

ABSTRAK

Seiring dengan berkembangnya teknologi, SMS (*Short Message Service*) merupakan sarana telekomunikasi yang paling sering digunakan disemua kalangan masyarakat baik masyarakat menengah keatas maupun masyarakat menengah kebawah. Terkadang pesan yang dikirimkan melalui SMS memiliki sifat rahasia padahal pesan melalui SMS merupakan pesan plaintext sehingga orang yang tidak berhak membacanya dapat dengan mudah mengambil atau membacanya.

Oleh karena itu diperlukan sebuah enkripsi agar pesan yang sifatnya rahasia tadi dapat terjaga kerahasiaannya. Dalam kasus ini penulis menerapkan Algoritma Cramer Shoup sebagai Algoritma yang akan digunakan untuk enkripsi pesan. Dimana Algoritma Cramer Shoup merupakan Algoritma Asimetrik yang kunci untuk mengenkripsi (kunci publik) dan mendekripsikan (kunci privat) pesannya berbeda. Sehingga pengirim dan penerima tidak perlu takut dalam melakukan pertukaran kunci.

Pada tugas akhir ini, penulis mengimplementasikan Algoritma Cramer Shoup untuk membuat aplikasi enkripsi SMS berbasis J2ME. Aplikasi enkripsi SMS ini dianalisis dari kecepatan proses dalam pembangkitan kunci, enkripsi pesan, dan dekripsi pesan. Selain itu penggunaan memori untuk pembangkitan kunci, enkripsi pesan, dan dekripsi pesan juga diukur. Lalu untuk analisis keamanannya menggunakan metode Avalanche Effect.

Dari hasil percobaan, Algoritma Cramer Shoup merupakan salah satu algoritma yang tepat untuk enkripsi pesan. Tetapi mengingat Algoritma Cramer Shoup merupakan algoritma asimetrik dimana komputasinya membutuhkan sumber daya yang besar maka perangkat seluler yang digunakan untuk enkripsi berpengaruh pada kecepatan proses dan maksimum jumlah bit yang dapat digunakan.

Kata kunci: SMS, enkripsi, Cramer Shoup, asimetrik, J2ME