Kriptografi dalam Kartu Cerdas (*Smart Card*) *Touch n Go*

Tasya - 13515064
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13515064@std.stei.itb.ac.id

***Abstract*— Dalam kehidupan sehari-hari, secara tidak langsung kriptografi sangat membantu kegiatan kita. Salah satu manfaat dari kriptografi adalah dalam bidang *security*, kartu pintar, dsb. . Dewasa ini, kartu pintar merupakan salah satu solusi yang ditawarkan bagi masyarakat yang menjunjung tinggi mobilitas. Dengan menggunakan kartu pintar (*smart card*), masyarakat dapat melakukan pembayaran dengan praktis, mudah, dan aman. Hal ini disebabkan oleh adanya kriptografi yang menjamin keamanan data-data sang pengguna. Salah satu penggunaan kartu pintar ini adalah dalam teknologi *Touch n Go* yang salah satu penggunaannya adalah dalam membayar fasilitas jalan tol. *Touch n Go* ini adalah teknologi yang dikembangkan oleh negara Malaysia yang sekarang telah diadopsi oleh Indonesia dalam pengaplikasian yang sama, yaitu untuk membayar fasilitas jalan tol.**

***Kata Kunci*— Kriptografi, *Smart Card, Touch n Go*.**

I. PENDAHULUAN

Tanpa kita sadari, dalam kehidupan sehari-hari kita telah banyak bersentuhan dengan pengaplikasian kriptografi. Kriptografi umunya dipakai dalam bidang *security* data. Salah satu aplikasi kriptografi yang dekat dengan kita dalah kartu pintar atau yang biasa dikenal dengan istilah *smart card*.

Smart card awalnya ditemukan pertama kali dalam bentuk *plastic card* pada tahun 1930. Namun, kegunaan dari *plastic card* tersebut baru diketahui pada tahun 1950-an. Kemudian, *plastic card* ini berkembang menjadi kartu kredit yang sangat populer di kalangan masyarakat dewasa ini. Selain itu, masih banyak kegunaan dari *plastic card*, misalnya sebagai kartu identitas, untuk mengakses sebuah ruangan, ataupun untuk membayar belanjaan.

Jenis antarmuka dari *smart card* yang paling sering digunakan adalah *contact interface* yang biasanya dimasukkan ke dalam alat pembaca (*card reader*) sehingga terjadi kontak fisik secara langsung antara kartu dengan alat. Kartu pintar ini menyimpan berbagai data, seperti kunci privat, sertifikat digital, dan informasi penting lainnya. Selain itu, pada umumnya kartu pintar juga menyimpan nomor kartu dan identitas pemiliknya. Penggunaan *smart card* ini umumnya dikombinasikan dengan PIN yang ditentukan oleh pemilik kartu.

Plastic card yang dibuat pertama kali masih berupa kartu bisnis biasa, informasi yang terdapat di dalamnya pun sudah sulit untuk disalin, namun masih bias dibaca oleh manusia. Adanya teknik *emboss* (memberi relief di kartu) memudahkan penyalinan informasi yang ada di kartu ke kertas karbon, walaupun dalam prosesnya masih memerlukan *key-punch* dalam system terkomputerisasi.

Setelah itu, muncul teknologi *magnetic stripe*. Dengan hadirnya teknologi ini, sebagian proses yang tadinya dilakukan secara manual mulai dapat dilakukan secara otomatis. Namun, *magnetic stripe* tidak menghilangkan fungsi kartu sebagai identitas dan sangat terhubung kepada sang pemilik kartu. Adanya foto atau tanda tangan merupakan salah satu cara untuk melakukan otentifikasi, walaupun cara ini dinilai sangat tidak efektif.

Salah satu kegunaan kartu pintar ini adalah dalam teknologi ***Touch n Go***, yaitu kartu pintar yang digunakan untuk membayar pennggunaan sarana jalan tol. Sistem pembayaran ini menggunakan sarana elektronik. Teknologi ini dinilai sangat bermanfaat di kalangan masyarakat karena banyaknya masyarakat yang membutuhkan jalur bebas hambatan. Teknologi ini dapat dikembangkan menjadi "dompet cerdas" apabila kemanannya dapat dijamin.

