BAB I

PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Dengan seiring perkembangan kemajuan teknologi saat ini, membuat sebuah informasi sangat penting. Bahkan ada yang mengatakan bahwa kita sudah berada di sebuah *"information-based society"*. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun individual (pribadi). Hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi. Sangat pentingnya nilai sebuah informasi menyebabkan seringkali informasi diinginkan hanya boleh di akses oleh orang-orang tertentu.[1]

Masalah keamanan merupakan salah satu aspek paling penting dalam dunia teknologi informasi terutama bagi sebuah perusahaan, insitusi atau organisasi yang mempunyai dokumen-dokumen rahasia dan penting. Mereka mengamankan dokumen-dokumen tersebut agar terhindar dari gangguan orang lain. Sekarang ini, sebagian besar dokumen-dokumen di simpan dalam bentuk file bertipe .txt. Semua orang terbiasa dan akrab dengan file ini karena bersifat fleksibel, kapasitas yang kecil dan aplikasi pengolah kata dalam bentuk notepad sudah tersedia dalam

[1] Budi rahardjo, Keamanan sistem informasi berbasis internet, hal 1-2

sistem operasi *windows* sehingga sangat memudahkan siapa saja ketika menggunakan aplikasi ini.

Secara umum data dikategorikan menjadi dua, yaitu data yang bersifat rahasia dan data yang bersifat tidak rahasia. Data yang bersifat tidak rahasia biasanya tidak begitu diperhatikan. Yang sangat perlu diperlukan adalah data yang bersifat rahasia, di mana setiap informasi yang ada didalamnya akan sangat berharga bagi pihak yang membutuhkan karena data tersebut dapat dengan mudah digandakan. Untuk mendapatkan informasi didalamnya, biasanya dilakukan berbagai cara yang tidak sah. Keamanan data biasanya terkait hal-hal berikut:

1. Fisik, dalam hal ini pihak yang tidak berwenang terhadap data berusaha mendapatkan data dengan melakukan kegiatan sabotase atau penghancuran tempat penyimpanan data.
2. Organisasi, dalam hal ini pihak yang tidak berwenang untuk mendapatkan data melalui kelalaian atau kebocoran anggota yang menanggani data tersebut.
3. Ancaman dari luar, dalam hal ini pihak yang tidak berwenang untuk mendapatkan data melalui media komunikasi dan juga melakukan pencurian data yang tersimpan di dalam komputer.

Melihat pada kenyataan semakin banyak data yang di proses dengan komputer dan di kirim melalui perangkat komunikasi elektronik, maka ancaman terhadap pengamanan data akan semakin meningkat. Salah satu serangan terhadap keamanan adalah: *Interception* yaitu pihak yang tidak berwenang berhasil

mengakses data atau informasi, yang mana serangan ini bisa terjadi pada jaringan *LAN* atau bahkan pada komputer yang tidak terhubung jaringan sekalipun.[2]

Untuk mengatasi masalah keamanan tersebut, salah satu metode yang bisa digunakan adalah ilmu steganografi dan ilmu kriptografi. Kriptografi merupakan tehnik penyandian data. Dengan tehnik kriptografi data disandikan atau di enkripsi menjadi data rahasia sehingga data itu tidak akan berarti apa-apa bagi pihak yang tidak berwenang yang berhasil mengakses aset atau informasi[3]. Data rahasia yang telah dienskripsi dan di terima oleh penerima dapat di ubah lagi atau di deskripsi ke data asli sehingga dapat di pahami.

Algoritma kriptograpi *Caesar Cipher Substitution* atau dikenal pula dengan istilah *classical enkripsi techniques* menggambarkan pendekatan dasar pada *symmetric enkripsi* yang digunakan saat ini dan tipe dari *cryptanalytic attacks yang* harus diantisipasi. Dua dasar pembentukan blok pada *enkripsi techniques* yaitu *substitution* dan *transposition. Substitution techniques* adalah satu teknik yang huruf-huruf di *plaintext* diganti dengan huruf-huruf lain, atau dengan angka-angka, atau dengan simbol-simbol. Jika sebuah *plaintext* ditampilkan sebagai sebuah urutan bits, maka *substitusion ivolves* mengganti *bit patterns* dengan *ciphertext bit patterns*.

Algoritma venegere merupakan jenis transposition Metode ini mengubah posisi karakter atau bit dari data jelas. *Cipher Transposition* yang tertua dari

---

[2] Ibid. hal 20

[3] Rinaldi munir, buku teks ilmu komputer algoritma dan pemograman dalam bahasa pascal dan c

metode ini adalah *cipher scystale* yang dimiliki nenek moyang orang Yunani pada 400 SM. Perubahan posisinya dikenal sebagai *Delphi-k,* dan disusun dalam kbaris.

