Implementasi Steganografi Dalam Pembatasan Akses Info Pada Data Pribadi

Calvin Irwan, 13507010
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
If17010@students.if.itb.ac.id

***Abstrak*—Makalah ini membahas cara melindungi data pribadi yang dipublikasi ke sebuah grup / kumpulan orang , namun data tetap tidak bisa diakses. Sekarang ini kemajuan di bidang elektronik sudah sangat pesat, sehingga semua hal tersimpan dalam bentuk elektronik terutama dokumen dan dokumen dalam bentuk elektronik sangatlah rentan terhadap gangguan dari luar seperti pihak yang tidak berwenang bisa mendapatkan informasi dari dokumen tersebut. Apalagi bila dokumen tersebut berisi data yang bisa dibilang sangat pribadi seperti transkrip IP atau pendapatan perbulan. Apalagi dengan adanya mekanisme pengunggahan dokumen tersebut ke sebuah milis misalnya untuk menampilkan file dokumen tersebut, akan semakin berbahaya karena banyak sekali pihak yang dapat melihatnya secara Cuma-Cuma. Oleh karena itu pada makalah ini akan dibahas mekanisme pengamanan data pribadi melalui Steganografi. Steganografi juga biasanya diperkuat dengan kriptografi yang juga merupakan ilmu yang mempelajari cara-cara menyambunyikan pesan. Jenis-jenis kriptografi amat beragam, namun yang akan digunakan pada makalah ini adalah vigenere cipher.**

***Kata Kunci*—transkrip IP, kriptografi, steganografi, vigenere cipher**

I. PENDAHULUAN

Banyak sekali dokumen-dokumen yang bersifat pribadi seperti daftar nilai yang seringkali bisa diakses oleh orang lain dan hal ini menyebabkan rasa malu atau tidak senang bagi pemilik dokumen. Seperti pada pengumuman nilai contohnya, tidak semua orang ingin dilihat nilainya, ataupun pada contoh kasus sebuah perusahaan yang ingin mengumumkan list pengukuran kinerja masing-masing pegawai. Dengan adanya steganografi dan enkripsi yang dilakukan oleh aplikasi ini tidak seluruh isi dokumen dapat terlihat, kunci seseorang hanya dapat membuka enkripsi data yang berkaitan dengannya sehingga tidak dapat melihat data orang lain hal ini juga menghemat biaya , apabila sebelumnya data pribadi dikirimkan satu-satu perorang, sekarang data dapat dikumpulkan pada satu file dokumen namun seseorang tersebut tetap hanya dapat melihat data pribadi miliknya.

Sebenarnya masalah diatas dapat ditanggulangi dengan cara mengirim data pribadi per-orang, maksudnya adalah dengan mengirim data tersebut satu demi satu kepada orangnya masing-masing, namun cara tersebut terlalu banyak memakan cost seperti waktu dan tenaga layaknya algoritma *bruteforce* yang kurang mangkus dan sangkil. Belum lagi apabila data tersebut misalnya (penilaian terhadapap kinerja pekerja perusahaan sebuah departemen) yang di publikasi ke sebuah milis bisa sampai terbaca oleh departemen lain dalam bentuk yang belum terlindungi sama sekali. Oleh karena itu pada makalah ini akan dibahas mengenai cara untuk memecahkan cara tersebut.

II. TEORI DASAR

2.1 Steganografi

Steganografi adalah seni dan ilmu menulis pesan tersembunyi sedemikian rupa sehingga tak seorang pun, selain pengirim dan penerima yang dituju mengetahui isi pesan rahasia, suatu bentuk keamanan melalui ketidakjelasan. The Kata steganografi berasal dari bahasa Yunani dan berarti "tulisan tersembunyi" dari kata Yunani Steganos yang berarti "ditutupi atau dilindungi", dan graphein yang berarti "tulisan". Penggunaan tercatat pertama istilah ini pada 1499 oleh Johannes Trithemius dalam bukunya Steganographia, sebuah risalah pada kriptografi dan steganografi disamarkan sebagai sebuah buku tentang sihir. Umumnya, pesan akan muncul menjadi sesuatu yang lain: gambar, artikel, daftar belanja, atau beberapa covertext lain dan, klasik, pesan yang tersembunyi mungkin dalam tinta tak terlihat antara garis terlihat dari surat pribadi.

