha tersebut.

b. Otentikasi
Aspek ini memeriksa lalu mengonfirmasi identitas sebenarnya dari pihak yang terlibat dalam transaksi data atau nilai. Pada sistem otentikasi, hal ini diukur dengan menilai kekuatan dari mekanisme dan berapa banyak factor yang digunakan untuk mengonfirmasi identitas tersebut. Pada sistem PKI (*Public Key Infrastructure*), *digital signature* akan memverifikasi data dengan menghasilkan identitas yang dapat diverifikasi oleh seluruh pihak yang terlibat dalam transaksi.

c. Non-repudiation
Aspek ini menghilangkan kemungkinan transaksi tidak diakui oleh pihak yang terlibat.

d. Otorisasi dan delegasi
Aspek ini terkait dengan proses pemberian hak akses untuk sebuah data yang diinginkan. Delegasi merupakan pemanfaatan pihak ketiga untuk mengelola dan member sertifikasi ke seluruh pengguna dalam sistem, atau CA (*Certificate Authorities*).

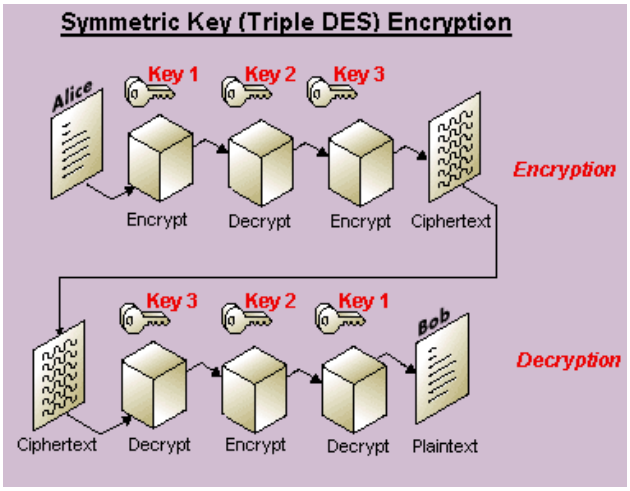
e. Auditing dan Logging
Aspek ini merupakan pemeriksaan dan perekaman *records* dan aktivitas untuk memastikan telah memenuhi aturan yang ada, dan untuk merekomendasikan perubahan jika ada.

f. Manajemen
Aspek ini akan terkait dengan pengelolaan peluncuran kartu, perubahan, maupun peraturan dalam sistem.

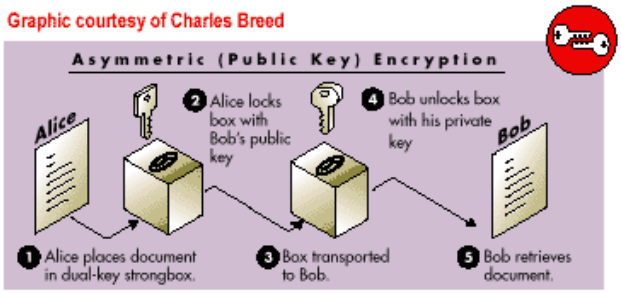
g. Kriptografi / *Confidentiality*
Aspek kerahasiaan dijaga dengan penggunaan enkripsi untuk melindungi informasi pada kartu. Kriptografi dimanfaatkan dalam beberapa hal, yaitu untuk :
   1. Melindungi keamanan data, dengan cara melakukan enkripsi pada data
   2. Memastikan integritas data, dengan cara mengenali jika data telah dimanipulasi tanpa ijin
   3. Memastikan data tetap unik dengan melakukan pengecekan bahwa data asli dan bukan merupakan kopi dari data yang asli. Pengirim melampirkan *identifier* yang unik pada ddata asli. Hal tersebut yang akan dicek oleh penerima.

h. Mekanisme keamanan data dan algoritma
Untuk merubah data dari plainteks ke cipherteks, dibutuhkan algoritma enkripsi dan kunci. Umumnya untuk algoritma simetri digunakan Triple-DES

dengan mode tiga kunci. Penggunaan algoritma tersebut dapat dilihat pada diagram di bawah ini :



Selain algoritma simetri, terdapat algoritma asimetri dengan algoritma RSA sebagai algoritma yang paling umum. Algoritma ini digambarkan pada diagram di bawah ini :



Parameter untuk keamanan data dan kartu harus ditentukan sejak awal oleh pihak yang mengeluarkan kartu. Terdapat dua metode dengan menggunakan kartu untuk sistem keamanan data, *host-based* dan *card-based.* Sistem yang paling aman adalah yang mengombinasikan kedua metode tersebut.

Pada metode *host-based, k*artu diperlakukan sebagai pembawa data sederhana. Perlindungan terhadap data dilakukan oleh komputer host. Data pada kartu dapat di enkripsi tetapi transfer ke host rentan terhadap serangan. Metode untuk meningkatkan keamanan dengan menulis kunci yang mengandung tanggal atau waktu dengan referensi rahasia ke kumpulan kunci pada host. Setiap kali kartu ditulis ulang, host dapat menulis referensi ke kunci. Hal ini membuat setiap transfer menjadi unik. Selain itu dapat pula ditingkatkan dengan penggunaan mekanisme sandi lewat.

