CRYPTOSYSTEM DAN CRYPTOGRAPHY

PERTEMUAN 3

PENGENALAN DASAR CRYPTOGRAPHY (KRIPTOGRAFI)

- Seni dan ilmu menjaga keamanan pesan adalah kriptografi
- Orang yang menggunakan kriptografi disebut Cryptographer
- Kriptanalisis (cryptanalysis) adalah praktisi dari kriptanalis, seni dan ilmu untuk memecahkan cipherteks (menampilkan dengan samaran)
- Cabang dari matematika yang mencakup kriptografi dan kriptanalis adalah kriptologi (cryptology) dan praktisinya disebut kriptologis (cryptologists)
- Cryptologist modern biasanya dilatih dan belajar teori matematika

ENKRIPSI DAN DEKRIPSI

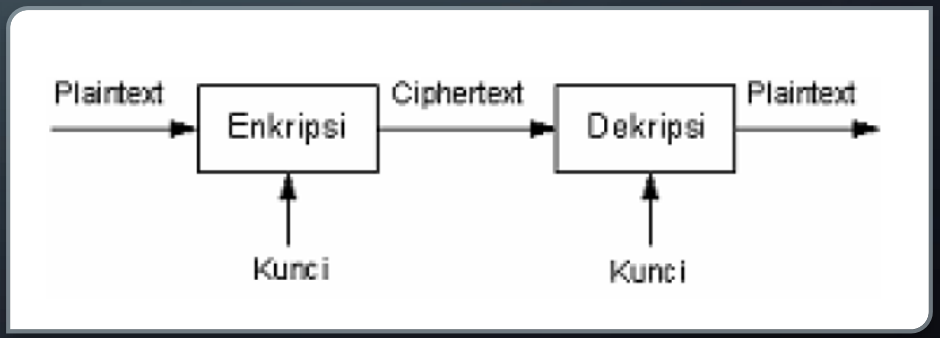
- Suatu pesan adalah plainteks (plaintext) atau cleartext
- Proses menyembunyikan pesan disebut enkripsi (encryption)
- Pesan yang dienkripsi adalah cipherteks (ciphertext)
- Proses pengembalian ciperteks ke plainteks disebut dekripsi (decryption)

ELEMEN KRIPTOGRAFI (1)

- Plaintext ditandai dengan M untuk pesan, atau P untuk plaintext.
- Bisa merupakan suatu aliran bit, file teks, bitmap, aliran suara digital, dan citra video digital
- M adalah data biner
- Ciphertext ditandai dengan C dan data biner, kadang-kadang ukurannya sama seperti M
- Fungsi enkripsi E, beroperasi pada M untuk menghasilkan C. berikut notasi matematikanya:
  - E(M) = C
- Sedangkan proses kebalikannya, yaitu fungsi dekripsi D beroperasi pada C untuk menghasilkan M:
  - D(C) = M

ELEMEN KRIPTOGRAFI (2)

- Fungsi matematika yang digunakan untuk melakukan enkripsi dan dekripsi disebut dengan cipher atau algoritma kriptografi
- Semua keamanan pada algoritma didasarkan pada kunci; bukan didasarkan pada rincian algoritma
- Produk menggunakan algoritma dapat mass-produced, sehingga jika seseorang penyusup mengetahui algoritmanya, tetap dia tidak bisa membaca pesan karena menggunakan kunci



TUJUAN KRIPTOGRAFI (1)

- Kerahasiaan (confidentiality): layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berkepentingan
- Autentikasi: layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (user authentication atau entity authentication) maupun mengidentifikasi kebenaran sumber pesan (data origin authentication). Layanan ini direalisasikan dengan menggunakan tanda tangan digital (digital signature)

TUJUAN KRIPTOGRAFI (2)

- Integritas data (data integrity): layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. Layanan ini direalisasikan dengan tanda tangan digital
- Tidak ada penyangkalan (non-repudiation): layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan

CRYPTOSYSTEM

- Suatu algoritma, ditambah semua kemungkinan plainteks, cipherteks, dan kunci
- Cryptosystem terbagi menjadi 2, yaitu algoritma simetris dan algoritma public-key

ALGORITMA SIMETRIS (SYMMETRIC)

- Disebut sebagai algoritma konvensional
- Algoritma dimana kunci enkripsi dapat dikalkulasi dari kunci dekripsi dan sebaliknya
- Kunci enkripsi dan kunci dekripsinya adalah sama
- Algoritma ini dapat disebut juga algoritma secret-key, single-key, atau one-key
- Membutuhkan persetujuan pengirim dan penerima terhadap kunci sebelum mereka melakukan komunikasi dengan aman

