Jenis-Jenis Serangan terhadap Kriptografi

Naila Fithria (13506036)
Jurusan Teknik Informatika ITB, Bandung, email: if16036@students.if.itb.ac.id

Abstract – *Makalah ini membahas serangan-serangan yang ditujukan terhadap kriptografi. Jenis-jenis serangan terhadap kriptografi dapat dibedakan berdasarkan ketersediaan data yang ada,metode penyadapan data yang biasanya dilakukan oleh penyerang, dan berdasarkan bagaimana cara dan posisi seseorang mendapatkan pesan-pesan dalam saluran komunikasi.*
Jenis serangan berdasarkan ketersediaan data yang ada, diklasifikasikan menjadi 7 macam, yaitu ciphertext-only attack, known-plaintext attack, chosen-plaintext attack, adaptive-chosen-plaintext attack, chosen-ciphertext attack, chosen-key attack, dan rubber-hose cryptanalysis.
Jenis-jenis serangan berdasarkan metode penyadapan data yang biasanya dilakukan oleh penyerang yaitu antara wiretapping, electromagnetic eavesdropping, atau acoustic eavesdropping.
Sedangkan, jenis serangan berdasarkan bagaimana cara dan posisi seseorang mendapatkan pesan-pesan dalam saluran komunikasi ada 4 macam, yaitu sniffing, replay attack, spoofing, dan man-in-the-middle.
Makalah ini akan membahas jenis-jenis serangan tersebut lebih mendalam.

Kata Kunci*: kriptografi, kunci, attack, informasi*

1. PENDAHULUAN

Kemajuan di bidang telekomunikasi dan komputer di masa ini sangatlah pesat, sebagai contoh kini pengiriman informasi atau pembayaran pembelian barang dapat dengan mudah dilakukan secara *on-line*.

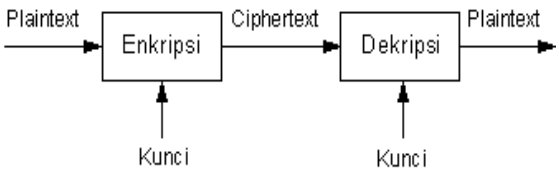
Kegiatan-kegiatan tersebut tentu saja akan menimbulkan resiko bila informasi yang berharga tersebut diakses oleh orang-orang yang tidak berhak. Misalnya, informasi mengenai nomor kartu kredit, bila informasi tersebut jatuh kepada orang yang tidak berhak, tentu akan digunakan untuk kepentingan yang tidak semestinya.

Sebelum tahun 1970-an, teknologi kriptografi digunakan terbatas hanya untuk tujuan militer dan diplomatik. Akan tetapi kemudian seiring berjalannya waktu, bidang bisnis dan perorangan mulai menyadari pentingnya melindungi informasi berharga melalui kriptografi.

1.1 Pengertian Kriptografi

Kriptografi adalah ilmu yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim, dapat tersampaikan dengan aman pada penerima dengan cara menyamarkannya dalam bentuk sandi yang tidak mempunyai makna. Keutamaan dari kriptografi adalah menjaga kerahasiaan pesan dari penyadap dan kriptanalis.

Suatu pesan yang tidak disandikan disebut sebagai plainteks (*plaintext)* atau dapat juga disebut sebagai *cleartext*. Sedangkan, pesan yang sudah disandikan disebut cipherteks (*ciphertext)*. Proses yang dilakukan untuk mengubah plainteks ke dalam cipherteks disebut enkripsi (*encryption* atau *encipherment*). Sedangkan proses untuk mengubah ciphertext kembali ke plaintext disebut dekripsi (*decryption* atau *decipherment*). Secara sederhana istilah-istilah di atas dapat digambarkan sebagai berikut :



Gambar 1: Proses Enkripsi/Dekripsi Sederhana

Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi. Seperi yang telah diketahui, enkripsi adalah proses mengubah suatu pesan asli (*plaintext*) menjadi suatu pesan dalam bahasa sandi (*ciphertext*).

