KONSEP KEAMANAN E-Commerce

Riya Widayanti
riyawidayanti@yahoo.com

ABSTRAK

Pentingnya keamanan dan kerahasiaan transaksi perniagaan ini bukan saja dengan media internet, namun juga pada media komunikasi lainnya. Jika wireless network (jaringan komunikasi udara tanpa kabel) ingin digunakan untuk transaksi perdagangan, maka tentu harus dilakukan pengamanan komunikasi yang memadai. Lagipula sebaiknya setiap transaksi perdagangan perlu diamankan ? Artinya, dengan menggunakan jaringan privatpun, sebaiknya ada langkah-langkah pengamanan data (terutama jika tidak mempercayai keamanan penyedia jaringan privat itu)

Kata Kunci : *Cryptography*, Enkripsi, Dekripsi

PENDAHULUAN

Ada beberapa transaksi yang perlu diamankan, sebagai contoh : transaksi penjualan online, transaksi keuangan, e-mail, file transer, tanda tangan suatu kontrak dalam bentuk digital, informasi dari perusahaan untuk publik (sehingga tidak bisa diubah-ubah orang lain), dan transaksi bisnis lainnya.

Teknologi dasar yang dipergunakan dalam pengamanan data untuk e-commerce, yakni kriptografi dengan fokus pada :

- *cryptography* (kriptografi)

PEMBAHASAN

1. Konsep Dasar Kriptografi

Kriptografi, sebagai batu bata utama untuk keamanan *e-commerce* : ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim pengirim dapat disampaikan kepada penerima dengan aman. Sifat-sifat dalam kriptografi meliputi :

1. kerahasiaan (confidential) dari pesan dijamin dengan melakukan enkripsi (penyandian), sehingga pesan yang telah disandikan itu tidak dapat dibaca oleh orang-orang yang tidak berhak.
2. Keutuhan (integrity) dari pesan, sehingga saat pesan itu dikirimkan tidak ada yang bisa mengutak-atik ditengah jalan. Sebagai contoh, dalam suatu transaksi pembayaran, sang pengirim pesan berkepentingan agar nilai cek digital sebesar Rp. 1.000.000,- tidak diubah orang lain menjadi Rp. 10.000.000,- ditengah jalan.
3. Jaminan atas identitas dan keabsahan (authenticity) jati diri dari pihak-pihak yang melakukan transaksi. Sekedar ilustrasi, dari sisi konsumen, harus ada jaminan bahwa www.ibu-dibyo.co.id adalah benar benar *ticket office* milik ibu dibyo di Cikini. Sebaliknya, seorang pedagang di internet juga perlu mengetahui apakah seorang konsumen

yang sedang berbelanja di websitenya benar-benar menggunakan kartu kredit miliknya sendiri.
4. Transaksi dapat dijadikan barang bukti yang tidak bisa disangkal (non repudiation) jika terjadi sengketa atau perselisihan pada transaksi elektronik yang telah terjadi.

Dalam kriptografi, ada dua proses utama :

1. Enkripsi (*encryption*) : yakni proses untuk mengubah pesan asli (plain text) menjadi pesan yang tersandikan atau pesan yang terrahasiakan (cipher text)
2. Dekripsi (*decryption*) : yakni proses mengubah pesan yang tersandikan (cipher text) kembali menjadi pesan pada bentuk aslinya (plain text).
    - *Key*
    - *Plain text*
    - *Cipher text*
    - *Plain text*

Proses enkripsi dan dekripsi

Proses enkripsi dan dekripsi mengunakan kunci (*key*). Jadi meskipun penyerang (*hacker*) mengetahui secara tepat algoritma enkripsi dan dekripsinya, namun jika penyerang itu tidak memiliki kunci yang tepat , maka penyerang itu tidak bisa menjebol saluran komunikasi antara pengirim dan penerima.