ALGORITMA PUBLIC-KEY

- Disebut juga asymmetric algorithms
- Memberikan solusi terhadap kelemahan enkripsi kunci simetris
- Setiap pengguna memiliki dua kunci:
  - kunci publik (public-key): dibagikan kepada semua pengguna
  - kunci pribadi (private-key): dirahasiakan dan hanya diketahui oleh pengguna
- Disebut sebagai public-key karena kunci enkripsi dapat dibuat menjadi publik
- Kunci enkripsi disebut public-key dan kunci dekripsi disebut private-key

PROTOKOL CRYPTOSYSTEM

- Suatu protokol yang menggunakan kriptografi
- Melibatkan algoritma kriptografi
- Untuk mencegah atau mendeteksi adanya cheating

JENIS PENYERANGAN PADA PROTOKOL

- Didasari oleh ilmu pengembalian plainteks dari pesan tanpa akses pada kunci, yang disebut Kriptanalis
- Penyerangan kriptanalitik yang diasumsikan bahwa kriptanalis memiliki pengetahuan yang sempurna dari algoritma enkripsi yang digunakan:
  - Ciphertext-only attack
  - Known-plaintext attack
  - Chosen-plaintext attack
  - Adaptive-chosen-plaintext attack
  - Chosen-ciphertext attack
  - Chosen-key attack
  - Rubber-hose crytanalysis

CIPHERTEXT-ONLY ATTACK

- Kriptanalis mempunyai cipherteks dari beberapa pesan, semua dienkripsi dengan menggunakan algoritma enkripsi yang sama
- Pekerjaan kriptanalis adalah menemukan kembali pesan plainteks sebanyak mungkin, atau bahkan menyimpulkan kunci yang digunakan untuk mengenkripsi pesan tersebut agar dapat mendekripsikan kembali pesan yang telah dienkripsi dengan kunci yang sama

KNOWN-PLAINTEXT ATTACK

- Kriptanalis mempunyai akses tidak hanya untuk cipherteks dari beberapa pesan, tetapi juga untuk plainteks pesan
- Pekerjaannya adalah menyimpulkan kunci yang digunakan untuk enkripsi pesan atau suatu algoritma untuk dekripsi pesan baru manapun yang dienkripsi dengan kunci yang sama

CHOSEN-PLAINTEXT ATTACK

- Kriptanalis tidak hanya mempunyai akses untuk cipherteks dan plainteks yang dihubungkan untuk beberapa pesan, tetapi juga memilih plainteks yang dapat dienkripsi
- Lebih kuat dibanding known-plaintext attack
- Kriptanalis dapat memilih blok plainteks spesifik untuk enkripsi yang menghasilkan informasi lebih tentang kunci
- Pekerjaannya adalah menyimpulkan kunci yang digunakan untuk enkripsi pesan atau suatu algoritma untuk dekripsi pesan baru manapun yang dienkripsi dengan kunci yang sama

ADAPTIVE-CHOSEN-PLAINTEXT ATTACK

- Merupakan kasus khusus dari chosen-plaintext attack
- Kriptanalis tidak hanya dapat memilih plainteks yang dienkripsi, tetapi juga dapat memodifikasi pilihannya berdasarkan pada hasil enkripsi sebelumnya
- Pada chosen-plaintext attack, suatu kriptanalis hanya dapat memilih satu blok plainteks yang besar untuk dienkripsi; pada adaptive-chosen-plaintext attack, dapat memilih suatu blok plainteks yang lebih kecil dan kemudian memilih yang lainnya berdasarkan pada hasil yang pertama

CHOSEN-CIPHERTEXT ATTACK

- Kriptanalis dapat memilih cipherteks yang berbeda untuk bisa dienkripsi dan mempunyai akses untuk plainteks yang didekripsi
- Serangan ini diterapkan untuk algoritma public-key
- Kadang-kadang efektif melawan algoritma simetris
- Kadang-kadang chosen-plaintext attack dan chosen-ciphertext attack sama-sama dikenal sebagai chosen-text attack

CHOSEN-KEY ATTACK

- Serangan ini tidak berarti bahwa kriptanalis dapat memilih kunci
- Mempunyai beberapa pengetahuan tentang hubungan antara kunci yang berbeda

RUBBER-HOSE CRYTANALYSIS

- Kriptanalis mengancam, memeras, atau menyiksa seseorang sampai mereka memberikan kuncinya
- Penyuapan kadang-kadang dikenal sebagai suatu purchase-key attack
- Ini semua adalah serangan yang sangat kuat dan sering juga menjadi cara yang terbaik untuk memecahkan algoritma

JENIS PENYERANGAN PADA JALUR KOMUNIKASI

- Sniffing
- Replay attack
- Spoofing
- Man in the Middle