Abstrak

MMS (Multimedia Messaging Service) adalah layanan komunikasi *messaging* yang telah ditetapkan standarnya oleh WAP dan 3GPP. Dalam MMS keamanan seakan menjadi suatu yang sangat penting seiring dengan perkembangan dalam hal teknologi ini. User yang ingin berkomunikasi bukan hanya mencari sekedar *privacy* dalam hal berkomunikasi, tetapi keaslian pesan juga menjadi suatu hal yang sama pentingnya dalam hal berkomunikasi. Karena adanya kebutuhan ini maka harus disediakan aplikasi yang memerlukan adanya suatu enkripsi pesan dan tanda tangan digital.

Salah satu solusi untuk menjaga keaslian data, integritas data, otentikasi dan nir penyangkalan adalah dengan menggabungkan algoritma enkripsi dan tanda tangan digital. Algoritma enkripsi yang digunakan adalah algoritma Rijndael, sedangkan algoritma tanda tangan digital-nya menggunakan ECDSA. Hasil enkripsi pesan yang dihasilkan oleh Algoritma Rijndael akan digabungkan dengan tanda tangan yang dihasilkan oleh algoritma tanda tangan ECDSA dan akan dikirimkan melalui jalur komunikasi. Penggabungan algoritma ini menghasilkan kerahasiaan (*confidentially),* integritas data (data integrity), otentikasi (*authentication*), nir penyangkalan (*non repudiation*).

Algoritma ECDSA dan Rijndael dapat digunakan dalam MMS yang memiliki hardware dengan resource terbatas seperti handphone. Dari percobaan dapat ditarik kesimpulan bahwa performansi proses signing dan verifying dengan menggunakan penggabungan antara algoritma tanda tangan ECDSA dan algoritma enkripsi Rijndael dipengaruhi oleh panjang kunci dari algoritma tersebut dan fungsi hash yang digunakan.

Kata kunci : MMS, Rijndael, ECDSA, fungsi hash, message digest, digital signature