Kriptografi pada Sistem e-Money

Adhi Darmawan S./13508088
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
rahmawan.sutjiadi@gmail.com

***Abstract*—Dalam kehidupan sehari-hari banyak orang yang merasa bahwa cash atau uang dalam bentuk nyata, sulit untuk disimpan, ditransaksikan, dan juga dibawa. Hal ini disebabkan oleh permasalahan dimana jumlah uang yang dibawa bervariasi. Tergantung dari nominal setiap "uang" yang dibawa, mulai dari uang kecil(coin), uang kertas(paper), sampai pada cek(check). Banyak merasa kesulitan disebabkan oleh sulitnya menghitung uang kembalian, hilangnya beberapa lembar uang, jatuhnya uang dari saku karena terlalu penuh, bahkan tidak aman karena bila tercuri atau terambil oleh orang lain dapat langsung dipakai tanpa prasyarat tertentu. Dengan kata lain, bentuk fisik dari uang dapat berkurang dengan kejadian-kejadian yang tidak terduga. E-money adalah salah satu bentuk penanganan untuk kejadian-kejadian tidak terduga tersebut, selain itu e-money juga digunakan untuk mempermudah kehidupan sehari-hari, e-money dapat digunakan untuk melakukan berbagai kegiatan transaksi hanya dengan satu alat(device/tools) yang melambangkan e-money tersebut.**

***Index Terms*— e-money, Cryptography, living gadget, DES**

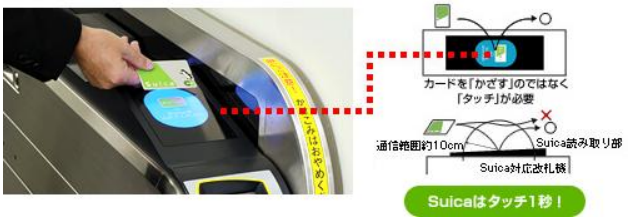
1. Pendahuluan

Pada perkembangannya prinsip, e-Money sudah tidak asing lagi digunakan. Tetapi pada pemakaiannya di kehidupan sehari-hari, penggunaan e-Money sangat riskan. Hal ini dikarenakan oleh bagaimana fisik dari e-Money berbentuk kartu, seperti ATM yang menyimpan informasi pribadi dan dapat dipalsukan bilamana keamanan untuk kartu tersebut kurang. Biarpun demikian e-Money saat ini dipakai untuk berbagai hal, salah satu Negara yang menggunakan e-Money pada kehidupan sehari-harinya adalah jepang, di Negara tersebut bentuk e-Moneyadalah berupa smart card yang mengunakan IC(Integrated Circuit) yang bernama Suica(Super Urban Intelligent CArd). Suica diterbitkan oleh East Japan Railroad Company dan telah digunakan untuk berbagai macam hal, pembayaran *train pass(*tiket kereta*), vending machine, convenient store*(Minimarket), *bus pass*(pembayaran transportasi bus), bahkan untuk makan di restoran umum.

Gambar 1.1
Bentuk penggunaan Suica untuk train pass

Ticket Gate, JR East

Gambar 1.2
Cara kerja Suica



Di Indonesia bentuk dari e-Money sudah direalisasikan, bernama kartu *FLAZZ* yang dikeluarkan oleh bank BCA. Saat ini biarpun masih sedikit, tetapi pemakaian katu *FLAZZ* milik bank BCA mulai diperbanyak, baik untuk membeli pulsa, makan di beberapa restoran tertentu, dan belanja di supermarket. Sayangnya bentuk dari penggunaan e-Money yang dipakai masih semi terbatas. Dimana penggunaan FLAZZ hanya pada tempat-tempat yang memiliki koneksi terhadap Bank BCA.

Gambar 1.3
Kartu FLAZZ

Gambar 1.4
Device FLAZZ

2. e-money

e-money adalah singkatan dari *electronic money*, dengan kata lain uang dalam bentuk informasi elektronik. electronic money dipakai sebagai ganti dari cash yang diterbitkan oleh sekelompok organisasi yang terbidang pada penyimpanan uang dengan kata lain secara umum electronic money mulai diterbitkan/disebarluaskan oleh pihak bank untuk mempermudah kehidupan sehari-hari dari pemegang akun bank. Bentuk e-money bila dilihat dari sejarahnya awalnya berupa rekening yang tersambung di seluruh cabang dan atm bank, kemudian terdapat kartu kredit dan debit yang mulai dipakai di kehidupan sehari-hari.

