BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring perkembangan teknologi keamanan ataupun kerahasian suatu data sangatlah penting. Bertukar data atau informasi melalui jaringan publik seperti internet ataupun menyimpan data pada sebuah media penyimpanan diasumsikan dapat menimbulkan kekhawatiran terhadap penyadapan ataupun pencurian data. Masalah-masalah tersebut tentunya tidak terlepas dari keamanan data itu sendiri.

Dalam mengamankan suatu dapat menggunakan kriptografi dan steganografi. Pada kriptografi data diubah menjadi bentuk yang tidak memiliki makna. Namum, hal ini diasumsikan dapat mengakibatkan kecurigaan karena hasil dari kriptografi tetap tersedia dan dapat dilihat. Sedangkan pada steganografi data rahasia disembunyikan kedalam media penyembunyi sehingga data rahasia tersebut tidak dapat di lihat lagi. Hal ini tentunya lebih aman dibandingkan dengan kriptografi. Akan tetapi, steganografi memerlukan *password* yang digunakan untuk proses penyembunyian dan pengekstraksan data pada media penyembunyi, *password* yang digunakan tentunya haruslah sama antara *password* penyembunyi data dan *password* pengekstraksan data. Permasalahan yang muncul adalah bagaimanakah cara mengirimkan kunci secara aman dan bagaimanakah aplikasi dapat mengetahui bahwa *password* yang digunakan pada saat menyembunyikan data telah sama dengan *password* yang digunakan pada saat mengekstrak data?. Permasalahan-permasalahan tersebut dapat teratasi dengan cara mengenkripsi terlebih dahulu data rahasia dengan sebuah kunci dan kemudian disembunyikan pada media

peyembunyi lalu kemudian kunci tersebut digunakan pula untuk melakukan proses pengekstraksan dan pendekripsian data rahasia, apabila kunci yang digunakan pada proses pengekstraksan tidak sama dengan kunci yang digunakan pada saat penyembunyian data, data pada media penyembunyi akan tetap terungkap namun hasil dekripsinyalah yang berbeda.

Oleh karena itu, kriptografi dan steganografi akan digunakan secara bersama-sama pada penelitian kali ini dan agar pengirim dan penerima memiliki kunci yang sama maka digunakanlah algoritma Diffie-Hellman untuk pembuatan kunci dan untuk proses enkripsi dan dekripsi digunakan algoritma Vigenere Cipher serta menggunakan metode *End Of File* pada teknik steganografi agar tidak merubah integritas media penyembunyi. Sehingga penelitian ini berjudul "Implementasi Kriptografi Diffie-Hellman, Kriptografi Vigenere Cipher dan Steganografi *End Of File* Untuk Keamanan Data"

1.2 Rumusan Masalah

Berdasarakan latar belakang diatas maka yang menjadi perumusan masalah dalam penelitian ini adalah:

1. Bagaimanakah keamanan suatu data dengan menggunakan metode kriptografi Diffie-Hellman , Vigenere Cipher dan steganografi *End Of File*.
2. Bagaimanakah pengaruh metode steganografi *End Of File* terhadap gambar penampung data rahasia.

1.3 Ruang Lingkup Penelitian

Mengingat luasnya permasalahan yang ada maka batasan penelitian ini adalah:

1. Algoritma kriptografi yang digunakan adalah algoritma Vigenere Chiper untuk enkripsi dan dekripsi dengan menggunakan kunci simetri yang dihasilkan oleh algoritma Diffie-Hellman (DH).
2. Algoritma steganografi yang digunakan adalah algoritma steganografi *End Of File* (EOF).
3. *File* yang digunakan sebagai *file* rahasia adalah *file* berformat *.txt, *.doc, *.docx, *.pdf, *.html, *.htm, *.xhtml.
4. *File* yang digunakan untuk menyembunyikan data adalah *file* gambar dengan ekstensi *.jpg, *.jpeg, *.png serta *.bmp.
5. Enkripsi dan dekripsi dilakukan pada isi *file.*

1.4 Tujuan Penelitian

Penelitian ini dilakukan dengan tujuan untuk menguji/mengetahui:

1. Keamanan suatu data dengan menggunakan metode kriptografi Diffie-Hellman, Vigenere Cipher dan steganografi *End Of File*.
2. Pengaruh metode steganografi *End Of File* terhadap *file* penampung data rahasia.

1.5 Manfaat Penelitian

Adapun manfaat yang dapat diperoleh dari penelitian ini adalah:

1. Data hasil enkripsi disembunyikan, sehingga kecurigaan terhadap data hasil enkripsi dapat terhindarkan.
2. Data yang disembunyikan pada gambar sulit / tidak dapat terbaca.
3. Integritas data dari *file* yang disisipi (gambar) tetap terjaga