PERTEMUAN 02

SERANGAN TERHADAP KRIPTOGRAFI

Sub Pembahasan

1. Kriptanalis
2. Tujuan Kriptografi
3. Serangan Kriptografi
4. Kompleksitas Serangan

Kriptanalisis dan kriptologi

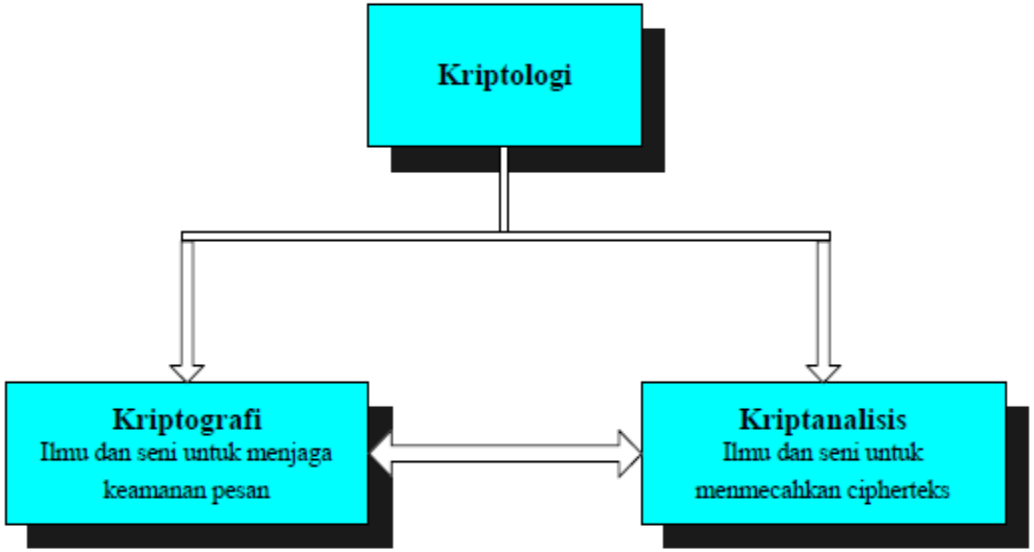
Kriptografi berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptanalisis.

Kriptanalisis (cryptanalysis) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis.

Jika seorang kriptografer (cryptographer) mentransformasikan plainteks menjadi cipherteks dengan suatu algoritma dan kunci maka sebaliknya

seorang kriptanalis berusaha untuk memecahkan cipherteks tersebut untuk menemukan plainteks atau kunci.

Kriptologi (cryptology) adalah studi mengenai kriptografi dan kriptanalisis. Baik kriptografi maupun kriptanalisis keduanya saling berkaitan, dapat dilihat seperti gambar dibawah ini :



Sumber: Renaldi Munir

Tujuan Kriptografi:

Tujuan kriptografi adalah memberikan layanan keamanan. Aspek keamanan sebagai berikut:

1. Kerahasiaan (confidentiality)

Layanan yang digunakan untuk menjaga isi pesan dari siapapun yang tidak berhak untuk membacanya

Tujuan kriptografi:

2. Integritas data(data integrity)

Layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman.

“Apakah pesan yang diterima masih asli atau tidak mengalami perubahan(modifikasi)?”.

Tujuan kriptografi:

3. Otentikasi (authentication)

Layanan yang untuk mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication*) dan untuk mengidentifikasi kebenaran sumber pesan (*data origin authentication*).

“Apakah pesan yang diterima benar-benar berasal dari pengirim yang benar?”

Tujuan kriptografi:

4. Nirpenyangkalan (non-repudiation)

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

Serangan terhadap kriptografi:

Berdasarkan keterlibatan penyerang dalam komunikasi, serangan dapat dibagi atas dua macam, yaitu:

A. **Serangan pasif (passive attack)**

Pada serangan ini, penyerang tidak terlibat dalam komunikasi antara pengirim dan penerima, namun penyerang menyadap semua pertukaran pesan antara kedua entitas tersebut. Tujuannya adalah untuk mendapatkan sebanyak mungkin informasi yang digunakan untuk kriptanalisis.

Beberapa metode penyadapannya antara lain:

1. Wiretapping: penyadap mencegat data yang ditransmisikan pada saluran kabel komunikasi dengan menggunakan sambungan perangkat keras.
2. Electromagnetic eavesdropping: penyadap mencegat data yang ditrasmisikan melalui saluran wireless, misalnya radio dan microwave.
3. Acoustic eavesdropping : menangkap gelombang suara yang dihasilkan oleh suara manusia.