Steganografi memasukan penyembunyian informasi dalam file komputer. Dalam steganography digital, komunikasi elektronik dapat memasukan steganografi didalam kode dari lapisan transportasi, seperti file dokumen, file gambar, program atau protokol. File media adalah file yang ideal untuk transmisi steganografi karena ukurannya yang besar. Sebagai contoh sederhana, pengirim mungkin mulai dengan sebuah file gambar tidak berbahaya dan

menyesuaikan warna dari setiap pixel ke-100 untuk sesuai dengan huruf dalam alfabet, perubahan yang terjadi akan begitu halus sehingga seseorang tidak menyadarinya.

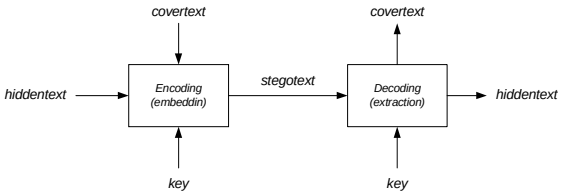
Properti steganografi

Embedded message (hiddentext): pesan yang disembunyikan. Bisa berupa teks, gambar, audio, video, dll

Cover-object (covertext): pesan yang digunakan untuk menyembunyikan embedded message. Bisa berupa teks, gambar, audio, video, dll

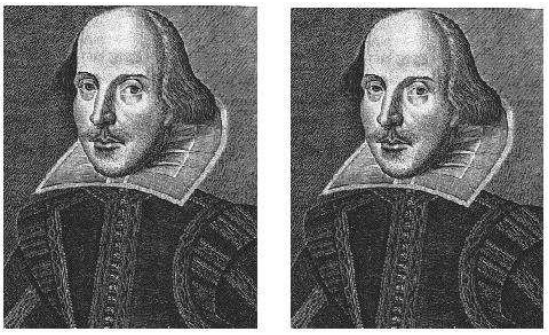
Stego-object (stegotext): pesan yang sudah berisi pesan embedded message.

Stego-key: kunci yang digunakan untuk menyisipan pesan dan mengekstraksi pesan dari stegotext.



Gambar 2.1 Skema Steganografi

Steganografi pada gambar dilakukan dengan metode LSB yaitu dengan mengganti beberapa bit pada gambar dengan cara memasukan bit dari file yang ingin disamarkan. Memiliki skema yang sama seperti gambar di atas namun *covertext* berubah menjadi *coverimage* dan *hiddentext* berubah menjadi *hiddenfile.*



Gambar 2.2 contoh Steganografi pada gambar

2.2 Kriptografi

Kata cryptography berasal dari bahasa Yunani: krupto (hidden atau secret) dan grafh (writing) Artinya "secret writing"

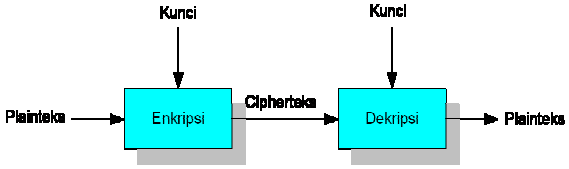
Definisi lama: Kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya.

Definisi baru: Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (*message*) [Schneier, 1996].

Algoritma kriptografi (*cipher*)
- aturan untuk enchipering dan dechipering, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi pesan. "art and science to keep message secure"

Kunci: parameter yang digunakan untuk transformasi enciphering dan dechipering. Jika kekuatan kriptografi ditentukan dengan menjaga kerahasiaan algoritmanya, maka algoritma kriptografinya dinamakan algoritma restricted.

Algoritma resricted tidak cocok lagi saat ini. Kriptografi modern mengatasi masalah ini dengan menggunakan kunci. Kunci bersifat rahasia (secret), sedangkan algoritma kriptografi tidak rahasia (public).



