PROTEKSI WEB & EMAIL

What's Web ?

- Web → mempresentasikan informasi dalam bentuk teks, gambar, suara, dll dalam bentuk *hypertext* dan dapat diakses oleh perangkat lunak yang disebut *browser*.
- Web Browser → program / aplikasi yang digunakan untuk membuka halaman web
- Web Server → perangkat lunak server yang berfungsi menerima permintaan HTTP /HTTPS dari klien dan mengirimkan hasilnya dalam bentuk halaman web (dokumen HTML)

Why Learn Web Security ?

- Kegunaan dari web tidak hanya untuk *browsing*, tetapi juga untuk melayani *end user* melalui antarmuka *browser* mereka.
- Komponen Web menggunakan berbagai protokol dan layanan untuk memberikan konten yang diinginkan *end user*.
- Banyak pemilik website tidak memperhatikan keamanan website mereka

Why Learn Web Security ?

- Kebanyakan pemilik website tidak……
  - mereka menganggap bahwa perusahaan mereka masih kecil dan tidak mungkin ada hacker yang mau melirik
  - *hacker* menggunakan *tools/software* otomatis untuk menemukan situs yang memiliki kriteria kelemahan-kelemahan tertentu.

Why Have To Be Secured ?

- Website adalah *brand*, pintu depan, bahkan sebagian merupakan wadah/media yang pertama kali menghubungkan perusahaan dengan *customer.*
- Semakin besar interaksi customer dengan website, makin tinggi kebutuhan keamanan untuk website tersebut.

Why Have To Be Secured ?

- Serangan *hacker* berdampak buruk pada relasi bisnis, baik itu *bussiness to bussiness* maupun *bussiness to consumer*
- *Hacker* dapat menyisipkan *malware* yang bekerja mengambil data *customer*

Why Have To Be Secured ?

- Pemilik website menginginkan posisi website mereka berada di peringkat teratas mesin pencarian
  - menyewa jasa konsultan
  - malware yang berada di dalam website mengambil *resource server*, yang menyebabkan pengunjung / google susah mengakses website atau malah membuat sistem *down*
  - website masuk dalam daftar hitam google.

Why Have To Be Secured ?

- Dari sebuah website, *hacker* melangkah lebih dalam ke server, kemudian melihat semua isi file yang berada di server
- Jika server terhubung dengan jaringan, maka lebih banyak lagi yang ia peroleh.

Why Have To Be Secured ?

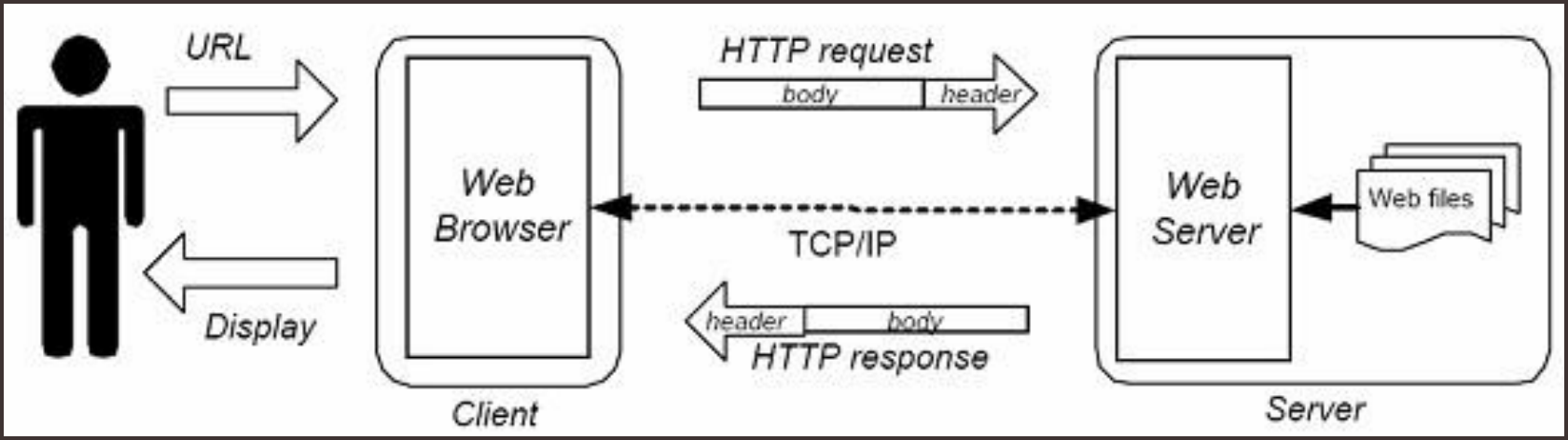
- Beberapa hal dan motivasi *hacker* :
  - Mengambil/menghapus data (file & database)
  - Meletakkan backdoor file (untuk keluar masuk hacker)
  - Menjual data perusahaan kepada kompetitor perusahaan sejenis.
  - Menanam malware untuk melakukan eksekusi kode jahat (evil code) ke server/website lain.
  - Membuat sistem down

