Teknik-teknik Kriptanalisis

Anggun Hapsari, Ronny Perdana, Risvelina

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : if11028@students.if.itb.ac.id, if11052@students.if.itb.ac.id, if10022@students.if.itb.ac.id.

Abstrak

Kriptanalis dapat diartikan sebagai sebuah pihak yang berusaha menemukan rahasia (*plaintext* atau kunci) dari suatu pesan yang telah terenkripsi (*chipertext*), atau dengan kata lain, melakukan proses kriptanalisis. Kriptanalis bekerja secara informal, berada di pihak lawan. Namun terkadang cara-cara yang digunakan oleh para kriptanalis, dipraktekan oleh pihak-pihak yang berkepentingan dalam rangka menguji ketahanan suatu algoritma enkripsi/dekripsi. Pada makalah ini akan dibahas beberapa teknik kriptanalisis, mekanisme yang dilakukan, algoritma enkripsi/dekripsi yang telah berhasil dipatahkan oleh teknik kriptanalisis yang bersangkutan dan bahkan metoda yang dapat digunakan pada algoritma enkripsi/dekripsi untuk mematahkan teknik kriptanalisis tersebut. Pada akhirnya akan diberikan kesimpulan mengenai berbagai teknik kriptanalisis yang dibahas.

***Kata kunci**:kriptanalis*, *kriptanalisis*, *ciphertext*

1. Pendahuluan

Kriptanalisis adalah sebuah studi mengenai *cipher*, *ciphertext* atau *cyrptosystems* yang bertujuan menemukan kelemahan dalam sistem penyandian, sehingga dimungkinkan untuk memperoleh *plaintext* dari *ciphertext* yang ada, tanpa perlu mengetahui kunci ataupun algoritma pembangun *ciphertext* tersebut. Cara ini disebut dengan memecahkan *cipher*, *ciphertext* atau *cryptosystem* [1)].

Dalam memecahkan *cipher*, dilakukan pencarian kesalahan dalam desain atau implementasi dari *cipher* itu sendiri sehingga dapat mengurangi jumlah kunci yang harus dicoba ketika melakukan *brute force attack* (mencoba memecahkan *cipher* dengan menggunakan semua kunci yang mungkin sampai akhirnya ditemukan satu kunci yang benar). Contohnya, jika kunci yang digunakan untuk mengenkripsi sepanjang 2^{128} , maka *brute force attack* akan mencoba semua kunci yang mungkin , yaitu sebanyak 2^{128} (atau rata-rata 2^{127}) kali untuk menemukan kunci yang tepat. Iterasi sebesar itu masih belum dapat dilakukan secara cepat oleh sistem komputasi saat ini. Dengan adanya studi kriptanalisis, telah ditemukan cara pengekstraksian *plaintext* hanya dalam 2^{40} kali iterasi. Walaupun belum sepenuhnya terpecahkan, namun *plaintext* telah dapat diekstrak dari *cipher* dengan menggunakan sumberdaya komputasi yang relatif jauh lebih kecil.

2. Teknik-teknik Kriptanalisis

Terdapat beberapa teknik dalam melakukan kriptanalisis, tergantung kepada akses yang dimiliki oleh kriptanalis, apakah melalui *ciphertext*, *plaintext*, ataupun aspek lain dari sistem kriptografi. Berikut adalah beberapa tipe penyerangan yang umum dipakai untuk memecahkan sandi :

1. Known-Plaintext Analysis

Dengan prosedur ini, kriptanalis mengetahui sebagian isi *plaintext* dari *ciphertext* yang berhasil didapatkan. Menggunakan informasi yang ada ini, kriptanalis berusaha untuk mencari kunci yang digunakan untuk menghasilkan *ciphertext*.

Pesan-pesan yang memiliki format terstruktur memberikan peluang kepada kriptanalis untuk menebak *plaintext* dari *ciphertext* yang bersesuaian. Contoh dari pesan-pesan terstruktur ini adalah *email* dengan kolom *from*, *to*, *subject*, kemudian salam penutup dan pembuka pada surat seperti ”dengan hormat”, salam, dan lainnya.

Dimiliki [9)]:

C1=Ek(P1) dan P1
C2=Ek(P2) dan P2
....
Ci=Ek(Pi) dan Pi

Deduksi :

kunci

Linear Cryptanalysis adalah salah satu algoritma yang termasuk ke dalam serangan *known-plaintext*. *Linear Cryptanalysis* diperkenalkan oleh Mitsuru Matsui pada tahun 1993. Pada algoritma ini penyerang akan mempelajari fungsi linear yang merepresentasikan hubungan antara *ciphertext* dan *plaintext* untuk mendapatkan kunci.