II. LANDASAN TEORI

2.1 Kriptografi

Secara etimologi kata kriptografi (*Cryptography*) berasal dari bahasa Yunani, yaitu kryptos yang artinya yang tersembunyi dan graphein yang artinya tulisan (Prayudi, 2005). Awal mula kriptografi dipahami sebagai ilmu tentang menyembunyikan pesan (Sadikin, 2012), tetapi seiring perkembangan zaman hingga saat ini pengertian kriptografi berkembang menjadi ilmu tentang teknik matematis yang digunakan untuk menyelesaikan persoalan keamanan berupa privasi dan otentikasi (Diffie, 1976).

Pada kehidupan sehari-hari, komunikasi sangatlah penting. Secara umum, komunikasi berarti

penyampaian informasi atau pesan dari pengirim kepada penerima. Pesan adalah data atau innformasi yang dapat dimengerti maknanya, biasa disebut sebagai plainteks (*plaintext* atau *cleartext*). Pesan yang disampaikan bias dalam berbagai bentuk, misalnya dalam bentuk teks, gambar, musik, video, tabel, grafik, ataupun berbagai macam data lainnya. Proses penyampaian pesan tersebut juga dapat melalui berbagai macam metode.

Tidak jarang, pesan yang hendak disampaikan kepada orang lain tersebut merupakan sebuah pesan yang rahasia. Dalam hal ini, pengirim menginginkan bahwa pesannya tidak dapat dimengerti orang lain, kecuali sang penerima pesan. Dengan bantuan kriptografi, hal semacam ini dapat dilakukan. Solusinya adalah dengan mengubah *plaintext* menjadi *chipertext* (chiperteks) atau *cryptogram* (kriptogram). *Chipertext* adalah *plaintext* yang sudah tidak bermakna lagi karena sudah disandikan. Pada saat *chipertext* sampai pada penerima pesan, *chipertext* tersebut dapat diterjemahkan kembali menjadi *plaintext* menggunakan suatu metode tertentu sehingga penerima pesan dapat mengerti isi pesan yang dimaksud. Dengan begitu, isi pesan yang terdapat dalam *plaintext* hanya diketahui oleh pengirim dan penerima pesan. Adapun proses pengubahan *plaintext* menjadi *chipertext* disebut sebagai **enkripsi**, sedangkan pengubahan *chipertext* menjadi *plaintext* disebut **dekripsi**. Kedua proses ini dapat bermacam-macam caranya, tergantung fungsi yang disepakati oleh pengirim dan penerima pesan. Fungsi untuk melakukan enkripsi dan dekripsi tidak harus sama.

Kriptografi dapat diaplikasikan di berbagai benda di sekitar kita, mulai dari kartu SIM yang terdapat pada telepon genggam, kartu ATM, computer, dan masih banyak lagi. Namun, hampir semua pengaplikasian tersebut fisiknya berupa *smart card*. *Smart card* dipilih karena dapat menyimpan berbagai data dan informasi privat yang rahasia dengan aman sehingga diperlukan kriptografi untuk menjamin keamanannya.

2.2 *Smart Card*

Smart card sering juga disebut sebagai *chip card* atau *integrated circuit* (IC). *Smart card* adalah *plastic card* yang mengandung *memory chip* dan *microprocessor* yang membuat kartu ini dapat menambah, menghapus, bahkan mengubah informasi yang terkandung di dalamnya. Data pada setiap transaksi yang dilakukan pada umumnya akan diasosiasikan dengan sebuah nilai, informasi, atau keduanya. Kemudian, data tersebut akan disimpan dan diproses oleh *chip* yang ditanamkan pada kartu tersebut. Pada saat melakukan transaksi, akan digunakan sebuah "alat pembaca" yang merupakan bagian dari sebuah sistem komputer. Teknologi yang dikembangkan dengan *smart card* ini sudah dipakai di berbagai bidang, misalnya dalam pelayanan bank, hiburan, transportasi, bahkan sampai merambah ke bidang kesehatan. Dewasa ini, teknologi yang semula memanfaatkan *magnetic stripe* ataupun *barcode* mulai beralih ke *smart card* karena penghitungan *return on investment* yang dibuktikan oleh pengeluar kartu setiap tahunnya.

Pada awalnnya, *smart card* digunakan untuk menyimpan nilai telepon agar terhindar dari pencuri. Hal ini diterapkan di benua Eropa sekitar 30 tahun yang lalu. Setelah melihat kebutuhan masyarakat, selanjutnya *smart card* dikembangkan dalam berbagai kebutuhan lain, misalnya dalam transaksi jual beli barang ataupun media penyimpanan data.