Gambar 2.1
Bentuk fisik rekening bank

Gambar 2.2
Kartu Debit dan Kredit

Tetapi kartu debit hampir tidak dapat digunakan dalam transaksi untuk menjaga keamanan rahasia dalam kartu tersebut. Sedangkan kartu kredit memerlukan beberapa persyaratan yang ketat karena berlaku secara internasional.

Persyaratan kartu kredit berupa :

1. Usia pemegang kartu minimal usia kerja atau usia dewasa di Negara tersebut.
2. Pemegang kartu memiliki penghasilan sejumlah tertentu yang ditentukan oleh instansi pemberi kartu kredit.
3. Setiap bulan pemilik kartu wajib membayar sejumlah yang digunakan beserta tambahan biaya dari penggunaan kartu tersebut.
4. Kartu kredit hanya dapat digunakan dengan batas tertentu yang ditetapkan sesuai dengan jenis kartu kredit tersebut.

Setelah pemakaian gadget handheld berupa handphone, token, dan internet mulai merambah. Dengan perkembangan teknologi demikian, pemakaian teknologi tersebut membuahkan perkembangan e-money ke bentuk transaksi secara on-line atau dengan kata lain tanpa tatap muka, seseorang dapat bertransaksi dengan layanan bank yang baru bernama internet banking.

Gambar 2.3
Bentuk Internet Banking(PayPal)

Dengan layanan ini seseorang dapat mengirimkan atau bertransaksi tanpa harus membawa uang dalam bentuk kasar, cukup dengan suatu alat yang terhubung dengan jaringan *global network*. Pemakaian teknologi ini telah digunakan dalam banyak hal, seperti jual beli internasional melalui internet dengan nama *e-commerce*.

Gambar 2.4
Bentuk e-commerce(Android Market)

Contoh dari organisasi yang telah menggunakan teknologi ini adalah amazon.com, android market, visa, dan banyak perusahaan lainnya yang bertransaksi secara internasional. Tetapi, karena keterbatasan penggunaan dalam bagaimana dibutuhkannya suatu device yang terhubung langsung pada *global network*, sedangkan tidak semua orang memiliki device tersebut. Selain itu, tidak selalu koneksi internet di beberapa wilayah selalu terhubung dengan *global network*. Oleh karena itu dikembangkanlah lagi sebuah bentuk kartu dengan IC yang dapat merekam jumlah uang dan transaksi yang dilakukan sehingga tidak harus sealu terhubung dengan internet tetapi dapat ditangguhkan dulu dalam kartu tersebut, lalu dikirimkan pada central network(server) saat menemukan device yang memungkinkan hal tersebut. Di Jepang artu ini bernama Suica[Super Urban Intelligent CArd]

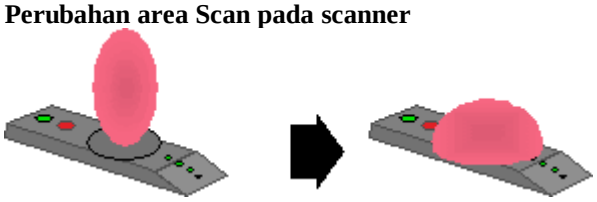
3. Suica[Super Urban Intelligent CArd]

