BAB I
PENDAHULUAN

I.1. Latar Belakang

Seiring perkembangan zaman, kebutuhan manusia akan informasi semakin meningkat. Ditengah-tengah perkembangan teknologi informasi yang kian semarak, internet tidak lagi menjamin penyediaan informasi yang aman. Berbagai mesin-pencari (*search-engine*) terus berkembang ditambah dengan serangan *virus*, penyadap, *spam* maupun *hacker* yang menjamur dapat mencuri data-data bersifat rahasia. Mengatasi hal tersebut berbagai cara untuk meningkatkan keamanan data terus dikembangkan, diantaranya kriptografi dan steganografi.

Steganografi adalah seni dan ilmu menyembunyikan data pada media lain sebagai *cover* (misalnya citra) sehingga terlihat samar. Kriptografi adalah seni dan ilmu menjaga kerahasiaan. Pada kriptografi, data asli diubah menjadi bentuk lain yang tidak dapat dibaca. Penggabungan steganografi dan kriptografi secara bersamaan dapat meningkatkan pengamanan data.

Metode penggabungan steganografi dan kriptografi banyak dikembangkan. Pada umumnya teknik yang digunakan yaitu dengan mengenkripsi pesan terlebih dahulu (kriptografi), kemudian menyisipkannya ke media *cover* (steganografi). Namun, proses penyisipan dapat berpengaruh pada kualitas media *cover* tersebut.

Upaya untuk meminimalisir perubahan kualitas *cover* dapat dilakukan dengan penyisipan pada bit terakhir (*least significant bit*). Perubahan kualitas *cover* tidak tampak kasat mata. tetapi penyisipan pada bit terakhir dapat mengakibatkan pesan rusak ketika citra dikompresi. Ketahanan terhadap *robust* dapat dilakukan dengan pemilihan pada bit pertama (*most significant bit*), tetapi justru mengakibatkan perubahan kualitas *cover* menjadi tampak dan dapat dicurigai.

Least significant bit adalah bagian dari barisan data biner (basis dua) yang mempunyai nilai paling tidak berarti/paling kecil. Letaknya adalah paling kanan dari barisan bit. Least significant bit sering kali digunakan untuk kepentingan penyisipan data ke dalam suatu media digital lain, salah satu yang memanfaatkan

UPN "VETERAN" JAKARTA

Least significant bit sebagai metode penyembunyian adalah steganografi audio, foto dll .

Berdasarkan uraian diatas maka penulis ingin membuat sebuah aplikasi pesan dengan menerapkan kriptografi algoritma Data Encryption Standart (DES) dan steganografi Metode Least Significant Bit (LSB) agar keamanan yang dihasilkan lebih baik. Gabungan kriptografi dan pesan jarang dipakai dalam pembuatan pesan rahasia yang berarti menyulitkan para criptanalis dalam membongkar dan menyadap pesan yang dihasilkan. Karena criptanalis biasanya hanya membongkar kunci dari kriptografi lalu mendapatkan plaintex nya sementara untuk aplikasi yang penulis buat hasilnya berupa simbol yang perlu diterjemahkan atau di pecahkan lagi dalam huruf latin.

I.2. Rumusan Masalah

Berdasarkan latar belakang di atas, maka masalah yang dapat dirumuskan adalah sebagai berikut :

a. Bagaimana membuat aplikasi untuk mengamankan pesan elektronik dengan menerapkan Metode Least Significant Bits (LSB) dan kriptigrafi DES karena Perlunya tingkat keamanan pesan yang tinggi dalam pengiriman pesan rahasia.
b. Bagaimana membuat pesan elektronik agar terhindar dari penipuan dan pembajakan pesan dalam format digital.
c. Bagaimana membuat pesan elektronik menjadi aman seiring Semakin Mudahnya mengakses data melalui internet dan media sosial lainnya mengakibatkan orang sembarangan mengirimkan, mereply dan menfordward pesan.

