

Abstrak

Internet telah menjadi bagian dari kehidupan sehari-hari sebagai salah satu wahana komunikasi dalam bisnis maupun untuk pribadi. Namun ternyata internet tidak terlalu aman karena merupakan media komunikasi umum yang dapat digunakan oleh siapapun sehingga sangat rawan terhadap penyadapan informasi oleh pihak-pihak yang tidak berhak mengetahui informasi tersebut. Salah satu cara yang digunakan untuk mendapatkan jaminan keamanan informasi rahasia ini adalah dengan menyandikan isi informasi menjadi suatu kode-kode yang tidak dimengerti sehingga apabila disadap maka akan kesulitan untuk mengetahui isi informasi yang sebenarnya.

Pada tugas akhir ini dilakukan analisa terhadap performa algoritma kriptografi ElGamal yang diimplementasikan di sistem operasi yang berbeda, yaitu Windows XP dan Ubuntu dengan melihat waktu yang dibutuhkan untuk proses enkripsi dan proses dekripsi, serta ukuran file setelah proses enkripsi.

Pada uji coba yang dilakukan ternyata waktu yang dibutuhkan untuk proses pembentukan kunci, proses enkripsi, dan proses dekripsi lebih cepat jika diimplementasikan di Windows XP dibandingkan diimplementasikan di Ubuntu.

Kata kunci: kriptografi, ElGamal, enkripsi, dekripsi, Windows Xp, Ubuntu.