Abstrak

SMS (*Short Messaging Service*) merupakan layanan pengiriman pesan dalam lingkungan komunikasi bergerak. Dalam melakukan pengiriman pesan melalui SMS, keamanan pesan merupakan hal yang sangat penting. Pesan yang diamankan bukan hanya pada aspek kerahasiaan, tetapi juga bagaimana pesan tersebut pada saat dikirimkan tidak diubah oleh seseorang sehingga pesan tersebut benar-benar asli. Untuk mengatasi masalah tersebut diperlukan tandatangan digital atau *digital signature.*

Salah satu cara untuk melakukan *digital signature* pada pesan yaitu dengan menggunakan fungsi *hash*. Pembentukan tanda-tangan digital dilakukan dengan menghitung *message digest* dari pesan dengan menggunakan fungsi *hash* satu arah. Kemudian mengenkripsi *message digest* dengan algoritma kriptografi kunci publik. Tanda-tangan digital yang sudah terbentuk diletakkan ke pesan tersebut, lalu keduanya dikirimkan malalui saluran komunikasi. Salah satu algoritma kriptografi kunci-publik yang sering digunakan untuk pembentukan tanda-tangan digital adalah algoritma *ECDSA* (Elliptic Curve Digital Signature Algorithm). Sedangkan fungsi hash satu-arah yang sering digunakan adalah SHA(*Secure Hash Algorithm*).

ECDSA sangat cocok untuk dimplementasikan pada SMS yang biasanya melibatkan peralatan mobile device atau hand phone yang memiliki resource yang terbatas. Hal ini dikarenakan ECDSA memiliki kunci yang relatif lebih kecil dibandingkan dengan kriptopgrafi kunci publik yang lain.

Dari percobaan yang telah dilakukan dapat ditarik kesimpulan bahwa performansi dari ECDSA pada kasus keamanan SMS ini hanya dipengaruhi oleh panjang kunci yang digunakan, Sedangkan algoritma SHA yang digunakan tidak membarikan pengaruh.

Kata Kunci : SMS, ECDSA, fungsi *hash*, *message digest*, *digital signature*