Gambar 2.3 Skema Kriptografi

Vigenere Cipher

Vigenere Cipher adalah sebuah algoritma yang termasuk kedalam cipher abjad-majemuk (polyalpabetic substitution cipher). Cipher ini pertama kali dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigènere pada abad 16 (tahun 1586). Tetapi sebenarnya Giovan Batista Belaso telah menggambarkannya pertama kali pada tahun 1553 seperti ditulis di dalam bukunya La Cifra del Sig. Giovan Batista Belaso

Gambar 2.4 Blaise de Vigenere

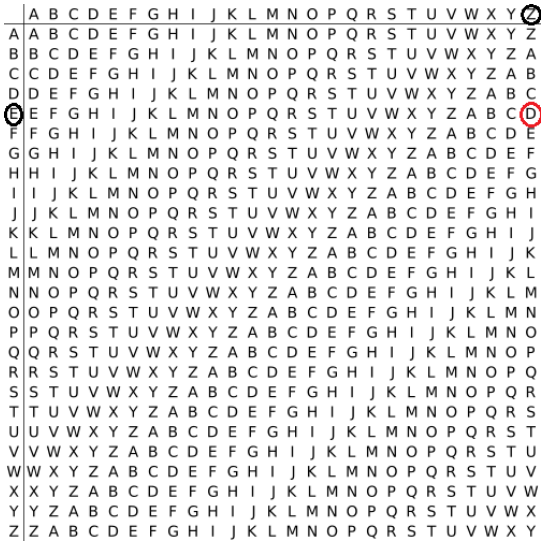
Algoritma tersebut baru dikenal luas 200 tahun kemudian yang oleh penemunya cipher tersebut kemudian dinamakan Vigènere Cipher.

Algoritma ini menjadi terkenal karena kesulitannya untuk dipecahkan. Matematikawan Charles Lutwidge Dodgson menyatakan bahwa algoritma ini tidak

terpecahkan. Pada tahun 1917, ilmuwan Amerika menyatakan bahwa Vigenere cipher adalah sesuatu yang tidak mungkin dtranslasikan. Namun hal ini terbantahkan oleh kasiski yang berhasil memecahkan algoritma ini pada abad ke-19.

Cara kerja algoritma ini adalah dengan menggeser huruf dari plain text yang ingin dienkripsi dengan sebuah kunci yang ditentukan sendiri oleh pengguna.

Algoritma *Vigenere Cipher* ini menggunakan bujursangkar *vigenere* dalam melakukan enkripsi. Setiap baris pada bujur sangkar menyatakan huruf-huruf *ciphertext* yang diperoleh dengan *Caesar Cipher*. Untuk lebih memperjelas, dapat dilihat gambar dibawah ini. kolom menunjukan huruf dari plaintext sedangkan baris menunjukan huruf dari kunci *vigenere*. Dapat dilihat pada gambar huruf "Z" dienkripsi dengan huruf "E" menjadi huruf "D".



Gambar 2.5 Bujursangkar Vigenere

Jika panjang dari kunci lebih pendek dari panjang *plaintext*, maka kunci akan diulang secara periodik hingga kunci dengan *plaintext* sama panjangnya. Contohnya adalah sebagai berikut:

Plaintext : Makalah Kriptografi
Kunci : Calvin

Maka hasil dari proses *vigenere cipher* adalah sebuah *ciphertext*

Plaintext	: makalah kriptografi
Kunci	: c al vin calvincalvin
Ciphertext	: oavvtnj kcdxgqgcvnv

Apabila metode Vigenere Cipher ini ditranslasikan menjadi sebuah algoritma pemrograman, secara sederhana notasi algoritmik yang digunakan untuk melakukan enkripsi adalah sebagai berikut