$$C = EK(M)$$

dimana

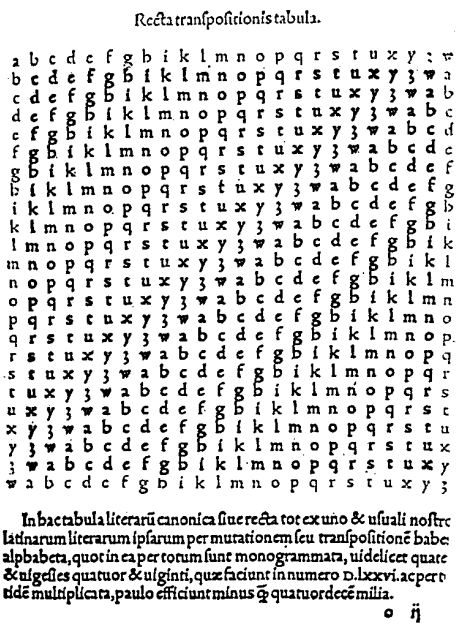
M = pesan asli
E = proses enkripsi
K= kunci
C = pesan dalam bahasa sandi (untuk ringkasnya disebut sandi)

Sedangkan dekripsi adalah proses mengubah pesan dalam suatu bahasa sandi menjadi pesan asli kembali.

$M = DK(C)$
D = proses dekripsi

Pada saat proses enkripsi kita menyandikan pesan M dengan suatu kunci K lalu dihasilkan pesan C. Sedangkan pada proses dekripsi, pesan C tersebut diuraikan dengan menggunakan kunci K sehingga dihasilkan pesan M yang sama seperti pesan sebelumnya.

Dengan demikian keamanan suatu pesan tergantung pada kunci yang digunakan.


Recta tranſpoſitionis tabula.

In hac tabula literarū canonica ſiue recta tot ex uno & uſuali noſtrę latinarum literarum ipſarum permutationem ſeu tranſpoſitionē babe alphabeta, quot in ea per totum ſunt monogrammata, uidelicet quate & uigeſies quatuor & uiginti, quæ faciunt in numero D.lxxvi. ac perd tidē multiplicata, paulo efficiunt minus q̄ quatuordecē milia.

o ij

Gambar 2: Contoh Cipherteks

1.2 Fungsi Kriptografi

Dalam teknologi informasi, terus menerus dikembangkan cara untuk menangkal berbagai bentuk serangan seperti penyadapan dan pengubahan data yang dikirimkan. Salah satu cara yang ditempuh mengatasi masalah ini adalah dengan menggunakan kriptografi yang menggunakan transformasi data sehingga data yang dihasilkan tidak dapat dimengerti oleh pihak yang tidak berhak mengakses. Transformasi ini memberikan solusi pada dua macam masalah keamanan data, yaitu masalah privasi (*privacy*) dan keautentikan (*authenticatioan*). Privasi mengandung arti bahwa data yang dikirimkan hanya dapat dimengerti informasinya oleh penerima yang sah atau berhak. Sedangkan keotentikan mencegah pihak ketiga untuk mengirimkan data yang salah atau mengubah data yang dikirimkan.

Sehingga, kriptografi diharapkan dapat memenuhi kriteria-kriteria sebagai berikut:

1. Kerahasiaan (*confidentiality*), yang dapat terjamin dengan adanya enkripsi (penyandian).
2. Keutuhan (*integrity*) atas data-data pembayaran, yang dapat terjamin dengan penggunaan fungsi hash. Fungsi hash adalah fungsi yang secara efisien mengubah string input dengan panjang berhingga menjadi string output dengan panjang tetap yang disebut nilai hash.
3. Jaminan atas identitas dan keabsahan (*authenticity*) pihak-pihak yang melakukan transaksi, yang terjamin dengan digunakannya password atau sertifikat digital. Sedangkan keautentikan data transaksi dapat terjamin dengan menggunakan tanda tangan digital.
4. Transaksi dapat dijadikan barang bukti yang tidak bisa disangkal (*non-repudiation)* dengan memanfaatkan tanda tangan digital dan sertifikat digital.

2. PEMBAHASAN

2.1 Kriteria Keamanan Kriptografi

Sebuah algoritma kriptografi dikatakan aman (*computationally secure*) bila memenuhi tiga kriteria berikut:

1. Persamaan matematis yang menggambarkan operasi algoritma kriptografi sangat kompleks sehingga algoritma tidak mungkin dipecahkan secara analitik.
2. Biaya untuk memecahkan chiperteks melampaui nilai informasi yang terkandung di dalam chiperteks tersebut.
3. Waktu yang diperlukan untuk memecahkan chiperteks melampaui lamanya waktu informasi tersebut harus dijaga kerahasiaannya.

2.1 Penyerangan terhadap Kriptografi

Selain ada pihak yang ingin menjaga agar pesan tetap aman, namun ada juga pihak-pihak yang ingin mengetahui pesan rahasia tersebut secara tidak sah. Bahkan ada pihak-pihak yang ingin agar dapat mengubah isi pesan tersebut.

