PENGGUNAAN KRIPTOGRAFI DAN STEGANOGRAFI BERDASARKAN KEBUTUHAN DAN KARAKTERISTIK KEDUANYA

Rachmansyah Budi Setiawan – NIM : 13507014

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if17014@students.if.itb.ac.id

Abstrak

Makalah ini membahas tentang penggunaan kriptografi dan steganografi dalam mengamankan pesan dan/atau data. Kriptografi merupakan ilmu yang digunakan untuk mengamankan pesan atau data dengan cara mengubahnya (disebut juga dengan enkripsi) menjadi pesan atau data lain dengan algoritma sandi tertentu sehingga tidak sembarang orang bisa mengetahui pesan atau data aslinya. Sementara itu, steganografi merupakan ilmu yang juga digunakan untuk melindungi pesan atau data dengan cara menyelubunginya di dalam pesan atau data lain.

Meskipun sekilas terlihat mirip, namun keduanya memiliki beberapa perbedaan. Salah satunya adalah wujud pesan atau data yang telah dirahasiakan. Kriptografi memiliki beberapa keunggulan dibandingkan steganografi, begitu juga sebaliknya. Oleh karena itu diperlukan pemahaman terhadap karakteristik keduanya supaya dalam mengamankan pesan atau data, seseorang dapat menggunakan teknik yang tepat.

***Kata kunci**:* kriptografi, steganografi, enkripsi, dekripsi, *watermark, plaintext, ciphertext*

1. Pendahuluan

Di zaman yang semakin modern ini, keamanan seolah-olah terlihat semakin terjamin. Padahal pada kenyataannya, kemajuan zaman dan teknologi juga diiringi dengan meningkatnya ancaman terhadap keamanan. Ancaman juga bukan hanya terjadi terhadap keamanan yang bersifat fisik (misalnya pencurian, penipuan) namun juga terjadi untuk hal-hal yang sifatnya maya, seperti pesan yang seharusnya hanya boleh diketahui orang tertentu.

Upaya pengamanan terhadap pesan sebenarnya sudah dilakukan oleh manusia sejak jaman dulu. Salah satu upaya yang dilakukan manusia pada jaman dulu dalam mengamankan pesan yang akan mereka sampaikan dapat dilihat pada masa Julius Caesar, sewaktu ia mengirimkan pesan kepada tentaranya di medan perang. Pesan yang ia kirim diubah menjadi pesan rahasia dengan cara menggeser alfabet sebanyak tiga huruf ke depan, misalnya A menjadi D, B menjadi E, dan seterusnya. Beberapa masa setelah itu, cara menyembunyikan pesan tersebut dikenal sebagai salah satu metode dalam kriptografi.

Meskipun menyembunyikan pesan dengan kriptografi dapat memperkecil resiko keamanan, namun masih terdapat celah-celah yang dapat terlihat oleh pencuri pesan dalam pesan rahasia. Salah satunya adalah pesan rahasia yang tercipta umumnya tidak dapat dibaca secara normal sehingga dapat menimbulkan kecurigaan. Oleh karena itu, manusia kembali mengembangkan cara untuk menyembunyikan pesan yang dapat mengeliminasi kelemahan tersebut. Akhirnya manusia menemukan ilmu baru, yaitu steganografi.

Dengan ditemukannya steganografi, bukan berarti pengiriman pesan menjadi aman sepenuhnya. Meskipun memiliki kelebihan dibandingkan kriptografi, steganografi pun memiliki kelemahan. Oleh karena itu, pengirim pesan harus mempertimbangkan berbagai aspek dalam mengamankan pesannya dan mempertimbangkan metode apa yang sebaiknya digunakan dalam mengamankan pesannya.

2. Kriptografi

Sebelum membandingkan kriptografi dan steganografi lebih jauh, ada baiknya kita mengetahui terlebih dahulu definisi dan hal-hal yang berhubungan dengan keduanya. Dengan cara tersebut, kita dapat melihat dan membandingkan keduanya lebih mudah.