Suica diterbitkan oleh Japan East Railroad Company, dengan tujuan mempermudah transaksi serta memperlancar jalur pembelian tiket pada jam sibuk kerja. Secara umumnya Suica adalah kartu pra-bayar tunai elektronik yang dikembangkan di Jepang yang dapat digunakan untuk membeli layanan dan produk di daerah stasiun kereta, kereta bawah tanah, dan bus, serta di mesin penjual otomatis dan minimarket. Kartu ini dapat dibeli di mesin penjual khusus di stasiun kereta terutama di daerah Kantou(metropolitan Tokyo), Kansai (metropolitan Osaka), Sendai, dan Niigata. Meskipun pembayaran minimum untuk satu kartu adalah 2000 yen (US $ 17.90) yang diperlukan untuk membeli kartu. Tetapi sebenarnya hanya 1500 yen (US $ 13,42) tunai elektronik yang awalnya tersimpan pada kartu, sebagai returnable deposit dari 500 yen (US $ 4,47) yang dibebankan. Saat pelanggan membayar untuk produk dan jasa, uang yang masing-masing dipotong dibebankan pada kartu. Suica dapat diisi ulang pada mesin khusus di stasiun kereta. Cara kerja Suica adalah berupa pendekatan kartu Suica pada scanner device, dan secara otomatis scanner akan mendeduksi uang dari kartu, lalu menunjukkan jumlah uang yang tersisa. Biarpun penggunaan Suica memiliki sisi negatif, tetapi efek positif yang diberikan lebih banyak daripada sisi negatif yang terbawa. Suica, biarpun harus diisi ulang hanya pada beberapa area tertentu, tetapi dapat menjadi pengganti cash yang dibawa oleh orang tersebut. Selain itu, Suica juga mempermudah proses penggunaan tiket kereta, dimana seseorang harus memasukkan tiket kereta dan mengambilnya lagi di jalan keluar pada saat menaiki kereta, dan harus sekali lagi melakukan hal tersebut saat turun dari kereta. Sejarah Suica dimulai dari nama "suisui" dari suara yang dihasilkan saat menggunakan, yang berarti lancar(smooth) dengan "ka" yang merupakan singkatan dari card. Dengan kata lain Suica bila diartikan secara kasar adalah, kartu lancar atau kartu pemerlancar.

3.1. Pengembangan Suica

Suica diciptakan karena pada awalnya sistem tiket kereta yang merepotkan dikembangkan dengan sistem magnet kurang berhasil, yang kemudian mendorong penggunaan IC(Integrated Circuit), hal ini dikarenakan IC memiliki kapabilitas penyimpanan 100 kali lebih banyak daripada magnetic tickets. Tetapi hal ini mendorong permasalahan baru dimana sistem tiket kereta masih menggunakan CPU untuk read only dan mencatat semua transaksi perjalanan sebanyak lebih dari 15 juta penumpang setiap hari. Dan hal tersebut tidak mungkin dicatat oleh fisik database server komputer. Sehingga daripada menggunakan read only card, digunakanlah read/write card, dimana masing-masing kartu menyimpan setiap transaksinya sendiri. Di fase terakhir dari pengembangan kartu ini, dibuat scanner yang *contactless* dimana cukup dengan mendekatkan kartu pada scanner cukup untuk membaca dan menulis informasi yang diperlukan. Hal ini mempermudah proses penggunaan kartu, dimana tidak perlunya mengeluarkan kartu dari dompet untuk ditempelkan pada mesin scanner. Area scan dari scanner juga diubah, dari menggunakan bentuk elips menjadi bentuk dome.

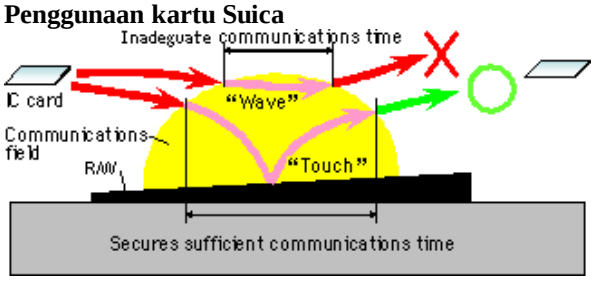
Gambar 3.1
Perubahan area Scan pada scanner



3.2. Teknologi Suica

Kartu Suica beroperasi dengan menggunakan RFID (Radio-Frequency IDentification), Dengan teknologi ini, gelombang radio yang digunakan memberikan rangkaian terintegrasi daya yang cukup untuk mengoperasikan sementara chip yang berada dalam jangkauan pemancar gelombang radio. Sehingga data juga dapat diterima dan dikirimkan menggunakan gelombang radio. Kartu Suica menggunakan teknologi contactless, tetapi waktu yang diperlukan untuk read/write informasi transaksi kurang bila pengguna hanya mengenai sekilas daerah scanner, untuk itu diciptakan suatu teknik "touch and go" di mana kartu tersebut harus ditekan secara singkat pada scanner agar dapat menerima dan mengirimkan data sementara dalam gelombang radio. Desain teknik yang paling efisien untuk dasar dari scanner ini adalah untuk menempatkannya pada sudut derajat 15 dan menyalakannya dengan sebuah layar LED.