Ilmu untuk mendapatkan pesan yang asli dari pesan yang telah disandikan tanpa memiliki kunci untuk membuka pesan rahasia tersebut disebut kriptoanalisis. Sedangkan usaha untuk membongkar suatu pesan sandi tanpa mendapatkan kunci dengan cara yang sah dikenal dengan istilah serangan (*attack*).

2.2 Jenis-Jenis Serangan terhadap Kriptografi

Di bawah ini dijelaskan beberapa macam penyerangan terhadap pesan yang sudah dienkripsi, berdasarkan ketersediaan data yang ada, dan tingkat kesulitannya bagi penyerang, dimulai dari yang paling sulit adalah :

1. *Ciphertext only attack*, penyerang hanya mendapatkan ciphertext dari sejumlah pesan yang seluruhnya telah dienkripsi menggunakan algoritma yang sama. Sehingga, metode yang digunakan untuk memecahkannya adalah *exhaustive key search*, yaitu mencoba semua kemungkinan yang ada untuk menemukan kunci.

2. *Known plaintext attack*, dimana penyerang selain mendapatkan sandi, juga mendapatkan pesan asli. Terkadang disebut pula *clear-text attack.*

3. *Choosen plaintext attack*, sama dengan known plaintext attack, namun penyerang bahkan dapat memilih penggalan mana dari pesan asli yang akan disandikan. Serangan jenis ini lebih hebat daripada *known-plaintex*t attack, karena kriptoanalis dapat memilih plainteks tertentu untuk dienkripsikan, yaitu plainteks-plainteks yang lebih mengarahkan penemuan kunci.

4. *Chosen-ciphertext attack.* Pada tipe ini, kriptoanalis dapat memilih cipherteks yang berbeda untuk didekripsi dan memiliki akses atas plaintext yang didekripsi.

5. *Chosen-key attack.* Kriptoanalis pada tipe penyerangan ini memiliki pengetahuan tentang hubungan antara kunci-kunci yang berbeda dan memilih kunci yang tepat untuk mendekripsi pesan.

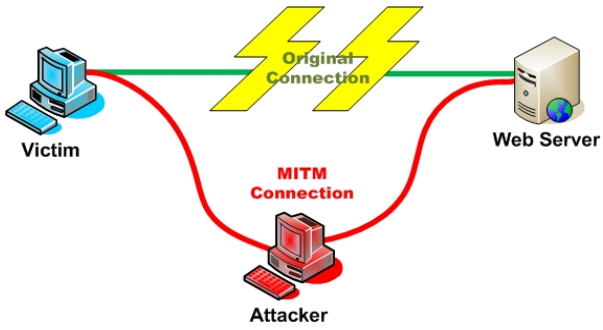
6. *Rubber-hose cryptanalysis*. Pada tipe penyerangan ini, kriptoanalis mengancam, menyiksa, memeras, memaksa, atau bahkan menyogok seseorang hingga mereka memberikan kuncinya. Ini adalah cara yang paling ampuh untuk mendapatkan kunci.

7. *Adaptive – chosen – plaintext attack.* Penyerangan tipe ini merupakan suatu kasus khusus *chosen-plaintext attack*. Kriptoanalis tidak hanya dapat memilih plainteks yang dienkripsi, ia pun memiliki kemampuan untuk memodifikasi pilihan berdasarkan hasil enkripsi sebelumnya.
   Dalam *chosen-plaintext attack*, kriptoanalis mungkin hanya dapat memiliki plainteks dalam suatu blok besar untuk dienkripsi; dalam *adaptive-chosen-plaintext* attack ini ia dapat memilih blok plainteks yang lebih kecil dan kemudian memilih yang lain berdasarkan hasil yang pertama, proses ini dapat dilakukannya terus menerus hingga ia dapat memperoleh seluruh informasi.

Berdasarkan bagaimana cara dan posisi seseorang mendapatkan pesan-pesan dalam saluran komunikasi, penyerangan dapat dikategorikan menjadi:

1. *Spoofing*: Penyerang – misalnya Diman – bisa menyamar menjadi Adi. Semua orang dibuat percaya bahwa Diman adalah Adi. 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.