Untuk algoritma yang menggunakan fungsi XOR, suatu fungsi linier sederhana dapat dibentuk dan dipecahkan dengan probabilitas sebesar 1 (pasti dipecahkan). Sedangkan untuk fungsi yang lebih kompleks seperti S-Box, akan dicari suatu fungsi linear ,yang memiliki probabilitas sebesar p, dengan memaksimalkan $|p-½|$. Untuk seluruh teks *cipher* akan didapatkan fungsi [5)]:

$$P[i1, i2, . , ia] \oplus C[j1, j2, . , jb] = K[k1, k2, . , kc] \quad ....(1)$$

Dimana **i1, i2, . . , ia, j1, j2, . . , jb** dan **k1, k2, . . , kc** menggambarkan lokasi bit tetap. Fungsi ini didapatkan melalui konkatenasi satu siklus fungsi linier. Suatu fungsi linier dikatakan cukup tepat apabila memiliki $p \neq ½$. Sebagai contoh, fungsi linear untuk mendekati kunci yang dibangun menggunakan algoritma DES memiliki probabilitas sebesar $½+2^{-24}$.

Algoritma berbasis XOR, termasuk ke dalam algortima enkripsi/dekripsi yang tidak aman karena dapat dipecahkan menggunakan *linear cryptanalysis*.

2. Chosen-Plaintext Analysis

Kriptanalis telah dapat menghasilkan *plaintext* dari *ciphertext* yang ada, namun kuncinya sendiri belum ditemukan. Pada serangan jenis ini kriptanalis dapat memilih *plaintext* tertentu untuk dienkripsikan, yaitu *plaintext* yang lebih mengarahkan penemuan kunci.

Kriptanalis berusaha untuk menemukan kunci pembangun *ciphertext* dengan membandingkan keseluruhan *ciphertext* dengan *plaintext* yang ada. Teknik enkripsi RSA (Rivest-Shanir-Adleman) telah terbukti dapat dipecahkan menggunakan teknik analisis ini.

Dimiliki [9]:

C1=Ek(P1) dan P1
C2=Ek(P2) dan P2
....
Ci=Ek(Pi) dan Pi

Deduksi :

kunci

Differential Analysis adalah sebuah teknik yang dikembangkan oleh Eli Biham dan Adi Shamir. Teknik ini memberikan suatu cara untuk menemukan beberapa bit kunci dari *plaintext* dan *ciphertext* yang tersedia, dengan begitu jumlah kemungkinan kunci yang akan dicoba pada *exhaustive key search* atau *brute force attack* dapat berkurang drastis, mengurangi waktu kalkulasi.

Differential Analysis secara garis besar membahas pola lengkap dari bit-bit mana saja yang berubah dan tidak berubah pada proses pengubahan input menjadi output. Prinsip dasar dari *Differential Analysis* adalah [2]:

”Suatu ciphertext memiliki karakteristik dimana terdapat suatu konstanta X sehingga untuk banyak pasangan *plaintext* A dan B dimana B=(A xor X), jika sebuah pernyataan bernilai benar tehadap kunci, E(B,k) = (E(A,k) xor Y) untuk beberapa konstanta Y akan benar dengan probabilitas diatasnya (kemungkinan acak)”

3. Ciphertext-Only Analysis

Pada teknik ini, kriptanalis hanya berbekal *ciphertext* saja, tanpa adanya pengetahun mengenai *plaintext*. Teknik ini membutuhkan akurasi yang tinggi dalam melakukan penaksiran mengenai bagaimana sebuah pesan dapat disandikan.

Teknik ini dapat bekerja lebih baik dengan dukungan adanya pengetahuan tambahan mengenai teks. Misalnya dengan pengetahuan bahwa plainteks asal ditulis dalam bahasa inggris maka kriptanalis dapat menghitung frekuensi huruf dari chiperteks kemudian membandingkannya dengan frekuensi rata-rata huruf pada teks berbahasa inggris. Namun cara penghitungan frekuensi huruf seperti ini hanya bekerja untuk *plaintext* yang didekripsi menggunakan teknik substitusi satu ke satu.