Sejak ditemukannya teknologi *smart card* ini, masyarakat semakin nyaman untuk melakukan transaksi, mulai dari pembayaran belanja, listrik, fasilitas umum, kesehatan, transportasi, maupun penggunaannya dalam perpustakaan. *Smart card* juga telah terbukti menjadi salah satu media pennyimpanan yang aman sebab *smart card* mampu melindungi data, mulai dari penyimpanan sandi lewat (*password*) yang tidak hati-hati, hingga melindungi dari sistem *hack* yang canggih.

Pada zaman ini, penggunaan *smart card* sangat dekat dengan kehidupan sehari-hari semua orang. Hal ini disebabkan oleh biaya untuk mengelola riset sandi lewat (*password*) pada organisasi sangat tinggi, sehingga penggunaan kartu pintar ini merupakan salah satu solusi yang efektif dari segi biaya. Penggunaan *smart card* dalam kehidupan sehari-hari di antaranya sebagai berikut:

a) Karti kredit sebagai alat pembayaran serta penyimpanan nilai.
b) Kartu SIM pada telepon genggam untuk komunikasi.
c) Salah satu fasilitas yang dikeluarkan oleh bank.
d) *E-commerce*.
e) Kartu pintar yang menyimpan konten digital.
f) Informasi layanan kesehatan.

Dari beberapa penggunaan umum *smart card* di atas, yang akan menjadi focus makalah ini adalah penggunaan *smart card* sebagai alat pembayaran, terutama pembayaran sarana transportasi. Dalam hal ini, kartu pintar akan berisi nilai nominal uang yang dimiliki oleh pemilik kartu serta identitas dari pemiliknya. Tentu saja, nilai tersebut akan berkurang setiap kali pengguna melakukan transaksi dan dapat diisi ulang.

2.3 ***Touch n Go*** *Smart Card*

Touch n Go adalah salah satu perusahaan Malaysia yang mengembangkan *smart card* dalam bidang pembayaran transportasi, yaitu pembayaran

fasilitas jalan tol. Dengan membawa ***Touch n Go*** *smart card*, para penggunanya dapat membayar layanan jalan bebas hambatan tanpa membawa uang *cash*.

Smart card yang dikeluarkan oleh ***Touch n Go*** berukuran cukup ringkas, hanya sebesar ukuran kartu kredit dan terbuat dari plastik. Kartu ini juga dilengkapi dengan *microchip* MIFARE dari Philips. Sistem yang digunakan juga cukup besar, sehingga dapat memroses hingga 800 kendaraan perjam untuk menghilangkan antrian pada loket tol. Untuk dapat menggunakan kartu ini dengan lebih maksimal, dapat digunakan alat SmartTAG agar dapat diproses hingga 1.200 kendaraan dalam waktu satu jam.

Berikut ini adalah *smart card* yang dimiliki oleh **TnG**, yaitu:

1. Kartu *Prepaid*
   a. Kartu standard
      Kartu ini adalah kartu standar yang penggunaannya mirip dengan kartu *top-up* pada umumnya.
   b. Kartu PLUSMiles
      Kartu yang bias didapatkan juga di *North-South Expressway*.
2. Kartu *Postpaid*
   a. Kartu *Fleet Xs*
      Kartu ini ditargetkan untuk membayar biaya jalan tol (jalur bebas hambatan). Di kartunya terdapat identitas perusahaan, nomor registrasi kendaraan, dan kategori dari kendaraan.
   b. Kartu *Biz Xs*
      Kartu yang mirip dengan kartu standar, tapi kartu ini dikhususkan untuk pengguna korporasi.
3. Kartu *Auto-reload*
   a. Kartu *Zing*
      Kartu ini dapat disambungkan ke kartu *Visa, MasterCard,* atau *American Express* yang bekerja sama dengan bank-bank yang terdapat di Malaysia. Jika saldo dalam kartu *Zing* ini sudah kurang dari 50 Ringgit, maka secara otomatis saldo akan ditambahkan sebesar 100 Ringgit yang diambil dari saldo bank yang tersambung ke kartu tersebut. Namun, setiap dilakukan *reload* secara otomatis, pengguna dikenakan denda sebesar 2 Ringgit. Kartu *Zing* ini juga hanya dapat menggunakan fasilitas *auto-reload* apabila digunakan untuk membayar fasilitas tol, namun jika kartu ini dipakai untuk membayar fasilitas transportasi lain (misalnya pembayaran parkir atau tiket kereta), kartu ini tidak akan melakukan *auto-reload*.