I.3. Tujuan dan Manfaat

I.3.1. Tujuan

Tujuan yang dicapai dalam penelitian ini adalah membangun aplikasi dengan penerapan Metode Least Significant Bit (LSB) dan kriptografi untuk pengamanan pesan (*message)* atau dokumen berbasis simbol dengan metode *DES* sehingga menjadi solusi dalam masalah keamanan message atau dokumen agar

sampai pada penerima dengan aman Pengamanan pesan (*message)* dan dokumen dijamin dengan hasil proses *verifikasi.*

I.3.2. Manfaat

Hasil dari penelitian ini diharapkan dapat memberikan manfaat antara lain

a. Bagi para pengguna jaringan komunikasi terutama pada saat pertukaran pesan dan informasi melalui e-mail dapat dilakukan secara aman.
b. Menjadi referensi bagi kegiatan penelitian yang berhubungan dengan Penerapan Metode Least Singnificant Bits (LSB) dan kriptografi menggunakan Data Encryption Standart (DES) untuk meningkatkan keamanan data.

I.4. Ruang Lingkup Masalah

Dalam penulisan skripsi ini, penulis membatasi pembahasan dalam hal berikut :

a. Sistem dan aplikasi yang dibuat untuk membuat pesan kombinasi pesan simbol Metode Least Significant Bits (LSB) dengan kriptografi Data Encryption Standart (DES).
b. Dokumen yang dapat dibaca dalam proses kriptografi ini adalah dokumen dengan format awal *(plaintext)* .txt dan hasil dengan format *(chipertext)* .ces (Caesar Encryption)
c. Dokumen yang dapat dibaca dalam proses steganografi adalah image (citra) dengan format .png .jpg yang di ubah kedalam bentuk biner

I.5. Luaran Yang Diharapkan.

Luaran yang diharapkan dalam skripsi ini berupa membangun sebuah aplikasi dengan penerapan Metode Least Significant Bit (LSB) dan kriptografi untuk pengamanan pesan (*message)* atau dokumen berbasis simbol dengan metode *DES* sehingga menjadi solusi dalam masalah keamanan message atau dokumen agar sampai pada penerima dengan aman Pengamanan pesan (*message)* dan dokumen dijamin dengan hasil proses *verifikasi.*

I.6. Sistematika Penulisan

Dalam pembuatan tugas akhir ini terdapat penjelasan mengenai isi dan bagian dari laporan tersebut. Dimana setiap bagian laporan yang akan menerangkan isi laporan. Sehingga terbentuklah suatu bagian isi dari laporan yang disebut bab. Sedangkan bab adalah bagian dari isi buku, dalam laporan ini dibuat secara berurutan untuk melaporkan hasil suatu laporan yang telah dibuat. Tugas akhir ini ditulis dengan sistematika sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi tentang deskripsi umum isi proposal seminar yang meliputilatar belakang, batasan masalah, manfaat dan tujuan, ruang lingkup, luaran sistem yang diharapkan, metodologi penelitiandan sistematika pembahasan.

BAB II LANDASAN TEORI

Bab ini berisi uraian tentang berbagai literatur yang berkaitan dengan teori, konsep, prosedur, metode, dan proses yang digunakan sebagai referensi dalam penulisan penelitian ini.

BAB III METODOLOGI PENELITIAN

Bab ini berisi tentang langkah-langkah penelitian yang digunakan sebagai pemecahan permasalahan penelitian untuk mencapai tujuan penelitian.

BAB IV ANALISA DAN PERANCANGAN SISTEM

Dalam bab ini membahas tentang analisa sistem berjalan, perancangan sistem, struktur navigasi menu, *story board*, diagram usecase, diagram activity, diagram sequence, evaluasi, desain kebutuhan sistem, dan hasil.

BAB V PENUTUP

Dalam bab ini berisi kesimpulan dari pembuatan skripsi dan aplikasi ini. Serta saran yang diharapkan untuk pengembangan aplikasi ini.

DAFTAR PUSTAKA

DAFTAR RIWAYAT HIDUP