What Should Be Secured ?

- Dari sudut pandang sistem :
  - Mengamankan server yang memberikan konten kepada user melalui Web.
  - Mengamankan transportasi informasi antara user dan server melalui Web.
  - Mengamankan komputer user dari serangan melalui koneksi Web.

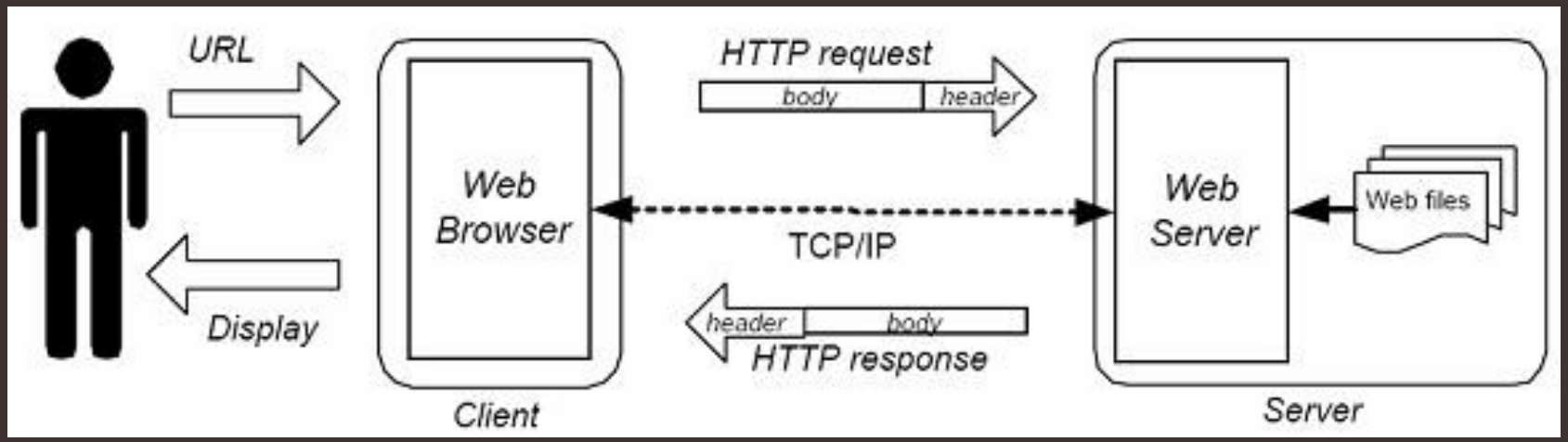
Sistem Kerja Web

1. *User* mengakses website berupa URL melalui *Web Browser* (media untuk menuju URL yang diakses),
2. *Web Browser* mengirimkan permintaan berupa HTTP *Request* kepada *Web Server* melalui layer TCP/IP