Kriptografi adalah ilmu untuk menjaga kerahasiaan pesan. Meskipun begitu, kriptografi juga sering disebut sebagai sebuah seni, karena memang diperlukan kreativitas dalam mencari metode untuk mengamankan pesan. Tujuan utama dari kriptografi tentu saja untuk mengamankan pesan. Pengamanan pesan yang dilakukan mencakup beberapa aspek yang termasuk dalam aspek keamanan informasi, yaitu:

- Kerahasiaan (menjaga isi pesan dari pihak yang tidak memiliki otoritas)
- Integritas data (menjaga data tidak berubah secara tidak sah)
- Autentikasi (masalah identifikasi data)
- Non-repudiasi (mencegah penyangkalan pembuatan/pengiriman oleh yang membuat/mengirim)

Dalam ilmu kriptografi, sering juga disebutkan istilah enkripsi dan dekripsi. Enkripsi sendiri adalah proses mengubah pesan sebenarnya menjadi sandi rahasia. Sementara itu dekripsi, kebalikan dari enkripsi, adalah proses mengembalikan sandi rahasia kembali menjadi pesan yang sebenarnya.

Kriptografi merupakan ilmu untuk menyembunyikan isi pesan, maka terdapat juga ilmu untuk menemukan isi pesan yaitu kriptanalisis. Selain untuk menemukan isi pesan, kriptanalisis juga dapat digunakan untuk menguji kehandalan algoritma sandi yang digunakan.

Dalam melakukan enkripsi dan dekripsi, diperlukan aturan khusus agar pesan yang diubah pengirim dapat dipahami oleh penerima. Aturan atau algoritma yang dimaksud adalah algoritma sandi. Algoritma sandi yang baik harus bisa membingungkan (menyulitkan rekonstruksi menjadi pesan sebenarnya tanpa algoritma dekripsi) dan meleburkan (menghilangkan karakteristik pesan sebenarnya). Selain itu, algoritma sandi yang baik dan handal adalah algoritma sandi yang kekuatan pengamanannya terletak pada kunci, bukan pada kerahasiaan algoritma itu sendiri.

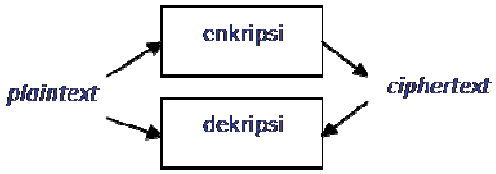
Proses enkripsi dan dekripsi dihubungkan sebagai sebuah relasi antara dua himpunan, himpunan elemen pesan (teks terang/*plaintext*) dan himpunan elemen sandi (*ciphertext*).

E(P) = C ; D(C) = P

E = enkripsi P = *plaintext*
D = dekripsi C = *ciphertext*

Algoritma sandi dapat dibedakan berdasarkan beberapa hal:

- Berdasarkan zaman: klasik dan modern
- Berdasarkan kerahasiaan kunci: kunci rahasia dan kunci public
- Berdasarkan kesamaan kunci enkripsi dan dekripsi: kunci simetris dan kunci asimetris.



Gambar 1. Diagram enkripsi-dekripsi secara umum

2.1 Algoritma Sandi Simetris

Pada algoritma sandi simetris, kunci yang digunakan untuk mengubah *plaintext* menjadi *ciphertext* sama dengan kunci yang digunakan untuk mengembalikan *ciphertext* kembali menjadi *plaintext*. Berdasarkan jumlah data per proses dan alur pengolahan data didalamnya , algoritma sandi simetris dapat dibagi menjadi:

- Block-cipher
  Membagi *plaintext* yang akan dikirimkan ke dalam blok-blok dengan panjang tertentu dan setiap blok dienkripsi dengan menggunakan kunci yang sama
- Stream-cipher
  Mengenkripsi data per satuan data, seperti bit atau byte, dengan menggunakan kunci yang merupakan hasil pembangkitan dari kunci sebelumnya

Contoh algoritma yang menggunakan kunci simetris adalah DES (Data Encryption Standard) dan blowfish. Metode yang digunakan oleh Julius Caesar di atas juga salah satu contoh algoritma sandi simetris.

2.2 Algoritma Sandi Asimetris

Kebalikan dari algoritma sandi simetris, pada algoritma sandi asimetris digunakan kunci yang berbeda dalam enkripsi dan dekripsi, yang biasanya disebut kunci publik (untuk enkripsi) dan kunci privat (untuk dekripsi). Contoh algoritma sandi asimetris adalah RSA.

3. Steganografi

Secara harfiah, steganografi yang berasal dari bahasa Yunani ini memiliki arti "menulis terselubung" (steganos = terselubung, graphein = menulis). Steganografi adalah ilmu menulis atau menyembunyikan pesan tersembunyi dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia. Hal ini tentu tidak sama dengan kriptografi, karena pada kriptografi meskipun arti pesan yang sebenarnya disamarkan, namun kenyataan bahwa ada pesan tidak disamarkan. Steganografi juga sering disebut sebagai seni, seperti kriptografi.

