

ABSTRAK

STEGO-KRIPTO BERBASIS *NOISE* DENGAN MENGUNAKAN KURVA ELIPTIK

Menyadap pesan dan mengubah isi pesan menjadi salah satu cara curang yang dilakukan para pebisnis untuk menjatuhkan pesaingnya. Teknik *hacking* yang semakin berkembang menjadikan sebuah pesan tidak lagi terjaga kerahasiaannya. Selain itu, pencurian data yang bersifat pribadi juga menjadi salah satu masalah yang harus diatasi. Teknik kriptografi dan steganografi menjadi salah satu solusi untuk mengatasi masalah tersebut.

Tugas akhir ini membahas tentang teknik kriptografi yang digunakan untuk meningkatkan keamanan suatu pesan. Teknik yang digunakan adalah kriptografi-steganografi yang berbasis *noise*. Teknik ini merupakan gabungan dari teknik kriptografi dan steganografi, dimana sebuah *noise* akan dienkrip dan disisipkan di antara deretan pesan yang dikirim. Algoritma yang digunakan adalah algoritma El-Gamal kurva eliptik (*Elliptic Curve Cryptography*) yang kemudian dimodifikasi (*Modified El-Gamal*). Algoritma ini juga yang akan digunakan pada proses dekripsi di penerima, dimana penerima akan mengidentifikasi pesan yang bernilai acak dan besar (*noise*), yang merupakan titik di luar kurva dari persamaan kurva yang telah ditentukan sebagai persamaan proses enkripsi dan dekripsi.

Dengan teknik tersebut, sebuah *noise* akan terlihat seperti pesan terenkripsi biasa. Sehingga, hanya penerima yang berhak yang mengetahuinya. Maka dari itu, semakin banyak *noise* yang disisipkan, maka waktu dekripsi penerima berhak akan semakin cepat dan kompleksitasnya juga menurun. Sedangkan penerima tidak berhak memerlukan waktu yang lebih lama saat mendekripsi pesan dan juga kompleksitasnya meningkat. Dengan demikian, tugas akhir ini menjawab isu tersebut, dimana tingkat keamanan sebuah pesan akan meningkat dan terjaga kerahasiannya.

Kata kunci : *Kriptografi-Steganografi, Elliptic Curve Cryptography, Modified El Gamal, Noise*