Pengantar E-*Business* dan E-*Commerce*

Pertemuan Ke-5

(Keamanan Sistem *E-Commerce*)

Noor Ifada
noor.ifada@if.trunojoyo.ac.id

Sub Pokok Bahasan

- Pendahuluan
- Pilar Keamanan Sistem E-Commerce
- Ancaman Keamanan di Internet
- Enkripsi vs Dekripsi
- Ancaman Keamanan di Internet

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

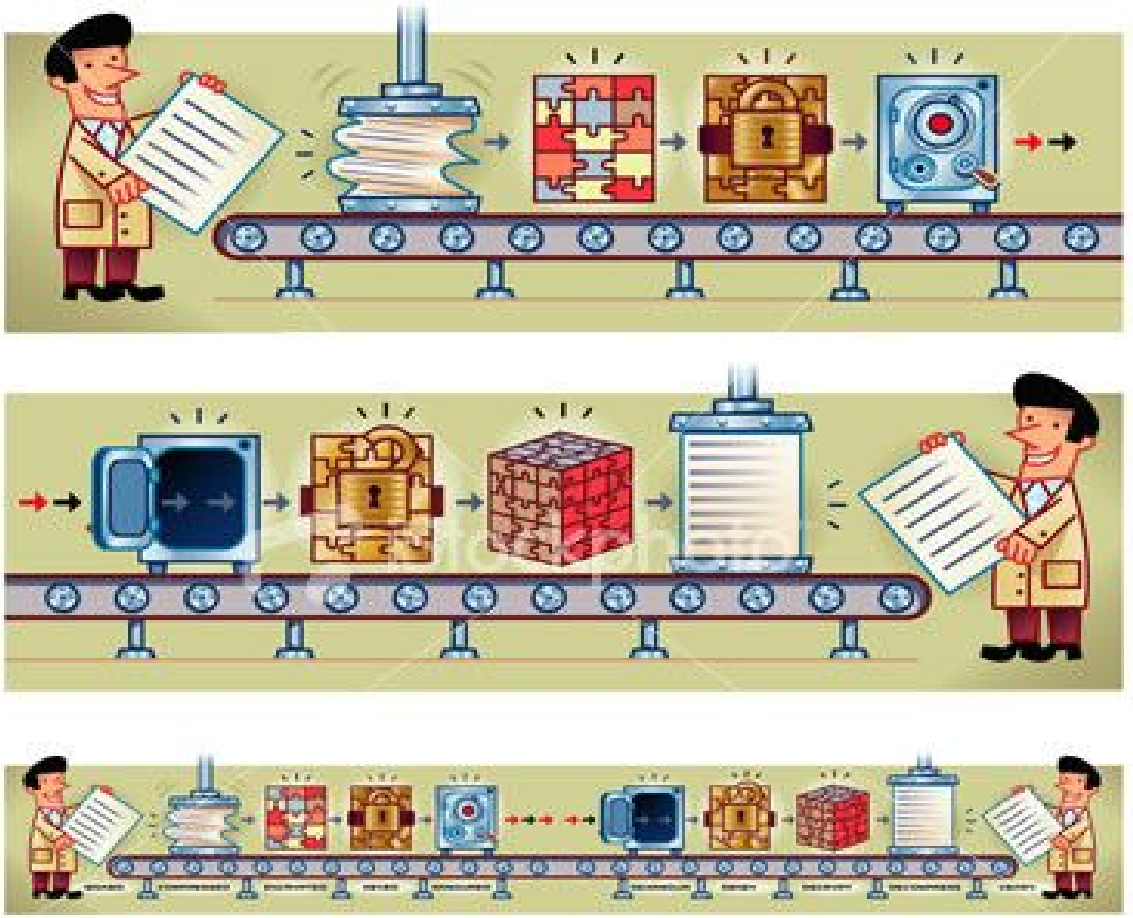
- ***Authentication* (keabsahan pengirim)**
  - Identitas pengguna/pengirim data teridentifikasi (tidak ada kemungkinan penipuan)
- ***Confidentiality* (kerahasiaan data)**
  - data tidak dapat dibaca oleh pihak yang tidak berhak
- ***Integrity* (keaslian data)**
  - data tidak dapat diubah secara tidak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