Cara menggunakan kartu-kartu layanan yang disediakan oleh **TnG** relatif mudah. Pada saat ingin menggunakan jalan tol, pengguna hanya tinggal menyentuhkan kartu ke alat pembaca kartu yang ada di setiap loket masuk, lalu menyentuhkannya kembali pada alat pembaca yang terdapat di loket keluar. Saldo pada kartu akan dikurangi sesuai dengan jarak yang ditempuh oleh pemilik kartu, yang otomatis tercatat pada saat pengguna menyentuhan kartunya kepada alat pembaca.

Agar lebih memudahkan pengguna, kartu ini juga dielngkapi dengan alat ekstensi, yaitu SmartTAG atau OBU (*TAG On Broad Unit*) yang memungkinkan pengguna menggunakan kartu dari dalam kendaraan. Pada pelaksanaannya, fasilitas ini mendapat beberapa kritik dari penggunanya, terutama keluhan karena adanya biaya yang harus dibayarkan ketika melakukan pengisian nilai pada kartu atau hendak melakukan penggantian kartu. Selain itu, pengguna dikenakan pajak jika menggunakan fasilitas ini dalam keadaan tertentu.

Namun, tujuan dibuatnya kartu ini dinilai sudah berhasil, yaitu menurunkan tingkat antrian pada loket jalan tol. Faktanya, 4 juta dari 20 juta populasi masyarakat Malaysia telah menggunakan fasilitas ini.

III. ANALISIS

Pada bagian ini, akan dijabarkan bagaimana kriptografi menjadi bagian dari *smart card*, tingkat keamanan data dan informasi privat yang tersimpan di dalam kartu, serta analisis penggunaan *smart card* di Indonesia.

A) Kriptografi menjadi Bagian dari *Smart Card*

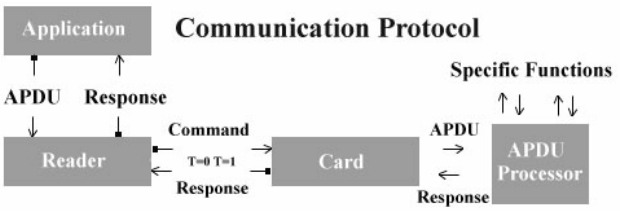
Karena *smart card* pada umumnya menyimpan data-data penting yang merupakan privasi dari pemiliknya, maka harus ada perlindungan *security* yang diterapkan. Ada 4 aspek keamanan yang harus diperhatikan dalam *smart card*, yaitu komunikasi, perangkat keras, sistem operasi, dan perangkat lunaknya.

A.1 Komunikasi

Smart card dapat berkomunikasi dengan *Card Accepting Device* (CAD) melalui sebuah paket data kecil yang disebut APDUs (*Application Protocol Data Units*). Ada beberapa karakteristik yang membuat pihak luar sulit untuk menyerang sistem, yaitu:

- *Bit rate* yang kecil (9600 bit per detik) dan menggunakan saluran transmisi *bi-directional serial* (standar ISO 7816/3).
- Menggunakan modus *half duplex* untuk mengirimkan informasi (data hanya berjalan dalam satu arah pada suatu waktu).
- Komunikasi yang terjalin akan dijelaskan di bawah ini.

Namun, setiap perangkat eksternal berkomunikasi dengan kartu sehingga membuatnya lebih rentan terhadap serangan dari luar melalui *link* komuninkasi.



Gambar 1: Komunikasi Protokol

Smart cart dan CAD menggunakan protocol otentikasi aktif bersama-sama untuk mengidentifikasi satu sama lain. Kartu ini akan menghasilkan nomor acak dan mengirimkannya ke CAD yang kemudian akan mengenkripsi nomor dengan kunci enkripsi bersama sebelum kembali ke kartu. Kartu ini kemudian membandingkan hasil yang dikembalikan oleh CAD dengan kunci enkripsi sendiri. Pasangan ini juga dapat melakukan operasi secara terbalik.

Setelah komunikasi didirikan, setiap pesan antara pasangan tersebut akan diverifikasi melalui kode otentikasi pesan. Jika data ada yang diubah (untuk alas an apapun, termasuk kesalahan transmisi), pesan harus dipancarkan kembali. Namun, jika *chip* memiliki memori yang memadai, data dapat diverifikasi dengan menggunakan tanda tangan digital.

