PERTEMUAN 09

KRIPTOGRAFI DALAM KEHIDUPAN SEHARI-HARI

SUB PEMBAHASAN

- ✓ Kartu Cerdas (Smart Card)
- ✓ Transaksi Lewat Anjungan Tunai Mandiri (ATM)
- ✓ Pay TV
- ✓ Komunikasi dengan Telepon Seluler
- ✓ E-commerce di Internet dan SSL
- ✓ Pengamanan E-mail dengan PGP (Pretty Good Privacy)

Kartu Cerdas

- ✓ Kartu cerdas yang mirip kartu kredit dapat melayani banyak fungsi, mulai dari otentikasi sampai penyimpanan data.
- ✓ 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

- ✓ 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

- ✓ 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.

Kartu Cerdas

- ✓ 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.

Kartu Cerdas

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

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

ATM

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

ATM

- ✓ 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 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

PAY TV

- ✓ PayTV adalah siaran TV yang hanya dapat dinikmati oleh pelanggan yang membayar saja, sedangkan pemilik TV yang tidak berlangganan tidak dapat menikmati siarannya.
- ✓ Siaran PayTV dipancarkan secara broadcast, namun hanya sejumlah pesawat TV yang berhasil menangkap siaran tersebut yang dapat ‘mengerti’ isinya.
- ✓ Pada sistem PayTV, sinyal broadcast dienkripsi dengan kunci yang unik. Orang-orang yang berlangganan Pay TV pada dasarnya membayar untuk mengetahui kunci tersebut.

PAY TV

- ✓ 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.

PAY TV

- ✓ 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.

KOMUNIKASI TELP SELULAR

- ✓ 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.

KOMUNIKASI TELP SELULAR

- ✓ 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)
- ✓ Pada GSM diperlukan dua kebutuhan keamanan yaitu:
  1. Otentikasi penelpon (user authentication), yang merupakan kebutuhan bagi sistem.
  2. Kerahasiaan (confidentiality) pesan (data atau suara), yang merupakan kebutuhan bagi pelanggan.

KOMUNIKASI TELP SELULAR

Dua kebutuhan ini dipenuhi dengan penggunaan kartu cerdas (smart card) personal yang disebut kartu SIM(Subscriber Identity Modulecard). 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.
3. Pin (jika di-set oleh pengguna)
4. Program enkripsi.

KOMUNIKASI TELP SELULAR

Secara keseluruhan, sistem keamanan GSM terdiri atas dalam 3 komponen, yaitu:

1. Kartu SIM
2. Handset (pesawat telepon seluler)
3. Jaringan GSM

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.'

E-Commerce di Internet

- ✓ Sekarang banyak orang berbelanja melalui *web* di internet.
- ✓ Pembayaran barang dilakukan dengan menggunakan kartu kredit, yang berarti bahwa pembeli harus mengirimkan kode PIN kartu kredit dan informasi lainnya melalui internet.
- ✓ *Browsing web* secara aman adalah fitur paling penting pada *e-commerce*.
- ✓ *Secure Socket Layer* (SSL) adalah protokol yang digunakan untuk *browsing web* secara aman.
- ✓ Protokol ini memfasilitasi penggunaan enkripsi untuk data yang rahasia dan membantu menjamin integritas informasi yang dipertukarkan antara *website* dan *web brwoser* (misalnya *Netscape*, *Interner Explorer*, dsb).

