Teknik Keamanan Data Menggunakan Steganografi dan Kriptografi dengan Algoritma Vernam Chiper

Kharisma Nugrahandani Restuti - 13512601
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
kharisma.nr@students.itb.ac.id

Abstrak*—Teknologi informasi dan komunikasi telah berkembang pesat dan berpengaruh besar pada kehidupan manusia. Oleh sebab itu, kebutuhan akan terjaminnya keamanan dalam proses penyampaian dan penyimpanan pesan menjadi sangat penting. Untuk menjamin keamanan pesan tersebut diperlukan adanya sebuah proses penyandian. Salah satu usaha penyandian pesan yakni dengan kriptografi. Dengan kriptografi inilah pesan melalui proses enkripsi atau penyandian yang dilakukan ketika pesan akan dikirim, akan mengubah data asli menjadi data yang tidak terbaca oleh pihak yang tidak berkepentingan, melainkan hanya oleh pihak yang mempunyai kunci dekripsi. Salah satu algoritma kriptogafi adalah algorima Vernam Chiper, yang mampu mengamankan informasi termasuk file. Sehingga dapat digunakan untuk mengamankan file. File adalah media yang telah digunakan banyak orang dalam mengirim dan menerima data di era komputer sekarang ini. Pesan yang tidak dapat dibaca oleh pihak yang tidak berkepentingan ini juga akan menimbulkan kecurigaan, sehingga diperlukan adanya steganografi yang bertujuan agar pesan yang telah disisipi pesan rahasia akan tampak sama dengan pesan biasa. Hal ini akan mengurangi kecurigaan pihak yang tidak berkepentingan terhadap pesan rahasia tersebut.*

Kata kunci : *kriptografi, steganografi, file, Vernam Chiper.*

1. PENDAHULUAN

Seiring perkembangan teknologi yang kian pesat, penyampaian informasi dan pengiriman data dapat dilakukan dengan mudah, dengan berbagai media dan fasilitas yang tersedia sekarang ini. Dengan perkembangan yang kian pesat dan mudah ini, tentu masalah keamanan menjadi suatu hal yang sangat penting dalam proses pengiriman dan penyimpanan data.

Untuk menjamin keamanan dan keutuhan data, perlu dilakukan proses penyandian. Kriptografi mampu menjadi solusi dari masalah tersebut. Kriptografi dapat menjamin keamanan data-data pada suatu file. Data tersebut disandikan atau dienkripsi menjadi suatu symbol tertentu sehingga tidak mampu dibaca selain pihak yang memegang kunci dekripsi. Dalam perkembangan ilmu kriptografi sekarang ini, telah tercipta berbagai algoritma, salah satunya adalah algoritma *Vernam Chiper*. Algortima ini termasuk dalam algoritma kriptografi modern dan merupakan algoritma *stream chiper*.

Namun penggunaan kriptografi dalam keamanan file masih dirasa kurang. Setelah file tersebut dienkripsi menjadi data yang tidak terbaca oleh pihak yang tidak berkepentingan, akan menimbulkan kecurigaan, sehingga perlu dilakukan penyembunyian file ke dalam file-file lain, sehingga pihak ketiga ini tidak akan curiga terhadap pesan rahasia yang dikirim. Langkah ini disebut steganografi.

Steganografi adalah cara yang efektif untuk menghilangkan kecurigaan pihak-pihak yang tidak berkepentingan tersebut. Kebanyakan algortima steganografi menggunakan sebuah kombinasi dari jenis teknik yang digunakan untuk melakukan sebuah tugas dalam penyembunyian pesan rahasia dalam sebuah selubung file.

Pada steganografi, penyembunyian file ini dibuat sedemikian rupa, sehingga pihak lain tidak menyadari bahwa ada pesan lain di dalam pesan yang dikirim. Pesan inti tersebut tetap dipertahankan keamanan dan keutuhannya, hanya saja saat pengiriman disamarkan atau disembunyikan dengan berbagai cara. Hanya pihak penerima yang sah yang dapat mengetahui isi file tersebut, termasuk pesan rahasia yang terdapat di dalamnya.