A.2 Perangkat Keras

Semua data dan sandi lewat pada *smart card* disimpan dalam EEPROM dan dapat dihapus atau dimodifikasi oleh tegangan tertentu. Oleh karena itu, pada beberapa prosesor keamanan dipasang sensor perubahan lingkungan. Namun karena sulit untuk menemukan tingkat sensivitas yang tepat dan adanya fluktuasi tegangan ketika listrik dipasok ke *smart card*, metode ini jarang diterapkan. Serangan lain yang sering terjadi adalah dengan memanaskan *controller* dalam panas tinggi atau memancarkan sinar UV yang terfokus pada EEPROM sehingga kunci keamanan akan hilang. Serangan yang paling bahaya adalah serangan fisik, di mana kartu digunting dan prosesornya diambil. Dengan mengubah tata letak *chip*, semuanya dapat direkayasa.

Solusi untuk masalah ini adalah:

a) Teknologi penghalang (*technology barrier*)
   Advanced 0.6 micron technology sangat efektif untuk mengurangi ukuran dan konsumsi daya dari kartu. Hal ini membuat SPA eksternal atau mekanisme DPA menjadi sulit untuk membedakan antara fluktuasi kartu normal dan fluktuasi terkait data.
b) Desain yang kuat (*robust design*)
   Sebuah desain yang mudolar memungkinkan variasi *hardware* baru termasuk variasi kustom yang akan diproduksi dengan cepat dan efisien, sehingga memungkinkan respon yang cepat untuk scenario penyerangan yang baru.
c) Kontrol memori untuk multiaplikasi (*memory control for multiapplication*)
   Memory Access Control yang disempurnakan akan memberikan dukungan sistem operasi yang aman untuk kartu yang tujuannya untuk multiaplikasi.

A.3 Operating Sistem

Data yang disimpan pada *smart card* diatur dalam sebuah hirarki pohon. Data ini memiliki satu master *file* (akar), beberapa *file* dasar (EF), dan beberapa *file*khusus (DF).

Untuk meningkatkan *security*, ada lima tingkat "hak akses" ke *file* (baik DF maupun EF). Semakin tinggi tingkatannya, semakin kuat pengamanannya.

1. *Always* (ALW): akses ke *file* dapat dilakukan tanpa ada batasan.
2. *Card holder verification 1* (CHV1): akses hanya dapat dilakukan ketika nilai CHV1 valid.
3. *Card holder verification 2* (CHV2): akses hanya dapat dilakukan ketika nilai CHV2 valid.
4. *Administrative* (ADM): akses pada tingkat ini hanya dapat dilakukan oleh mereka yang memiliki tanggung jawab otoritas administrative yang tepat.
5. *Never* (NEV): akses *file* dilarang.

Namun, hanya dengan mendapatkan validasi CHV2 tidak cukup untuk mengakses *file* yang membutuhkan CHV1. CHV1 dan CHV2 dilengkapi dengan 2 PIN kemanan, PIN yang pertama adalah PIN identifikasi pengguna umum, sedangkan PIN yang lain adalah PIN blokir tertentu yang terlah tersimpan dalam kartu.

A.4 Perangkat Lunak

Perangkat lunak juga mempunyai andil dalam keamanan *smart card*. Perangkat lunak yang digunakan harus terjamin selalu menghasilkan data enkripsi yang benar.

B) Keamanan Data dan Informasi

Pada dasarnya, keamanan yang dimaksud adalah perlindungan terhadap data dan informasi yang ada agar tidak jatuh ke pihak yang tidak berhak. Ada beberapa aspek yang dijaga pada keamanan data dan informasi, termasuk pada *smart card*:

a) Integritas Data
   Fungsi ini memastikan karakter dari dokumen dan transaksi. Karakter dari keduanya akan diperiksa dan dikonfirmasi isinya. Integritas data yang diperoleh dengan kriptografi elektronik yang memberikan identifikasi unik pada data, misalnya sidik jari atau retina mata. Jika suatu saat terdapat percobaann untuk mengubah identitas ini, maka akan terjadi peringatan akan adanya perubahan data tersebut.
b) Otentikasi
   Aspek ini memeriksa lalu mengonfirmasi identitas sebenarnya dari semua pihak yang terlibat dalam transaksi data maupun nilai. Pada sistem otentikasi, hal ini diukur dengan menilai kekuatan dari mekanisme dan berapa factor yang digunakan untuk mengonfirmasi identitas tersebut. Pada sistem *Public Key Infrastructure* (PKI), tanda tangan digital akan memverifikasi data dengan menghasilkan identitas

yang dapat diverifikasi oleh seluruh pihak yang terlibat dalam transaksi tersebut.