Steganografi meliputi banyak sekali cara untuk menyembunyikan pesan rahasia. Cara yang dimaksud termasuk tinta yang tidak tampak, microdots, pengaturan kata, tanda tangan digital, jalur tersembunyi dan komunikasi spektrum lebar.

Steganografi juga sering digunakan untuk menyembunyikan pesan dalam format digital. Format yang digunakan bermacam-macam, bisa berupa image (bmp, jpeg, gif), audio (wav, mp3) , atau lainnya (txt, pdf). Untuk format atau media yang berbeda, metode yang digunakan untuk menyembunyikan pesannya juga berbeda-beda. Beberapa metode yang biasanya digunakan, yaitu:

1. Modifikasi LSB (Least Significant Bit)

   Dasar dari metode ini adalah pengetahuan akan bilangan biner atau bilangan basis 2, yang hanya terdiri dari '1' dan '0'. Kedua bilangan yang menjadi dasar dari kerja komputer ini sering disebut dengan istilah bit. Susunan dari beberapa bit akan membentuk suatu informasi. Istilah yang umum dikenal adalah byte, yaitu kumpulan delapan bit data.

   Dalam satu byte data, bit yang paling berpengaruh terhadap informasi yang dikandungnya biasanya adalah bit paling awal/paling kiri. Bit inilah yang dinamakan Most Significant Bit (MSB). Semakin ke kanan, bit-bit tersebut semakin kecil pengaruhnya terhadap keutuhan data yang dikandung. Bit paling akhir/paling kanan inilah yang dinamakan Least Significant Bit (LSB).

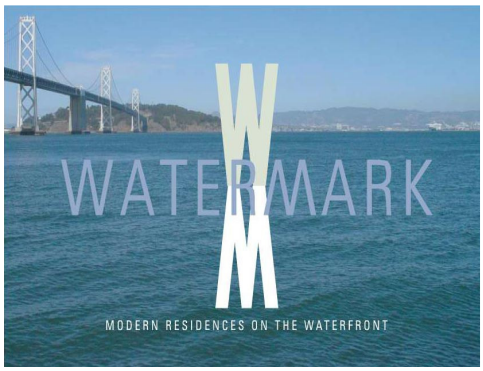
   Teknik Steganografi modifikasi LSB dilakukan dengan memodifikasi bit-bit yang tergolong LSB pada setiap byte dalam sebuah file. Bit-bit LSB ini akan dimodifikasi dengan menggantikan setiap LSB yang ada dengan bit-bit informasi lain yang ingin disembunyikan. Contohnya pada file bitmap 24 bit, pesan dapat disimpan pada LSB tiap komponen penyusun warna (merah, hijau, biru). Maka untuk tiap pixel pada file bitmap 24 bit, dapat disimpan informasi sebanyak 3 bit.

   Teknik ini termasuk cukup sederhana, namun terkadang kualitas dari file yang ditumpanginya sedikit banyak akan terpengaruh. Misalnya untuk file bitmap 24 bit di atas, warnanya akan sedikit berubah meskipun mungkin tidak akan dapat disadari oleh mata manusia normal.

2. Mask dan Filtering

   Teknik Steganografi dengan metode ini biasanya menggunakan file gambar sebagai medianya. Biasanya metode ini lebih dikenal dengan nama *digital watermark*. *Watermark* merupakan proses untuk mencantumkan sebuah informasi rahasia di dalam sebuah gambar, yang mana informasi rahasia tersebut sebenarnya juga merupakan bagian dari gambar itu. Tidak seperti teknik modifikasi LSB yang menghilangkan beberapa bagian dari informasi yang ditumpanginya, teknik ini sama sekali tidak mengganggu informasi yang ditumpangi karena sebenarnya informasi rahasia tersebut merupakan satu kesatuan dengan informasi yang ditumpanginya. Informasi rahasia akan tampak ketika

gambar yang ditumpanginya dimodifikasi, misalnya dengan meningkatkan *contrast*, *brightness*, atau hal lain, mengubah warna pada bagian tertentu, dan banyak lagi. Teknik *watermarking* seperti ini hanya mungkin digunakan pada gambar-gambar 24-bit dan *grayscale*. *Digital Watermark* telah banyak digunakan misalnya untuk menandai sebuah gambar hasil karya seorang desainer, dokumen-dokumen penting dalam bentuk gambar, dan lain-lain.