Ancaman Keamanan di Internet

Ancaman	Solusi Keamanan	Fungsi	Teknologi
Pencegatan data, pembacaan dan modifikasi data secara tidak sah	Enkripsi (*encryption*)	Menyandikan data	Enkripsi Simetrik dan Enkripsi Asimetrik (algoritma DES, RSA, PGP, dsb)
Kecurangan (*fraud*) oleh pihak yang tidak diketahui identitasnya	Otentikasi	Verifikasi identitas pengirim dan penerima	Tanda tangan digital (*digital signature*)
Akses tidak sah terhadap data milik orang lain	Firewall	Menyaring dan melindungi lalu lintas data di jaringan/server	Firewall; VPN (Virtual Private Network)

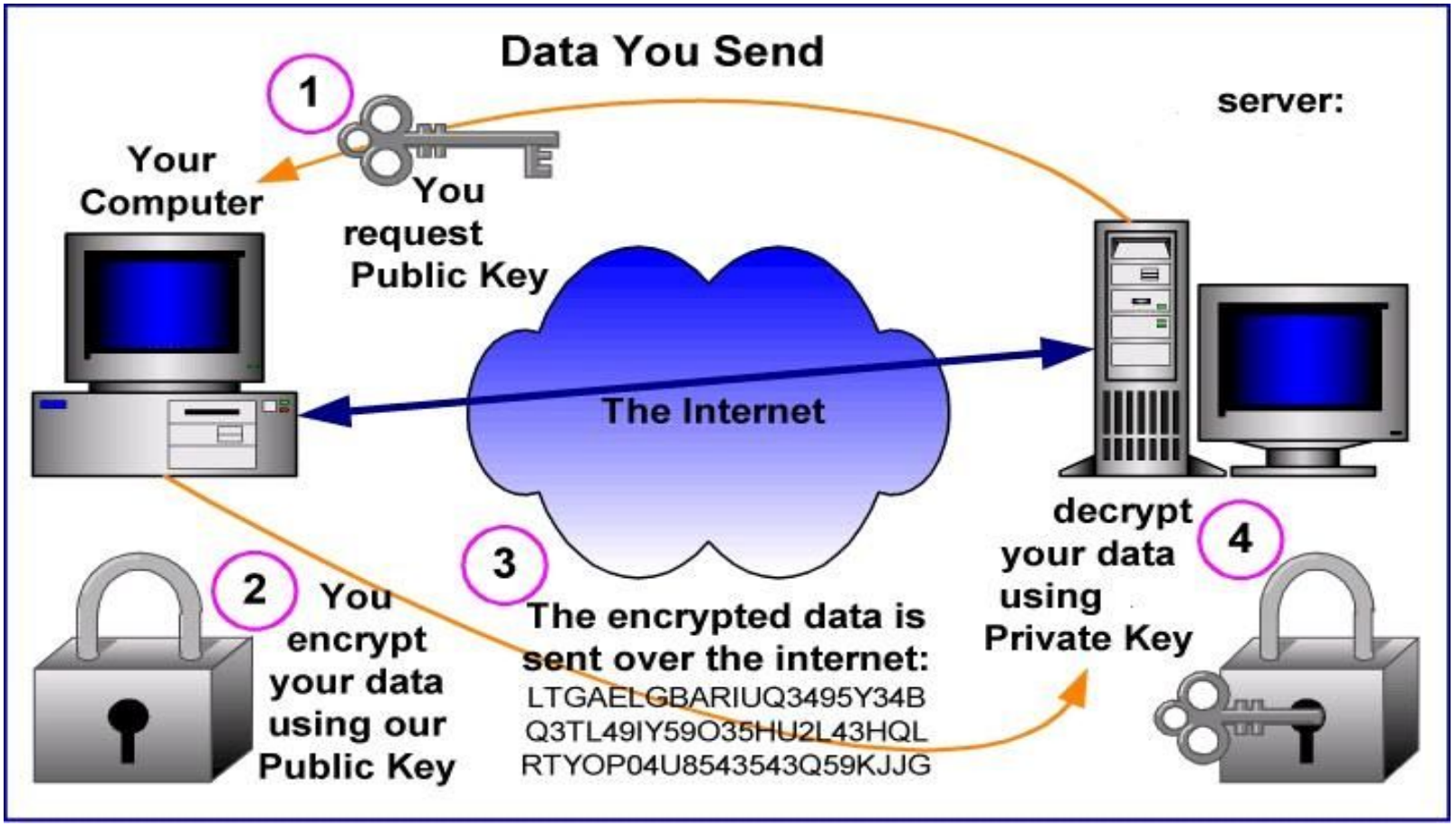
Enkripsi vs Dekripsi

- Enkripsi berarti mengkodekan data ke format tertentu menggunakan kunci rahasia
- Dekripsi mendekodekan data yang terenkripsi ke format asli



Enkripsi vs Dekripsi (contd-2)

- Contoh: Enkripsi RSA



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 (contd-2)

- 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 (contd-3)

