Bahan Kuliah ke-25

IF5054 Kriptografi

Kriptografi dalam Kehidupan Sehari-hari (Bagian 1)

Disusun oleh:

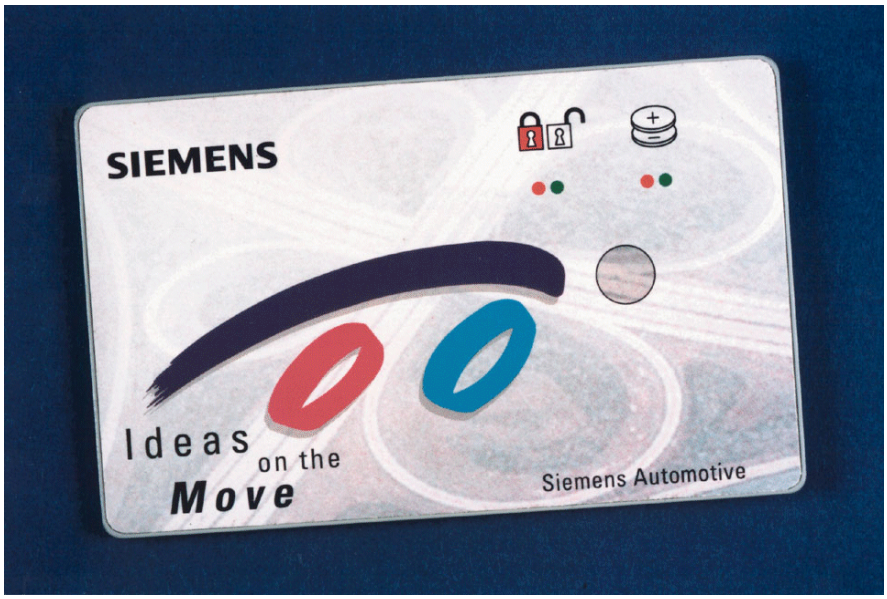
Ir. Rinaldi Munir, M.T.

Departemen Teknik Informatika
Institut Teknologi Bandung
2004

25. Kriptografi dalam Kehidupan Sehari-hari

25.1 Kartu Cerdas (*Smart Card*)

- Salah satu aplikasi PKI yang tumbuh sangat pesat adalah kartu cerdas. Kartus cerdas yang mirip dengan kartu kredit dapat melayani banyak fungsi, mulai dari otentikasi sampai penyimpanan data.



Smart Card
The smart card completely replaces keys for functions like door locking, ignition switch, immobilization and exterior locks. In addition to these security features, it can performs tasks such as personalized seat, mirror and cilmate adjustments.

- Kartu cerdas yang paling populer adalah *memory card* dan *microprocessor card*. *Memory card* mirip dengan *floppy disk*, sedangkan *microprocessor card* mirip dengan komputer kecil dengan sistem operasi, sekuriti, dan penyimpanan data.

- Kartu cerdas mempunyai beberapa jenis antarmuka (*interface*) yang berbeda. Jenis antarmuka yang umum adalah *contact interface*, yang dalam hal ini kartu cerdas dimasukkan ke dalam alat pembaca (*card reader*) dan secara fisik terjadi kontak fisik antara alat dan kartu.

- Kartu cerdas menyimpan kunci privat, sertifikat digital, dan informasi lainnya untuk mengimplementaiskan *PKI*. Kartu cerdas juga menyimpan nomor kartu kredit dan informasi kontak personal (no telpon). Sertifikat digital ditandatangani oleh *card issuer* (*CA*) untuk mensertifikasi kunci publik pemilik kartu.

- Penggunaan kartu cerdas dikombinasikan dengan *PIN* (*Personal Identification Number*). Jadi, ada dua level yang harus dari penggunaan kartu cerdas, yaitu memiliki kartu cerdas itu sendiri dan mengetahui *PIN* yang mengakses informasi yang disimpan di dalam kartu.

- Komputer *server* mengotentikasi kartu dengan cara mengirimkan suatu nilai atau *string* (yang disebut *challenge*) ke kartu untuk ditandatangani dengan menggunakan kunci privat (yang tersimpan di dalam kartu), lalu tanda-tangan tersebut diverifikasi oleh mesin dengan menggunakan kunci publik pemilik kartu.