Gambar 3.2
Penggunaan kartu Suica



Secara spesifik, pengiriman dan penerimaan data pada kartu Suica menggunakan teknik FeliCa(Felicity Card) yang dikembangkan oleh Sony. Dengan detail gelombang radio yang digunakan adalah13.56 MHz dan transmisi data sebesar 212 kbps. FeliCa menggunakan algoritma Manchester Encoding untuk encoding data yang ditransmisi antara kartu dan scanner karena, pada saat kartu bergerak pada daerah scanner muncul noise yang menggangu pengiriman dan penerimaan data antara kartu dan scanner. Manchester Encoding digunakan karena lebih resistan pada noise dibandingkan algoritma lain. Cara kerja Manchester Encoding adalah sebagai berikut: Manchester Encoding mengkodekan 0 sebagai penurunan tegangan dari beberapa tegangan positif maksimum ke nol tegangan. Sebaliknya, kenaikan tegangan dari tegangan nol ke tegangan positif maksimum digunakan untuk menyatakan 1. Saat kartu menyentuh scanner, kartu harus diakui oleh pemindai, lalu data dienkripsi, dan akhirnya data harus ditransmisi kembali. Semua ini terjadi dalam waktu kurang dari 0,1 detik. Jika transaksi tidak terselesaikan, maka kartu tersebut akan dikembalikan ke keadaan semula. Hal ini untuk mencegah kesalahan bilamana jika transaksi hanya sebagian selesai.

