BAB I

PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Di era globalisasi ini, di mana segala sesuatu berjalan dengan cepat dan instan, kemajuan teknologi semakin memudahkan manusia untuk berkomunikasi dan saling bertukar informasi. Tetapi dengan kemajuan teknologi itu, dapat diubah oleh orang lain yang tidak berhak. Masalah keamanan dan kerahasiaan data merupakan hal yang sangat penting baik dalam suatu organisasi yang berupa komersial (perusahaan), perguruan tinggi, lembaga pemerintahan, maupun pribadi. Terlebih jika arus data tersebut berada dalam suatu jaringan komputer yang terhubung ke jaringan publik atau internet. Banyak orang kemudian berusaha menyiasati bagaimana mengamankan informasi yang dikomunikasikannya, atau menyiasati bagaimana mendeteksi keaslian dari informasi yang diterimanya.

Citra digital telah digunakan secara luas dalam berbagai macam proses sehingga perlindungan citra digital dari pihak yang tidak memilki hak akses menjadi sangat penting. Pemerintah, militer, badan keuangan, rumah sakit, dan perusahaan swasta telah menggunakan citra digital untuk menyimpan informasi penting, misalnya hasil pemeriksaan pasien (untuk rumah sakit), area geografi (untuk penelitian), posisi musuh (untuk militer), produk baru (untuk perusahaan swasta), status keuangan, dan lain-lain.

Oleh karena itu, untuk menghindari hal yang tidak diinginkan terjadi, digunakanlah sebuah program khusus enkripsi data. Saat ini banyak beredar program khusus enkripsi data, pada umunya program tersebut tidak hanya menyediakan satu metode saja, tetapi beberapa jenis sehingga kita dapat memilih yang menurut kita paling aman. Dengan arus informasi yang semakin global, kriptografi telah menjadi suatu bagian yang tidak dapat dipisahkan dari sistem keamanan jaringan.

Kriptografi ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Ada berbagai algoritma kriptografi yang sekarang ini telah dan sedang di kembangkan salah satu diantaranya algoritma kunci simetris dan asimetris (pembagian berdasarkan kunci). Salah satu algoritma kriptografi adalah *Tiny Encryption Algorithm (TEA). Tiny Encryption Algorithm* TEA merupakan algoritmasandi yang diciptakan oleh David Wheeler dan Roger Needham dari Computer Laboratory, Cambridge University, England pada bulan November 1994. Algoritma ini merupakan algoritma penyandian *block cipher* yang dirancang untuk penggunaan memory yang seminimal mungkin dengan kecepatan proses yang maksimal. TEA diklaim mempunyai tingkat keamanan yang tinggi jika dibandingkan dengan algoritma kriptografi sejenis. Keunggulan utama dari TEA adalah keringanan prosesnya, operasi-operasi yang digunakan hanya berupa operasi bit biasa, tanpa substitusi, permutasi ataupun operasimatrik.

Bertitik tolak dari permasalahan tersebut, penulis merasa perlu mengembangkan suatu aplikasi yang dapat melakukan proses enkripsi dan dekripsi yang tingkat keamanannya tidak diragukan. Maka dari itu, penulis tertarik untuk mengambil judul **"Kriptografi File Citra Menggunakan Algoritma *Tiny Encription Algorithm (TEA)*".**

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang yang telah diuraikan diatas, maka yang menjadi permasalahan yang penulis rumuskan sebagai berikut:

1. Bagaimana melakukan proses enkripsi dan dekripsi file citra menggunakan Algoritma *Tiny Encryption Algorithm (TEA).*
2. Bagaimana membuat aplikasi yang dapat digunakan untuk mengamankan file citra .

1.3 BATASAN MASALAH

Penelitian ini mempunyai batasan-batasan masalah sebagai berikut :

1. Hanya membahas mengenai proses penyandian pesan yang meliputi : proses enkripsi dan dekripsi file citra menggunakan Algoritma TEA serta mengimplementasikannya dalam program sederhana.
2. Menggunakan gambar citra yang berformat *bitmap.*
3. Citra yang digunakan adalah foto hasil scan ijazah atau sertifikat.
4. Tidak membahas mengenai mekanisme pemecahan kunci sandi (kriptanalisis).
5. Tidak membahas mengenai mekanisme perhitungan Fungsi Hash SHA-1.
6. Menggunakan bahasa pemograman Delphi 7.0

1.4 TUJUAN PENELITIAN

Tugas akhir ini bertujuan untuk :

1. Merancang suatu sistem keamanan file citra yang dapat digunakan dalam hal pengamanan file citra agar tidak dapat di ganggu ataupun di akses oleh pihak yang tidak berhak meskipun digunakan pada jaringan yang tidak aman, sehingga keamanan file citra tetap terjaga.
2. Mengimplementasikan enkripsi dan dekripsi pada file citra dengan menggunakan algoritma *Tiny Encryption Algorithm (TEA).*

1.5 MANFAAT PENELITIAN

Manfaat penelitian adalah sebagai berikut :

1. Dapat menjadi solusi menjaga kerahasian dalam pertukaran informasi yang melalui jaringan.
2. Perangkat lunak yang dibangun dapat menjadi salah satu alternatif untuk mengenkripsi dan mendekripsi file citra.