Implementasi keamanan data ditujukan untuk membantu mengatasi masalah keamanan dokumen yang di buat atau di simpan dari pencurian dokumen baik yang penting maupun yang umum tapi bersifat rahasia sehingga orang lain tidak dapat mengetahui isi dari dokumen tersebut.

Penggabungan dua teknik keamanan data yakni kriptografi dengan menggunakan metode *venegere dan Caesar subsitution* dan steganografi diharapkan mampu mengamanankan data hanya dengan menggunakan metode kriptografi dasar. Dimana kritpografi berfungsi untuk mengkodekan data sedangkan steganografi berfungsi untuk menyisipkan pesan, sehingga pesan yang sudah dienkripsi kemudian disembunyikan sehingga keberadaan pesan sulit untuk diketahui.

Berdasarkan uraian di atas, penulis mencoba mengimplementasikan steganografi dan kriptografi dalam bentuk program dan menjadikannya sebagai bahan untuk penelitian skripsi dengan judul **"IMPLEMENTASI STEGANOGRFI DENGAN PENGGABUNGAN KRIPTOGRAFI METODE VINEGERE DAN CAESAR SUBSITUTION"**

1.2 RUMUSAN MASALAH

Berdasarkan uraian di atas yang meliputi latar belakang maka dapat di peroleh rumusan masalah sebagai berikut:

1. Bagaimana menyisipkan sebuah pesan kedalam suatu gambar dan mengubah pesan tersebut menjadi kode-kode yang tidak dikenali sehingga tidak bisa dibaca dan mengubah kode-kode tersebut kembali kebentuk aslinya agar dapat dibaca.
2. Bagaimana mengimplementasikan metode steganografi dan algoritma kriptograpi dengan metode *vinegere dan caesar substitution* kedalam kode-kode program sehingga dapat dihasilkan aplikasi yang dapat menyisipkan sebuah pesan kedalam gambar dan mengamankan pesan tersebut.

1.3 BATASAN MASALAH

Berdasarkan latar belakang yang ada dan untuk menghindari terjadinya pelebaran masalah yang akan diuraikan, maka ditentukan batasan masalah dari permasalahan yang di hadapi sebagai berikut:

1. Algoritma kriptografi yang di pakai untuk mengkodekan data adalah algoritma venegere dan Caesar subtitution.
2. Jenis plainteks yang digunakan adalah dalam bentuk text dengan format dokumen dengan bertipe .txt.
3. Data yang digunakan untuk menyisipkan hasil pengkodean adalah data dalam bentuk citra atau gambar yang berekstensi *.bmp.

4. Metode yang digunakan untuk menyisipkan hasil pengkodean kedalam data yang lainnya adalah motode LSB (*Least Significant Bit*).
5. Aplikasi hanya bisa dijalankan pada system operasi windows.

1.4 TUJUAN PENELITIAN

Tujuan yang ingin dicapai dalam penelitian ini adalah mampu merancang dan membuat aplikasi penyandian dan penyisipan data dalam bentuk teks dengan menggunakan *covertext* citra yang berekstensi *bitmap* dengan menggunakan algorima *venegere* dan *caesar subtitution* dan LSB.

1.5 MANFAAT PENELITIAN

1. Dapat membantu mengatasi masalah keamanan dokumen dalam hal ini difokuskan pada data teks .txt.
2. Dapat membantu mengatasi masalah keamanan data yang tersimpan dalam komputer baik yang terhubung dalam jaringan maupun yang tidak terhubung ke dalam jaringan.

1.6 METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah :

1. Pengamatan (*Observation*) : Yaitu metode pengumpulan data dengan mengadakan pengamatan secara langsung terhadap obyek penelitian.
2. Kearsipan (*Documentation*) : Yaitu metode pengumpulan data berdasarkan dokumen-dokumen yang telah ada untuk dilakukan analisa.

3. Kepustakaan (*Library*) : Yaitu metode pengumpulan data menggunakan pustaka-pustaka yang telah ada untuk digunakan sebagai referensi atau bahkan digunakan sebagai bahan pembanding.

1.7 SISTEMATIKA PENULISAN LAPORAN PENELITIAN

Laporan penelitian ini disusun secara sistematis dalam masing-masing bab dan pada masing-masing bab akan diuraikan masalah-masalah sebagai berikut:

Bab I : Pendahuluan

Membahas tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika laporan.

Bab II : Landasan Teori

Menjelaskan dan menguraikan tentang pengenalan sistem secara umum dan perangkat lunak yang akan digunakan oleh penulis dalam menyusun sistem.

Bab III: Perencanaan Sistem

Membahas tentang rancangan system secara rinci, rancangan desain, rancangan basis data, rancangan input, rancangan output dan rancangan IPO.

Bab IV: Implementasi Sistem

Membahas tentang penerapan rencana implementasi, kegiatan implementasi dan manual program.

Bab V : Penutup

Membahas tentang kesimpulan dari hasil analisa serta saran-saran dari semua kegiatan pembuatan skripsi ini.