3.2. Keamanan Suica(Algoritma Enkripsi)

Untuk memberikan rasa aman, pada setiap transaksi diberikan kunci baru yang tercipta setiap transaksi dilakukan. Kunci tersebut digunakan sebagai masukan dalam enkripsi algoritma Triple-DES[Data Encrypption Standard] yang diciptakan oleh kerja sama antara IBM dan NSA[National Security Agency] pada tahun 1976. DES adalah jenis algoritma enkripsi yang dikenal sebagai "block cipher". Ini berarti bahwa algoritma ini digunakan untuk mengenkripsi data dalam blok yang ditetapkan dalam ukuran tertentu. Untuk DES, ukuran blok adalah 64 bit, Masukan untuk blok cipher adalah pesan plaintext yang akan dienkripsi, Output untuk cipher blok adalah ciphertext, yang merupakan versi terenkripsi plaintext, dengan ukuran yang sama dengan pesan plaintext asli. Untuk DES, ukuran input plaintext dan ciphertext keluaran adalah 64 bit. Pada akhir masukan, sebuah kunci rahasia juga digunakan sebagai masukan. Karena DES bersifat simetris, kunci yang digunakan sama dan algoritma dengan sedikit perubahan digunakan untuk mendekripsi ciphertext kembali ke plaintext asli. Untuk DES, panjang kunci ini adalah 64 bit, tetapi hanya 56 bit digunakan karena setiap bit kedelapan digunakan untuk pengecekan paritas dan diabaikan. Adapun penjelasan sederhana dari algoritma DES, DES didasarkan pada "dua teknik dasar enkripsi: confusion and diffusion". DES dibagi menjadi 16 putaran. Setiap putaran menggunakan kunci untuk melakukan substitusi dan permutasi pada plaintext asli. Menentukan plaintext asli dari ciphertext sangat sulit tanpa mengetahui kuncinya. Salah satu pendekatan serangan adalah dengan hanya mencoba setiap kunci yang mungkin. Serangan brute force biasanya memakan waktu lama, karena semua 256 kunci harus dicoba. Karena algoritma ini adalah umum, ahli kriptologi banyak telah mempelajari algoritma, mencari kelemahan. Satu terkenal kelemahan terletak pada kunci sendiri. Enam puluh empat "kunci lemah" telah diidentifikasi yang memiliki sifat tertentu yang membuat plaintext lebih mudah ditemukan. Sebuah metode yang dikenal sebagai " differential cryptanalysis" telah terbukti lebih efektif daripada serangan brute force dalam mengungkap kunci, tetapi hanya berguna bila penyerang dapat memilih beberapa plainteks asli. Metode lain yang dikenal sebagai "linear cryptanalysis" juga dapat digunakan untuk memulihkan kunci lebih cepat daripada pencarian yang melelahkan, tetapi juga membutuhkan pengetahuan tentang plaintext. Akhirnya, ahli kriptologi banyak yang curiga bahwa NSA telah menciptakan "backdoor" untuk DES, karena mereka membantu untuk menciptakan misterius S-boxes (kotak substitusi), yang digunakan untuk menggantikan plaintext dengan nilai yang berbeda. Pada tahun 1978, AS Senat Komite Intelijen menyatakan bahwa DES tidak memiliki kelemahan dieksploitasi tersebut. Dengan kekuatan pengolahan komputer saat ini, kelemahan nyata dari DES terletak pada panjang kunci dan blok pendek, yang masing-masing hanya 56 dan 64 bit. Karena telah banyak percobaan dan juga beberapa keberhasilan dalam beberapa cara pemecahan algoritma DES, akhirnya pada tahun 1999 hanya boleh digunakan sebagai legalisasi sistem dan untuk berikutnya, wajib menggunakan “triple”DES. Bila menggunakan skema enkripsi triple, berbagai kombinasi tombol, mode enkripsi, dekripsi dan mode dapat digunakan. Sebagai contoh, plaintext dapat dienkripsi sekaligus dengan satu tombol. Output ini (ciphertext) dienkripsi lagi dengan kunci yang berbeda. Akhirnya, output ini (ciphertext 2) dienkripsi ketiga kalinya dengan kunci ketiga. Ini adalah versi triple DES yang menggunakan NIST[National Institute of Standards and Technology]. Secara resmi disebut "Triple Data Encryption Algorithm" (TDEA), yaitu algoritma enkripsi yang menggunakan 3 kunci yang berbeda dan algoritma DES 3 kali untuk mengenkripsi dan mendekripsi data

Gambar 3.3
Triple DES disederhanakan

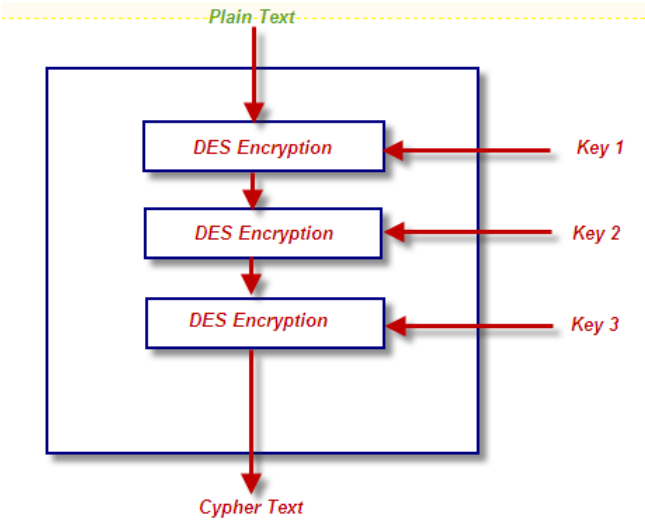
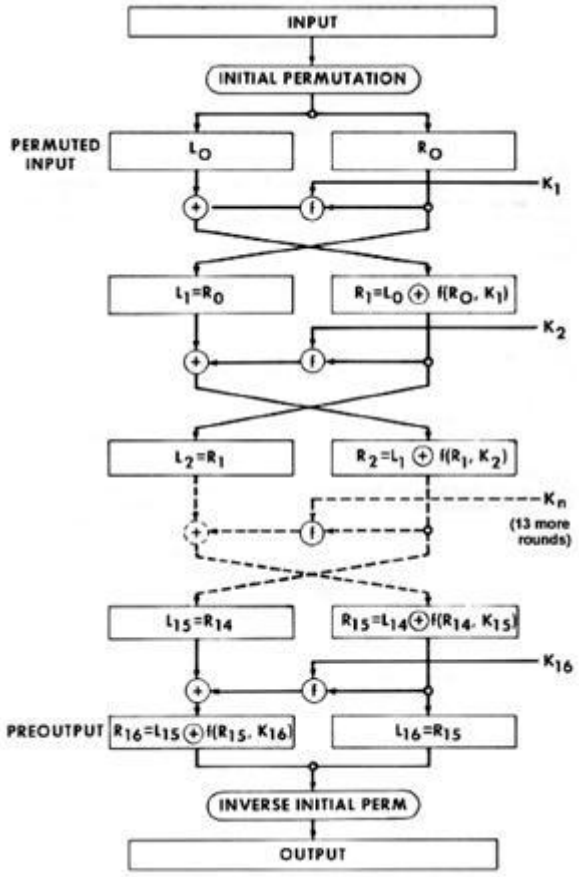