- 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 (contd-4)

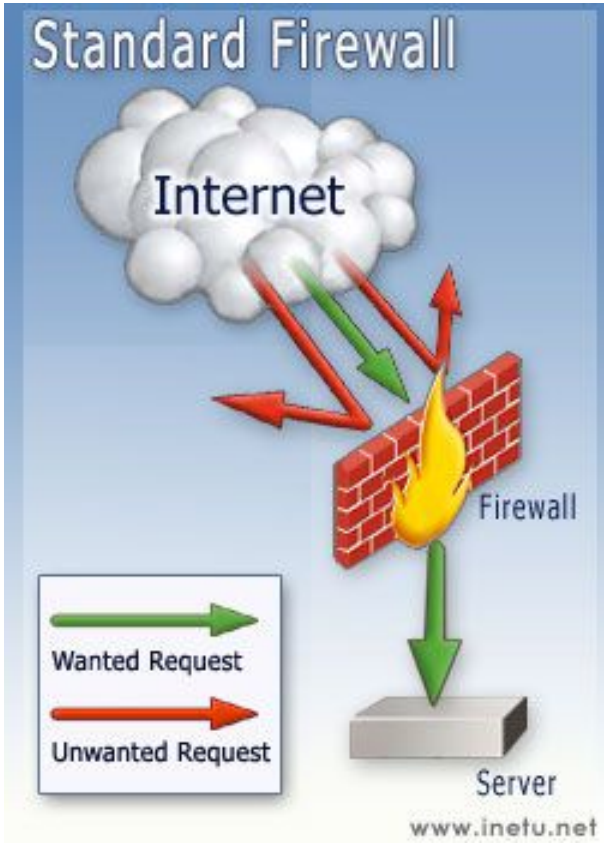
- Keamanan untuk e-Mail:
  - Privacy-Enhanced Mail (PEM)
    - standar Internet untuk mengamankan e-mail menggunakan kunci publik maupun kunci simetris.
    - saat ini mulai berkurang penggunaannya karena ia tidak dirancang dan dikembangkan untuk menangani surat elektronik yang memiliki berbagai jenis 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 (contd-5)

- 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 menggunakan berbagai program e-mail

Standar Keamanan di Internet (contd-6)

- Keamanan untuk Jaringan:
  - 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 (contd-7)

- 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 banyak, namun memiliki fleksibilitas yang lebih tinggi)

Standar Keamanan di Internet (contd-7)

- 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*