Abstrak

Pertukaran informasi melalui jaringan publik, merupakan suatu kebutuhan yang mutlak pada masa teknologi informasi ini. Permasalahan muncul karena informasi ini dilewatkan pada jaringan publik, memungkinkan pihak tertentu yang tidak mempunyai hak terhadap informasi tersebut menggunakan informasi tersebut, salah satu teknik yang digunakan untuk mengamankan informasi tersebut adalah dengan menggunakan teknik kriptografi.

Berdasarkan kuncinya kriptografi dikelompokkan menjadi *private key cryptography* dan *public key cryptography,* pada *private key cryptography* entitas yang akan berkomunikasi menggunakan kunci yang sama dalam mengenkripsi dan mendekripsi, sedangkan pada *public key cryptography* digunakan kunci berbeda dalam mengenkripsi dan mendekripsi. Pada *public key cryptography* terdapat tiga pendekatan dalam keamanannya, yaitu *Integer Factorization Problem*, *Discrete Logarithm Problem* dan *Elliptic Curve Discrete Logarithm Problem*.

Pada tugas akhir ini, diimplementasikan pendekatan *Elliptic Curve* pada algoritama ElGamal dalam proses penyandian. Pada implementasi tersebut, dianalisis performansi waktu, penggunaan memori dan kecepatan pada proses penyandian data pada kondisi data uji yang berbeda dan tipe kurva yang berbeda. Hasil pengujian menunjukkan bahwa waku proses semakin menigkat dengan kenaikan ukuran data uji dan tipe kurva yang digunakan, penggunaan memori pada proses semakin berkurang dengan kenaikan tipe kurva.

Kata kunci: Kriptografi, *private key cryptography, public key cryptography, Elliptic Curve*, *El Gamal*.