BAB I
PENDAHULUAN

1.1 Latar Belakang

Dengan hadirnya teknologi pengiriman pesan semakin mudah dilakukan. Sebelumnya, pengiriman pesan dilakukan secara manual dari mengantar langsung, dikirim dengan media hewan seperti merpati bahkan pesan rahasia yang dikirim dengan menggundul kepala si pengantar dan menuliskannya di kepala tersebut. Begitu banyak cara pengiriman pesan yang dilakukan hingga hadirnya teknologi. Namun, perkembangan teknologi, semakin banyak pula cara pihak-pihak yang tidak berkepentingan untuk mencuri isi pesan tersebut.

Hingga ditemukan kriptografi sebagai cara mengirimkan pesan dengan menyamarkan isi pesan tersebut. Salah satu fungsi kriptografi adalah kerahasian data, namun kriptografi yang sering dipakai justru dibobol oleh pihak yang tidak memiliki hak akses terhadap data rahasia. Sebut saja *brute force* dimana sang pembobol berusaha memecahkan data rahasia dengan kemungkinan-kemungkinan kunci yang dipakai dan masih banyak cara lain yang digunakan untuk mendapatkan pesan rahasia (The Security Divison of EMC, 2009).

Kriptografi adalah suatu ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi telah ada dan digunakan sejak berabad-abad yang lalu dikenal dengan istilah kriptografi klasik, yang bekerja pada mode karakter alfabet. Berbagai macam teknik keamanan telah dikembangkan untuk melindungi dan menjaga kerahasiaan pesan agar terhindar dari orang yang tidak berhak. Keamanan dan kerahasiaan merupakan aspek penting yang dibutuhkan dalam proses pertukaran pesan/informasi melalui jaringan/*internet*, karena turut berkembang pula kejahatan teknologi dengan berbagai teknik interupsi, penyadapan, modifikasi, maupun fabrikasi. Tanpa adanya jaminan keamanan, orang lain dapat dengan mudah mendapatkan pesan/informasi yang dikirimkan melalui jaringan/*internet*.

Dalam dunia kriptografi, pesan yang akan dirahasiakan disebut *plaintext*. Pesan yang sudah diacak disebut *ciphertext*. Proses untuk mengkonversi *plaintext* menjadi *ciphertext* disebut enkripsi. Proses untuk mengembalikan *plaintext* dari *ciphertext* disebut dekripsi. Algoritma kriptografi (*ciphers*) adalah fungsi-fungsi matematika yang digunakan untuk melakukan enkripsi dan dekripsi. Dalam kriptografi diperlukan kunci yaitu kode untuk melakukan enkripsi dan dekripsi.

Penelitian ini menggunakan dua algoritma berbeda yaitu algoritma *rail fence* dan ElGamal penggabungan algoritma simetri dan asimetri yang juga disebut dengan *hybrid cryptosystem.* Berdasarkan uraian tersebut penulis mengambil penelitian dengan judul "Kriptografi *Hybrid* Algoritma Rail Fence dan Algoritma ElGamal dalam Pengamanan Data Berbasis Teks" dengan harapan bisa mengembangkan aplikasi kriptografi berbasis teks dengan keamanan ganda pada waktu tertentu.

1.2 Rumusan Masalah

Sesuai dengan latar belakang di atas yang terkait dengan rumusan masalah kriptografi hybrid algoritma *rail fence* dan algoritma ElGamal dalam pengamanan data berbasis teks adalah sebagai berikut :

1. Bagaimana menerapkan pasangan kunci menggunakan kombinasi algoritma *rail fence* dan algoritma ElGamal?
2. Bagaimana menerapkan enkripsi dan dekripsi data teks dengan kombinasi algoritma *rail fence* dan algoritma ElGamal?
3. Bagaimana unjukkerja sistem dalam mengetahui waktu yang digunakan pada proses pengamanan data teks?

1.3 Batasan Masalah

Berdasarkan permasalahan pengamanan data berbasis teks menggunakan kriptografi *hybrid* algoritma *rail fence* dan algoritma ElGamal maka peneliti hanya meneliti enkripsi dan deskripsi dengan mempertimbangkan gabungan kerumitan perhitungan algoritma ElGamal dan algoritma *rail fence* berdasarkan waktu.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk membuat aplikasi kriptografi keamanan *file* teks yang menggunakan metode kombinasi algoritma *rail fence* dan algoritma ElGamal.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah dapat digunakan sebagai langkah awal untuk membangun sistem kriptografi dengan menggunakan metode *hybrid cryptosystem*. Program aplikasi yang juga dapat dijadikan bahan untuk penelitian lebih lanjut dibidang yang berkaitan.

1. Manfaat dari penelitian ini adalah untuk mempermudah pengguna mengamankan data berbasis data teks.
2. Perangkat lunak yang dirancang dapat digunakan sebagai *tools* kriptografi pengamanan data teks dengan kunci privat dengan metode kombinasi algoritma *rail fence* dan algoritma ElGamal.