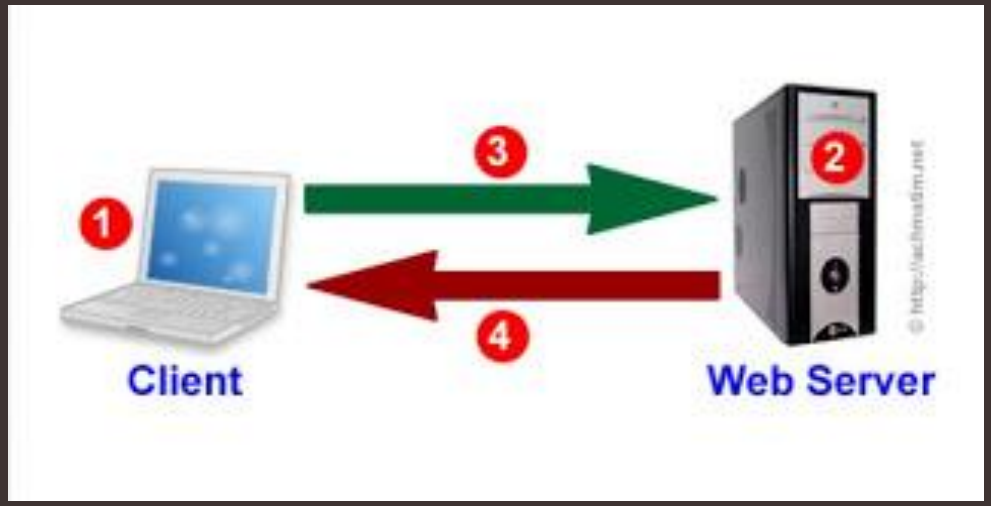
Sistem Kerja Web

3. *Web Server* memberikan *Web Files* yang di-request (jika ada) melalui HTTP *Response* melalui layer TCP/IP,
4. *Web Browser* menerima *Web Files*, dan kemudian dikirimkan kepada *User* berupa *Display*.



Sistem Kerja Web Server

- Pada dasarnya tugas web server :
  - Menerima permintaan (*request*) dari *client*, dan
  - Mengirimkan apa yang diminta oleh *client* (*response*).



Sistem Kerja Web Server

1. Client (user) meminta suatu halaman ke server untuk ditampilkan dikomputer client. Misalnya dengan mengetikkan suatu alamat/URL di browser http://www.google.com.
2. Melalui protokol http, dicarilah komputer bernama www.google.com.
3. Jika ditemukan, maka seolah-olah terjadi permintaan, "hai google, ada client yang minta halaman utama ni.., ada dimana halamannya?". Inilah yang disebut request.

Sistem Kerja Web Server

4. Dari sisi server, web server mendapat permintaan halaman utama google dari *client*, si server akan mencari halaman sesuai permintaan.
5. Jika ditemukan, maka halaman yang diminta akan dikirimkan ke *client*,
6. Jika tidak ditemukan, maka server akan memberi pesan "404. *Page Not Found*", yang artinya halaman tidak ditemukan.

Penanganan Ancaman Pada Web

- Mencegah user yang tidak sah untuk mengakses data sensitif
  - Otentikasi: mengidentifikasi user untuk menentukan apakah mereka adalah orang yang berwenang
  - Akses kontrol: mengidentifikasi sumber daya yang membutuhkan perlindungan dan siapa saja yang memiliki akses kepada mereka
- Mencegah penyerang mencuri data selama transmisi
  - Enkripsi (biasanya dengan *Secure Sockets Layer*)

Authentication

- Mengumpulkan informasi *user* ID dari *end user* ("*log in*")
  - biasanya melalui dialog / antarmuka browser
  - informasi user ID biasanya mengacu pada username dan password
- Memindahkan informasi *user* ID ke server web
  - Tidak aman (HTTP) maupun aman (HTTPS = HTTP melalui SSL)

Authentication

- Verifikasi ID dan *password* ('keamanan database')
  - Realms menyimpan username, password, dll, dapat diatur dengan cara LDAP, RDBMS, dll
  - Validasi: cek di server web jika user ID & password match dengan yang ada di Realms.
- Menjaga otentikasi user sebelumnya untuk operasi HTTP selanjutnya

What is Secure Sockets Layer (SSL)?