Pada kriptografi, pesan diubah menjadi bentuk lain atau symbol-simbol yang tidak bermakna. Pesan yang sudah dienkripsi akan mencurigakan karena ketidakbermaknaannya tersebut, sehingga dengan ada steganografi akan mengurangi atau menghilangkan kecurigaan dari pesan yang dikirim, pesan tersebut akan nampak seperti sebuah pesan biasa. Hanya saja kelemahan dari steganografi ini, apabila format pesan yang dikirim diubah, pesan rahasianya bisa hilang.

Penggunaan kedua teknik ini, steganografi dan kriptografi, akan lebih menjamin keamanan suatu file pada proses pengiriman dan penyimpanan pesan, sehingga diharapkan tidak terjadi pencurian maupun penyadapan data.

2. LANDASAN TEORI

2.1 Data

Data adalah sesuatu yang belum mempunyai arti

bagi penerimanya dan masih memerlukan adanya suatu pengolahan. Data bisa berwujud suatu keadaan, gambar, suara, huruf, angka, matematika, bahasa ataupun symbol-simbol lainnya yang bisa kita gunakan sebagai bahan untuk melihat lingkungan, objek, kejadian ataupun suatu konsep. [2]

Sedang informasi merupakan hasil pengolahan dari sebuah model, formasi, organisasi maupun suatu perubahan bentuk dari data yang memiliki nilai tertentu dan bisa digunakan untuk menambah pengetahuan bagi yang menerimanya.

2.2 File

File atau berkas adalah sekumpulan data yang berhubungan yang diberi nama dan tersimpan di dlam media penyimpanan sekunder. File memiliki ekstensi yang merupakan penandaan jenis file melalui nama file. Ekstensi file ini ditulis setelah nama file dan dipisahkan dengan titik.

Pada sistem lama, ekstensi hanya diperbolehkan maksimal 3 huruf, seperti doc, exe, txt. Batasan tersebut dihilangkan pada sistem yang baru, contohnya : jpeg, docx, mpeg. [3]

2.3 Kriptografi

Kriptografi merupakan ilmu untuk penyandian data. Ilmu ini telah dikenal sejak kurang lebih 1900 sebelum masehi dan sudah mulai dipelajari manusia sejak tahun 400 SM pada zaman Yunani kuno. Bidang ilmu ini terus berkembang seiring dengan kemajuan peradaban umat manusia. Sejarah telah dipenuhi oleh orang-orang yang berusaha merahasiakan pesan rahasia mereka dari pihak yang tidak berkepentingan.

Keperluan akan teknik kriptografi yang lebih canggih tidak dapat dihindari, terlebih pada era informasi seperti sekarang ini. Pelayanan informasi semakin meningkat seiring dengan perkembangan teknologi.

Kriptografi berbasis pada algoritma pengkodean data informasi yang mendukung kebutuhan dari dua aspek keamanan informasi, yaitu *secrecy* (perlindungan terhadap kerahasiaan data informasi) dan *authenticity* (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan).

Kriptografi berasal dari kata “Crypto” yang berarti rahasia dan “graphy” yang berarti tulisan. Jadi dapat dikatakan bahwa kriptografi adalah tulisan yang tersembunyi. Dengan adanya tulisan yang tersembunyi ini, orang-orang tidak mengetahui bagaimana tulisan tersebut disembunyikan dan tidak diketahui bagaimana cara membaca maupun menerjemahkan tulisan tersebut. William Stallings mendefinisikan kriptografi sebagai “the art and science of keeping messages secure”[4].

Kriptografi menjadi dasar keamanan komputer dan jaringan karena merupakan sarana pendistribusian data dan informasi. Data-data tersebut diamanankan dengan berbagai metode oleh pengirim sehingga orang lain tidak dapat mengenali isi data tersebut.

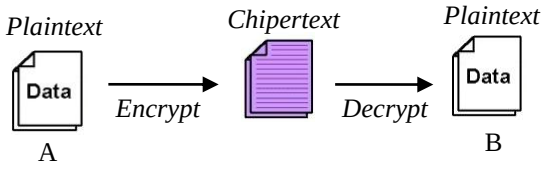
Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu pesan asli (*plaintext*) menjadi suatu pesan dalam bahasa sandi (*chipertext*).