2. Kriptografi Kunci Simetrik

Ini adalah jenis kriptografi yang paling umum dipergunakan. Kunci untuk membuat pesan yang disandikan sama dengan kunci untuk membuka pesan yang disandikan itu. Jadi pengirim pesan dan penerima pesan harus memiliki kunci yang sama persis . Siapapun yang memiliki kunci tersebut termasuk pihak-pihak yang tidak diinginkan dapat membuat dan membongkar rahasia cipher text . Problem yang paling jelas disini terkadang bukanlan masalah Encryption dan Decryption pengiriman ciphertextnya , melainkan *masalah bagaimana meyampaikan kunci simetris rahasia tersebut kepada pihak yang diinginkan*. Dengan kata lain ada masalah *pendistribusian kunci rahasia.*
Contoh : algoritma kunci Simetris yang terkenal adalah DES (data encryption standart), TripleDES, IDEA, Blowfish, Twofish, AES (advanced encryption standard) dan RC-4.

3. Kriptografi kunci publik / kunci asimetrik

Teknik kriptografi kunci publik mencoba menjawab permasalahan pendistribusian kunci pada teknologi kriptografi kunci simetrik. Dalam kriptografi kunci publik, setiap pihak memiliki sepasang kunci :

1. Sebuah kunci publik yang didistribusikan kepada umum/ khalayak ramai.
2. Sebuah kunci privat yang harus disimpan dengan rahasia dan tidak boleh diketahui orang lain.

Dalam ilustrasi yang akan dijabarkan nanti, guna mempermudah penjelasan kita akan menggunakan beberapa nama ganti orang yakni **Anto, Badu, Chandra** dan **Deni** untuk mempresentasikan pihak-pihak yang melakukan transaksi.

Ada dua kegunaan mendasar dari setiap pasangan kunci privat :

1. Membungkus pesan sehingga kerahasiaannya terjamin . Siapapun Anto, Chandra dan Deni dapat mengirim pesan rahasia kepada Badu dengan cara mengenkripsi pesan asli (plain text) dengan kunci publik milik

Badu. Karena yang memiliki pasangan kunci
Enkripsi dan Dekripsi. Maka tentu yang bisa membuka pesan rahasia hanyalah Badu.

2. Menandatangani pesan untuk menjaga keotentikan pesan. Jika Anto hendak menandatangani suatu pesan , maka Anto akan menggunakan kunci privatnya untuk membuat tanda tangan digital. Semua orang lainnya (Badu, Chandra , Deni) bisa memeriksa tanda tangan itu jika memiliki kunci publik Anto.

4. Fungsi *Hash* Satu Arah

Fungsi *hash* berguna untuk menjaga keutuhan (*integrity*) dari pesan yang dikirimkan. Bagaimana jika Anto mengirimkan surat pembayaran kepada Badu sebesar 1 juta rupiah, namun ditengah jalan Maman (yang ternyata berhasil membobol sandi entah dengan cara apa) membubuhkan angka 0 lagi dibelakangnya sehingga menjadi 10 juta rupiah ? Dimana dari pesan tersebut harus utuh, tidak diubah-ubah oleh siapapun, bahkan bukan hanya oleh Maman , namun juga termasuk oleh Anto, Badu dan gangguan pada transmisi pesan (*noise*). Hal ini dapat dilakukan dengan fungsi hash satu arah (*one way hash function*), yang terkadang disebut sidik jari (*fingerprint*), *hash, message integrity check* , atau *manipulation detection code.*

Saat Anto hendak mengirimkan pesannya, dia harus membuat sidik jari dari pesan yang akan dikirim untuk Badu. Pesan (yang besarnya dapat bervariasi) yang akan di hash disebut *pre-image*, sedangkan outputnya yang memiliki ukurannya tetap, disebut hash value (nilai hush).

Kemudian , melalui saluran komunikasi yang aman, dia mengirimkan sidik jarinya kepada Badu. Setelah Badu menerima pesan si Anto tidak peduli lewat saluran komunikasi yang mana, Badu kemudian juga membuat sidik jari dari pesan yang telah diterimanya dari Anto.

Kemudian Badu membandingkan sidik jari yang dibuatnya dengan sidik jari yang diterimanya dari Anto. Jika kedua sidik jari itu identik, maka Badu dapat yakin bahwa pesan itu tidak diubah-ubah sejak dibuatkan sidik jari yang diterima dari Badu. Jika pesan pembayaran 1 juta rupiah itu diubah menjadi 10 juta rupiah, tentunya akan menghasilkan nilai *Hash* yang berbeda.