- Komputer *server* perlu menyimpan kunci publik *card issuer* untuk memvalidasi sertifikat digital.

- Banyak peralatan *mobile* yang menggunakan kartu cerdas untuk otentikasi. Namun kartu cerdas masih tidak menjamin keamanan secara total. Jika peralatan *mobile* hilang atau dicuri, sertifikat digital dan kunci privat di dalam kartu cerdas (yang terdapat di dalam peralatan tersebut) berpotensi diakses oleh pencuri untuk mengakses informasi rahasia.

- Telpon seluler dengan teknologi *GSM* memiliki kartu cerdas yang terintegrasi di dalam *handphone.* Pemilik *handphone* memiliki opsi untuk men-set *PIN* untuk proteksi tambahan, sehingga jika *handphone* hilang atau dicuri, *handphone* tidak dapat digunakan tanpa mengetahui *PIN* tersebut.

- Kartu cerdas *Wireless Identity Module* (*WIM*) termasuk di dalam *Wireless Application Protocol* (*WAP*). Kartu *WIM* memproteksi komunikasi dan transaksi *mobile* dengan tanda-tangan digital. Kartu *WIM* menyediakan keamanan untuk sertifikat digital, manajemen kode *PIN*, kunci, dan tanda-

tangan digital. *WIM* menyimpan algoritma enkripsi yang diperlukan di daam kartu cerdas. Semua fungsi yang diperlukan untuk sistem *PKI* dimasukkan ke dalam karu cerdas.

- Dengan menggunakan kartu cerdas, pengguna dapat mengakses informasi dari berbagai peralatan dengan kartu cerdas yang sama.

25.2 Transaksi lewat Anjungan Tunai mandiri (ATM)

- Anjungan Tunai Mandiri atau *Automatic Teller Machine* (*ATM*) digunakan nasabah bank untuk melakukan transaski perbankan. Utamanya, kegunaan *ATM* adalah untuk menarik uang secara tunai (*cash withdrawal*), namun saat ini *ATM* juga digunakan untuk transfer uang (pemindahbukuan), mengecek saldo, membayar tagihan kartu ponsel, membeli tiket kereta api, dan sebagainya.

- Transaksi lewat *ATM* memerlukan kartu magnetik (disebut juga kartu *ATM*) yang terbuat dari plastik dan kode *PIN* (*Personal Information Number*) yang berasosiasi dengan kartu tersebut.

- *PIN* terdiri dari 4 angka yang harus dijaga kerahasiannya oleh pemilik kartu *ATM*, sebab orang lain yang mengetahui *PIN* dapat menggunakan kartu *ATM* yang dicuri atau hilang untuk melakukan penarikan uang.

- *PIN* digunakan untuk memverifikasi kartu yang dimasukkan oleh nasabah di *ATM*. Proses verifikasi dilakukan di komputer pusat (*host*) bank, oleh karena itu harus ada komunikasi dua arah antara *ATM* dan komputer *host. ATM*

mengirim *PIN* dan informasi tambahan pada kartu ke komputer *host*, *host* melakukan verifikasi dengan cara membandingkan *PIN* yang di-*entry*-kan oleh nasabah dengan *PIN* yang disimpan di dalam basisdata komputer *host*, lalu mengirimkan pesan tanggapan ke *ATM* yang menyatakan apakah transaksi dapat dilanjutkan atau ditolak.

- Selama transmisi dari *ATM* ke komputer *host*, *PIN* harus dilindungi dari penyadapan oleh orang yang tidak berhak.

- Bentuk perlindungan yang dilakukan selama transmisi adalah dengan mengenkripsikan *PIN*. Di sisi bank, *PIN* yang disimpan di dalam basisdata juga dienkripsi.

- Algoritma enkripsi yang digunakan adalah *DES* dengan mode *ECB*. Karena *DES* bekerja dengan mengenkripsikan blok 64-bit, maka *PIN* yang hanya terdiri dari 4 angka (32 bit) harus ditambah dengan *padding bits* sehingga panjangnya menjadi 64 bit. *Padding bits* yang ditambahkan berbeda-beda untuk setiap *PIN*, bergantung pada informasi tambahan pada setiap kartu *ATM*-nya.

