BAB I

PENDAHULUAN

I.1 Latar Belakang

Pada zaman modern ini, teknologi pengiriman pesan makin sering digunakan. Tetapi apabila pesan yang ingin dikirimkan bersifat rahasia, maka pesan tersebut harus dimodifikasi agar hanya dapat dimengerti oleh penerima yang dituju. Hal ini dapat dilakukan dengan memakai kriptografi.

Kriptografi visual adalah teknik merahasiakan pesan khusus untuk citra [1] yang pertama kali diperkenalkan oleh Naor dan Shamir pada tahun 1994, dan menggunakan Kriptografi Visual (2,2)[9]. Sama halnya dengan kriptografi biasa, kriptografi visual mempunyai dua tahap: enkripsi dan dekripsi. Enkripsi adalah mengubah pesan awal (plain image) menjadi sebuah pesan yang bersifat rahasia (cipher image), sedangkan dekripsi adalah tahap mengubah kembali pesan rahasia (cipher image) menjadi pesan awal (plain image). Dalam kerjanya, kriptografi membutuhkan teknik ataupun algoritma untuk melakukan enkripsi dan dekripsi, salah satu algoritma yang bisa dipakai adalah algoritma ElGamal.

Algoritma ElGamal pertama kali dikenalkan oleh Taher ElGamal pada tahun 1985. Algoritma ini adalah algoritma kunci publik dan keamanannya terletak pada kesulitan untuk mencari logaritma diskrit[2]. Algoritma ElGamal telah sering digunakan untuk mengenkripsi dan mendekripsikan text, email, file, dan software. Pada tugas akhir ini, algoritma ElGamal akan digunakan sebagai algoritma kriptografi visual untuk mengenkripsi dan mendekripsikan satu gambar.

I.2 Perumusan Masalah

1. Bagaimana menyembunyikan gambar rahasia dengan Kriptografi Visual menggunakan algoritma ElGamal ?
2. Bagaimana performansi hasil yang diperoleh dari hasil dekripsi dibandingkan dengan citra rahasia aslinya ?

I.3 Tujuan Penelitian

1. Merealisasikan penyembunyian gambar dengan Kriptografi Visual menggunakan algoritma ElGamal dengan bantuan perangkat lunak MATLAB.
2. Membandingkan performansi gambar sebelum dilakukan enkripsi menggunakan kriptografi ElGamal dengan gambar hasil dekripsinya.

I.4 Pembatasan Masalah

1. Gambar yang dipakai dalam kriptografi visual ini berupa gambar berwarna.
2. Ukuran citra yang digunakan adalah 400x400 piksel.
3. Realisasi penyembunyian gambar rahasia dilakukan dengan menggunakan bantuan perangkat lunak MATLAB.

I.5 Sistematika Pembahasan

Sistematika penulisan yang akan digunakan untuk menyusun laporan Tugas Akhir ini adalah sebagai berikut:

Bab I : Pendahuluan

Pada bab ini dijelaskan latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi, serta sistematika pembahasan yang digunakan untuk menyusun laporan Tugas Akhir.

Bab II : Landasan Teori

Pada bab ini dijelaskan teori-teori yang digunakan sebagai referensi penulis dalam pengerjaan Tugas Akhir ini. Teori yang diuraikan berkaitan dengan metode Kriptografi Visual dan algoritma ElGamal.

Bab III : Perancangan Perangkat Lunak

Pada bab ini dijelaskan mengenai sistem dari Tugas Akhir ini serta perancangan perangkat lunak dengan menggunakan software MATLAB.

Bab IV : Pengujian dan Analisis Hasil Uji

Bab ini berisikan percobaan-percobaan yang dilakukan terhadap perangkat lunak dan menampilkan data pengamatan serta analisis hasil percobaan.

Bab V : Kesimpulan dan Saran

Bab ini berisikan kesimpulan dari hasil percobaan yang telah didapatkan dari Tugas Akhir serta saran-saran yang dapat digunakan untuk membantu dalam pengembangan Tugas Akhir ini.