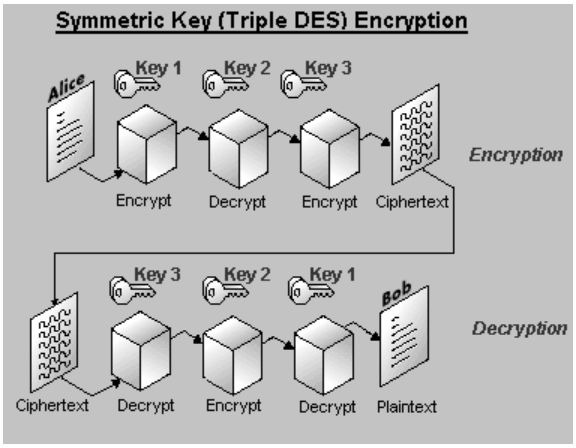
c) *Non-repudiation*
Aspek ini akan menghilangkan kemungkinan transaksi yang tidak diakui oleh pihak-pihak yang terlibat.

d) Otorisasi dan Delegasi
Aspek ini terkait dengan proses pemberian hak akses untuk melihat informasi tertentu. Delegasi merupakan pemanfaatan pihak ketiga untuk mengolah dan member sertifikasi ke seluruh pengguna dalam sistem.

e) Manajemen
Aspek ini merupakan aspek yang terkait dengan konsumen. Aspek ini terkait dengan peluncuran kartu, aturan-aturan yang harus dipenuhi jika seseorang ingin menjadi salah satu pemegang kartu, maupun aturan-aturan yang harus dipenuhi untuk melakukann pengubahan nilai pada kartu.

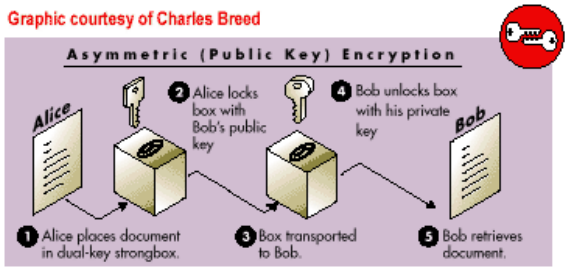
f) Kriptografi
Kriptografi sangat erat digunakan untuk menjaga keamanan data-data yang terdapat dalam kartu. Beberapa hal yang ditangani oleh kriptografi adalah:
- Melindugi keamanan data, dengan membuat data-data penting menjadi sebuah *chipertext*.
- Memastikan integrasi data dengan mengenali perubahan ganjal yang tandanya bahwa data telah dimanipulasi tanpa izin.
- Memastikan data tetap memiliki keunikannya sendiri dengan melakukan pengecekan bahwa data yang ada adalah data asli, bukan data salinan. Hal ini dapat dilakukan dengan menyocokan *identifier* yang dicantumkan oleh pengirim pada data yang diserahkan.

g) Mekanisme Data dan Algoritma
Untuk mengubah data dari *plaintext* menjadi *chipertext*, dibutuhkan sebuah algoritma enkripsi dan sebuah kunci. Pada umumnya, untuk algoritma simetri, digunakan *Triple-DES* dengan metode tiga kunci. Penggunaan algoritma tersebut dapat dilihat pada diagram di bawah ini:



Gambar 2: Symmetric Key (Triple-DES) Encryption

Selain itu, terdapat juga algoritma asimetrik yang pada umumnya digunakan adalah algoritma RSA. Algoritma RSA tersebut dapat digambarkan pada diagram di bawah ini:



Gambar 3 Assymetric Encryption

Parameter untuk keamanan data dan kartu harus ditentukan sejak awal oleh semua pihak yang terlibat dalam pembuatan *smart card*. Ada beberapa metode yang dapat digunakan untuk mengamankan data, misalnya *host-based* dan *card-based*. Dengan mengombinasikan kedua metode ini, sistem keamanan yang terbentuk dapat dibilang paling aman.