5. Membuat sidik jari pesan

Untuk membuat sidik jari tersebut tidak dapat diketahui oleh siapapun, sehingga siapapun tidak dapat memeriksa keutuhan dokumen atau pesan tertentu. Tak ada algoritma rahasia dan umumnya tak ada pula kunci rahasia. Jaminan dari keamanan sidik jari berangkat dari kenyataan bahwa hampir tidak ada dua pre-image yang memiliki *hash value* yang sama. Inilah yang disebut dengan sifat *collision free* dari suatu fungsi *hash* yang baik. Selain itu , sangat sulit untuk membuat suatu pre-image jika hanya diketahui *hash* valuenya saja.

Contoh algoritma fungsi *hash* satu arah adalah MD-4, MD-5 dan SHA .

Message authentication code (MAC) adalah satu variasi dari fungsi hash satu arah, hanya saja selain *pre-image* , sebuah kunci rahasia juga menjadi input bagi fungsi MAC.

6. Tanda Tangan digital

Badu memang dapat merasa yakin bahwa sidik jari yang datang bersama pesan yang diterimanya memang berkorelasi. Namun bagaimana Badu dapat merasa yakin bahwa pesan itu berasal dari Anto ? Bisa saja saat dikirimkan oleh Anto melalui saluran komunikasi yang tidak aman, pesan tersebut diambil oleh Maman. Maman kemudian mengganti isi pesan tadi, dan membuat lagi sidik jari dari pesan yang baru diubahnya itu. Lalu, Maman mengirimkan lagi pesan beserta sidik jarinya itu kepada Badu, seolah-olah dari Anto. Untuk mencegah pemalsuan, Anto membubuhkan tanda tangannya pada pesan tersebut. Dalam dunia elektronik, Anto membubuhkan tanda tangan digital pada pesan yang akan dikirimkan untuk Badu, sehingga Badu dapat merasa yakin bahwa pesan itu memang dikirim Anto.

Sifat yang diinginkan dari tanda tangan digital diantaranya adalah :

1. Tanda tangan asli (otentik), tidak mudah ditulis/ ditiru oleh orang lain.
   Pesan dan tanda tangan pesan tersebut juga dapat menjadi barang bukti sehingga penandatangan tidak bisa menyangkal bahwa dulu ia tidak pernah menandatanganinya.
2. Tanda tangan itu hanya sah untuk dokumen (pesan) itu saja .
   Tanda tangan itu tidak bisa dipindahkan dari suatu dokumen ke dokumen lainnya .Ini juga berarti bahwa jika dokumen itu diubah, maka tanda tangan digital dari pesan tersebut tidak sah lagi.
3. Tanda tangan itu dapat diperiksa dengan mudah.
4. Tanda tangan itu dapat diperiksa oleh pihak-pihak yang belum pernah bertemu dengan penandatangan.
5. Tanda tangan itu juga sah untuk kopi dari dokumen yang sama persis.

Meskipun ada banyak skenario, ada baiknya kita perhatikan salah satu skenario yang cukup umum dalam penggunaan tanda tangan digital .

Tanda tangan digital memanfaatkan fungsi hash satu arah untuk menjamin bahwa tanda tangan itu hanya berlaku untuk dokumen yang bersangkutan saja. Bukan dokumen tersebut secara keseluruhan yang ditandatangani, namun biasanya yang ditandatangani adalah sidik jari dari dokumen itu beserta ***time stamp***-nya dengan menggunakan kunci privat. *Time stamp* berguna ***untuk berguna untuk menentukan waktu pengesahan dokumen***.

7. Pembuatan tanda tangan digital

Keabsahan tanda tangan digital itu dapat diperiksa oleh Badu. Pertama-tama Badu membuat lagi sidik jari dari pesan yang diterimanya. Lalu Badu mendekripsi tanda atangan digital Anto untuk mendapatkan sidik jari yang asli. Badu lantas membandingkan kedua sidik jari tersebut. Jika kedua sidik jari tersebut sama, maka dapat diyakini bahwa pesan tersebut ditandatangani oleh Anto.