- Karena panjang *PIN* hanya 4 angka, maka peluang ditebak sangat besar. Seseorang yang memperoleh kartu *ATM* curian atau hilang dapat mencoba semua kemungkinan kode *PIN* yang mungkin, sebab hanya ada $10 \times 10 \times 10 \times 10 = 10.000$ kemungkinan kode *PIN* 4-angka.

  Untuk mengatasi masalah ini, maka kebanyakan *ATM* hanya membolehkan peng-*entry*-an *PIN* maksimum 3 kali, jika 3 kali tetap salah maka *ATM* akan 'menelan' kartu *ATM*. Masalah ini juga menunjukkan bahwa kriptografi tidak selalu dapat menyelesaikan masalah keamanan data.

- Beberapa jaringan *ATM* sekarang menggunakan kartu cerdas sehingga memungkinkan penggunaan kriptografi kunci publik. Kartu *ATM* pengguna mengandung kunci privat dan sertifikat digital yang ditandatangani oleh *card issuer* (*CA*) untuk mensertifikasi kunci publiknya. *ATM* mengotentikasi kartu dengan cara mengirimkan suatu *string* ke kartu untuk ditandatangani dengan menggunakan kunci privat, lalu tanda-tangan tersebut diverifikasi oleh *ATM* dengan menggunakan kunci publik pemilik kartu.

- Seperti semua sistem yang berbasis sertifikat digital, terminal *ATM* perlu memiliki salinan kunci publik *card issuer* dengan maksud untuk memvalidasi sertifikat digital. Hal ini direalisasikan dengan menginstalasi kunci publik tersebut ke dalam mesin *ATM*.

25.3 *Pay TV*

- *Pay TV* adalah siaran TV yang hanya dapat dinikmati oleh pelanggan yang membayar saja, sedangkan pemilik TV yang tidak berlangganan tidak dapat menikmati siarannya.

- Siaran *Pay TV* dipancarkan secara *broadcast*, namun hanya sejumlah pesawat TV yang berhasil menangkap siaran tersebut yang dapat 'mengerti' isinya.

- Pada sistem *Pay TV*, sinyal *broadcast* dienkripsi dengan kunci yang unik. Orang-orang yang berlangganan *Pay* TV pada dasarnya membayar untuk mengetahui kunci tersebut.

- Bagaimana mengetahui bahwa kunci tersebut dimiliki oleh pelanggan yang sah, dan bukan orang yang mengetahui kunci tersebut dari pelanggan lainnya?

  Solusi yang umum adalah setiap pelanggan diberikan kartu cerdas (*smart card*) yang mengandung kunci privat (*private key*) yang unik dalam konteks algoritma kriptografi kunci-publik.

- Kartu cerdas dimasukkan ke dalam *card reader* yang dipasang pada pesawat TV. Selanjutnya, pelanggan *Pay* TV dikirimi kunci simetri yang digunakan untuk mengenkripsi siaran. Kunci simetri ini dikirim dalam bentuk terenkripsi dengan menggunakan kunci publik pelanggan. *Smart card* kemudian mendekripsi kunci simetri ini dengan kunci privat pelanggan. Selanjutnya, kunci simetri digunakan untuk mendekripsi siaran TV.

25.4 Komunikasi dengan Telepon Seluler (*GSM mobile phone*)

- Penggunaan telepon seluler (ponsel) yang bersifat *mobile* memungkinkan orang berkoumunikasi dari tempat mana saja.

- Telepon seluler bersifat nirkabel (*wireless*), sehingga pesan yang dikirim dari ponsel ditransmisikan melalui gelombang mikro (*microwave*) atau radio sampai ia mencapai *base station* (*BST*) terdekat, selanjutnya ditransfer ke ponsel penerim.

- *GSM* merupakan teknologi telepon seluler yang paling banyak digunakan di seluruh dunia.

- Karena menyadap sinyal radio jauh lebih mudah daripada menyadap sinyal pada saluran kabel, maka ini berarti *GSM* tidak lebih aman daripada telepon *fixed* konvensional.

- Untuk membuat komunikasi lewat ponsel aman, maka pesan dienkripsi selama transmisi dari ponsel ke *BST* terdekat. Metode enkripsi yang digunakan adalah metode *cipher* aliran (*stream cipher*).