Sedangkan dalam metode *card-based*, merupakan metode yang dilakukan pada kartu dengan mikroprosesor. Sebuah kartu atau sistem *token-based* memperlakukan kartu sebagai sebuah alat komputasi yang aktif. Interaksi antara host dan kartu berupa langkah untuk menentukan kartu dapat digunakan pada sistem atau tidak. Proses akan mengeccek apakah pengguna dapat diidentifikasi, otentikasi dan apakah kartu memiliki hak untuk melakukan transaksi. Kartu dapat meminta hal yang sama dari host sebelum melakukan transaksi. Akses pada informasi spesifik pada kartu dikontrol oleh sistem operasi internal kartu dan hak akses yang sebelumnya telah diset oleh pihak yang mengeluarkan kartu.

Proses perlindungan yang dilakukan pada saat transmisi pesan dimulai saat pesan dibuat, lalu pesan ditandatangani, dienkripsi dengan kunci privat pengirim, dikompresi, lalu dienkripsi menggunakan kunci random sesuai sesi transfer dan kunci publik penerima. Setiap transaksi akan dilakukan dengan enkripsi pesan menggunakan kunci random yang menandai sesi transmisi sehingga disaat terjadi perubahan akan terekam berdasarkan kunci unik sesi tersebut.

Pada umumnya penggunaan kartu cerdas memiliki aspek keamanan yang dapat diserang dari sisi transmisi data dan sisi fisik kartu. Prosedur di atas dilakukan untuk melindungi aspek keamanan pada saat transmisi. Data yang ditransfer dapat ditangkap oleh penyerang, tetapi sebelumnya dilakukan langkah-langkah enkripsi di atas sebagai mekanisme perlindungan.

Sisi fisik kartu memiliki kekurangan dalam aspek keamanan karena dapat dilakukan penyerangan secara fisik terhadap kartu untuk mendapatkan chip dan dilakukan pembacaan terhadap chip untuk mendapatkan informasi yang dilindunginya.

III. 2. 2 **Touch 'n Go**

Penggunaan kartu TnG, terutama pada yang berkaitan dengan kartu identitas MyKad memiliki informasi sensitive yang harus dilindungi. Algoritma kriptografi diaplikasikan dalam penyimpanan data di dalam chip, selain itu juga dilakukan proses enkripsi pada saat terjadinya transmisi data antara kartu dengan terminal.

III. 3 Analisis Penggunaan *Smart Card* di Indonesia

III. 3. 1 Keadaan Saat Ini

Pada saat ini penggunaan kartu cerdas di Indonesia telah banyak digunakan. Tipe yang paling banyak tentu adalah pada penggunaan kartu SIM pada telepon genggam. Selain itu pada penggunaan kartu ATM, serta penggunaan TV berbayar.

Ide mengenai kartu cerdas dalam pembayaran jalur bebas hambatan saat ini telah direalisasikan oleh Bank Mandiri dalam bentuk e-Toll card. Kartu ini merupakan kartu cerdas *contactless* untuk pembayaran jalur tol dengan kerja sama antara Bank Mandiri dengan tiga operator tol, yaitu PT Jasa Marga Tbk, PT Citra Marga Nusaphala Persada Tbk, dan PT Marga Mandala Sakti. Kartu ini dapat dibeli di Bank Mandiri dan di outlet Indomaret serta diisi ulang. Pengembangan lebih lanjut, kartu ini dapat dipakai untuk membeli bensin di SPBU, membayar parkir, serta melakukan pembelian di Indomaret. Penggunaan e-Toll card ini masih sedikit digunakan, tetapi jalur tol yang dapat digunakan dengan e-Toll card sedang terus diperluas.

III. 3. 2 Masa Datang

Penggunaan kartu cerdas sebenarnya tidak asing lagi di Indonesia. Khususnya dalam penggunaan sistem pembayaran elektronik e-Toll card dapat dimanfaatkan dengan lebih banyak. Pembelajaran dari kartu TnG

berhasil memperlihatkan manfaat yang dapat diambil dari penggunaan kartu cerdas pada aspek jalur bebas hambatan. Meskipun di Indonesia, selain pada kota besar seperti Jakarta, jalur bebas hambatan belum menjadi komponen yang dominan, penggunaan kartu cerdas dapat mempercepat transaksi yang terjadi dan mempermudah pengguna maupun pihak pengelola jalur tol. Pengguna dimudahkan karena tidak membutuhkan persiapan uang tunai dan tersita waktunya pada antrian yang ada di jalur pembayaran maupun pada saat pembayaran. Pengelola jalur tol akan dipermudah dengan tidak perlunya menyiapkan pecahan uang tunai maupun petugas dan cukup menggunakan alat pembaca pada loket pembayaran.