- Protokol yang dikembangkan pada tahun 1996 oleh Netscape untuk keamanan transmisi dokumen web pribadi melalui Internet.
- Menggunakan kunci pribadi dan publik untuk mengenkripsi data yang dikirim melalui koneksi SSL.
- Dengan konvensi, URL yang membutuhkan koneksi SSL dimulai dengan https bukan http.

What is Secure Sockets Layer (SSL)?

- SSL diperlukan ketika …
  - Ada proses login atau sign in (untuk melindungi nama pengguna dan password)
  - Mentransmisikan data sensitif secara online, seperti informasi kartu kredit, dll
  - Seseorang memerlukan privasi dan persyaratan keamanan

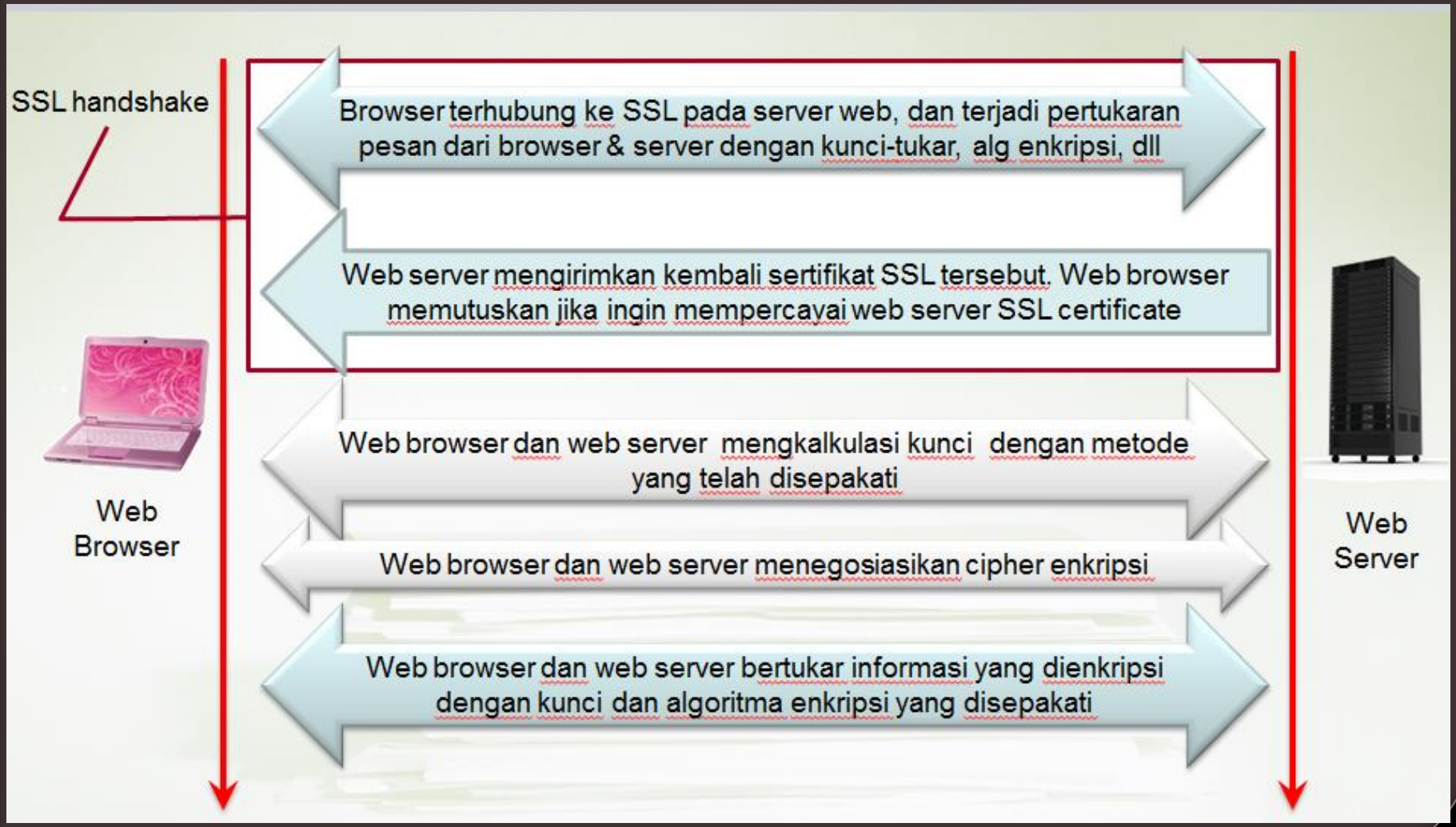
