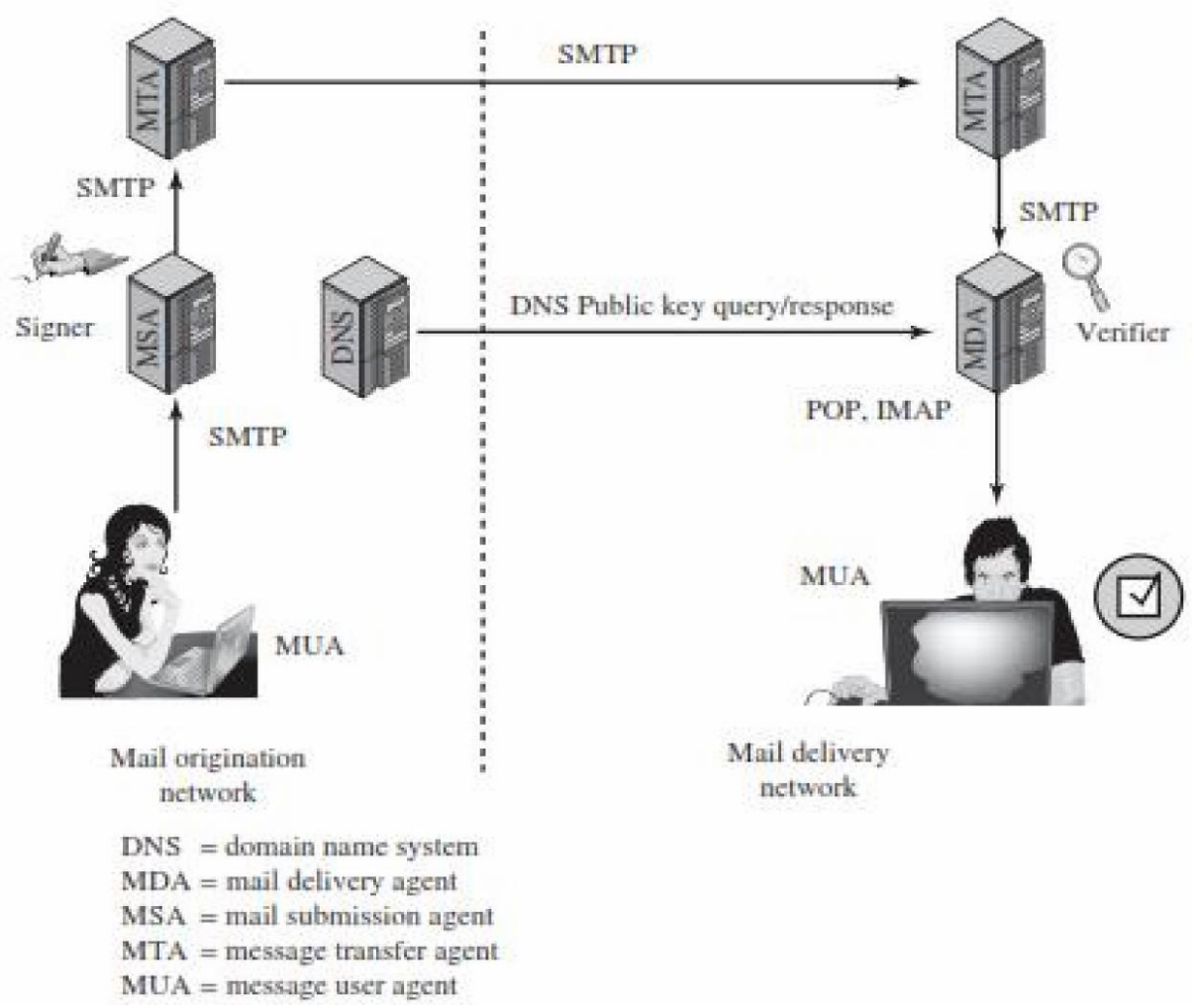
A. Materi Database Security

1. **Jelaskan tentang aspek dari Keamanan Basisdata**
   - Mambatasi akses ke data dan servis
   - Melakukan autentifikasi pada user
   - Memonitor aktivitas-aktivitas yang mencurigakan
2. **Jelaskan tentang Sql Injection serta contoh studi kasus nya**

   Injeksi SQL (*SQL Injection*) adalah sebuah teknik yang menyalahgunakan sebuah celah keamanan yang terjadi dalam lapisan basis data sebuah aplikasi. Celah ini terjadi ketika masukan pengguna tidak disaring secara benar dari karakter-karakter pelolos bentukan string yang diimbuhkan dalam pernyataan SQL atau masukan pengguna tidak bertipe kuat dan karenanya dijalankan tidak sesuai harapan.

B. Materi Network Security

1. **Jelaskan tentang pengamanan pada sistem layanan email**



2. **Jelaskan tentang pengamanan pada sistem layanan web**

   HTTPS (HTTP over SSL) merupakan kombinasi/gabungan dari HTTP dan SSL untuk menerapkan keamanan komunikasi antara Web Browser dan Web Server.

