ABSTRAK

Kata kunci:

algoritma AES, algoritma RSA, non-repudiation, confidentiality, tanda tangan digital, E-mail.

Penyadapan informasi dapat terjadi pada saat melakukan proses pertukaran informasi melalui e-mail. Proses penyandian diperlukan untuk mencegah terjadinya penyadapan informasi, karena proses tersebut dapat meningkatkan keamanan informasi. Kriptografi menyediakan beberapa layanan yang mendukung untuk meningkatkan keamanan informasi, yaitu: otentikasi (*authentication*), mencegah penyangkalan (*non-repudiation*), dan menjaga kerahasiaan (*confidentiality*). Penelitian ini difokuskan untuk menjaga kerahasiaan informasi dengan proses penyandian dan mencegah penyangkalan oleh pengirim informasi menggunakan proses tanda tangan digital.

Pada penelitian ini algoritma AES digunakan untuk menyandikan (mengenkripsi) file lampiran yang dikirim melalui e-mail. Algoritma AES memiliki tingkat keamanan yang tinggi karena memiliki 3 tipe kunci yang berbeda (AES-128, AES-192 dan AES-256) dan setiap putaran proses akan menghasilkan kunci (*subkey*) yang berbeda. Sedangkan untuk memudahkan proses distribusi kunci yang digunakan pada algoritma AES dan tanda tangan digital maka digunakan algoritma RSA. Kelebihan dari algoritma RSA adalah faktor keamanannya karena didasarkan pada kesulitan untuk memfaktorkan bilangan besar modulus n menjadi faktor-faktor primanya.

Penelitian ini bertujuan merancang perangkat lunak yaitu CARA (*Cryptosystem with AES and RSA Algorithm*) yang dapat digunakan untuk menjaga kerahasiaan informasi yang dikirimkan melalui e-mail sekaligus dapat mencegah penyangkalan oleh pengirimnya. Hasil penelitian ini akan dapat memberi rasa aman bagi pengirim dan penerima informasi.