Abstrak

MMS (*Multimedia Messaging Service*) merupakan layanan pengiriman pesan dalam lingkungan komunikasi bergerak dengan standar yang ditetapkan oleh Forum WAP dan 3GPP. Dalam melakukan pengiriman pesan melalui MMS, keamanan pesan merupakan hal yang sangat penting. Pesan yang diamankan bukan hanya pada saat pesan tersebut akan dikirimkan, tetapi juga bagaimana pesan tersebut pada saat dikirimkan tidak diubah oleh seseorang sehingga pesan tersebut benar-benar asli. Untuk mengatasi masalah tersebut diperlukan tanda-tangan 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[8]. Salah satu algoritma kriptografi kunci-publik yang sering digunakan untuk pembentukan tanda-tangan digital adalah algoritma RSA. Sedangkan fungsi hash satu-arah yang sering digunakan adalah SHA(*Secure Hash Algorithm*).

Dari hasil percobaan, algoritma RSA merupakan salah satu algoritma yang tepat untuk digunakan dalam pembuatan *digital signature* pada pengiriman pesan MMS. Karena penambahan ukuran *digital signature* pada pesan MMS tergolong kecil(berkisar 64-140 byte), sehingga tidak mempengaruhi biaya pengiriman MMS.

Kata kunci : MMS, RSA, fungsi *hash*, message digest, *digital signature*