ABSTRAK

Perkembangan teknologi informasi yang pesat dan dukungan komunikasi yang semakin baik menyebabkan pertukaran informasi melalui media Internet semakin berkembang pesat, pertukaran informasi digital ini pada penerapannya dibutuhkan suatu cara untuk menjaga keamanan, integritas, serta keaslian dokumen digital. Pada informasi digital, seperti e-mail, penerapan autentikasi dokumen tidak semudah pada bentuk kerasnya seperti surat, sifat dokumen digital yang tersimpan hanya berdasar angka biner '0' dan '1' menyebabkan kesulitan untuk memberi tanda khusus pada dokumen tersebut tanpa dapat dipalsu atau digunakan kembali.

Timbul dan berkembangnya teknik kriptografi memungkinkan pengamanan, pengecekan keutuhan, dan autentikasi data digital, sehingga pemberian tanda khusus pada dokumen digital dapat diwujudkan yaitu dengan tanda tangan elektronik.

Pada tugas akhir ini akan dibahas pembuatan suatu sistem yang menjamin autentikasi pesan dan autentikasi pengirim pesan pada sebuah e-mail dengan tanda tangan elektronik yang dapat diterapkan langsung pada Internet, dimana di dalamnya akan terdapat juga penerapan pembuatan web manajemen kunci yang mempunyai kemampuan untuk membuat pasangan kunci, mengirimkannya pada pengguna secara aman, dan pendistribusian kunci publiknya. Sistem yang dibuat ini menggunakan mekanisme tanda tangan digital RSA dengan appendix, dengan penggunaan fungsi hash MD5, dan kemampuan mengirim dan menerima e-mail berdasar protokol POP3 dan SMTP.

Pada akhir tugas akhir ini telah dibentuk sistem yang selain menjamin ke autetikasi pesan dengan autentikasi penanda tangan beserta fungsi tambahan teknik kriptografi RSA untuk menjamin keamanan e-mail dan file sehingga hanya dapat dilihat oleh orang yang bersangkutan. Sistem ini bisa dikembangkan lagi untuk memenuhi kebutuhan terhadap keamanan data pada jaringan global Internet.