KEAMANAN DALAM E-COMMERCE

Pendahuluan

- **Faktor keamanan:**
  - **pengelolaan dan penjagaan keamanan secara fisik**
  - **penambahan perangkat-perangkat elektronik (perangkat lunak dan perangkat keras) untuk melindungi data, sarana komunikasi serta transaksi**

Pilar Keamanan Sistem e-Commerce

- ***Authentication*** **(keabsahan pengirim)**
  - **Identitas pengguna/pengirim data teridentifikasi (tidak ada kemungkinan penipuan)**
- ***Confidentiality*** **(kerahasiaan data)**
  - **data tidak dapat dibaca oleh pihak yang tidak berhak**
- ***Integrity*** **(keaslian data)**
  - **data tidak dapat diubah secara tidak sah**
- ***Non-Repudiation*** **(anti-penyangkalan)**
  - **tidak ada penyangkalan pengiriman data (dari pihak penerima terhadap pihak pengirim)**

ANCAMAN KEAMANAN & SOLUSI

ANCAMAN	SOLUSI KEAMANAN	FUNGSI	TEKNOLOGI
Pencegatan data, pembacaan dan modifikasi data secara tidak sah	Enkripsi (Encryption)	Menyandikan data	Enkripsi simetrik (menggunakan kunci yang sama di sisi pengirim dan penerima) dan enkripsi asimetrik (menggunakan kunci yang berbeda di sisi pengirim dan penerima, misalnya enkripsi dg algoritma DES, RSA, PGP, dsb
Kecurangan (fraud) yang dilakukan oleh orang-orang yang identitasnya tidak diketahui	Otentikasi	Melakukan verifikasi thd identitas pengirim & penerima	Tanda tangan digital (digital signature)
Akses yg tidak sah oleh seseorang thd data milik orang lain.	Firewall	Menyaring serta melindungi lalu lintas data di jaringan atau di server	Firewall; jaringan maya pribadi

KRIPTOGRAFI

- Adalah Algoritma untuk proses keamanan komunikasi data dari pengintipan atau pembajakan oleh orang2 yg tdk berhak dg cara menyandikan data serta informasi yg dikirimkan.
- Algoritma kriptografi masa kini, sangat dimungkinkan dg hadirnya komputer2 yg memiliki prosesor berkinerja tinggi dan memiliki kemampuan pemrosesan data yg sangat tinggi, merupakan salah satu cara utk melakukan otentikasi thd pihak2 yg terlibat dalam perdagangan elektronik. Dlm hal ini metode yg digunakan adalah penyandian (enkripsi) data atau sering disebut sbg data encryption

KRIPTOGRAFI (2)

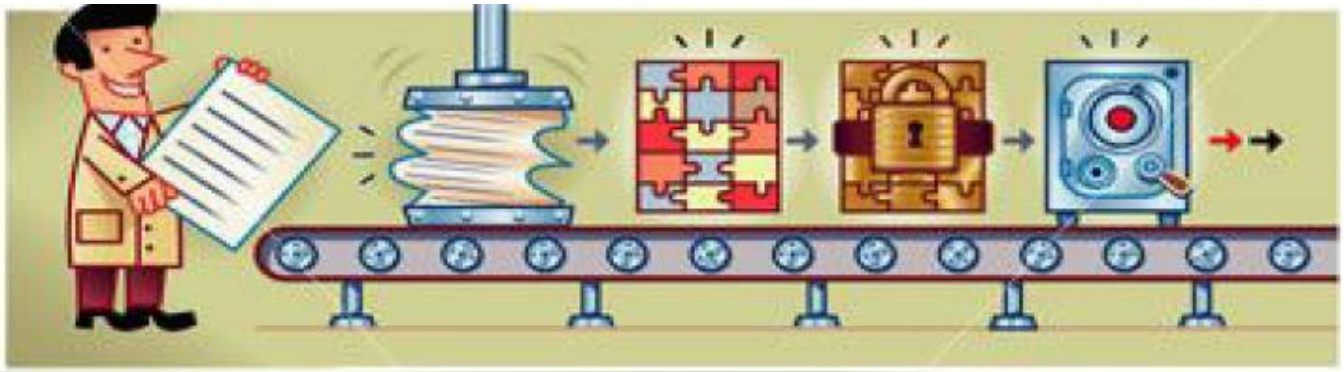
- Tiga sistem (algoritma) kriptografi asimetris, yaitu menggunakan kunci yg berbeda di sisi pengirim dan penerima, ada beberapa yg saat ini populer adalah :
  - Data Encryption Standard (DES)
  - Pretty Good Privacy (PGP)
  - Sistem Rivest, Shamir, Adleman (RSA)
- DES menggunakan kunci tunggal utk mengenkripsi dan dekripsi.
- RSA merupakan metode enkripsi yg populer menggunakan 2 kunci.