Enkripsi merupakan transformasi data dalam bentuk yang tidak dapat terbaca dengan kunci tertentu, bertujuan untuk meyakinkan privasi dengan menyembunyikan informasi dari orang-orang yang tidak dikehendaki, bahkan mereka yang memiliki akses ke data ter-enkripsi.

Sedangkan dekripsi merupakan kebalikan dari proses enkripsi, yaitu proses mengubah pesan dalam suatu bahasa sandi menjadi pesan asli.

C = E (M)	M = D (C)

Keterangan :
C = Pesan dalam bahasa sandi.
M = Pesan asli.
E = Proses enkripsi.
D = Proses dekripsi.



Gambar 2.1 Skenario komunikasi dasar kriptografi

Enkripsi dilakukan pada saat pengiriman dengan cara mengubah data asli menjadi data rahasia, sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengubah data rahasia menjadi data asli. Jadi, data yang dikirimkan selama proses pengiriman adalah data rahasia, sehingga data asli tidak dapat diketahui pihak yang tidak berkepentingan. Data asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia.

Kriptografi yang baik tidak ditentukan oleh seberapa rumit pengolahan data atau pesan yang disampaikan, melainkan ada beberapa syarat yang harus dipenuhi untuk mencapainya, yaitu :

a. Kerahasiaan. Pesan (*plaintext*) hanya bisa dibaca oleh pihak yang memiliki kewenangan.
b. Autentikasi. Pengirim pesan harus bisa diidentifikasi dengan pasti, penyusup harus dipastikan tidak bisa berpura-pura menjadi orang lain.
c. Integritas. Penerima pesan harus dapat memastikan bahwa pesan yang diterima tidak dimodifikasi pada saat proses transmisi data.
d. Non-Repudiation. Pengirim pesan harus tidak

bisa menyangkal pesan yang dikirim.

2.4 Steganografi

Steganografi berasal dari bahasa Yunani yaitu "Steganós" yang berarti menyembunyikan dan "Graptos" yang berarti tulisan. Sehingga steganografi artinya adalah tulisan yang disembunyikan. Steganografi adalah ilmu atau seni untuk menyembunyikan pesan rahasia dengan berbagai cara sehingga orang lain selain orang yang dituju, tidak akan menyadari keberadaan pesan rahasia tersebut.

Contohnya si pengirim mulai dengan file gambar biasa, kemudian mengatur warna setiap pixel ke-100 untuk menyesuaikan suatu huruf dalam alphabet, yang perubahannya begitu halus, sehingga tidak ada seorangpun yang menyadarinya jika tidak benar-benar diperhatikan.

Pesan steganografi pada umumnya muncul dengan bentuk lain seperti gambar, daftar belanjaan, artikel, atau pesan-pesan biasa lainnya. Pesan ini merupakan pesan yang menutupi, misalnya, suatu pesan bisa disembunyikan dengan menggunakan tinta yang tidak terlihat diantara garis-garis yang kelihatan.

Ada banyak sekali teknik steganografi penyembunyian pesan rahasia di dalam file-file lain yang mengandung gambar, text bahkan audio tanpa menunjukkan ciri-ciri perubahan yang nyata dalam kualitas maupun struktur dari file asli. Metode ini termasuk tinta yang tidak tampak, microdot, tanda tangan digital, jalur tersembunyi, pengaturan kata, serta komunikasi spectrum lebar.

Tujuan dari teknik steganografi ini adalah untuk menyembunyikan keberadaan suatu pesan rahasia. Kebanyakan praktek steganografi dilakukan dengan membuat perubahan tipis terhadap data digital yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh artikel biasa atau gambar yang tidak mencurigakan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.

Kelebihan steganografi adalah pesan yang dikirim tidak menarik perhatian orang lain. Pesan-pesan dalam kriptografi yang tidak disembunyikan, walaupun tidak dapat dipecahkan atau dibaca, tetap akan menimbulkan kecurigaan. Sehingga seringkali steganografi dan kriptografi digunakan secara bersamaan untuk menjamin keamanan suatu pesan yang dirahasiakan.

Pertama-tama suatu pesan steganografi (*plaintext*) dienkripsi dengan beberapa makna tradisional yang menghasilkan *chipertext*, kemudian *covertext* dimodifikasi dengan beberapa cara sehingga berisi *chipertext* yang menghasilkan *stegotext*. Misalnya ukuran huruf, jenis huruf, ukuran spasi, atau karakteristik lainnya dapat dimanipulasi untuk membawa pesan tersembunyi tersebut. Hanya penerima atau pemegang kunci dekripsi yang dapat membuka pesan dan mendepkripsikannya.