Sisi keamanan informasi pada kartu dapat diaplikasikan dengan menggunakan kriptografi seperti yang telah dimanfaatkan pada kartu debit ataupun kartu kredit. Algoritma simetri atau kunci privat dapat dimanfaatkan untuk mengenkripsi data, sedangkan algoritma asimetri atau kunci publik dapat dimanfaatkan untuk mengenkripsi tandatangan pesan. Fungsi hash dapat dimanfaatkan untuk mendapatkan *digital signature* dari pesan asli dan setiap transimi data dienkripsi dengan kunci unik yang menandai setiap sesi transfer.

Sisi keamanan lain yang lemah pada penggunaan kartu akan berada pada penyerangan kepada fisik kartu. Hal ini sulit untuk dicegah karena terkait dengan bahan pembangun kartu dan perlakuan terhadap kartu. Hal preventif yang dapat dilakukan adalah dengan mencegah jatuhnya kartu ke tangan selain pemilik.

Kartu e-Toll card yang dikeluarkan oleh Bank Mandiri pada saat ini belum banyak digunakan, salah satu penyebabnya adalah pihak yang mengeluarkan kartu merupakan suatu layanan bank yang spesifik. Untuk pengembangan ke depannya dan untuk memperluas penggunaan kartu e-Toll, jaringan bank yang dapat menggunakan layanan kartu ini lebih baik diperluas dan tidak terbatas dengan suatu bank tertentu. Hal ini tentu akan memperbesar angka pengguna kartu karena tidak adanya pembatasan tertentu bagi pengguna. Saat ini kartu dapat dibeli pada bank dan *merchant*, tetapi adanya layanan bank spesifik mempermudah sekaligus menutup kemungkinan bagi nasabah bank lain untuk memanfaatkan kartu. Oleh karena itu, perluasan layanan pada beragam bank akan memperluas penggunaan e-Toll card di Indonesia.

Setelah jumlah angka pengguna kartu meningkat, kartu e-Toll dapat diperluas penggunaannya menjadi uang ataupun dompet elektronik untuk dipakai berbelanja di *outlet* maupun *merchant* yang bekerja sama dengan pihak yang mengeluarkan kartu. Hal ini dapat dimanfaatkan dengan berkaca pada suksesnya kartu TnG dengan pengembangannya saat ini sebagai uang elektronik. Manusia dimudahkan dengan tidak perlunya membawa uang tunai maupun memikirkan uang kembali, dan mengalami transaksi yang jauh lebih cepat dalam aktivitas pembelian.

IV. KESIMPULAN

Pemanfaatan kartu cerdas pada kehidupan sehari-hari memiliki beragam bentuk, salah satunya adalah penggunaan kartu TnG di Malaysia yang peruntukkan awalnya sebagai sebuah sistem pembayaran elektronik bagi jalur bebas hambatan. Sistem ini berhasil meningkatkan pemrosesan transaksi, mempermudah, dan mempersingkat waktu yang dibutuhkan pada loket pembayaran serta dimanfaatkan oleh 13 juta penduduk Malaysia.

Kartu cerdas terutama pada TnG memanfaatkan algoritma kriptografi dalam melindungi data yang tersimpan pada chip serta proses transmisi data yang dilakukan antara kartu dan alat pembaca. Algoritma yang umum digunakan adalah Triple-DES dan RSA. Pemanfaatan algoritma dikombinasikan untuk meningkatkan keamanan, mulai dari penggunaan *digital signature*, enkripsi dengan kunci simetri, enkripsi dengan kunci asimetri, hingga enkripsi dengan kunci unik pertransaksi. Faktor keamanan lain yang penting selain perlindungan data yang ditransmisi adalah perlindungan fisik terhadap kartu itu sendiri karena penyerangan pada kartu merupakan penyerangan yang sulit dilawan. Perlindungan pada penyerangan seperti ini adalah dengan berusaha menjaga kartu tidak pernah dimiliki oleh pihak yang tidak berhak.

Aplikasi kartu cerdas seperti TnG di Indonesia telah dimulai dengan adanya e-Toll card. Bagaimanapun, untuk memperoleh manfaat seperti kartu TnG, Indonesia masih harus mengembangkan e-Toll card dengan cara memperluas jaringan bank yang menjadi pihak penyedia kartu. Selain itu layanan yang dimiliki oleh e-Toll card dapat dikembangkan ke arah dompet atau uang elektronik untuk menarik masyarakat menjadi penggunanya.

REFERENCES

[1] http://en.wikipedia.org/wiki/Smart_card
[2] http://people.cs.uchicago.edu/~dinoj/smartcard/security.html
[3] http://en.wikipedia.org/wiki/Touch_%27n_Go
[4] http://www.smartcardbasics.com/smart-card-overview.html

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 9 Mei 2011

Riffa Rufaida / 13507007