BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi komunikasi dan informasi yang pesat telah membawa perubahan bagi kehidupan manusia. Salah satu contoh nyata dari perkembangan teknologi komunikasi dan informasi adalah perkembangan internet yang memungkinkan pertukaran data dengan mudah melalui internet tersebut. Seiring dengan perkembangan tersebut, berbagai kejahatan teknologi komunikasi dan informasi juga turut berkembang. Berbagai ancaman dari keamanan komunikasi lewat jaringan telah menjadi perhatian bagi para pengguna internet, seperti interupsi, penyadapan, modifikasi, maupun fabrikasi. Tentunya ancaman ini akan berakibat pada data-data yang dikomunikasikan (Sukrisno, 2007).

Keamanan dan kerahasiaan data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan jaringan komputer saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Sistem-sistem vital, seperti sistem pertahanan, sistem perbankan, sistem bandar udara dan sistem-sistem yang lain setingkat itu, membutuhkan tingkat kemanan yang sedemikian tinggi. Hal ini disebabkan karena kemajuan bidang jaringan komputer dengan konsep open systemnya sehingga siapapun, dimanapun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut. Untuk menjaga keamanan dan kerahasiaan pesan, data, atau informasi dalam suatu jaringan komputer maka diperlukan beberapa enkripsi guna membuat pesan, data atau informasi agar tidak dapat di baca atau dimengerti oleh sembarang orang. Kecuali untuk penerima yang berhak (Kristanto, 2003).

Salah satu ilmu untuk menjaga keamanan dan kerahasiaan data atau informasi adalah kriptografi. Algoritma kriptografi pertama kali dikembangkan untuk mengijinkan organisasi tertentu yang ditunjuk untuk mengakses suatu informasi. *Julius caesar* dikenal sebagai orang yang pertama kali telah

mengembangkan algoritma kriptografi untuk mengirimkan pesan ke tentaranya. Algoritma kriptografi terdiri dari algoritma enkripsi dan algoritma dekripsi.

Citra *digital* telah digunakan secara luas dalam berbagai macam proses sehingga perlindungan citra digital dari pihak yang tidak memiliki hak akses menjadi sangat penting (Krikor, 2009).

Ada banyak model dan metode enkripsi, salah satu di antaranya adalah enkripsi dengan metode DES *(Data encryption standard)*. Metode ini merupakan salah satu algoritma kunci simetris yang berbentuk *block cipher*. Algoritma DES *(Data encrytion standard)* adalah algoritma *cipher block* yang populer karena dijadikan standard algoritma enkripsi kunci simetri. Algoritma DES *(Data encryption standard)* dikembangkan di IBM dibawah kepemimpinan W.L. Tuchman pada tahun 1972. Algoritma ini didasarkan pada algoritma lucifer yang dibuat oleh Horst feistel. Oleh sebab itu penelitian ini akan membangun sebuah **Aplikasi Enkripsi dan Dekripsi Dengan Algoritma DES *(Data encryption standard)* Untuk Citra Digital.**

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan diatas maka rumusan masalah yang akan dibahas adalah bagaimana membuat aplikasi enkripsi dan dekripsi dengan algoritma *Data encryption standard* (DES) untuk citra digital ?

1.3 Batasan Masalah

Batasan masalah yang akan dibahas pada aplikasi enkripsi dan dekripsi citra dengan algoritma *Data encryption standard* adalah :

1. Algoritma kriptografi yang digunakan untuk enkripsi dan dekripsi citra adalah algoritma DES *(Data encryption standard).*
2. File citra yang di enkripsi dan dekripsi dengan algoritma DES *(Data encryption standard)* adalah file citra dengan format bitmap 24 bit.

1.4 Tujuan Penelitian

Tujuan dari diadakannya penelitian ini adalah untuk membuat suatu aplikasi enkripsi dan dekripsi citra format bitmap dengan menggunakan algoritma *Data Encryption Standard.*

1.5 Manfaat Penelitian

Manfaat yang diharapkan pada penelitian ini adalah agar dapat meningkatkan keamanan informasi data citra dan mengurangi resiko manipulasi data citra oleh pihak lain yang tidak bertanggung jawab.

1.6 Metoda Penelitian

Metoda yang digunakan dalam pengumpulan data dan tahapan model pengembangan sistem pada penelitian ini menggunakan model *Waterfall*. Adapun tahapan-tahapan dari model *Waterfall* adalah sebagai berikut (Pressman, 1997).

1. Tahap Analisis

   Proses pengumpulan kebutuhan diintensifkan dan difokuskan, khususnya pada perangkat lunak. Untuk memahami sifat program yang dibangun, analis memahami informasi, tingkah laku, unjuk kerja dan antar muka *(interface)* yang diperlukan.

2. Tahap Desain

   Proses multi langkah yang berfokus pada empat atribut sebuah program yang berbeda, yaitu Struktur data, arsitektur perangkat lunak, representasi interface, dan detail (algoritma) prosedural. Proses desain menerjemahkan syarat/kebutuhan kedalam representasi perangkat lunak yang dapat demi kualitas sebelum dimulai pemunculan kode. Sebagaimana persyaratan, desain didokumentasikan dan menjadi bagian dari konfigurasi perangkat lunak.

3. Implementasi

Desain harus diterjemahkan kedalam bentuk mesin yang bisa dibaca. Langkah pembuatan kode melakukan tugas ini.

4. Pengujian

   Proses pengujian berfokus pada logika internal perangkat lunak, memastikan semua pernyataan sudah diuji, dan pada eksternal fungsional.

5. Pemeliharaan

   Perangkat lunak akan mengalami perubahan setelah disampaikan kepada pelanggan. Pemeliharaan perangkat lunak mengaplikasikan lagi setiap fase program sebelumnya dan tidak membuat yang baru lagi.

1.7 Sistematika Penulisan

Untuk memberikan gambaran mengenai isi laporan secara keseluruhan, berikut akan diuraikan secara singkat sistematika penulisan laporan sebagai berikut :

BAB 1 PENDAHULUAN

Berisi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metoda penelitian, dan sistematika penulisan.

BAB 2 LANDASAN TEORI

Pada bab ini diuraikan secara teoritis mengenai kriptografi, citra, kriptografi pada citra digital, dan algoritma DES *(Data encryption standard)*.

BAB 3 ANALISIS DAN PERANCANGAN

Beberapa hal yang akan dibahas pada bab ini, antara lain analisis sistem yang akan dibangun, *data flow diagram* sistem yang akan dibangun, dan rancangan antarmuka sistem yang akan dibangun.

BAB 4 IMPLEMENTASI DAN PENGUJIAN

Proses pembuatan perangkat lunak, tampilan perangkat lunak yang dibuat, dan hasil pengujian perangkat lunak.

BAB 5 PENUTUP

Bab ini berisi simpulan secara umum dan saran yang membangun untuk masa yang akan datang.