2.5 *Vernam Chiper*

Vernam Chiper merupakan algoritma kriptografi yang ditemukan oleh Mayor J. Maugborne dan G. Vernam. Algoritma ini berjenis *symmetric key* yang artinya kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Pada proses enkripsi, algoritma ini menggunakan cara streamchiper dimana chipper berasal dari hasil XOR (*Exclusive Or*) antara bit *plaintext* dan bit *key*. Algoritma *Vernam Chiper* diadopsi dari *one-time pad chiper*, dimana dalam hal ini karakter diganti dengan bit (0 atau 1). Dengan kata lain, *Vernam Chiper* merupakan versi lain dari *one-time pad chiper*.

Pada proses enkripsi, *chipertext* didapatkan dengan penjumlahan modulo 2 satu bit *plaintext* dengan satu bit kunci.

$$c_1 = (p_1 + k_1) \bmod 2 \qquad \ldots\ldots. 2.1$$

Keterangan :
c_1 = *Chipertext*
p_1 = *Plaintext*
k_1 = Kunci

Sedangkan pada proses dekripsi, untuk mendapatkan kembali pesan plaintext, diperoleh dengan penjumlahan modulo 2 satu bit chipertext dengan satu bit kunci :

$$p_1 = (c_1 + k_1) \bmod 2 \qquad \ldots\ldots. 2.2$$

Pada chipper aliran, bit hanya mempunyai dua buah nilai, sehingga proses enkripsi hanya menyebabkan dua keadaan pada bit tersebut, yaitu berubah atau tidak berubah. Dua keadaan tersebut ditentukan oleh kunci enkripsi yang disebut dengan aliran-bit-kunci (*keystream*). Oleh karena itu, operasi penjumlahan modulo 2 identik dengan operasi bit dengan operator XOR, maka persamaan 2.1 dapat ditulis secara sederhana dengan :

$$c_1 = (p_1 \text{ XOR } k_1) \qquad \ldots\ldots. 2.3$$

Sedangkan proses dekripsinya, dapat ditulis dengan:

$$p_1 = (c_1 \text{ XOR } k_1) \qquad \ldots\ldots. 2.4$$

Dalam operator logika XOR, hasil akan T(*True*) apabila salah satu dari kedua operan (tetapi bukan keduanya) bernilai T atau 1. Dengan kata lain, apabila diaplikasikan dlam bit maka operator XOR akan menghasilkan 1 jika dan hanya jika satu operan bernilai 1.

Contoh :

X: 00111010 10101011
Y: 10100100 01010101
Hasil : 10011110 11111110

Sedangkan suatu bilangan dalam biner apabila di- XOR-kan dengan dirinya sendiri akan menghasilkan 0.

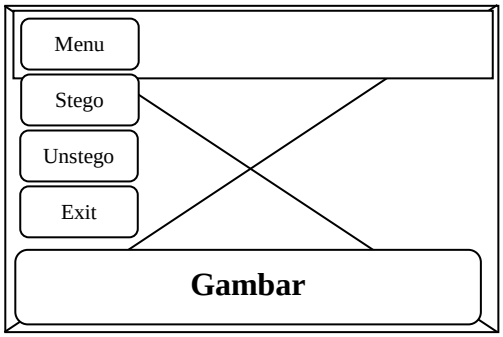
Contoh :
X: 01010101 10101010
Y: 01010101 10101010
Hasil : 00000000 00000000

3. PEMBAHASAN APLIKASI

Dalam pembahasan ini, permodelan menggunakan dua buah aktor yaitu pengirim dan penerima. Aktor tersebut mempunyai karakteristik yang berbeda dalam hal menggunakan aplikasi dan file yang telah diproses.

Pengirim adalah seseorang yang mengirimkan sebuah file yang telah di enkripsi dan disembunyikan pada file induk atau file lain agar tidak terlihat kasat mata oelh pihak-pihak yang tidak berkepentingan.