E-Commerce di Internet

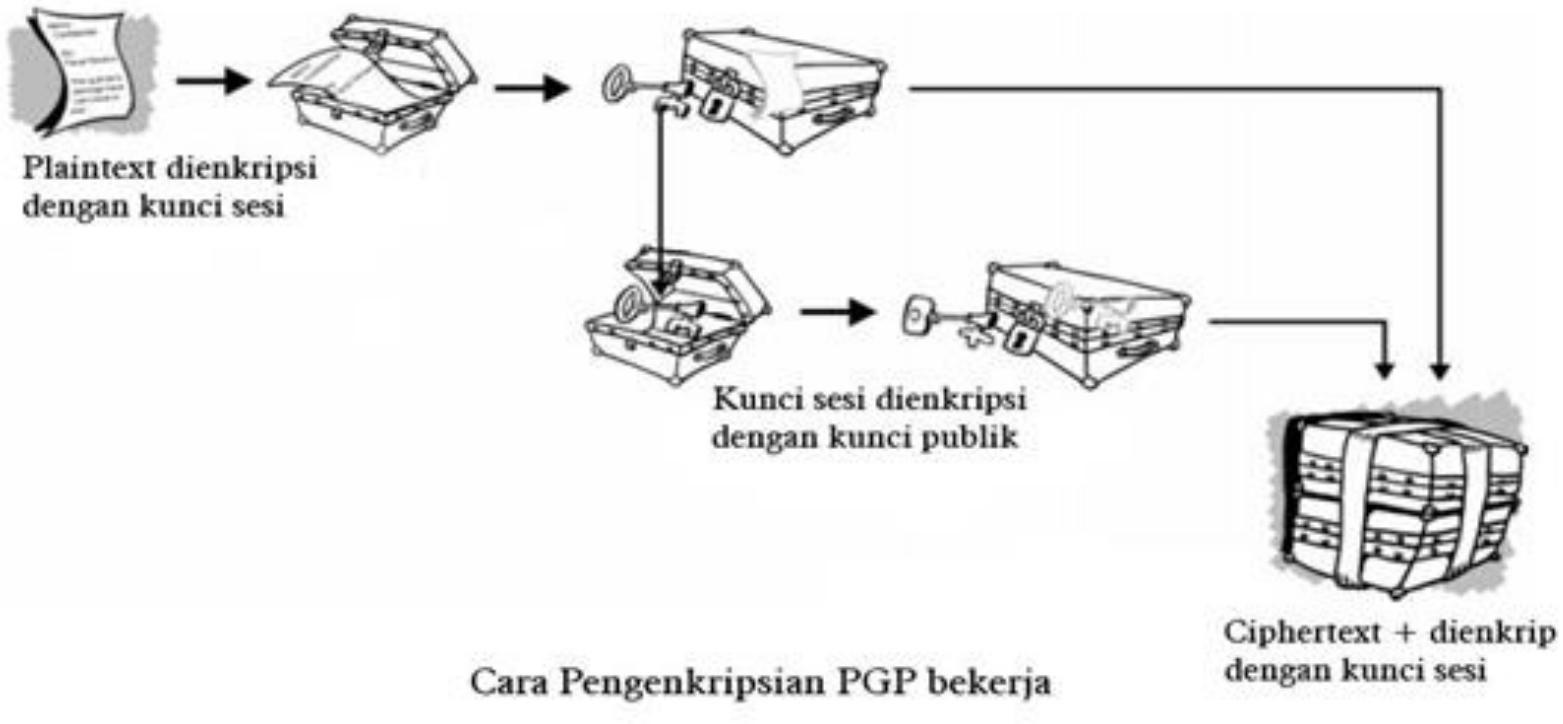
- ✓ SSL adalah contoh protokol *client-server*, yang dalam hal ini *web browser* adalah *client* dan *website* adalah *server*.
- ✓ *Client* yang memulai komunikasi, sedangkan *server* memberi respon terhadap permintaan *client*.
- ✓ Fungsi paling dasar yang digunakan SSL adalah membentuk saluran untuk mengirimkan data terenkripsi, seperti data kartu kredit, dari *browser* ke *website* yang dituju

Pengamanan E-mail dengan PGP (Pretty Good Privacy)

- ✓ *Pretty Good Privacy* disebut (PGP) adalah Suatu metode program enkripsi informasi yang memiliki tingkat keamanan cukup tinggi bersifat rahasia dengan menggunakan “Private-Public Key” sebagai dasar autentifikasinya sehingga jangan sampai dengan mudah diketahui oleh orang lain yang tidak berhak.
- ✓ PGP dikembangkan oleh Phill Zimmermann pada akhir tahun1980
- ✓ PGP merupakan program yang digunakan untuk mengenkripsi satu atau lebih dokumen.
- ✓ Dengan PGP, hanya orang – orang tertentu saja yang bisa membaca file – file enkripsi tersebut.

- ✓ Bagaimana PGP sebagai program enkripsi dokumen bisa digunakan untuk pengiriman e-mail?
- ✓ Program PGP mengenkripsi isi mail yang kita tulis menjadi sebuah file. File tersebut dibaca oleh program mail yang kemudian dikirimkan ke tujuan.
- ✓ Penerima e-mail harus menyimpan mail tersebut ke dalam sebuah file. File tersebut dideskripsi sehingga isi mail aslinya akan terlihat
- ✓ Jadi, mail yang dikirimkan adalah dalam bentuk terenkripsi sehingga tidak dapat dibaca dengan mudah oleh orang – orang yang tidak memiliki akses membaca mail tersebut.

Prinsip Kerja PGP



Cara Pengenkripsian PGP bekerja

Cara Kerja Enkripsi PGP

Prinsip – prinsip kerja dari PGP

1. PGP menggunakan teknik yang disebut Public-key encryption dengan dua kode yang saling berhubungan secara intrinsik, namun tidak mungkin untuk memecahkan satu dan yang lainnya.
2. Jika membuat suatu kunci, secara otomatis akan dihasilkan sepasang kunci yaitu public key dan secret key.
3. PGP menggunakan dua kunci yaitu kunci public (proses enkripsi) dan privet (proses deskripsi).
4. Menggunakan dua kuci tersebut dikarenakan adanya conventional crypto, disaat terjadi transfer informasi kunci, suatu secure channel diperlukan.

Daftar Pustaka

- Nandang Iriadi. Analisis Keamanan E-mail Menggunakan Pretty Good Privacy. 2011. https://ejournal.bsi.ac.id/ejurnal/index.php/paradigma/article/view/3422.
- Alamsyah. Implementasi Keamanan E-mail Dengan Menggunakan Pgptray. 2011. Majalah Ilmiah Mektek.