Figure: Working Of Triple DES Algorithm

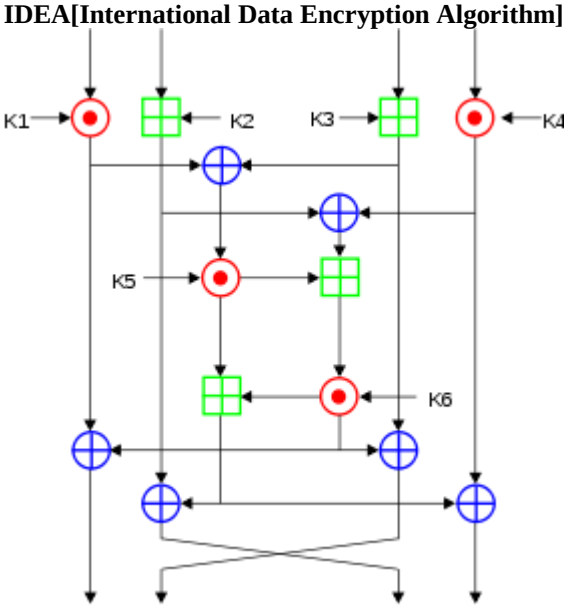
www.sanjaal.com

Gambar 3.4
Keseluruhan Triple DES



Dengan kunci 56-bit, ber-set tiga kunci membentuk "key bundle" yang setara dengan kunci dari panjang 2^{168}. Sebaliknya, Triple DES digunakan dengan FiliCa Sony menggunakan 2 kunci dan berurutan menggunakan enkripsi, dekripsi, dan enkripsi. Algoritma ini bekerja dengan menggunakan kunci pertama dengan enkripsi DES. Output untuk ini adalah masukan untuk dekripsi DES, tetapi dengan tombol kedua. Akhirnya, output dari ini dekripsi dengan kunci kedua adalah masukan untuk enkripsi lain dengan kunci pertama. Ini memberikan panjang kunci efektif adalah sejumlah 2^{112}. Untuk menambakhan keamanan dalam penggunaan algoritma, karena "triple-DES" juga sudah umum digunakan, maka IC card yang digunakan juga diamankan kembali dengan enkripsi PGP(Pretty Good Privacy) yang juga menggunakan bentuk lain dari block cipher yaitu IDEA.

Gambar 3.5
IDEA[International Data Encryption Algorithm]



Dengan menggunakan 64 bit block dan 256 bit key, IDEA menggunakan teknik yang mirip dalam enkripsi dan dekripsi. Dan secara keseluruhan IDEA sudah terbukti immune dari beberapa bentuk penyerangan, dan penyerangan tersebut tersusun dari 6 ronde didasarkan oleh 2^{64} known plaintexts dan $2^{126.8}$ operation.oleh karena itu bentuk dari enkripsi dengan PGP telah divalidasi dan disertifikasi oleh EAL4 sebagai pendiri keamanan terandalkan untuk Smart Cards sedunia.