$$C_i = E_K(M_i) = (M_i + K_i) \mod 26$$

Dan dekripsi seperti

$$M_i = D_K(C_i) = (C_i - K_i) \mod 26.$$

Dimana

Pi = Karakter *Plaintext*
Ci = Karakter *Ciphertext*
Ki = Karakter kunci

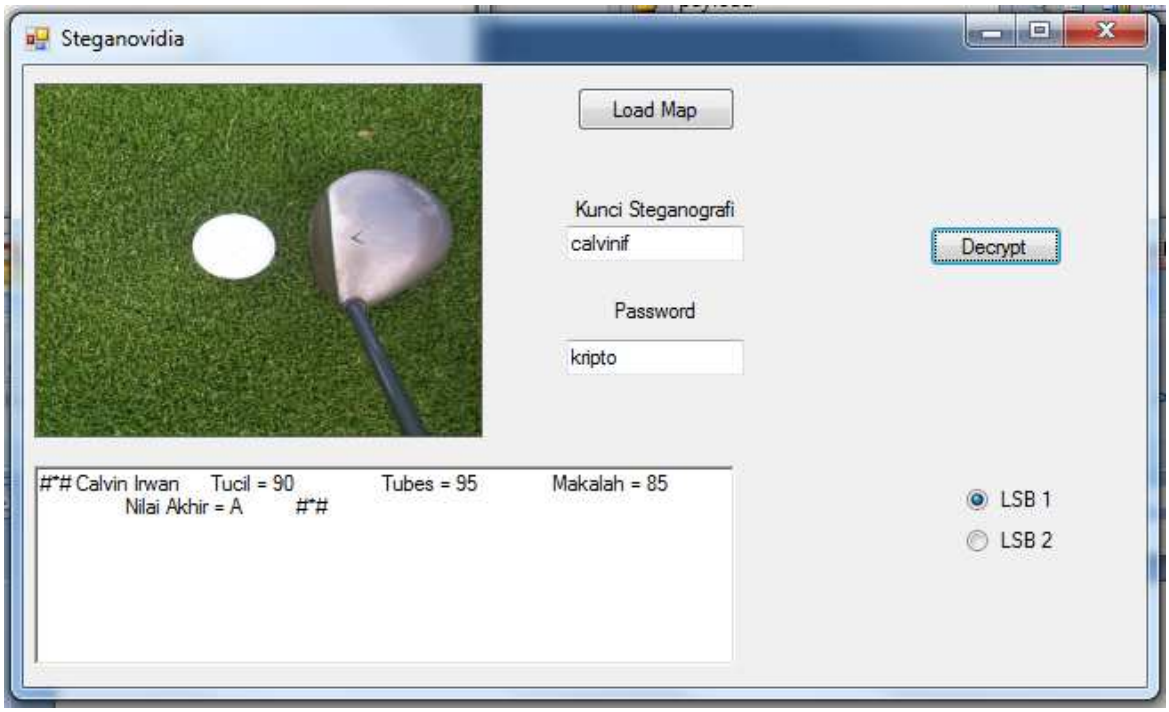
III. IMPLEMENTASI

Saat ini diperlukan sebuah mekanisme perlindungan terhadap sebagian konten file maksudnya adalah dari sebuah file yang mengandung 100 informasi mungkin seseorang hanya bisa mengakses 70 dari 100, 50 dari 100, atau bahkan 1 dari 100, tergantung dari kewenangan orang tersebut. hal ini diperlukan untuk membuat sebuah file yang efektif karena dari pada membuat 100 file text yang berisikan 1 informasi, akan lebih baik membuat i file text yang memuat 100 informasi.

Penerapan steganografi pada proteksi data pribadi dapat dilakukan dengan menyisipkan file text yang berisi informasi pribadi sekumpulan orang (untuk seterusnya pada makalah ini saya akan menggunakan nilai sebuah mata pelajaran sebagai contoh file), kedalam sebuah gambar yang kemudian gambar tersebut akan diunggah.

Gambar yang telah terunggah kemudian di unduh oleh pihak-pihak yang bersangkutan (pada kasus ini adalah mahasiswa). Kemudian mahasiswa membuka sebuah perangkat lunak pendekripsi file yang disisipkan dengan steganografi.

3.1 Tampilan antarmuka program



Gambar 3.1 Tampilan Antarmuka Perangkat Lunak

Program ini dibuat dengan menggunakan bahasa c#, idenya adalah pada program ini user hanya perlu memasukkan gambar yang telah diunduh kedalam program ini dengan cara melakukan "klik" pada tombol "Load Map" kemudian memasukkan kunci dari steganografi seperti pada dekriptor steganografi umumnya, namun yang membuat program ini berbeda dari pengolah steganografi biasanya adalah pada bagian password, dimana password ini adalah kunci dari masing-masing pemilik file sehingga bersifat rahasia dan unik (diatur oleh admin untuk menjaga keunikan password). Password itulah yang merupakan kunci vigenere untuk mentranslasi isi dari file tersebut. Kemudian dari hasil translasi seluruh isi file, dilakukan penyaringan agar hasil yang dikeluarkan hanya hasil berupa tulisan yang berhasil di dekripsi.