- Masalah keamanan lain adalah identitas penelpon. Operator seluler harus dapat mengidentifikasi suatu panggilan (*call*) dan mengetahui identitas penelpon (apakah penelpon merupakan pengguna/pelanggan dari operator seluler tersebut atau pengguna/pelanggan dari operator lain).

- Jadi, pada *GSM* diperlukan dua kebutuhan keamanan lainnya, yaitu:
  1. otentikasi penelpon (*user authentication*), yang merupakan kebutuhan bagi sistem,

2. kerahasiaan (*confidentiality*) pesan (data atau suara), yang merupakan kebutuhan bagi pelanggan,

- Dua kebutuhan ini dipenuhi dengan penggunaan kartu cerdas (*smart card*) personal yang disebut kartu *SIM* (*Subscriber Identity Module card*). Kartu *SIM* berisi:
  1. identitas pelanggan/pengguna operator seluler berupa *IMSI* (*International Mobile Subscriber Identity*) yang unik nilainya,
  2. kunci otentikasi rahasia sepanjang 128-bit yang diketahui hanya oleh operator. Nilai ini digunakan sebagai kunci pada protokol otentikasi dengan menggunakan program enkripsi yang dipilih oleh operator (algoritma *A2*, *A3*, atau *A5*).
  3. *PIN* (jika di-set oleh pengguna)
  4. Program enkripsi.

- Secara keseluruhan, sistem keamanan *GSM* terdiri atas dalam 3 komponen, yaitu:
  1. Kartu *SIM*
  2. *Handset* (pesawat telepon seluler)
  3. Jaringan *GSM* (seperti jaringan *ProXL*, *Simpati*, *IM3*). Setiap jaringan dioperasikan oleh operatornya masing-masing (*Excelcomindo*, *Telkomsel*, *Satelindo*). Komputer operator (*host*) memiliki basisdata yang berisi identitas (*IMSI*) dan kunci otentikasi rahasia semua pelanggan/pengguna *GSM*.

Otentikasi Penelpon

- Otentikasi penelpon dilakukan melalui protokol otentikasi dengan mekanisme *challenge – response*.

- Ketika pengguna ponsel melakukan panggilan (*call*), identitasnya dikirim ke komputer operator via *BST* untuk keperluan otentikasi.

  Karena *BST* tidak mengetahui kunci otentikasi kartu *SIM*, dan bahkan tidak mengetahui algoritma otentikasi, maka komputer operator melakukan verifikasi pengguna dengan cara mengirimkan suatu nilai acak (128 bit) yang disebut *challenge* ke *SIM card* penelpon.

- Kartu *SIM* mengeluarkan *response* dengan cara mengenkripsi *challenge* 128-bit tersebut dengan menggunakan kunci otentikasi yang terdapat di dalam kartu.

- Enkripsi terhadap *challenge* menghasilkan keluaran 128-bit; dari 128-bit keluaran ini hanya 32 bit yang dikirim dari kartu *SIM* ke *BST* sebagai *response*. *BST* meneruskan *response* ke komputer operator.

  Ketika *response* sampai di komputer operator, komputer operator melakukan perhitungan yang sama dengan yang dilakukan oleh kartu *SIM*; yang dalam hal ini komputer mengenkripsi *challenge* yang dikirim tadi dengan menggunakan kunci otentikasi penelpon (ingat, komputer operator mengetahui kunci otentikasi semua kartu *SIM*), lalu membandingkan hasil enkripsi ini (yang diambil hanya 32 bit) dengan *response* yang ia terima. Jika sama, maka otentikasi berhasil, dan penelpon dapat melakukan percakapan.

- Sebagaimana dijelaskan di atas, dari 128-bit hasil enkripsi, hanya 32 bit yang dikirim sebagai *response*. Jadi, masih ada 96 bit sisanya yang hanya diketahui oleh kartu *SIM*, *BST*, dan komputer operator.

Kerahasiaan Pesan

- *SIM card* juga berisi program *stream cipher* (algoritma *A5*) untuk mengenkripsi pesan dari ponsel ke *BST*. Kunci enkripsi panjangnya 64 bit, yang diambil dari 96 bit sisa dari *response SIM card*. Perhatikan bahwa kunci enkripsi 64-bit ini berbeda setiap kali proses otentikasi dilakukan (mengapa?). Hal ini memenuhi prinsip algoritma *OTP* (*one-time pad*).