Penerima adalah seseorang yang akan menerima file yang dikirimkan oleh pengirim. Penerima bertugas untuk membuka file yang telah dikirimkan, kemudian didekripsi dan dipisahkan dengan file induk atau file yang dikirimkan sebelumnya.

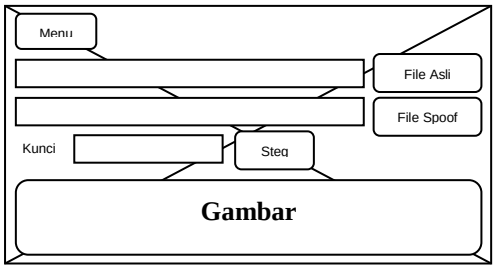


Gambar 3.1 : *StoryBoard* Menu Utama

Submenu-submenu dalam menu utama di atas antara lain :

a. Submenu *Stego*
   Submenu *Stego* merupakan submenu yang digunakan untuk menyembunyikan file.
b. Submenu *Unstego*
   Submenu *Unstego* merupakan submenu yang digunakan untuk mengembalikan file yang telah disembunyikan sebelumnya.
c. Submenu *Exit*
   Submenu *Exit* merupakan submenu yang digunakan untuk keluar dari aplikasi.

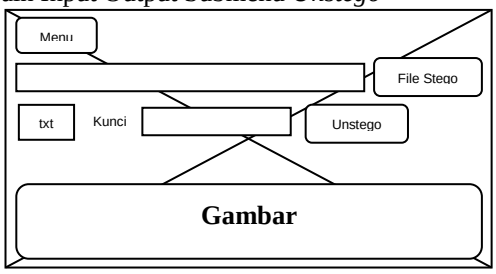
3.1 Desain Input Output Submenu *Stego*



Gambar 3.2 : *Storyboard* submenu *Stego*

Pada submenu *Stego* ini terdapat 3 *text box* yaitu 2 *text box* untuk memasukkan *file* dan 1 *text box* untuk kunci. Kemudian terdapat 3 *command button* yaitu 2 untuk mengambil *file* dan 1 untuk proses *stego* serta 1 label kunci.

3.2 Desain Input Output Submenu *Unstego*



Gambar 3.3 : *Storyboard* pada submenu *Unstego*

Pada submenu *Unstego* ini terdapat 3 *text boxt* yaitu untuk memasukkan *file*, memasukkan kata kunci dan untuk memberikan ekstensi *file* yang nantinya akan terbentuk. Selain itu terdapat 2 *command button* yaitu untuk mengambil *file* dan proses *unstego*. Kemudian terdapat 1 label kunci.

3.3 Implementasi

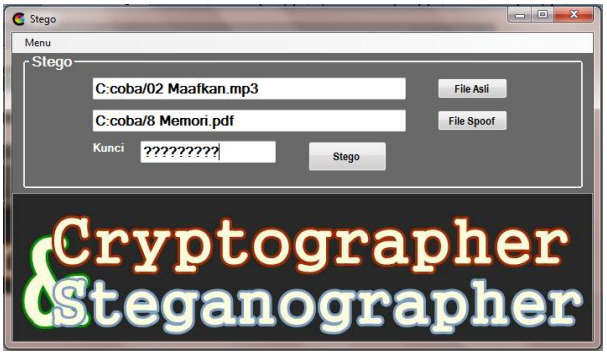
Pada program Kripto dan Stego ini dimulai dengan menekan tombol “Menu” yang terdapat pada sis kiri atas program, kemudian dilanjutkan dengan memilih submenu “Stego” terlebih dahulu.

Gambar 3.4 : Tampilan awal program

Gambar 3.5 : Tampilan submenu *Stego*

Gambar 3.6 : Tampilan Submenu *Unstego*

3.4 Analisa Program



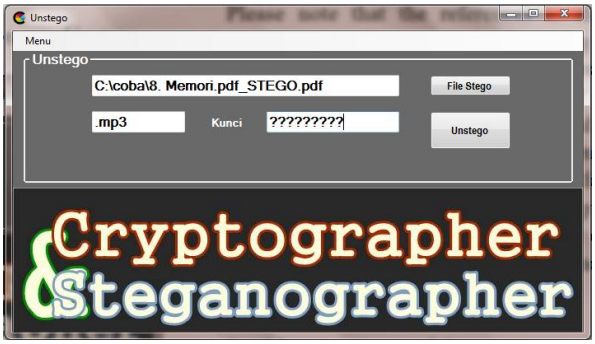
Gambar 3.7 : Submenu *Stego File*

Pada gambar diatas, file akan dikripto dan distego. Langkah awal yang dilakukan setelah tampilan utama (Gambar 3.4) muncul adalah dengan meng-klik tombol menu dan pilih submenu stego.