3.2 Cara Kerja Program

Cara kerja program ini sesungguhnya hanyalah sebuah pemanfaatan vigenere sederhana yaitu dengan cara pemberian password yang berbeda pada setiap data perorang sehingga seseorang tersebut hanya bisa melihat nilainya, contoh :

Diberikan daftar nilai dari lima orang mahasiswa dengan password yang berbeda.

#*# Calvin Irwan Tucil = 90 Tubes = 95 Makalah = 85 Nilai Akhir = A #*# password = itb

#*# Lebron James Tucil = 90 Tubes = 55 Makalah = 75 Nilai Akhir = B #*# password = tbi

#*# Ahmad Ranieri Tucil = 0 Tubes = 35 Makalah = 0 Nilai Akhir = E #*# password = calvin

#*# Laras Sati Tucil = 60 Tubes = 65 Makalah = 65 Nilai Akhir = C #*# password = kripto

#*# Hannah Bieber Tucil = 0 Tubes = 55 Makalah = 65 Nilai Akhir = D #*# password = syalala

Kemudian setiap data dienkripsi sesuai password masing-masing menjadi

Œ …‰•ÃÕêË×"«ÛëÃ×"k½éÅÒà,¦"›™"k½éÄÎç,¦"›
"k¶ÕÍÊàÃÑ"Ÿ‰¬—
rÂËÕÕË‰µÍÑÝÔ‰±,ª"kŒ …

—
ŒŒ"®ÎÖÔØâ,³ÕÏÎç,rÈ×ÌÝÎ‰±,¢¤,rÈ×ËÙÕ‰±,
©,rÁÃÔÕÎÊÜ,¦"™ }°ÒàÃÒ"£ÔÜËÛ"Ÿ‰¶,r—
ŒŒ"

†‹ –ªÖÐÂÐ–»ÏÑÊÑèÒ lµáÙÒÚƒ Œ–
™ lµáØÎáƒ Œ© l®ÍáÊÚÄÉŒ³‰ "j°ßÕÏÌ -á
Ñ×Õ ©–® l„–™‰

œŒ ÀÐÝÓÜ ÇÐßÛ‰yÈäÎÛÕ ± ¡¢‰yÈäÍ×Ü
± ¡§‰yÁÐÖÓÕÑÜ ¨'Ÿ¥}½ÔÞÊÙ"°ÖÚÒâ"¬‹µ

‰y—™ ’‰
–
£„Œ©ÍÏáÚÉŒ£ÕÆÕÞÓŒjÀÖÖâÍŒ Œ £,µáÃÑÔ “¶ ¡–ŒjÀÚÌÍÍÍÉ“¶ ¢–u¯ÜåÂÕ -ÌÛâÓŒ Œ¥“,„–„

Setelah ke lima data tadi dienkripsi, hal yang selanjutnya dilakukan adalah memasukan text yang telah terenkripsi tadi kedalam sebuah text file yang selanjutnya akan disisipkan kedalam stego image.

Cara melakukan dekripsinya adalah dengan cara memasukan password yang telah disediakan dalam antarmuka program, misalnya password yang dipilih adalah “itb” maka hal yang terjadi didalam program adalah sebagai berikut.

Setelah text didekripsi dengan kunci “itb” maka keluaran dari program adalah seperti:

#*# Calvin Irwan Tucil = 90 Tubes = 95 Makalah = 85 Nilai Akhir = A #*#¡–
5#↑ 2EZtkd▪ ├ ?sfZ…├ þfnX{e┴ O├ .B├ þfnWwl┴ O ├ *G├ þ_Z`seVz├ 220*← G^~Z^2:`zbg26┴ T├ þ5#↑ 2 ¡–
$"← 4AbnY\4R[oa]†i→ Lmwif!5↑ 40→ Lmvem!5↑ G5 → EY afb`↑ Q 1 F}l[j↑ 9 hcs↑ 54E→
← "7 –¨%(*'Lnt_z'Snvg'┼ T,egs'=-8.'┼ T,dcz'=-83'┼ Mnm_shh-?-=< [kjhp Nmfpy J"A'┼ #7%-'¡"A← ↑ Gd[qU*:adljq#ö^mb d↑ <#A├ A Z]r*B8"* LxcYkdU1M
@- Msq`lKcg j↑ <#11├┼ 4← –

