Abstrak

SMS (*Short Messaging Service*) merupakan layanan pengiriman pesan dalam lingkungan komunikasi bergerak. Selain efektif, SMS tidak memerlukan biaya yang mahal sehingga banyak orang yang menggunakan layanan tersebut. 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 *DSA* (Digital Signature Algorithm). Sedangkan fungsi hash satu-arah yang sering digunakan adalah SHA(*Secure Hash Algorithm*).

DSA sangat cocok untuk dimplementasikan pada SMS yang biasanya melibatkan peralatan mobile device atau hand phone yang memiliki resource yang terbatas. Dari percobaan yang telah dilakukan dapat ditarik kesimpulan bahwa performansi dari DSA pada kasus keamanan SMS ini dipengaruhi oleh panjang kunci yang digunakan dan juga algoritma SHA .

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