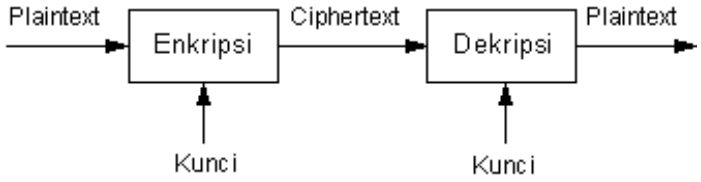
KRIPTOGRAFI

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.

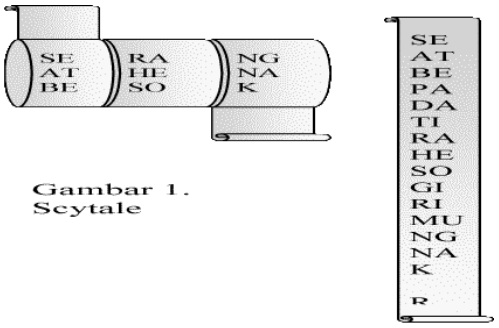
6. JENIS PENYERANGAN PADA JALUR KOMUNIKASI

- *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 :

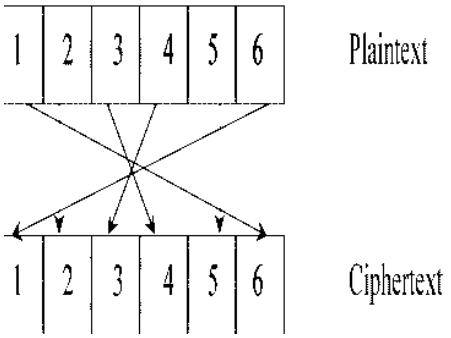
5	K		G	BLOK 1
		K	R	BLOK 2
T	D	R	A	BLOK 3
E	A	I	F	BLOK 4
K	S	P	I	BLOK 5
N	A	T		BLOK 6
I	R	O		BLOK 7

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.

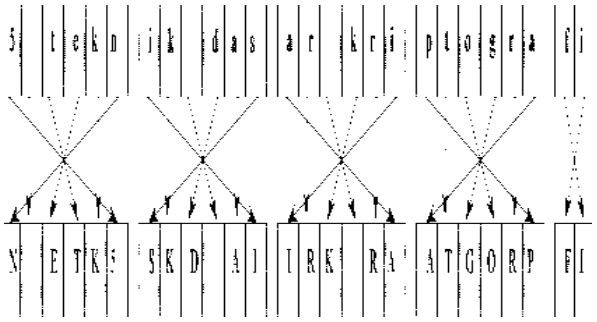
c. Permutasi

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

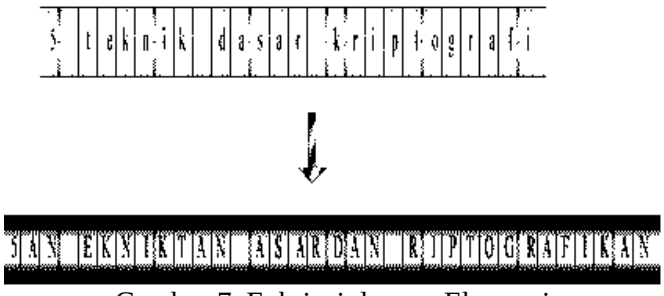
Dengan menggunakan aturan diatas, maka proses enkripsi dengan permutasi dari plaintext adalah sebagai berikut :


Gambar 6. Proses Enkripsi dengan Permutasi

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

d. Ekspansi

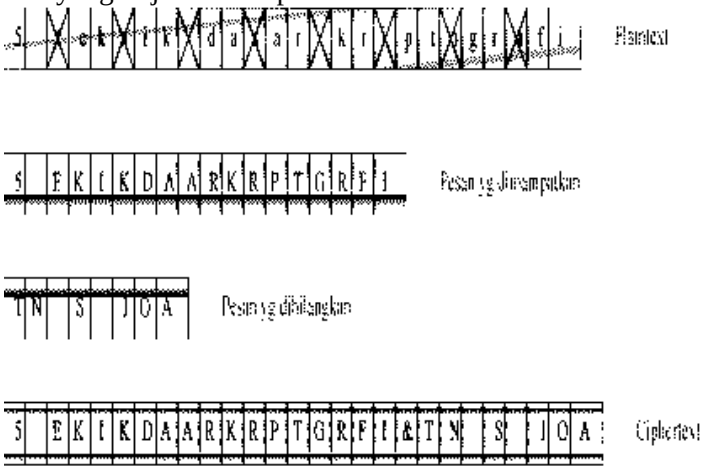
Suatu metode sederhana untuk mengacak pesan adalah dengan memelarkan pesan itu dengan aturan tertentu. Salah satu contoh penggunaan teknik ini adalah dengan meletakkan huruf konsonan atau bilangan ganjil yang menjadi awal dari suatu kata di akhir kata itu dan menambahkan akhiran "an". Bila suatu kata 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.