Use of an SSL Certificate

- Untuk mengaktifkan koneksi SSL, server membutuhkan sertifikat SSL yang ditandatangani oleh *Certificate Authority* (CA).
- CA memverifikasi ID dari pemilik sertifikat ketika sertifikat SSL dikeluarkan.
- Setiap Sertifikat SSL berisi informasi yang unik dan otentik tentang pemilik sertifikat, seperti ID, lokasi, kunci publik, dan tanda tangan dari CA.

Use of an SSL Certificate

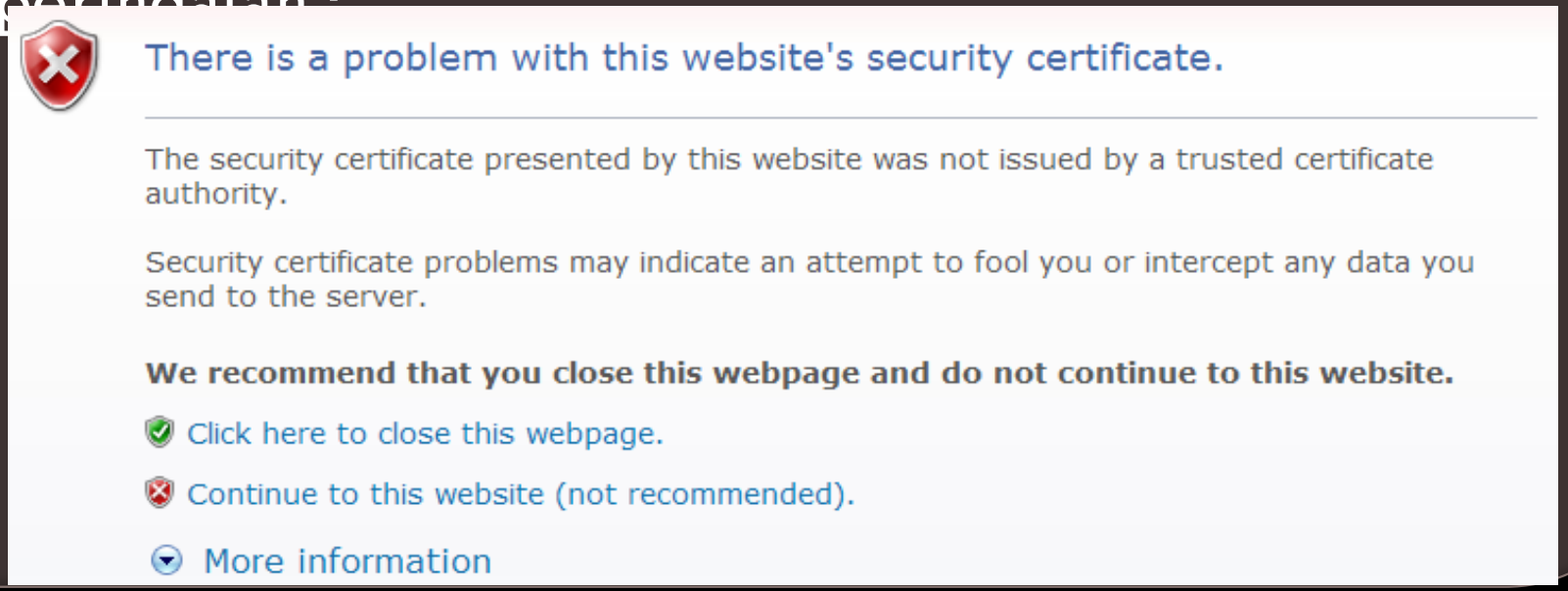
- Hal ini menegaskan bahwa Anda benar-benar user yang sah.
- Sertifikat SSL memungkinkan enkripsi informasi selama transaksi online dengan cara menggunakan *cryptosystem hybrid*.

