

## ABSTRAK

Kemajuan di bidang teknologi informasi telah memungkinkan berbagai pihak (diantaranya industri musik) untuk melakukan interaksi dengan konsumen melalui jaringan komputer. Kegiatan-kegiatan tersebut akan menimbulkan resiko bilamana informasi yang sensitif dan berharga diakses oleh pihak-pihak yang tidak berkepentingan, sehingga dibutuhkan sistem keamanan data yang tepat. Salah satu cara untuk mengatasi masalah tersebut adalah dengan metode enkripsi file.

Dari segi konsumen / pengguna, tentu *response time* yang cepat merupakan suatu parameter yang sangat penting dalam pengaksesan suatu file MP3. Pada tugas akhir ini akan dibahas teknik partisi block cipher yang diharapkan dapat meningkatkan performansi dekripsi yang dilakukan secara “*online*”. Metodologi yang digunakan dalam penelitian kali ini adalah metodologi studi literatur, perancangan dan implementasi, pengujian dan analisa, pengambilan kesimpulan .

Hasil dari tugas akhir ini adalah implementasi enkripsi dan dekripsi menggunakan algoritma twofish untuk file MP3 dengan teknik partisi block cipher. Parameter yang dianalisa yaitu ukuran plaintext vs ukuran ciphertext, waktu dekripsi, waktu dekripsi antar partisi vs non partisi, jumlah partisi optimal pada ukuran file tertentu.

Kata kunci :

*Enkripsi, dekripsi, Algoritma twofish, file MP3.*