INTI SARI

Teknologi informasi dan komunikasi saat ini berkembang sangat pesat, khususnya internet. Hal ini berdampak pada meningkatnya penggunaan internet sebagai media komunikasi, transfer data hingga transaksi kuangan. Namun disamping itu terdapat kekurangan dan cenderung tidak aman (unreliable). Oleh karena itu, keamanan menjadi faktor utama yang harus dipenuhi. Aspek keamanan data dapat diatasi dengan menggunakan kriptografi yang tujuannya memberikan keamanan pada sebuah data. RSA dan El Gamal merupakan algoritma kriptografi kunci public yang dapat memberikan keamanan terhadap data, yaitu dari aspek kerahasiaan, dan autentikasi. Untuk merahasiakan data adalah dengan mengubahnya menjadi ciphertext menggunakan proses enkripsi, sedangkan untuk keperluan otentikasi data adalah menggunakan tanda tangan digital.

Dalam penelitian ini akan membahas algoritma RSA dan El Gamal dalam menangani proses pembangkitan kunci, enkripsi dan tanda tangan digital. Implementasi perangkat lunak dilakukan menggunakan bahasa pemrograman Java. Selanjutnya dilakukan beberapa pengujian untuk mengetahui tingkat performansi masing-masing algoritma dalam menangani proses enkripsi dan tanda tangan digital. Perbandingan kinerja algoritma RSA dan Elgamal ditampilkan dalam bentuk grafik.

Kesimpulan yang diperoleh adalah, dari segi kecepatan proses, El Gamal mampu menangani proses enkripsi dan tanda tangan digital lebih cepat dibanding RSA, sedangkan pada proses pembangkitan kunci, RSA lebih cepat. Berdasarkan percobaan proses enkripsi, baik RSA maupun El Gamal menghasilkan cipher berukuran lebih besar daripada ukuran file asli sebelum enkripsi. Selain itu, ukuran kunci berbanding lurus dengan kecepatan proses. Semakin besar ukuran kunci yang digunakan, maka proses enkripsi maupun tanda tangan digital akan semakin lama.

Kata kunci: Kriptografi, RSA, El Gamal, Tanda tangan digital, Enkripsi.