Serangan terhadap kriptografi:

B. **Serangan Aktif (Active attack)**

Pada jenis serangan ini, penyerang mengintervensi komunikasi dan ikut mempengaruhi sistem untuk keuntungan dirinya.

Misalnya penyerang mengubah aliran pesan seperti menghapus sebagian cipherteks, mengubah cipherteks, menyisipkan potongan cipherteks palsu, me-replay pesan lama, mengubah informasi yang tersimpan, dan sebagainya.

Serangan terhadap kriptografi:

Berdasarkan banyaknya informasi yang diketahui oleh kriptanalis, maka serangan dapat dikelompokkan menjadi lima jenis, yaitu:

1. Ciphertext-only

Adalah jenis serangan yang paling umum namun paling sulit, karena informasi yang tersedia hanyalah cipherteks saja. Kriptanalis memiliki beberapa cipherteks dari beberapa pesan, semuanya dienkripsi dengan algoritma yang sama.

2. Known-plaintext
Adalah jenis serangan dimana kriptanalis memiliki pasangan plainteks dan cipherteks yang berkoresponden.

3. Chosen-plaintext
Serangan jenis ini lebih hebat dari pada known-plaintext attack, karena kriptanalis dapat memilih plainteks yang dimilikinya untuk dienkripsikan, yaitu plainteks-plainteks yang lebih mengarahkan penemuan kunci.

4. Chosen-ciphertext attack
Adalah jenis serangan dimana kriptanalis memilihcipherteks untuk didekripsikan dan memiliki akses ke plainteks hasil dekripsi.

5. Chosen-text
Adalah jenis serangan yang merupakan kombinasi chosen-plaintext attack dan chosen-chiphertext attack.

Serangan terhadap kriptografi:

Berdasarkan teknik yang digunakan dalam menemukan kunci, maka serangan dapat dibagi menjadi 4, yaitu:

1. Exhaustive attack atau brute force attack

Adalah serangan untuk mengungkap plainteks atau kunci dengan menggunakan semua kemungkinan kunci.

Diasumsikan kriptanalis mengetahui algoritma kriptografi yang digunakan oleh pengirim pesan. Selain itu kriptanalis memiliki sejumlah cipherteks dan plainteks yang bersesuaian.

2. Analytical attack

Pada jenis serangan ini, kriptanalis tidak mencoba-coba semua kemungkinan kunci tetapi menganalisis kelemahan algoirtma kriptografi untuk mengurangi kemungkinan kunci yang tidak ada.

Diasumsikan kriptanalis mengetahui algoritma kriptografi yang digunakan oleh pengirim pesan. Analisis dapat menggunakan pendekatan matematik dan statistik dalam rangka menemukan kunci.

3. Related-key attack

Kriptanalis memiliki cipherteks yang dienkripsi dengan dua kunci berbeda.
Kriptanalis tidak mengetahui kedua kunci tersebut namun ia mengetahui hubungan antara kedua kunci, misalnya mengetahui kedua kunci hanya berbeda 1 bit

4. Rubber-hose cryptanalysis

Ini mungkin jenis serangan yang paling ekstrim dan paling efektif.
Penyerang mengancam, mengirim surat gelap, atau melakukan penyiksaan sampai orang yang memegang kunci memberinya kunci untuk mendekripsi pesan.

Kompleksitas serangan

Kompleksitas serangan dapat diukur dengan beberapa cara, yaitu :

1. Kompleksitas data (data complexity)

Jumlah data (plainteks dan cipherteks) yang dibutuhkan sebagai masukan untuk serangan. Semakin banyak data yang dibutuhkan untuk melakukan serangan, semakin kompleks serangan tersebut, yang berarti semakin bagus sistem kriptografi tersebut.

2. Kompleksitas waktu (time complexity)

Waktu yang dibutuhkan untuk melakukan serangan. Semakin lama waktu yang dibutuhkn untuk melakukan serangan, berarti semakin bagus kriptografi tersebut

3. Kompleksitas ruang memori (space/storage complexity)

Jumlah memori yang dibutuhkan untuk melakukan serangan. Semakin banyak memori yang dibutuhkan untuk melakukan serangan, berarti semakin bagus sistem kriptografi tersebut.

Daftar Pustaka

- http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2006-2007/Makalah1/Makalah1-003.pdf