C. Materi Kriptografi

1. **Jelaskan prinsip kerja dari kryptografi**

   Kriptografi terdiri dari dua kegiatan yang saling berkaitan. Dua proses tersebut adalah enkripsi dan dekripsi. Enkripsi adalah mengubah data atau yang disebut dengan istilah plain text dalam kriptografi menjadi sebuah kode acak yang tidak dapat dibaca yang disebut dengan chiper text.

   Jadi dapat disimpulkan proses kerja kriptografi adalah sebagai berikut

   - Data / plain text dienkripsi dengan algoritma tertentu hingga mendapat chiper text
   - Chiper text tersebut dikirimkan ke tujuan
   - Chiper text didekripsi ulang menjadi data yang bisa dibaca oleh manusia

2. **Jelaskan layanan yang disediakan oleh kryptografi**

   1. Kerahasiaan (confidentiality)

      Layanan yangdigunakan untuk menjaga isi pesan dari siapapun yang tidak berhak untuk membacanya
   2. Integritas data (data integrity)

      Layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman
   3. Otentikasi (Authentication)

      Layanan untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*) dan untuk mengidentifikasi kebenaran sumber pesan (*data oriign authentication*)
   4. Anti Penyangkalan (non repudiation)

      Layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal mengirim pesan atau penerima pesan menyangkal telah menerima pesan.

3. **Jelaskan algoritma kriptografi klasik dan modern serta sebutkan contoh nya !**

   1. Kriptografi Klasik : Belum menggunakan Komputer, biasanya masih menggunakan model subsitusi atau transposisi pada pesan. Kriptografi klasik umumnya merupakan teknik penyandian dengan kunci simetrik dan menyembunyikan pesan yang memiliki arti ke sebuah pesan yang nampaknya tidak memiliki arti, biasa digunakan dengan metode Subsitusi dan Transposisi. Contoh :

      – Caesar, Subsitusi, Affine, Vigenere, Hill dll (berbasis subsitusi)

      – Transposisi Columnar, Permutasi dll (berbasis transposisi)
   2. Kriptografi Modern : Sudah menggunakan komputer, contoh dengan menggunakan Algoritma Kriptografi. Kriptografi modern dibuat sedemikian kompleks sedemikian sehingga kriptanalis sangat sulit memecahkan cipherteks tanpa mengetahui kunci. Algoritma kriptografi modern umumnya beroperasi

dalam mode bit ketimbang mode karakter. Operasi dalam mode bit berarti semua data dan informasi (baik kunci, plainteks, maupun cipherteks) dinyatakan dalam rangkaian (string) bit biner, 0 dan 1 dengan menggunakan perangkat komputer. Contoh :

– Kriptografi Simetri, ex: DES, Blowfish, Rinjdael dll

– Kriptografi Asimetri (Nirsimetri) atau Kunci Public, ex: RSA, Elgamal, Rabin, Diffie Hellman dll.

D. Materi Steganografi

1. **Jelaskan perbedaan antara kryptografi dan steganografi**

   Kriptografi: menyembunyikan isi (content) pesan

   – Tujuan: agar pesan tidak dapat dibaca oleh pihak ketiga (lawan)

   Steganografi: menyembunyikan keberadaan (existence) pesan

   – Tujuan: untuk menghindari kecurigaan (conspicuous) dari pihak ketiga (lawan)

2. **Jelaskan steganografi pada dunia modern**

   Diperkenalkan oleh Simmons – 1983. Dilakukan dalam konteks USA – USSR nuclear non proliferation treaty compliance checking. Steganografi di dunia modern biasanya mengacu pada informasi atau suatu arsip yang telah disembunyikan ke dalam suatu arsip citra digital, audio, atau video.

3. **Jelaskan kriteria steganografi yang bagus**

   Imperceptible; Keberadaan pesan rahasia tidak dapat dipersepsi secara visual atau secara audio (untuk stego - audio).

   Fidelity; Kualitas cover-object tidak jauh berubah akibat penyisipan pesan rahasia.

   Recovery; Pesan yang disembunyikan harus dapat diekstraksi kembali.

   Capacity; Ukuran pesan yang disembunyikan sedapat mungkin besar

4. **Jelaskan tipe steganografi dan sebutkan contoh nya**

   1. Pure stegan ography
      - Tidak membutuhkan kunci sama sekali.
      - Keamanan steganografi seluruhnya bergantung pada algoritmanya.

   Contoh: Null Cipher

   2. Secret (or symmetric) key Steganography
      - Menggunakan kunci yang sama untuk embedding dan extraction.

   Contoh:

   - kunci untuk pembangkitan bilangan acak

   - kunci untuk mengenkripsi pesan dengan algoritma kriptografi simetri (DES, AES, dll)

   3. Public-key Steganography
      - Menggunakan dua kunci: kunci publik untuk embedding dan kunci privat untuk extraction.