Pada gambar 3.7 menunjukkan bahwa file asli yang akan disembunyikan adalah "02 Maafkan.mp3" pada partisi "C" dan direktori "coba".

Yang terdapat pada *text box* "File Spoof" merupakan file induk dimana file ini sebagai tempat persembunyian dari file asli. langkah kedua adalah memilih file induk dimana file asli nantinya akan disembunyikan. Dalam hal ini, file yang dikehendaki adalah file "8. Memori.pdf" sebagai tempat persembunyian file aslinya.

Langkah selanjutnya adalah memberikan kata kunci sebagai keamanan data. Pada gambar 3.7 terdapat tanda tanya (?) yang sebenarnya adalah kata sandi. Kemudian tekan tombol "Stego" untuk memproses ke langkah selanjutnya. File yang sudah diproses tadi akan tersimpan pada partisi "C" pada direktori "coba" dengan nama file "8. Memori.pdf_STEGO.pdf".



Gambar 3.8 : Submenu *Unstego File*

Pada gambar di atas menunjukkan tampilan submenu Unstego. Submenu ini diakses dengan menekan "Menu" kemudian memilih submenu "Unstego". Pada submenu *Unstego* ini terdapat proses pengembalian file yang telah diproses pada submenu *Stego*, dengan cara memasukkan file yang telah di-*stego*. Klik tombol "File Stego" kemudian cari file yang telah di-*stego*. Pada gambar 3.8 terlihat lokasi filenya yaitu pada partisi "C", direktori "coba" dengan nama file "8. Memori.pdf_STEGO.pdf". Langkah selanjutnya yaitu menentukan ekstensi file, pada gambar menunjukkan ekstensi file yaitu .mp3. Kemudian masukkan kata kunci yang telah dijanjikan sebelumnya sehingga hanya pihak tertentu saja yang dapat mengetahui kata kunci tersebut. Setelah itu klik tombol "Unstego" untuk memulai proses pemisahan file menjadi file asli seperti sedia kala, sehingga berakhirlah proses penyembunyian file dan file asli tersebut dapat dibaca oleh penerima.

4. KESIMPULAN

Dari hasil perancangan aplikasi kriptografi dengan algoritma *Vernam Chiper* dan Steganografi ini, dapat diambil kesimpulan sebagai berikut :

1. Aplikasi dapat mengacak dan menyembunyikan file dengan aman dan tidak menimbulkan kecurigaan pada pihak lain, hal tersebut sebagai manfaat dari pengaplikasian kriptografi dan steganografi itu sendiri. Pada file hasil, tidak menimbulkan efek yang dapat merusak ataupun mengganggu kinerja file sebelumnya.
2. Penggabungan dua buah file yang berbeda ekstensi menghasilkan file dengan *memory* yang lebih besar dikarenakan gabungan dari ukuran kedua file tersebut.
3. Dengan penambahan metode steganografi pada kriptografi, keamanan data dapat lebih terjamin dan tidak menimbulkan kecurigaan terhadap pesan rahasia yang telah di-enkripsi pada proses kriptografi.

REFERENSI

[1.] H. Rosen, Kenneth. *Discrete Matematics and Its Applications, Sixth Edition*. New York: McGraw.Hill International Edition, 2007.

[2.] Anonimous, *Pengertian Data dan Informasi*, www.kuliah.dinus.ac.id/edi-nur/sb1-7.html, (Diakses pada 17 Desember 2012, pukul 20.15 WIB)

[3.] Salton, Gerard. *Automatic Text Processing.* Addison : Wesley Publising Company. 2003.

[4.] Stallings, Williams, *Cryptography and Network Security : Principles and Practices, 4th edition*, Upper Saddle River : Prentice Hall Inc., 2006

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, 18 Desember 2012

ttd

Kharisma Nugrahandani Restuti - 13512601