Untuk perlindungan lebih jauh, pelanggan juga dapat mendaftarkan informasi diri untuk kartu Suica. Jika mereka memberikan nama mereka, tanggal lahir, dan jenis kelamin saat membeli kartu Suica, maka kartu mereka dapat dibatalkan dan mereka bisa mendapatkan kartu baru jika mereka kehilangan kartu lama mereka atau dicuri. Secara praktisnya belum pernah ada organisasi atupun individual yang dapat melakukan tindak kriminal seperti manggandakan ataupun mendapatkan profit dari kartu Suica dikarenakan berbagai fasilitas keamanan yang diberikan.

4. Analisis pemakaian teknologi e-money di Indonesia

Saat ini Indonesia telah mempraktekan berbagai teknik e-money, yaitu :

a. Rekening : sudah digunakan saat pendirian instansi bank.
   (contoh: Bank Danamon)
b. Kartu Debit dan Kredit : digunakan sesuai dengan kebutuhan pemegang akun bank.
   (contoh: Bank BNI)
c. Internet Banking: Sudah digunakan pada bank yang sudah memiliki sistem tersebar.
   (contoh: Bank Mandiri)
d. e-commerce : digunakan oleh insitusi dan beberapa bank yang terlegalisasi secara internasional.
   (contoh: ber-logokan VISA/MasterCard/PayPal)
e. Smart Card : digunakan oleh bank dengan koneksi pada beberapa institusi lain.
   (contoh: BCA FLAZZ)

Tetapi pada nyatanya penggunaan e-money masih belum terdistribusi secara rata ataupun penuh. Hal ini dikarenakan besarnya biaya yang dibutuhkan untuk pengimporan serta pemasangan berbagai fasilitas pendukung e-money menggantikan fasilitas yang lama, beserta waktu dan pendidikan yang dibutuhkan dalam mengajarkan cara pemakaian dan kegunaan e-money dalam kehidupan sehari-hari menggantikan cara konvensional(cash).

5. Kesimpulan

Kesimpulan yang didapat dari pembahasan ini adalah:

a. Dengan e-money, kekurangan cash dapat tertutupi, dan tidak terjadi loss of money secara berlebihan karena pencurian atau kehilangan.
b. Biarpun file tercuri tetap aman karena tidak ada file tanpa enkripsi keamanan yang berlipat.
c. Penggunaan algoritma kriptografi pada smart card masih dapat berkembang dan diperluas. Seperti menggunakan smart card untuk menyimpan data pada handphone sehingga transaksi juga dapat dilakukan hanya dengan membawa handphone.
d. e-money relative aman karena tidak ada pihak kriminal yang dapat mendapat profit dengan menggunakan e-money dalam tindak kriminal.

.

6. Saran

Penggunaan e-money dalam smart card diharapkan dapat lebih dikembangkan di berbagai aspek, sehingga suatu saat penggunaan smart card bukan hanya sebatas transaksi pembayaran, tetapi juga koordinasi dengan informasi pribadi dan juga gadget sehari-hari, seperti handphone dan juga kendaraan dapat digunakan bersamaan dengan smart card.

Sebagai contoh :

a. Pembayaran otomatis jalan tol dengan identitas kendaraan.
b. Identifikasi masuk-keluar parkir dengan smart phone berisi STNK.
c. Pemesanan makanan secara on-line dengan wireless dari dalam kendaraan dengan restoran terdekat.
d. Identifikasi dan verivikasi data diri.(e-KTP)

7. Daftar Pustaka

[1] Munir, Rinaldi. (2012). Bahan Kuliah IF5054 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung.
[2] en.wikipedia.org
[3] http://www.jreast.co.jp
[4]http://en.**wikipedia**.org/**wiki**/Suica
[5]www2.hawaii.edu/~walbritt/research/itm431.doc
[6]http://www.rcis.aist.go.jp
[7]http://www.bca.co.id/id/individual/produk_dan_layanan/e-banking/flazz-bca/flazz_bca.jsp

Ttd
Adhi Darmawan Sutjiadi
13508088
ITB Students of Informatics Engineering