How SSL Works?



CA Root Certificate

- Web browser membutuhkan sertifikat utama CA yang mengeluarkan sertifikat SSL ke web-server untuk memverifikasi apakah server web terpercaya.
- Jika browser tidak memiliki / mempercayai sertifikat utama CA , kebanyakan browser web akan memberi peringatan :



Types of Web Application Security

- Ada dua jenis aplikasi untuk keamanan web :
  - Keamanan Deklaratif
  - Keamanan Program

Declarative Security

Keamanan secara otomatis ditangani oleh sistem, hanya perlu melakukan konfigurasi (pada file web.xml)

- Untuk mencegah akses yang tidak sah
  - Menggunakan aplikasi *Web deployment descriptor* (web.xml) untuk menyatakan bahwa URL tertentu membutuhkan perlindungan.
  - Server secara otomatis meminta user untuk memasukkan *username* dan *password*, melakukan verifikasi, dan melacak user yang telah dikonfirmasi sebelumnya.

Declarative Security

- Untuk melindungi data yang dikirimkan melalui jaringan
  - Menggunakan web.xml untuk mengkonfigurasi URL supaya hanya bisa diakses dengan SSL.
  - Jika user mencoba mengakses URL yang dilindungi melalui HTTP biasa, server secara otomatis mengarahkan mereka ke HTTPS (SSL) yang sesuai.

Program Security

Semua keamanan (otentikasi, akses kontrol, dll) dilakukan oleh program yang dibuat oleh user.

- Untuk mencegah akses yang tidak sah
  - mengotentikasi user atau memverifikasi bahwa user telah dikonfirmasi sebelumnya.
- Untuk melindungi data yang dikirimkan melalui jaringan
  - SSL adalah metode umum untuk melindungi data pada jaringan. Hanya perlu mengarahkan permintaan ke https URL secara eksplisit dalam program.

PROTEKSI EMAIL

Proteksi Transmisi Email

- PGP [*Pretty Good Privacy*]
  - merupakan program kriptosistem yang berfungsi untuk mengenkrip dan mendekrip data sedemikian hingga data tersebut hanya bisa dibaca oleh yang berhak membacanya.
  - menggunakan key pair untuk enkripsi dan dekripsi dokumen.
  - Key pair: 'private key' dan 'publik key'.

Proteksi Transmisi Email

- PGP [*Pretty Good Privacy*]
  - Private key digunakan untuk mendekrip dokumen yang terenkripsi
  - Publik key fungsinya untuk mengenkrip atau menyandi dokumen.
  - Publik key ini yang dibagi-bagikan ke teman atau relasi, sehingga mereka bisa menggunakannya untuk mengenkripsi dokumen elektronik yang ditujukan untuk mereka, atau menguji digital signature dokumen yang dikirim.

