ABSTRAK

Kemampuan Internet untuk mengirim dan menerima dokumen bisa dimanfaatkan untuk berbagai hal, misalnya untuk transaksi jual beli dan *e-banking*. Untuk keperluan seperti transaksi jual beli, kerahasiaan data yang dikirim haruslah terjamin keamanannya. Untuk menjamin kerahasiaan data, salah satu cara yang dapat digunakan adalah dengan melakukan enkripsi atau pengkodean data sehingga hanya user yang berhak saja yang dapat melihat isi data.

Teknik enkripsi atau pengkodean data dapat dikembangkan untuk mendukung penerapan tanda tangan digital. Dengan teknik tanda tangan digital maka suatu data yang telah dikirim melalui internet bisa dipastikan apakah data tersebut telah diubah isinya atau belum serta siapa pengirimnya.

Tanda tangan digital memiliki beberapa mekanisme pembuatan, serta ada standar yang disebut *Digital Signature Standard* (DSS). Algoritma yang dihasilkan sesuai standar tersebut dikenal dengan *Digital Signature Algorithm* (DSA). Inti dari mekanisme pembuatan tanda tangan digital adalah penerapan teknik kriptografi dan fungsi hashing.

Tugas akhir ini bertujuan untuk membuat komponen tanda tangan digital dengan kriptografi kunci publik RSA dan DSA serta fungsi hash MD5, dimana komponen yang dihasilkan nantinya dapat digunakan dalam pengembangan aplikasi yang menggunakan fasilitas tanda tangan digital.

Uji coba dilakukan melalui tahap verifikasi yang bertujuan untuk mengetahui apakah komponen dapat menandatangani dokumen teks sesuai dengan ruang lingkup yang sudah ditentukan. Dari uji coba ini dapat diambil kesimpulan bahwa setiap fasilitas komponen telah berjalan dengan benar.