KRIPTOGRAFI (3)

- **PGP melakukan enkripsi dan membuat *digital signature pada file, melakukan dekripsi dan verifikasi pada file yang memiliki digital signature,* dan mengelola koleksi kunci PGP yang dimiliki.**

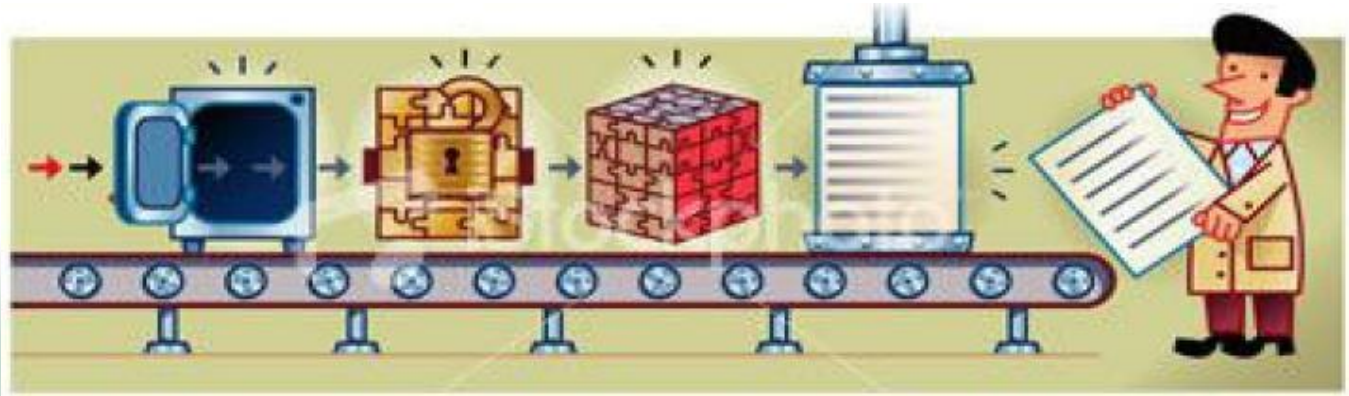
Enkripsi vs Dekripsi

Enkripsi berarti pengkodekan data ke format tertentu menggunakan kunci rahasia

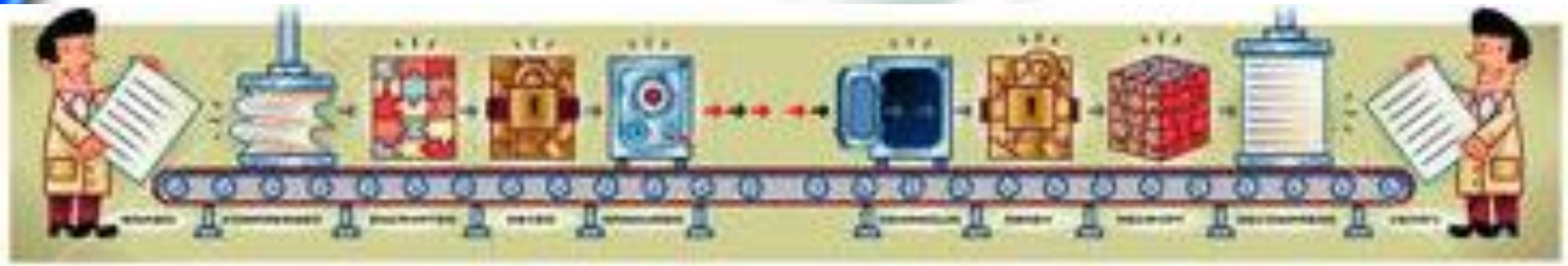


Enkripsi vs Dekripsi

- **Dekripsi mendekodekan data yang terenkripsi ke format asli**

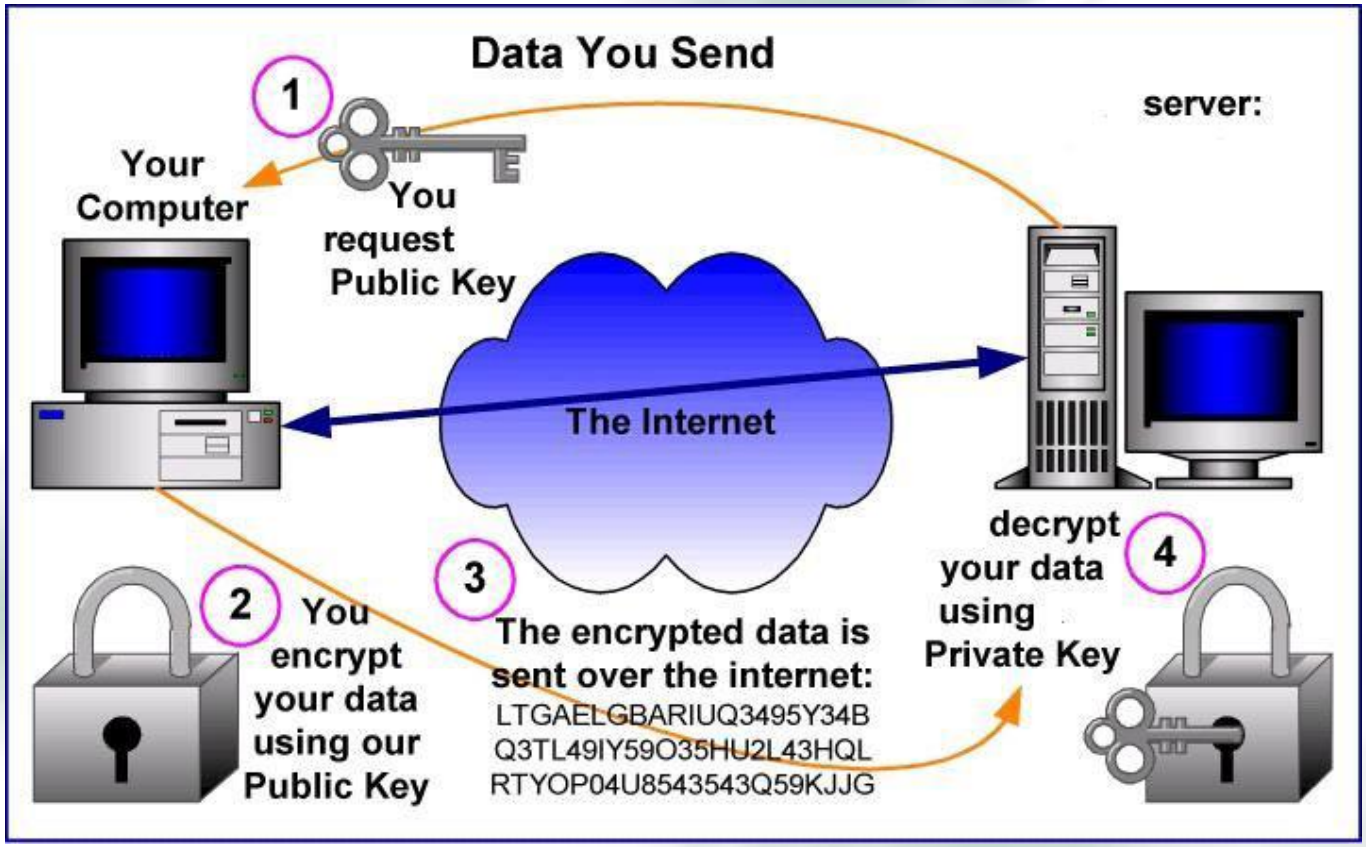


Enkripsi vs Dekripsi



Enkripsi vs Dekripsi

Contoh: Enkripsi RSA



Kelebihan dan Kelemahan berbagai sistem kriptografi

TIPE ENKRIPSI	KEUNGGULAN	KELEMAHAN
Kunci Simetrik	Cepat	Kunci di kedua sisi (pengirim dan penerima sama)
	Dapat dg mudah diimplementasikan di perangkat keras	Sukar untuk mendistribusikan kunci Tidak mendukung tanda tangan digital
Kunci Publik	Menggunakan 2 kunci yg berbeda	Lambat dan membutuhkan komputasi yg intensif
	Relatif mudah utk mendistribusikan kunci	
	Memungkinkan pemeliharaan integritas lewat tanda tangan digital	