2. *Man-in-the-middle* : Jika spoofing terkadang hanya menipu satu pihak, maka dalam skenario ini, saat Adi hendak berkomunikasi dengan Badu, Diman di mata Adi seolah-olah adalah Badu, dan Diman dapat pula menipu Badu sehingga Diman seolah-olah adalah Adi. Diman dapat berkuasa penuh atas jalur komunikas ini, dan bisa membuat berita fitnah.



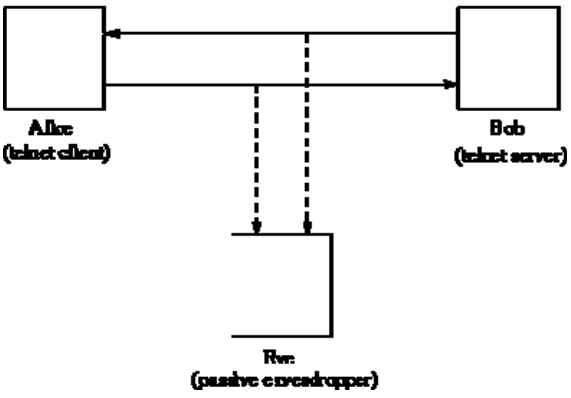
Gambar 3: Ilustrasi *Man-in-the-middle Attack*

3. *Sniffing*: secara harfiah 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.

4. *Replay attack* : Jika seseorang bisa merekam pesan-pesan *handshake* (persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak.

Serangan dilakukan secara aktif bilamana penyerang mengintervensi komunikasi dan ikut mempengaruhi sistem untuk keuntungan dirinya atau penyerang mengubah aliran pesan seperti menghapus sebagian cipherteks, mengubah cipherteks, menyisipkan potongan cipherteks palsu, me-*replay* pesan lama, mengubah informasi yang tersimpan, dan sebagainya. *Man-in-the-midle, replay attack, dan spoofing* termasuk jenis serangan ini.

Serangan dilakukan secara pasif, terjadi bilamana penyerang tidak terlibat dalam komunikasi antara pengirim dan penerima atau penyerang hanya melakukan penyadapan untuk memperoleh data atau informasi sebanyak-banyaknya.



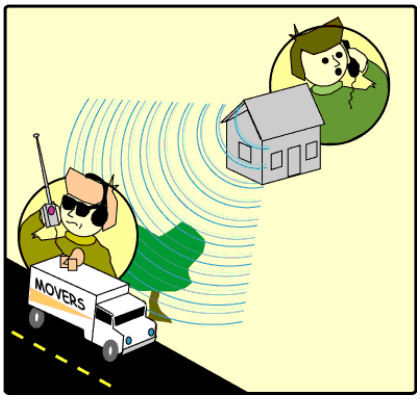
Gambar 4: Ilustrasi Serangan Pasif

Beberapa metode penyadapan data yang biasanya dilakukan oleh penyerang:

1. *Electromagnetic eavesdropping*
   Penyadap mencegat data yang ditransmisikan melalui saluran wireless, misalnya radio dan *microwive*.

2. *Acoustic Eavesdropping*.
   Menangkap gelombang suara yang dihasilkan oleh suara manusia.

3. *Wiretapping*
   Penyadap mencegat data yang ditransmisikan pada saluran kabel komunikasi dengan menggunakan sambungan perangkat keras.



Gambar 5: Ilustrasi *Wiretapping*

Jenis-jenis serangan berdasarkan teknik yang digunakan untuk menemukan kunci:

1. *Brute force attack* atau *Exhaustive attack*
   Serangan brute-force adalah sebuah teknik serangan yang menggunakan percobaan terhadap semua kunci yang mungkin untuk mengungkap plainteks/kunci.

   Pendekatan ini pada awalnya merujuk pada sebuah program komputer yang mengandalkan kekuatan pemrosesan komputer dibandingkan kecerdasan manusia. Sebagai contoh, untuk menyelesaikan sebuah persamaan kuadrat seperti $x^2+7x-44=0$, di mana x adalah sebuah integer, dengan menggunakan teknik serangan brute-force, penggunanya hanya dituntut untuk membuat program yang mencoba semua nilai integer yang mungkin untuk persamaan tersebut hingga nilai x sebagai jawabannya muncul. Istilah brute force sendiri dipopulerkan oleh Kenneth Thompson, dengan mottonya: "*When in doubt, use brute-force*" (jika ragu, gunakan brute-force).

   Teknik ini adalah teknik yang paling banyak digunakan untuk memecahkan password, kunci, kode atau kombinasi. Cara kerja metode ini sangat sederhana yaitu mencoba semua kombinasi yang mungkin.