- Enkripsi
- Sidik Jari
- Kunci Privat
- Anto
- Tanda tangan Digital Anto

8. Panjang kunci dan keamanannya

Pembobolan kunci mungkin saja terjadi. Besar kecilnya kemungkinan ini ditentukan oleh panjangnya kunci. Semakin panjang kunci semakin sulit pula untuk membobolnya dengan *brute force attack.*

9. *Key Backup & Recovery*

Tujuan dari adanya kriptografi adalah memberikan proteksi kerahasiaan pada data. Dengan kritografi kunci publik, kerahasiaan terjamin karena kunci privat yang dipergunakan untuk proses deskripsi digital, hanya diketahui oleh pemilik kunci privat yang sah.

Ada beberapa hal yang bisa memaksa kunci privat juga diback up oleh pihak ketiga yang dipercaya (trusted third party/ TTP), misalnya : kunci privatnya yang ada dalam harddisk, secara tidak sengaja sengaja terhapus, smart card yang dipergunakannya hilang atau rusak, ada pegawai kantor yang mengenskripsi data-data penting perusahaan menggunakan kunci publiknya, sehingga saat pegawai kantor berhenti bekerja, perusahaan tidak bisa membuka data-data penting tersebut.

Perlu dicatat,bahwa yang dibackup oleh TTP hanya *private descrition key* (kunci privat yang dipergunakan untuk mendeskripsi pesan), bukan *private signing key* ,(kunci yang dipergunakan untuk membuat tanda tangan) . Hal ini disebabkan karena kalau yang di backup adalah pivate signing key, maka dikuatirkan terjadi pemalsuan tanda tangan.

Dalam kasus dimana private signing key-nya hilang, maka terpaksalah sertifikat yang berkaitan dibatalkan (di-revoke).

10. Time Stamping

Dalam bisnis, waktu terjadinya kesepakatan, kontrak atau pembuatan surat amatlah penting. Oleh karena itu, diperlukan suatu mekanisme khusus untuk menyediakan `waktu' yang terpercaya dalam infrastruktur kunci publik. Artinya,'waktu' tersebut tidak didapatkan dari `clock' setiap komputer, namun didapatkan dari satu sumber yang dipercaya. Penyedia jasa sumber `waktu' yang dipercaya, juga termasuk kategori TTP.

Waktu yang disediakan oleh *time stamp server* ,tidaklah harus tepat sekali, karena yang paling penting adalah waktu `relatif' dari suatu kejadian lain. Misalnya suatu transaksi *purchase order* terjadi sebelum transaksi *payment.*

Meskipun demikian ,memang lebih bagus kalau waktu yang bersumber dari *time stamp server* mendekati waktu resmi (dari Badan Meteorologi dan Geofisika/BMG).

KESIMPULAN

Perdagangan melalui internet tidak hanya penjual dan pembeli tetapi banyak peran yang ikut dalam terwujudnya e-commerce. Seperti : Jasa pengiriman atau pos, jasa jaringan perbankan internasional, Web Server (Penyedia Web site).

Jaminan yang diberikan Toko online bergantung pada perjanjian kerjasama antara toko dan jasa pengiriman, Dalam hal ini kita harus hati-hati dalam memilih atau mengakses online-shop pada saat membeli barang maupun jasa.

Pengiriman barang dari gudang perusahaan sampai ke pembeli bukan suatu hal yang sederhana, karena pengiriman lintas negara harus mengikuti aturan bea-cukai di negara pengirim maupun penerima. Oleh sebab itu jasa pengiriman barang ini menjadi sangat vital, karena membutuhkan jasa pengiriman yang cepat dan aman.

Seringkali cyber shop memberikan jaminan baik dalam hal produknya dan pengirimannya karena Pelayanan yang diberikan tidak jauh berbeda toko yang offline. Dan pelayanan terhadap konsumen merupakan hal yang terpenting dalam mencari pelanggan.

DAFTAR PUSTAKA

Martin James. 1990. Information Enggineering : Design & Construction. Book I, II, III. Prentice Hall Inc

Sammervile. 1989. Software Enggineering. Third Edition. Addison Wesley