

INTISARI

Aplikasi kriptografi *CBC* dan *checksum* MD5 mengimplementasikan algoritma kriptografi *Cipher Block Chaining* dan algoritma *Message Digest 5* untuk meng-enkripsi data teks yang tersimpan dalam berkas. Algoritma kriptografi *CBC* merupakan salah satu metode kriptografi *modern* menggunakan aliran blok dan tipe kunci simetris yang hasilnya merupakan hasil enkripsi dari blok sebelumnya. Aplikasi ini dibangun menggunakan bahasa pemrograman Java 2 SE .

Algoritma kriptografi MD5 digunakan untuk fungsi *checksum* yakni fungsi untuk menjaga keamanan seperti otentikasi dan integritas berkas. Cipertek yang dihasilkan merupakan gabungan dari kode *hash* algoritma MD5 dan enkripsi plantek+kunci dengan Algoritma *CBC*.

Berdasarkan hasil pengujian aplikasi atau sistem yang dibangun dapat berjalan dengan baik mengaplikasikan algoritma kriptografi *CBC* dan algoritma kriptografi MD5. Berkas berisi data teks dapat dibuka dan terbaca dengan baik, proses enkripsi dan dekripsi pada berkas tersebut juga telah dilakukan berbagai percobaan tingkat kesalahan untuk menguji validitas aplikasi ini.

Kata kunci : *CBC*, *JAVA*, Kriptografi, MD5