Pada metode *host-based*, kartu dianggap sebagai pembawa data sederhana. Perlindungan terhadap data dilakukan oleh computer *host*. Data pada kartu dapat dienkripsi, tetapi pada saat data ditransfer ke *host*, sangat 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 sesuatu ditulis di kartu, *host* dapat menulis referensi ke kunci. Hal ini membuat setiap transfer menjadi unik.

Pada metode *card-based*, metode yang dilakukan pada kartu adalah dengan memanfaatkan *microprocessor*. Metode ini memperlakukan kartu sebagai sebuah alat komputasi yang aktif. Interaksi antara *host* dan kartu merupakan sebuah langkah untuk menentukan kartu dapat digunakan pada sistem atau tidak. Proses akan mengecek apakah pengguna dapat diidentifikasi, diotentikasi, dan apakah kartu memiliki hak untuk melakukan transaksi. Kartu juga dapat meminta hal yang sama dari *host* sebelum transaksi dilakukan. Akses pada informasi spesifik pada kartu dikontrol oleh sistem operasi internal kartu dan hak akses yang sebelumnya telah diset oleh pihak yang mengeluarkan kartu.

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

C) **Touch n Go**

Para pengguna kartu **TnG** pada umumnya memiliki

informasi atau data yang personal atau rahasia, sehingga informasi tersebut harus dilindungi. Oleh karena itu, algoritma kriptografi diaplikasikan dalam penyimpanan data di dalam *chip*. Selain itu, enkripsi dan dekripsi juga diterapkan pada saat terjadi transaksi.

D) Penggunaan *Smart Card* di Indonesia

Dewasa ini, penggunaan *smart card* di Indonesia sudah cukup meluas. Penggunaan yang paling menonjol adalah dalam bidang telekomunikasi, yaitu sebagai kartu SIM yang digunakan di telepon genggam sebagai identitas nomor telepon. Selain itu, kartu pintar juga sudah digunakan sebagai kartu ATM. Indonesia juga sudah mulai menerapkan *e-Toll* seperti negara Malaysia.

e-Toll ini telah diterapkan oleh Bank Mandiri bekerja sama dengan PT Jasa Marga Tbk, PT Marga Mandala Sakti, dan PT Citra Marga Nusaphala Persada Tbk. Kartu ini dapat diperoleh di Indomart ataupun langsung dari Bank Mandiri. Kartu ini juga tentu dapat diisi ulang melalui Indomart. Selanjutnya, kartu ini sudah dapat dipakai untuk melakukan pembayaran di SPBU, membayar parkir, serta melakukan transaksi di Indomart. Namun sayangnya, penggunaan teknologi *e-Toll* ini masih jarang karena hanya terbatas pada pengguna Bank Mandiri saja.

Penggunaan *smart card* di Indonesia sebetulnya sudah tidak asing lagi di kalangan masyarakat. Sebagian besar masyarakat telah menggunakan kartu ini sebagai alat pembayaran saat melakukan transaksi pembelian. Namun, penggunaan *smart card* sebagai alat untuk membayar jalur bebas hambatan masih jarang digunakan. Akibatnya, masih sering terjadi antrian yang menumpuk pada loket pembayaran.

Sisi keamanan informasi pada kartu dapat diaplikasikan dengan menggunakan kriptografi seperti yang diterapkan di dalam kartu kredit. Algoritma simetri atau kunci privat dapat dimanfaatkan untuk melakukan enkripsi data, sedangkan algoritma asimetri atau kunci public dapat dimanfaatkan untuk melakukan enkripsi terhadap tandatangan pesan. Untuk mendapatkan tanda tangan digital, dapat diterapkan fungsi *hash*.

Kartu pintnar *e-Toll* yang dikeluarkan oleh Bank Mandiri masih jarang digunakan karena terlalu spesifik kepada pengguna Bank Mandiri saja. Untuk ke depannya, diharapkan adanya kartu pintar *e-Toll* yang tidak terbatas pada suatu bank tertentu sehingga minat public terhadap *smart card* tersebut akan meningkat. Setelah pengguna kartu pintar *e-Toll* meningkat, kartu pintar ini dapat diperluas menjadi semacam "dompet elektronik" untuk dipakai berbelanja di berbagai *outlet* sehingga masyarakat tidak perlu membawa banyak uang *cash* ataupun banyak kartu pada saat yang bersamaan. Dengan demikian, masyarakat juga tidak perlu dipusingkan untuk menghitung uang kembali yang seharusnya diterima.