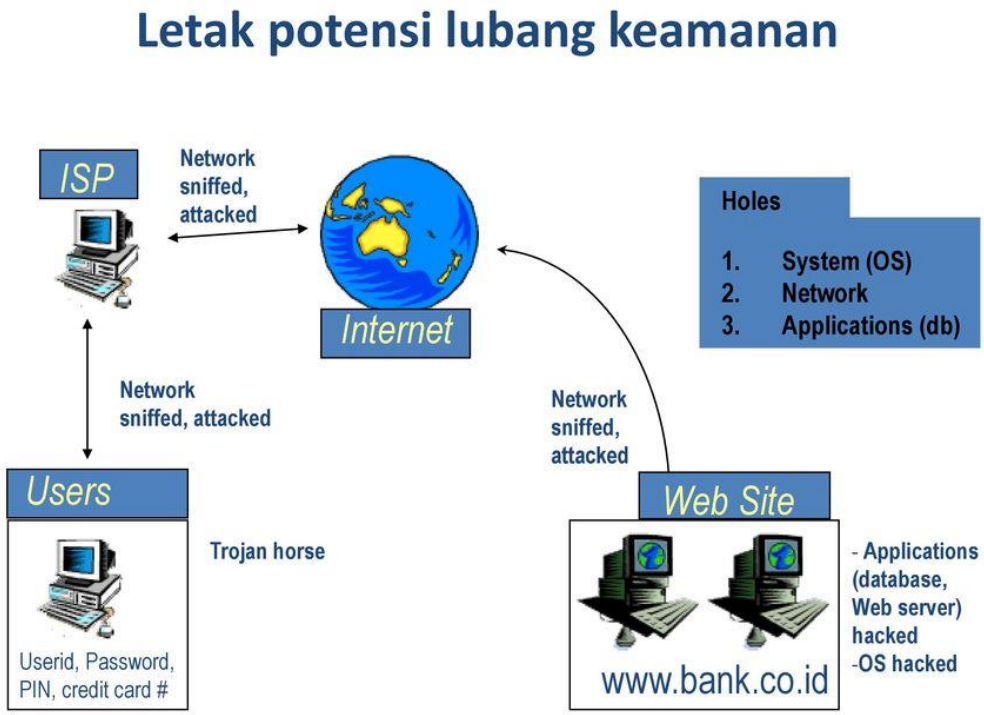
   Contoh:

   - kunci publik RSA untuk mengenkripsi hidden message

   - kunci privat RSA untuk mendekripsi hidden message

E. Materi Evaluasi Sistem Keamanan Komputer

1. Jelaskan letak potensi lubang keamanan pada sistem komputer



2. Jelaskan cara evaluasi sistem keamanan !

• Evaluasi dapat dilakukan secara

1. Manual (melelahkan)
   - Melihat servis yang diberikan oleh sebuah server. Servis diberikan melalui TCP atau UDP dengan port tertentu. Seperti telnet: port 23, SMTP: port 25, HTTP/WWW: port 80, POP: port 110, dst.
   - Menguji SMTP secara manual, dengan telnet localhost 25
2. Otomatis (meggunakan tools)
   - Dengan melakukan proses probing secara otomatis
     - UNIX : nmap, strobe, tcpprobe
     - Windows 95/98/NT : SuperScan, Netlab, Ogre
   - Deteksi melalui
     – Unix : Courtney, Portsentry
     – Windows : attacker

3. Jelaskan etika penggunaan tools pada sistem keamanan komputer

a. Menyerang sistem milik sendiri untuk mengevaluasi
b. Jangan melakukan evaluasi terhadap sistem orang lain tanpa ijin
c. Banyak program attack yang dapat diperoleh dari Internet

4. **Jelaskan tentang penetration testing**

   Merupakan pekerjaan yang dilakukan seorang penyusup (intruder) yang dapat melakukan penyusupan ke sistem. Biasanya dilakukan dari jaringan eksternal (external network) dengan informasi yang dibatasi. Lanjutannya, dengan menambahkan beberapa informasi dan diserang dari jaringan internal (internal network).

   Langkah-langkah:

   – Pertama : melakukan sebuah serangan (attack) dari external network; biasanya Internet atau extranet; informasi terbatas; informasi yang dibutuhkan sebuah daftar IP addresses dan time frame untuk melakukan test. Penguji harus memasukkan (submit) sebuah IP adress selama digunakan untuk melakukan penetrasi untuk mengabaikan filter oleh IDS.

   – Kedua : biasanya membawa dari external network, tetapi penambahan informasi. Penguji diberikan topologi, daftar sistem operasi dan aplikasi-aplikasi.

   – Ketiga : pengujian meliputi penyerangan dari internal network. Langkah ini harus dikoordinaikan dengan administrator lokal untuk melokalisasi dan menimialkan dampak dari business process.