Abstrak

Short Message Service (SMS) adalah salah satu layanan komunikasi bergerak yang sangat populer sekarang ini. Selain efektif, biaya yang murah menjadi pertimbangan untuk menggunakan layanan ini. Dalam melakukan pengiriman pesan melalui SMS, keamanan merupakan hal yang sangat penting. Keamanan di sini meliputi keamanan dari pesan maupun pihak-pihak yang berkomunikasi. Pihak-pihak yang berkomunikasi tentunya menginginkan agar isi pesan tetap terjaga keasliannya dan identifikasi pengirim dan penerima pun tetap terjaga kebenarannya. Untuk mengatasi masalah tersebut diperlukan adanya mekanisme otentikasi dan enkripsi pesan.

Message Authentication Code (MAC) merupakan salah satu cara untuk memeriksa integritas dan otentikasi dari suatu pesan berdasarkan kunci rahasia. Sedangkan untuk menangani kerahasiaan isi pesan digunakan algoritma enkripsi Rijndael. Fungsi *hash*satu arah yang digunakan dalam proses pembangkitan nilai *MAC*-nya adalah *Secure Hash Algorithm (SHA).*

Dalam tugas akhir ini penulis akan membangun suatu aplikasi yang mengimplementasikan metode *MAC* dan algoritma kriptografi Rijndael untuk otentikasi dan enkripsi pesan. Aplikasi dianalisis berdasarkan waktu respon untuk proses otentikasi, enkripsi, dan verifikasi.

Kata kunci: SMS, MAC, Rinjdael, fungsi *hash*, kunci rahasia.