Standar Keamanan di Internet

Standar	Fungsi	Aplikasi
Secure HTTP (S-HTTP)	Melindungi transaksi di Web	Browser, server Web, aplikasi internet
Secure Socket Layer (SSL)	Melindungi paket data pada lapisan jaringan	Browser, server Web, aplikasi internet
Secure MIME (S/MIME)	Melindungi lampiran email yang melintasi berbagai platform yang berbeda	Email dengan enkripsi RSA dan tanda tangan digital
Secure Wide-Area Nets (S/WAN)	Enkripsi antara firewall dan router	VPN – Virtual Private Network
Secure Electronic Transaction (SET)	Transaksi kartu kredit yang aman	Smartcard, server transaksi, e-Commerce

Standar Keamanan di Internet

- Keamanan untuk Aplikasi Web
  - S-HTTP dan SSL
- Keamanan untuk e-Mail
  - PEM, S/MIME, dan PGP
- Keamanan untuk Jaringan
  - Firewall

Standar Keamanan di Internet

Keamanan untuk Aplikasi Web:

- **S-HTTP**
  - **secara spesifik dirancang untuk mendukung protokol HTTP (Hypertext Transfer Protokol) dalam hal otorisasi dan keamanan dokumen**
- **SSL**
  - **Melindungi saluran komunikasi di antara 2 protokol bagian bawah dalam tumpukan protokol menurut standar TCP/IP.**
  - **Dapat juga digunakan untuk transaksi-transaksi selain yang berjalan di Web**
  - **Tidak dirancang untuk menangani keputusan keamanan berbasis pada otentikasi pada peringkat aplikasi atau dokumen → perlu metode tambahan untuk mengendalikan akses ke berkas (*file*) yang berbeda**

Standar Keamanan di Internet

Keamanan untuk e-Mail:

- Privacy-Enhanced Mail (PEM)
  - standar Internet untuk mengamankan e-mail menggunakan kunci publik maupun kunci simetris.
  - saat ini mulai berkurang penggunaannya karena ia tidak dirancang dan dikembangkan untuk menangani surat elektronik yang memiliki berbagai jenis lampiran (misalnya: gambar, suara serta video)
- Secure MIME (S/MIME)
  - standar baru untuk keamanan e-mail yang menggunakan algoritma-algoritma kriptografi yang telah memiliki hak paten dan dilisensi oleh RSA Data Security Inc
  - bergantung pada berbagai jenis otoritas sertifikat, apakah bersifat global atau perusahaan, untuk memastikan otentikasi

Standar Keamanan di Internet

Keamanan untuk e-Mail:

