BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan data telah menjadi aspek yang sangat penting dari suatu sistem informasi. Sebuah sistem informasi umumnya hanya ditujukan bagi segolongan tertentu. Oleh karena itu sangat penting untuk mencegahnya jatuh ketangan pihak – pihak lain yang tidak berkepentingan. Untuk melaksanakan tujuan tersebutlah dirancang suatu sistem keamanan yang berfungsi melindungi data dari suatu berkas maupun data dari suatu sistem informasi .

Upaya yang dapat dilakukan untuk mengamankan hasil tersebut diatas yaitu dengan kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga keamanan data ketika data dikirim dari suatu tempat ketempat yang lain dengan cara mengenkripsi isi dari berkas, sehingga pihak yang tidak terotentifikasi untuk merubah maupun menambah data akan sulit menerjemahkannya. Metode yang bisa digunakan, yaitu metode kriptografi MD5 (*Message Diggest 5*) dikombinasikan dengan metode CBC (*Cipher Block Chaining*) dengan pengacakan data menjadi *ciphertext* yang mengutamakan keamanan data itu sendiri.

1.2 Rumusan Masalah

Melihat latar belakang permasalahan yang telah dianalisa di atas maka dapat dirumuskan yaitu, bagaimana mengimplementasikan algoritma kriptografi MD5 dan CBC pada berkas menggunakan bahasa pemrograman Java untuk membantu meningkatkan keamanan keberadaan data-data yang telah disimpan.

1.3 Ruang Lingkup

Karena keterbatasan waktu dan pengetahuan penulis, maka ruang lingkup permasalahan karya tulis ini antara lain :

1. Algoritma kriptografi MD5 digunakan untuk fungsi *checksum* yakni fungsi untuk menjaga keamanan seperti otentikasi dan integritas berkas.
2. Cipertek yang dihasilkan merupakan gabungan dari kode *hash* algoritma MD5 dan enkripsi plantek+kunci dengan Algoritma CBC.
3. Berkas yang akan di-enkripsi (plantek) terbatas hanya pada berkas berisi teks sesuai dengan standar *charset* UTF-8(ANSII).
4. Berkas yang sudah ter-enkripsi (cipertek) hanya dapat disimpan dalam ekstensi .cbc saja.
5. Panjang kunci dibatasi hanya sampai 9 karakter saja.

1.4 Tujuan Penelitian

Tujuan penyusunan karya tulis tugas akhir (skripsi) ini adalah untuk merancang suatu aplikasi sederhana yang dapat mengimplementasikan algoritma kriptografi CBC dan MD5 untuk mengenkripsi data teks yang tersimpan dalam berkas.