IV. KESIMPULAN

Dalam kehidupan sehari-hari, ternyata masyarakat tidak lepas dari penggunaan salah satu cabang Matematika Diskrit, yaitu kriptografi. Kriptografi membantu permasalahan dalam bidang keamanan, terutama keamanan data privat masing-masing orang. Salah satu aplikasi yang menggunakan kriptografi adalah kartu pintar atau *smart card*.

Smart card menggunakan kriptografi untuk melindungi data yang tersimpan pada *chip* yang sudah ditanamkan di dalamnya. Selain itu, data transaksi yang dilakukan juga akan terlindungi dengan memanfaatkan kriptografi. Algoritma kriptografi yang umum digunakan adalah RSA dan *Triple*-DES. Kedua algoritma ini dikombinasikan untuk meningkatkan keamanaan pada saat menggunakan *digital signature*, enkripsi dengan kunci simetri maupun kunci asimetri, hingga enkripsi untuk kunci transaksi.

Salah satu bentuk pemanfaatan *smart card* yang diterapkan oleh negara Malaysia adalah kartu **TnG** (***Touch n Go***). Kartu **TnG** ini digunakan sebagai sistem pembayaran dalam penggunaan fasilitas jalan bebas hambatan. Dengan digunakannya sistem ini, masyarakat di Malaysia mendapatkan kemudahan saat melakukan transaksi, yaitu mempersingkat waktu yang dibutuhkan di loket pembayaran sertia para penggunanya tidak harus membawa uang *cash* untuk membayar.

Karena dinilai cukup efektif, maka Indonesia mengadaptasi teknologi ini dalam hal yang sama, yaitu pembayaran sarana jalur bebas hambatan. Dewasa ini, sudah banyak terdapat layanan *e-Toll* yang mempermudah masyarakat untuk melakukan transaksi pembayaran. Namun, jaringan yang dimiliki oleh Indonesia masih belum cukup besar. Diharapkan fasilitas *e-Toll* ini akan semakin berkembang seiring berjalannya waktu dan bias mencapai tahap "dompet elektronik" sehingga setiap orang hanya perlu membawa satu kartu sebagai penunjuk identitas dan dompet sebagai alat untuk melakukan transaksi. Dengan memperbesar sistem, masyarakat akan semakin tertarik untuk menggunakan teknologi ini karea akan membuat mobilitas masyarakat semakin tinggi sebab tidak harus membawa banyak uang secara fisik yang mampu mengundang kejahatan.

V. UCAPAN TERIMA KASIH

Penulis ingin mengucaokan terima kasih kepada Tuhan Yang Maha Esa, karena berkat bimbingan-Nya penulis dapat menyelesaikan makalah ini tepat pada waktunya dan berjalan dengan lancar. Penulis juga ingin berterima kasih kepada Bapak Dr. Ir. Rinaldi Munir, M.T. dan Ibu Dra. Harlili, M. Sc. karena telah memberikan kesempatan sehingga penulis dapat mengerjakan makalah ini.

REFERENSI

[1] Munir, Rinaldi, *Matematika Diskrit*, Bandung: Informatika, 2010.
[2] http://www.kajianpustaka.com/2014/01/pengertian-sejarah-dan-jenis-kriptografi.html
diakses pada tanggal 7 Desember 2016.
[3] http://smartcardkomas.blogspot.co.id/2009/11/smart-card.html
diakses pada tanggal 7 Desember 2016.
[4] http://people.cs.uchicago.edu/~dinoj/smartcard/security.html
diakses pada tanggal 7 Desember 2016.
[5] http://www.smartcardbasics.com/smart-card-overview.html
diakses pada tanggal 7 Desember 2016.
[6] http://www.touchngo.com.my/CMS/Business/Business-Products/Fleet-Pass/About-Fleet-Pass-Card/
diakses pada tanggal 8 Desember 2016.
[7] Sumber gambar 1:
http://people.cs.uchicago.edu/~dinoj/smartcard/comprotocol.gif
[8] Sumber gambar 2:
http://www.smartcardbasics.com/smart_card_images/panel7_3des.gif
[9] Sumber gambar 3:
http://www.smartcardbasics.com/smart_card_images/panel7a.gif

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, 8 Desember 2016

Tasya / 13515064