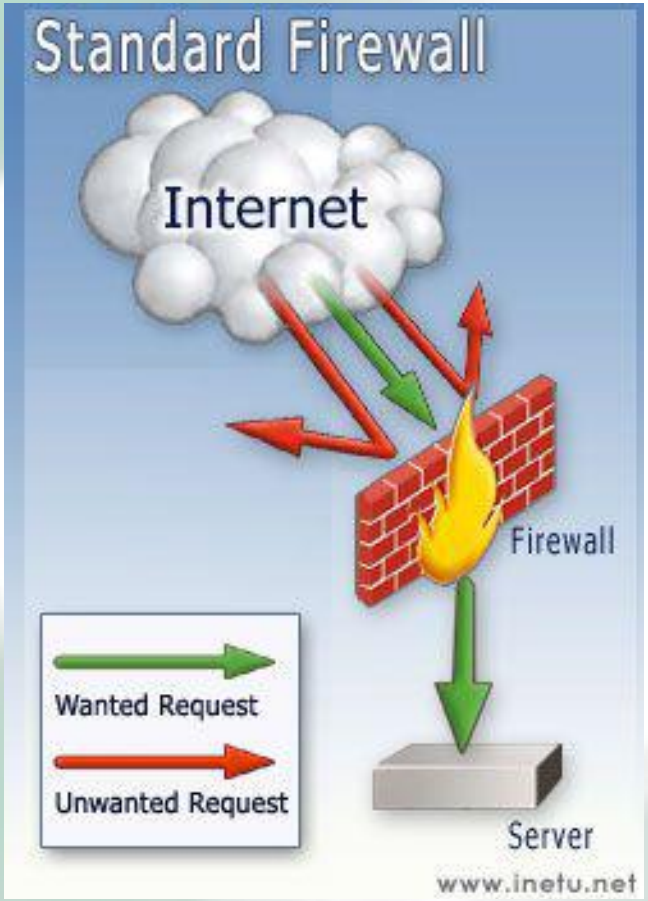
- **Pretty Good Privacy (PGP)**
  - **suatu aplikasi populer yang dikembangkan untuk pengiriman pesan dan berkas (file)**
  - **merupakan aplikasi keamanan yang paling banyak digunakan untuk e-mail, serta menggunakan berbagai standar enkripsi**
  - **Aplikasi-aplikasi enkripsi/deskripsi PGP tersedia bagi hampir semua sistem operasi dan pesan dapat dienkripsi**

Standar Keamanan di Internet

Firewall

- **melindungi serangan pada protokol individual atau aplikasi**
- **melindungi sistem komputer dari *Spoofing* (program-program merusak yang menyamar sebagai aplikasi yang bermanfaat)**
- **menyediakan titik tunggal kendali keamanan bagi jaringan (kontradiksi: Firewall dijadikan titik pusat perhatian Hacker untuk membobol jaringan)**
- **Firewall tidak memeriksa adanya virus pada berkas yang masuk, sehingga tidak dapat menjamin integritas data**
- **Firewall tidak melakukan otentikasi sumber data**

Standar Keamanan di Internet



Standar Keamanan di Internet

Keamanan untuk Jaringan:

- **Kategori dalam Firewall:**
  - **Statis:**

    1. mengijinkan semua lalu lintas data melewatinya, kecuali secara eksplisit dihalangi (*blocked*) oleh administrator firewall

    2. menghalangi semua lalu lintas data yang masuk, kecuali secara eksplisit diijinkan oleh administrator firewall
  - **Dinamis: layanan yang keluar masuk ditetapkan untuk periode waktu tertentu (membutuhkan sumber daya manusia yang lebih**

Standar Keamanan di Internet

Keamanan untuk Jaringan:

- **Karakteristik Firewall:**
  - **penyaringan paket (*packet filtering*)**
  - **penerjemahan alamat jaringan (*network address translation*)**
  - **proxy peringkat aplikasi (*application-level proxies*)**
  - **pemeriksaan keadaan (*stateful inspection*)**
  - **VPN (*Virtual Private Network*)**
  - ***real-time monitoring***