Gambar 2. Contoh gambar yang telah diberi watermark

3. Algoritma kompresi dan transformasi

   Kunci dari metode ini adalah seperti pada kompresi file gambar berformat JPEG. File gambar berformat JPEG memiliki kualitas gambar yang relatif tinggi namun dengan ukuran file yang tidak terlalu besar karena telah melalui proses kompresi dengan sebuah algoritma dan transformasi matematik, sehingga informasi gambar tersebut dapat disimpan dengan ukuran file yang kecil dengan tetap mempertahankan kualitasnya. Algoritma kompresi dan transformasi matematik JPEG ini memungkinkan sebuah informasi disimpan sebaik dan seefisien mungkin.

   Sebuah file rahasia dapat disisipkan ke dalam sebuah file gambar yang tidak melalui proses kompresi seperti format TIFF, misalnya dengan menggunakan algoritma JPEG ini. Sehingga setelah melalui proses ini akan didapatkan file gambar berformat TIFF tadi berubah menjadi berformat JPG dengan disertai "sesuatu" di dalamnya. Dengan menggunakan teknik ini, kualitas gambar aslinya bahkan hampir tidak terpengaruh, tidak seperti ketika menggunakan teknik modifikasi LSB.

4. Redundant Pattern Encoding

   Penerapan steganografi dengan metode ini adalah dengan menggambar pesan kecil pada kebanyakan gambar. Keuntungan dari metode ini adalah dapat bertahan dari *cropping* (kegagalan), Kerugiannya yaitu tidak dapat menggambar pesan yang lebih besar, sehingga pesan menjadi agak terbatas dan mungkin saja pesan yang ingin disampaikan oleh pengirim bahkan terlewatkan oleh penerima.

5. Spread Spectrum method

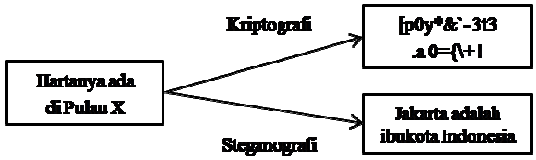
   Dengan teknik ini, pesan yang hendak disampaikan akan terpencar-pencar sebagai pesan yang diacak melalui gambar, tidak seperti dalam modifikasi LSB dimana pesan pasti terletak pada LSB. Untuk membaca pesan tersebut, penerima memerlukan algoritma sandi untuk membacanya yang berupa *crypto-key* dan *stego-key*. Kelemahan dari teknik ini yaitu masih rentan mengalami penyerangan berupa penghancuran atau pengrusakan dari kompresi dan proses gambar.

4. Perbandingan Steganografi dan Kriptografi

Kriptografi, sesuai dengan artinya dari bahasa Yunani yaitu menulis rahasia, mungkin terdengar relatif sama dengan steganografi, yaitu menulis terselubung. Namun sesungguhnya ada beberapa perbedaan yang bisa dilihat dari kedua metode tersebut.

Salah satu perbedaan dari kriptografi dan steganografi bisa juga dilihat jika arti dari keduanya ditelaah. Sebuah pesan rahasia, yang berhubungan dengan kriptografi, biasanya akan menimbulkan kecurigaan bagi yang tidak mengetahuinya pesan sebenarnya. Sementara itu sebuah pesan yang terselubung (berhubungan dengan steganografi) tidak akan menimbulkan kecurigaan secara langsung saat seseorang

melihat pesan tersebut karena pesan yang terlihat bukanlah pesan yang sebenarnya. Pesan yang telah dienkripsi dengan metode kriptografi manapun, umumnya terlihat kacau, aneh, dan tidak terbaca, sementara pesan yang disembunyikan dengan steganografi masih bisa terbaca oleh orang awam, sehingga tidak menimbulkan kecurigaan.



Gambar 3. Contoh perbedaan pesan yang disembunyikan dengan kriptografi dan steganografi

Perbedaan yang kedua adalah algoritma sandi yang digunakan dalam mengamankan pesan. Kebanyakan teknik kriptografi menggunakan aturan tertentu dalam mengubah *plaintext* menjadi *ciphertext*, dan sebaliknya. Sementara itu cara mengamankan pesan dalam steganografi umumnya didasari oleh kreativitas sang penyembunyi pesan. Hanya beberapa teknik dalam steganografi yang menggunakan algoritma tertentu dalam menyembunyikan pesan. Oleh karena itu, meskipun kriptografi dan steganografi sama-sama disebut sebagai ilmu dan seni, namun perbedaan ini membuat kriptografi lebih terlihat sebagai sebuah ilmu dan steganografi lebih terlihat sebagai sebuah seni.