Dimiliki [9]:

C1=Ek(P1)
C2=Ek(P2)
....
Ci=Ek(Pi)

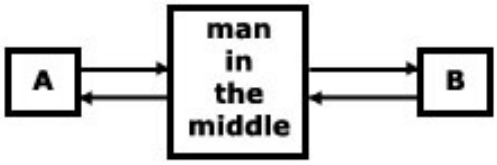
Deduksi :

P1,P2,….,Pi atau kunci

Algoritma kriptografi modern memiliki daya tahan yang lebih tinggi terhadap jenis serangan seperti ini.

4. Man-in-the-middle attack

Penyerang, yang dalam hal ini adalah kriptanalis, masuk kedalam saluran komunikasi antara kedua pihak yang akan saling bertukar kunci mereka. Penyerang menempatkan dirinya sedemikian sehingga kedua pihak tadi merasa bahwa mereka saling bertukar kunci, namun sebenarnya penyeranglah memberikan kunci-kunci yang nantinya digunakan oleh pihak-pihak tadi.



Gambar 1 Serangan kriptografi man-in-the-middle

Teknik ini dapat dipatahkan dengan menggunakan kombinasi fungsi *hash* dan algoritma kunci publik. B dapat memeriksa apakan kunci publik yang ia terima benar,

dengan cara memeriksa sidik jari (*fingerprint*). Sidik jari ini adalah suatu fungsi hash dari kunci publik tersebut yang diberikan melalui jalur yang berbeda dengan pengiriman kunci publik. Sidik jari digunakan karena ukurannya yang lebih kecil dibandingakan dengan kunci publik sehingga lebih mudah ditentukan nilai kebenarannya.

Cara lain untuk mematahkan serangan tipe ini adalah dengan menyimpan kunci publik dalam suatu basisdata online yang menjamin kebenaran dari kunci publik. Suatu CA (*Certificate Authority*) atau server kunci publik dapat memberikan keyakinan pada pengguna, pada saat mereka menyimpan (*download*) kunci, bahwa kunci tersebut bernilai benar.

5. Timing/differential power analysis

Sangat berguna jika digunakan melawan *smartcard*, yang menghitung perbedaan konsumsi elektrik dalam jangka waktu tertentu ketika microchip melakukan pengamanan informasi. Teknik ini dapat digunakan untuk memperoleh informasi mengenai perhitungan pembangkitan kunci yang digunakan dalam algoritma enkripsi dan fungsi-fungsi pengamanan lainnya. Teknik ini dapat ditangkal dengan menggunakan *random noise* ketika melakukan enkripsi, atau mengacak alur fungsi sehingga lebih sulit untuk melacak fluktuasi tenaga listrik yang terpakai. Tipe analisis ini dikembangkan oleh Paul Kocher dari *Cryptography Research*. Penyerangan seperti ini umumnya terlepas dari jenis algoritma kriptografi yang digunakan.

6. Correlation

Keterhubungan antara kunci dengan hasil pengenkripsian merupakan sumber utama yang akan digunakan oleh kriptanalis. Pada kasus yang paling mudah, kunci justru secara tidak sengaja terbocorkan oleh sistem krptografinya sendiri. Untuk kasus yang lebih kompleks, dicari keterhubungan antara informasi yang dapat diperoleh mengenai kriptosistem dan informasi mengenai perkiraan kunci.

Ide mengenai keterhubungan merupakan ide dasar pada kriptosistem.

7. Kesalahan dalam kriptosistem

Kesalahan dalam kriptosistem dapat digunakan dalam kriptanalisis dan bahkan dapat membocorkan kuncinya sendiri. Kesalahan tersebut dapat dimanfaatkan dalam kriptanalisis. Kesalahan disini dapat juga berupa kelemahan dari fungsi matematis yang digunakan oleh algoritma enkripsi/dekripsi atau pemilihan kunci lemah.

Algoritma RSA merupakan contoh algoritma yang memiliki kesalahan yang dapat diserang. Begitu pula algoritma DES, karena algoritma ini memiliki beberapa pasang kunci lemah.

7. Rubber-hose cryptanalysis

Serangan jenis ini dapat dikatakan sebagai serangan yang paling efektif dan dapat langsung memberikan hasil. Serangan ini berupa serangan langsung kepada pihak pengirim.

Rubber-hose attack didasarkan pada teori bahwa manusia yang berada dibawah tekanan akan menjadi lebih lemah. Di lain pihak, komputer tidak mengalami stress (dibawah tekanan) sehingga tidak akan terpengaruh dengan serangan semacam ini.

Pada serangan ini, pihak ketiga akan mengirimkan surat gelap, mengancam atau bahkan menyiksa hingga pihak pengirim mau memberikan kunci atau bahkan langsung memberikan *plaintext* yang besangkutan.

