

Abstrak

Saat ini, *Multimedia Messaging Service* (MMS) sudah sering digunakan untuk berkomunikasi lewat ponsel. Pesan yang dikirimkan pun beragam, mulai dari teks, audio, image, hingga video. Pesan yang dikirimkan ada pula yang bersifat rahasia, padahal pesan tersebut bisa saja dibaca oleh orang yang tidak berhak.

Oleh karena itu, diperlukan adanya enkripsi agar pesan MMS dapat terjaga kerahasiaannya. Salah satu algoritma enkripsi yang terkenal dengan keandalannya adalah *International Data Encryption Algorithm* (IDEA). Mode operasi enkripsi blok cipher yang digunakan adalah *Cipher Block Chaining* (CBC). Sedangkan untuk mengatasi keamanan dari sisi kunci, kunci di-*hash*-kan dengan fungsi *hash* MD5.

Pada tugas akhir ini, penulis membuat suatu aplikasi enkripsi MMS pada ponsel yang mendukung Java 2.0. Aplikasi enkripsi ini dianalisis dari waktu proses enkripsi dan dekripsi, ukuran pesan sebelum dan setelah enkripsi, memori yang terpakai pada proses enkripsi dan dekripsi, dan besar persentase *avalanche effect*.

Dari hasil percobaan, algoritma IDEA merupakan algoritma yang relatif kurang tepat untuk digunakan dalam proses enkripsi pada ponsel. Walaupun dilihat dari besar persentase *avalanche effect* yang dihasilkan memenuhi syarat sebagai algoritma yang baik, tetapi jika dilihat dari waktu yang digunakan untuk melakukan proses enkripsi dan dekripsi untuk pesan yang berukuran besar, seperti audio dan image, membutuhkan waktu yang lama.

Kata kunci: MMS, enkripsi, IDEA, CBC, MD5, java