Dengan mengetahui perbedaan, karakteristik, serta kelebihan dan kekurangan dari kriptografi dan steganografi, manusia dapat memilih metode apa yang akan digunakan dalam mengamankan data atau pesannya. Jika tempat penyimpanan data atau pesan yang diamankan juga disembunyikan, pemiliknya dapat menggunakan kriptografi saja untuk melindungi data atau pesannya, mungkin dengan alasan kemudahan mendekripsi jika sewaktu-waktu ingin dilakukan modifikasi terhadap data atau pesan tersebut. Namun jika pengirim pesan ingin menyampaikan pesan rahasia kepada orang tertentu saja yang tidak diketahui lokasinya, pengirim pesan dapat menyebarkan pesannya di public (misalnya melalui iklan pada media massa) dan menggunakan steganografi untuk mengubah pesan, sehingga pesan yang asli hanya dimengerti oleh orang yang memang dituju dan orang yang tidak berkepentingan tidak akan curiga terhadap pesan tersebut. Pengamanan bisa diperketat lagi jika data atau pesan diamankan dengan teknik dalam kriptografi kemudian *ciphertext* hasilnya diubah lagi dengan steganografi atau sebaliknya, dilakukan pengamanan dengan metode steganografi terlebih dahulu kemudian dienkripsi lagi sehingga menjadi pesan yang rahasia.

Perkembangan kriptografi dan steganografi memang membantu manusia dalam urusan mengamankan data dan pesan. Namun, semua itu bukan tanpa konsekuensi. Jika digunakan oleh pihak-pihak yang berniat tidak baik, kriptografi dan steganografi dapat menjadi berbahaya. Contohnya seorang pimpinan teroris dapat mengirimkan pesan rahasia kepada anak buahnya untuk melakukan penyerangan ke pusat pemerintahan negara. Ilmu yang tadinya dikembangkan demi kemudahan manusia, bisa jadi justru menambah permasalahan bagi manusia. Pada akhirnya, semua kembali kepada masing-masing individu, bagaimana cara memanfaatkan apa yang dimilikinya (harta, ilmu, kekuasaan) dan tujuan apa yang hendak dicapainya.

5. Kesimpulan

Setelah menelaah dan membandingkan kriptografi dan steganografi serta penggunaannya, ada beberapa hal yang dapat disimpulkan, yaitu:

1. Kesamaan kriptografi dan steganografi terletak pada tujuan penggunaannya, yaitu untuk melindungi pesan atau data.
2. Keunggulan kriptografi dibandingkan steganografi adalah pada umumnya teknik pada kriptografi memiliki algroritma yang pasti dalam enkripsi dan dekripsi pesan. Pada steganografi, biasanya lebih menggunakan kreativitas sehingga lebih bersifat sebagai sebuah seni.
3. Keunggulan steganografi dari kriptografi adalah kemampuan untuk mengeliminasi kecurigaan dari pihak-pihak yang tidak berkepentingan saat melihat pesan atau data yang telah diubah.
4. Karakteristik-karakteristik steganografi dan kriptografi yang telah disebutkan di atas dapat menjadi pertimbangan seseorang yang ingin melakukan pengamanan terhadap pesan atau data dalam memilih teknik apa yang tepat dalam pengamanan pesan atau datanya.

5. Kriptografi dan steganografi dapat juga dipakai bersamaan dalam melindungi pesan atau data untuk makin memperkecil resiko keamanan.

DAFTAR PUSTAKA

[1] Wikipedia®. (2008). Kriptografi. http://www.id.wikipedia.org/Kriptografi Tanggal akses: 3 Januari 2009 pukul 13.35

[2] Wikipedia®. (2008). Steganografi. http://www.id.wikipedia.org/Steganografi Tanggal akses: 3 Januari 2009 pukul 20.17

[3] Bimacipta. (2008). Steganografi http://www.bimacipta.com/stegano.htm Tanggal akses: 3 Januari 2009 pukul 20.30

[4] Blog Hadiwibowo. (2008). Steganografi http://hadiwibowo.wordpress.com/2006/08/29/steganografi/ Tanggal akses: 3 Januari 2009 pukul 21.00

[5] SF Watermark. (2008). Watermark http://sfwatermark.com Tanggal akses: 4 Januari 2009 pukul 18.10

[6] Munir, Rinaldi. (2008). Diktat Kuliah IF2091 Struktur Diskrit. Departemen Teknik Informatika, Institut Teknologi Bandung.