Hoax Email

- Hoax adalah suatu pemberitaan palsu / tidak jelas sumbernya dan biasanya isinya tidak benar.
- Hoax merupakan suatu usaha untuk menipu pembaca untuk mempercayai sesuatu dengan tujuan tertentu.

Hoax Email

- Ciri-ciri hoax:
  - Didistibusikan lewat email, fitur message dan sms
  - Berisi pesan yang membuat cemas, panik atau bisa berupa lelucon untuk membuat kebingungan para pembacanya, memprovokasi perubahan sosial atau membuat orang waspada akan sesuatu
  - Diakhiri dengan himbauan agar pembaca segera memforward warning tersebut. Akibatnya lalu lintas internet menjadi padat
  - Pengirim awal tidak diketahui.

Hoax Email

- Solusi agar terhindar dari hoax
  - Jika menerima email berisi warning tentang ancaman virus disertai himbauan agar menyebarkannya, maka warning tersebut dicek dulu kebenarannya
  - Periksa apakah warning asli dengan search di google
  - Selalu up date virus list pada software anti virus

Spam

- Spamming adalah mengirim mail yang tidak disukai / tidak diinginkan oleh penerimanya.
- Jumlah yang dikirim tidak hanya satu, bahkan ribuan dan isinya sama
- Posting yg mengakibatkan spamming biasanya:
  - Berita warning virus
  - Media buyer
  - Mlm
  - Surat berantai
  - Surat yang tidak berarti (junk mail)
  - Bombmail
  - Hoax email

Spam

- Akibat Spamming:
  - Emailbox tidak bisa diakses sama sekali
  - Hilangnya email-email penting
  - Rusaknya email server, sehingga mengakibatkan server tidak merespon perintah yang diberikan kepadanya
  - Bagi user yang memiliki bandwith kecil atau kuota dibatasi mengakibatkan tidak ada waktu luang baginya utk mengakses internet

Spam

- Ciri spam
  - Membuat crash suatu program dengan memakai buffer yang menggunakan input data terlalu besar
  - Mengirimkan suatu pesan ke newsgroup sehingga menyebabkan forum tersebut penuh dengan pesan yang tidak relevan
  - Mempostingkan artikel ke banyak newsgroup atau mailing list (ECP / *Excessive Cross Posting*)
  - Mombombardir newsgroup/mailing list dengan artikel yang sama (EMP / *Excessive Multi Posting*)
  - Mengirim email serupa yang tidak diharapkan terutama yang berkaitan dengan iklan suatu produk

Spam

- Cara menghindar spam
  - Tidak merespon email spam
  - Tidak mereply spamming mail dengan kata ‘remove’. (email akan dicatat sebagai email yang aktif).
  - Tidak mengakses web yg direkomendasikan dalam spamming mail. (Akses akan dimonitor dan berfungsi sebagai alat validitas alamat email)
  - Tidak sign up suatu situs yg menjanjikan bahwa alamat kita akan dihapus dari list spamming mail, karena dg menuliskan alamat berarti kita memberikannya

Mail Encryption

- Mengenkripsi email dengan PGP
  - Ketik email di suatu text editor (mis: notepad)
  - Copy text ke clipboard
  - Klik tombol kanan di PGP tray, dan klik "Encrypt Clipboard".
  - Pilih publik key si penerima, pindahkan ke recipient box. Selanjutnya klik "OK".
  - PGP akan mengenkrip clipboard dan hasilnya langsung tampil.
  - Pastekan isi clipboard ke e-mail atau text editor

Mail Decryption

- Mendekripsi email dengan PGP
  - Copy email ke clipboard, klik kanan di PGP tray dan klik "Decrypt/Verify Clipboard".
  - Ketik passphrasenya kemudian klik "OK".
  - Message akan muncul di suatu text window
- Beberapa web based e-mail account [hotmail, mailcity, rocketmail, dll] kadangkala menambahkan atau mengkonversikan sendiri sehingga isinya tidak otentik lagi.