   Salah satu contoh penggunaan *brute force* attack adalah *password cracker*. Sebuah password dapat dibongkar dengan menggunakan program bernama password cracker ini. Program password cracker adalah program yang mencoba membuka sebuah password yang telah terenkripsi dengan menggunakan sebuah algoritma tertentu dengan cara mencoba semua kemungkinan. Teknik ini sangatlah sederhana, tapi efektivitasnya luar biasa, dan tidak ada satu pun sistem yang aman dari serangan ini,

meski teknik ini memakan waktu yang sangat lama, khususnya untuk password yang rumit.

Namun ini tidak berarti bahwa password cracker membutuhkan *decrypt*. Pada prakteknya, mereka kebanyakan tidak melakukan itu. Umumnya, kita tidak dapat melakukan dekripsi password-password yang sudah terenkripsi dengan algoritma yang kuat.

Proses-proses enkripsi modern kebanyakan hanya memberikan satu jalan, di mana tidak ada proses pengembalian enkripsi. Namun, umumnya, tool-tool simulasi yang mempekerjakan algoritma yang sama yang digunakan untuk mengenkripsi password orisinal, dipakai. Tool-tool tersebut membentuk analisa komparatif. Program password cracker tidak lain adalah mesin-mesin ulet. Ia akan mencoba kata demi kata dalam kecepatan tinggi. Mereka menganut "Asas Keberuntungan", dengan harapan bahwa pada kesempatan tertentu mereka akan menemukan kata atau kalimat yang cocok.

2. *Analytical attack*

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

Analisis dilakukan dengan dengan memecahkan persamaan-persamaan matematika (yang diperoleh dari definisi suatu algoritma kriptografi) yang mengandung peubah-peubah yang merepresentasikan plainteks atau kunci.

Asumsi yang digunakan: kriptanalis mengetahui algoritma kriptografi.

Untuk menghadapi serangan ini, kriptografer harus membuat algoritma kriptografi yang kompleks sedemikian rupa sehingga plianteks merupakan fungsi matematika dari chiperteks dan kunci yang cukup kompleks, dan tiap kunci merupakan fungsi matematika dari chiperteks dan plainteks yang cukup kompleks.

Metode *analytical attack* biasanya lebih cepat menemukan kunci dibandingkan dengan *exhaustive attack.*

3. KESIMPULAN

Seiring dengan perkembangan jaman, perkembangan teknologi juga semakin pesat, terutama teknologi informasi dan semakin padatnya lalu lintas informasi. Hal ini menuntut adanya suatu komunikasi yang aman untuk pengiriman data. Kriptografi adalah jawaban dari permasalahan itu.

Dimana, kriptografi dapat digunakan untuk mencegah pihak ketiga yang tidak berhak untuk memasuki sistem komunikasi tempat pengiriman data yang kerahasiannya dilindungi .

Akan tetapi, di lain pihak, jenis-jenis serangan terhadap kriptografi semakin beragam dan semakin sulit untuk untuk dipatahkan. Metode-metode yang dipakai juga semakin variatif dan bermacam-macam.

Jenis-jenis serangan terhadap kriptografi bermacam-macam, dimulai dari penyadapan data, sampai dengan pemaksaan secara langsung kepada pengirim atau penerima data untuk membocorkan kuncinya.

Oleh karena itu, kriptografi demi memenuhi fungsinya agar dapat tersampaikan dengan aman pada penerima, dengan kerahasiaan yang terjaga serta otentik, juga harus senantiasa dikembangkan sedemikian mungkin sehingga dapat menangkal berbagai bentuk serangan terhadap dirinya.

DAFTAR REFERENSI

[1] Munir, Rinaldi. “Diktat Kuliah IF2153” *Matematika Diskrit*, Edisi Keempat, Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, Institut Teknologi Bandung, 2006, hal 21-25.

[2] Skma komunitas online. Kriptografi dan Pengamanan Komputer (2007). www.skma.org Tanggal Akses: 29 Desember 2007 20.44.

[3] http://www.geocities.com/amwibowo/resource/komparasi/bab3.html. Tanggal Akses: 29 Desember 21.17.

[4] Wikipedia, Ensiklopedia Bebas. Serangan Brute Force (2007). http://id.wikipedia.org/wiki/Serangan_brute-force Tanggal Akses: 29 Desember 21.02.

[5] Konsultan Linux. Pengenalan Kriptografi (2007). www.konsultanlinux.com. Tanggal Akses: 29 Desember 22.30.