Akan muncul hasil enkripsi seperti diatas. Pengguna pasti akan merasa tidak nyaman meskipun nilai sudah didapat, namun hasil dekripsi yang lain juga ikut bermunculan. Oleh karena itu sejak awal masukan file diberikan penanda berbentuk “#*#” agar program dapat memanggil fungsi untuk mendeteksi kapan mulai dan berakhirnya satu baris nilai pengguna, karena apabila password yang digunakan berbeda, kemungkinan terbentuknya “#*#” amatlah kecil hampir tidak mungkin pada kasus normal. Sehingga dari barisan simbol diatas, hanya baris:
”#*# Calvin Irwan Tucil = 90 Tubes = 95 Makalah = 85 Nilai Akhir = A #*#”
yang ditampilkan oleh program sebagai keluaran.

3.3 Notasi Algoritmik Penerapan Vigenere

```
//variable global

File_image image_from_user;
File_text encrypted_txt_file;
String plaintext;
String key;
String password;

//proses pada program

File_text = Stegano_decrypt (File_gambar, key);
Plaintext = Vigenere_decrypt (Detect_header(), File_text, password);

//keterangan beberapa fungsi

Stegano_decrypt (file input, string key) merupakan fungsi yang mengembalikan string hasil dekripsi Stegano dari file input dengan kunci key.

Vigenere_decrypt (string input, string password) merupakan fungsi yang mengembalikan string hasil dekripsi Vigenere dari string input dengan kunci password.

Detect_header (string_input) merupakan fungsi yang mengembalikan substring yang diawali 3 karakter “#*#” dan juga diakhiri “#*#” yang merupakan tanda bahwa barisan tersebut adalah output yang seharusnya.
```

IV. KEGUNAAN UNTUK MASYARAKAT

Dikarenakan kemudahan untuk melakukan pengumuman seuatu data via- e-mail dan via sarana pemberitaan online lainnya, penerapan pengamanan yang telah dibahas dalam makalah ini tentu akan mengurangi kekhawatiran masyarakat terhadap data yang dipublikasikan di sebuah media elektronik. Apalagi data tersebut bersifat pribadi seperti Nilai, atau berat badan ataupun nomor telepon. Kegunaan untuk mengamankan nilai seperti contoh pada makalah ini hanyalah salah satu dari berbagai jenis pemanfaatan lainnya.

V. KESIMPULAN

Pengamanan file data pribadi dengan menggunakan steganografi yang dilapisi dengan vigenere cipher merupakan salah satu cara yang cukup efektif. Bila sebelumnya pemberitaan biasa dilakukan kepada satu persatu orang, sekarang dengan mekanisme ini pemberitaan dapat dilakukan secara terpusat, namun tetap bisa menjaga privasi satu sama lain.

Steganografi yang dilakukan pada aplikasi ini sudah cukup menyaring kemungkinan buruk yang dapat terjadi apabila pengumuman tersebar luas ke khalayak umum, apalagi ada pemberian password. Vigenere cipher memang sudah dapat terpecahkan,

namun pada penggunaannya di aplikasi ini vigene cipher sudah cukup bermanfaat, selain melindungi file, vigenere juga menjadi sebuah metode saringan untuk dokumen yang telah berhasil didekripsi agar data yang keluar hanya data yang diperlukan.

REFERENSI

[1] Munir, Rinaldi. 2004. Slide Kuliah IF3048 Kriptografi, Departemen Informatika Institut Teknologi Bandung.

[2] www.cs.trincoll.edu/~crypto/historical/vigenere.html diakses pada tanggal 19 Maret 2011 pukul 16.00

[3] http://www3.telus.net/Voiculescu/vigenere/index.html. diakses pada tanggal 19 Maret 2011 pukul 21.00

[4] http://easybmp.sourceforge.net/steganography.html diakses pada tanggal 20 Maret 2011 pukul 19..00

[5] http://www.jjtc.com/stegdoc/sec313.html diakses pada tanggal 20 Maret 2011 pukul 16.00

[6] http://en.wikipedia.org/wiki/Vigen%C3%A8re_cipher. diakses pada tanggal 18 Maret 2011 pukul 19.00

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 23 Maret 2011

Ttd

Calvin Irwan
13507010