Serangan jenis ini tidak memandang tipe algoritma enkripsi/dekripsi, ia bekerja untuk mematahkan seluruh algoritma enkripsi/dekripsi. Karena alasan inilah

rubber-hose attack disebut sebagai serangan paling efektif.

Terdapat beberapa cara efektif untuk menghadapi serangan jenis ini, antara lain [10]:

- Tetap tenang dan gunakan steganografi
- Pindah di luar jangkauan pihak-pihak lawan, misalnya di luar negeri
- Tingkatkan ketahanan fisik
- Untuk menghindari serangan secara sosial. Menjauhlah dari orang-orang terdekat dan jangan bina hubungan dekat (teman) baru
- Gunakan *multipart key* yang membutuhkan lebih dari satu orang untuk melakukan enkripsi/dekripsi terhadap informasi
- Gunakan One-Time Pad dimana tidak mungkin memecahkan *ciphertext* tanpa menggunakan kunci, karena sifatnya yang terlalu panjang (sama dengan *plaintext*).

8. Serangan terhadap atau menggunakan hardware dari cryptosystem

Serangan jenis ini merupakan serangan jenis baru yang diprediksikan akan semakin sering muncul dengan semakin meluasnya penggunaan *mobile crypto devices*.

Serangan ini didasarkan kepada perhitungan rinci dari proses enkripsi yang dilakukan oleh suatu perangkat kripto. Dari informasi ini akan diperoleh informasi mengenai perhitungan kunci yang digunakan. Ide dasar dari serangan ini terkait erat dengan prinsip *correlation*.

Serangan jenis ini bersifat independen terhadap algoritma kriptografi yang digunakan oleh *mobile crypto devices* yang bersangkutan.

Kesimpulan

Keberhasilan kriptanalisis tergantung kepada kombinasi matematis, keingintahuan, intuisi, keuletan, sumberdaya komputasi yang memadai, dan seringkali keberuntungan.

Saat ini kriptanalisis digunakan di berbagai organisasi, seperti pada sebuah pemerintahan yang ingin menyusup ke dalam transmisi diplomatis dan militer pemerintah lainnya, perusahaan yang sedang memproduksi produk pengamanan dan menggunakan kriptanalis untuk mengetes produk tersebut, atau para hacker dan cracker yang berusaha untuk menyusup kedalam situs rahasia dengan mencari kelemahan dalam protokol pengamanannya. Kriptanalis akan selalu bertentangan dengan kriptografer, karena sementara kriptografer berusaha untuk mengamankan informasi, kriptanalis akan selalu berusaha mencari celah kelemahan dari sistem pengamanan tersebut.

Referensi

[1] Cryptanalysis - a Whatis_com definition, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214432,00.html, diakses tanggal : 28 desember 2004

[2] Differential and Linear Cryptanalysis, http://home.ecn.ab.ca/~jsavard/crypto/, diakses tanggal : 28 Desember 2004.

[3] Introduction to Cryptography, http://www.ssh.com/support/cryptography/introduction/cryptanalysis.html, diakses tanggal : 28 Desember 2004

[4] K. Fukushima, *Handwritten Aplhanumeric Character Recognition by the Neocognitron*, IEEE Trans. on Neural Networks, Vol. 2, No. 3, May 1991

[5] Linear Cryptanalysis, http://www.esat.kuleuven.ac.be/~abiryuko/Enc/e32.pdf, diakses tanggal : 28 Desember 2004.

[6] Linear Cryptanalysis: A Literature Survey, http://www.ciphersbyritter.com/, diakses tanggal : 28 Desember 2004.

[7] Man In The Middle Attack, http://www.fastfoodreviews.com/wiki/wiki.pl?search=Man-In-The-Middle_Attack, diakses tanggal 6 januari 2005.

[8] Munir, Rinaldi, Algoritma Kriptografi Modern, dibaca tanggal : 5 Januari 2005.

[9] Munir, Rinaldi, Serangan (*attack*) terhadap Kriptografi, dibaca tanggal : 5 Januari 2005.

[10] Rubber Hose Attack, http://www.fastfoodreviews.com/wiki/wiki.pl?search=Rubber_Hose_Attack, diakses tanggal 6 januari 2005.

[11] Tokita, Toshio et. al.,Cryptanalysis Technique to Evaluate the Strength of Ciphers, http://global.mitsubishielectric.com/pdf/advance/vol100/04Vol100_TR3.pdf, diakses tanggal : 28 Desember 2004.