BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi di zaman sekarang ini sudah semakin maju dengan sangat pesat. Semua lapisan masyarakat mayoritas sudah memanfaatkan teknologi di segala bidang dalam kehidupan sehari - hari. Ditambah lagi dengan adanya internet yang mudah diakses oleh siapapun dan kapanpun di seluruh dunia sehingga menjadi sarana untuk saling berkomunikasi, dan bertukar informasi. Internet menjadi perantara bagi pengguna untuk saling mengirim dan bertukar informasi. Informasi yang dikirimkan berupa informasi yang penting sampai informasi yang sangat rahasia. Namun, pengiriman data tidak menjamin bahwa data tersebut akan aman dari pihak ketiga yang diam – diam mengambil informasi tersebut.

Keamanan data merupakan salah satu yang harus diperhatikan dalam pengiriman data tersebut agar data yang dikirimkan tidak diketahui oleh pihak ketiga. Pihak ketiga atau sering disebut dengan *hacker* bisa saja dengan sengaja memanfaatkan celah – celah yang ada pada suatu sistem untuk masuk ke dalam sistem tanpa diketahui oleh siapapun dan mengambil semua data dan informasi yang penting termasuk data yang bersifat rahasia sekalipun. Terdapat beberapa metode untuk menjaga kerahasiaan data dan informasi tersebut agar tidak mudah diketahui orang lain yaitu dengan teknik kriptografi dan steganografi.

Teknik kriptografi merupakan teknik matematika persandian yang sudah digunakan sejak zaman dahulu yang bertujuan untuk menjaga kerahasiaan suatu pesan rahasia sehingga isi pesan yang dikirimkan hanya pengirim dan penerima pesan yang bisa membaca isi dari pesan rahasia tersebut. Teknik tersebut masih digunakan sampai sekarang dan sudah diaplikasikan ke sistem komputer. Terdapat banyak sekali macam – macam tehnik kriptografi salah satunya Algoritma Rijndael atau sering disebut AES *(Advanced Encryption Standard).*

Algoritma Rijndael merupakan kriptografi yang didesain oleh Vincent Rijmen dan John Daemen yang berasal dari Belgia. Algoritma tersebut keluar sebagai pemenang kontes algoritma kriptografi yang menggantikan algoritma DES (*Data Encryption Standard*) yang diadakan oleh NIST (*National Institutes of Standards and Technology*) milik pemerintah Amerika Serikat pada tanggal 26 November 2001. Algoritma Rijndael ini kemudian dikenal dengan algoritma AES (*Advanced Encryption Standard*) dan mengalami proses standardisasi oleh NIST menjadi *standard* algoritma kriptografi secara resmi pada tanggal 22 Mei 2002. (Eko, 2009).

Teknik Steganografi merupakan teknik menyembunyikan sebuah pesan rahasia atau *file* ke dalam media penyisipan berupa *file* media penyisipan seperti gambar, audio, dan video sehingga orang biasa tidak mengetahui bahwa ada suatu pesan atau *file* yang terdapat di dalam media penyisipan tersebut. Metode LSB *(Least Significant Bit)* adalah salah satu jenis metode tehnik steganografi.

Dari latar belakang permasalahan diatas, penulis bermaksud untuk mengimplementasikan salah satu jenis kriptografi yaitu Algoritma Rijndael (AES) untuk memenuhi kebutuhan keamanan pesan rahasia dan dikombinasikan dengan teknik steganografi metode LSB *(Least Significant Bit)* dalam penyisipan *file* ke dalam citra digital.

1.2 Rumusan Masalah

Berdasarkan pada latar belakang masalah maka rumusan masalah sebagai berikut:

1. Bagaimana rancangan algoritma Rijndael pada skema steganografi dengan metode LSB *(Least Significant Bit)* ?
2. Bagaimana mengimplementasikan algoritma Rijndael?
3. Bagaimana kinerja algoritma Rijndael pada steganografi dengan metode *Least Significant Bit* ?

1.3 Batasan Masalah

Berikut adalah batasan masalah yang digunakan :

1. Teknik kriptografi yang akan digunakan untuk enkripsi pesan menggunakan Algoritma Rijndael atau AES *(Advanced Encryption Standar)*.
2. Data yang disisipkan berformat teks (*.txt) dan dibuat secara manual.
3. Panjang *key* algoritma Rijndael yang akan digunakan adalah 128 bit.
4. Media steganografi berupa *file* gambar Bitmap (*.bmp).
5. Metode Steganografi yang digunakan adalah metode *Leat Significant Bit*.
6. Implementasi perangkat lunak menggunakan bahasa pemrograman JAVA.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah sebagai berikut:

1. Implementasi Algoritma Rijndael dalam steganografi *Least Significan Bit* yang berbentuk aplikasi desktop yang dapat digunakan untuk mengamankan dan menyembunyikan suatu pesan rahasia.
2. Analisis kinerja aplikasi algoritma rijndael dalam steganografi LSB .

1.5 Manfaat Penelitian

Manfaat yang diperoleh dalam penelitian ini adalah:

1. Memudahkan penyisipan pesan rahasia berupa *file* teks ke dalam citra digital agar tidak mudah diketahui oleh pihak yang tidak bertanggung jawab.
2. Dapat memberikan wawasan baru dalam mengembangkan penelitian serupa pada masa selanjutnya.

1.6 Metodologi Penelitian

Metodologi penelitian tugas akhir ini merupakan langkah kerja yang digunakan dalam pengerjaan tugas akhir ini agar lebih terarah. Metodologi yang digunakan dalam penyusunan tugas akhir ini adalah :

1. Analisis Masalah

Metode ini digunakan untuk menganalisis permasalahan yang ada yang menyebabkan mengapa penelitian ini dilakukan.

2. Analisis Kebutuhan

   Metode ini digunakan untuk menganalisis apa yang dibutuhkan untuk pembuatan sistem aplikasi meliputi spesifikasi *hardware,* analisis kebutuhan *software,* dan langkah – langkah yang digunakan dalam pembuatan aplikasi.

3. Perancangan

   Metode perancangan ini digunakan untuk merancang aplikasi yang akan dibangun meliputi perancangan *flowchart*, perancangan *data flow diagram* perancangan *user interface,* dan perancangan pengujian.

4. Implementasi

   Metode ini menggunakan hasil perancangan sistem yang telah dibuat sebelumnya dan diterapkan ke dalam sistem yang dibangun.

5. Pengujian

   Metode pengujian ini dilakukan untuk pengujian dari aplikasi yang telah dibuat.

1.7 Sistematika Penulisan

Untuk mempermudah pembaca agar memberikan gambaran secara menyeluruh tentang masalah yang dibahas , maka sistematika penulisannya sebagai berikut.

BAB I PENDAHULUAN

Bab ini membahas tentang pembahasan masalah umum meliputi latar belakang masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penelitian.

BAB II LANDASAN TEORI

Bab ini membahas tentang teori dasar yang digunakan sebagai sumber atau acuan dalam memahami permasalahan yang akan menjadi dasar dalam melakukan penelitian.

BAB III ANALISIS KEBUTUHAN DAN PERANCANGAN

Bab ini membahas tentang analisis kebutuhan apa saja yang dibutuhkan dalam pembangunan sistem dan perancangan sistem yang akan dibangun.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas tentang implementasi pembahasan dari sistem yang telah dibangun, analisis kinerja dari sistem, dan pengujian dari sistem yang sudah dibangun.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dari penelitian dan saran yang diperlukan untuk membangun sistem untuk lebih baik kedepannya lagi.