

BAB I

PENDAHULUAN

Pada bab ini akan dijelaskan mengenai latar belakang, perumusan masalah, tujuan, pembatasan masalah, serta sistematika penulisan laporan tugas akhir.

1.1 Latar Belakang

Pada saat ini informasi komputer dan interkoneksinya melalui jaringan sangat meningkat, tentu saja dalam hal ini sangat dibutuhkan keamanan data yang handal agar supaya terhindar dari penyadapan yang tidak diinginkan. Dalam hal ini keamanan data merupakan permasalahan yang sangat penting. Sistem enkripsi mempunyai kode-kode pengaman untuk mengacak data dan juga mempunyai kode-kode untuk mengembalikan data yang teracak ke data yang sebenarnya. Metoda yang dibahas pada tugas akhir ini adalah algoritma CAST.

1.2 Identifikasi Masalah

1. Bagaimana mengimplementasikan algoritma CAST ?
2. Bagaimana membuat program enkripsi dan dekripsi menggunakan algoritma CAST ?

1.3 Tujuan

Tugas akhir ini bertujuan untuk merancang program menggunakan algoritma CAST sebagai pengamanan file data.

1.4 Pembatasan Masalah

- Enkripsi yang digunakan hanya dengan menggunakan metoda CAST dengan panjang kunci maksimal 128 bit atau lebih dikenal dengan nama CAST-128.
- Enkripsi yang digunakan hanya untuk file yang berformat *txt* (berisi teks).

1.5 Spesifikasi Hardware

Program diuji dengan menggunakan CPU Athlon 1800 Mhz dengan memory sebesar 512 MB.

1.6 Spesifikasi Software

Program dibuat dengan menggunakan bahasa pemrograman Borland Delphi 6.

1.7 Sistematika Pembahasan

Materi pembahasan dalam laporan Tugas Akhir ini adalah

BAB I PENDAHULUAN

Bab ini menjelaskan mengenai latar belakang Tugas Akhir, tujuan Tugas Akhir, pembatasan masalah dan sistematika pembahasan.

BAB II TEORI PENUNJANG

Bab ini berisi berbagai macam landasan teori yang bersangkutan dengan enkripsi dan dekripsi algoritma CAST-128, yaitu antara lain : teori dasar kriptografi, algoritma simetrik dan asimetrik, mode enkripsi blok cipher, dan algoritma CAST-128.

BAB III PERANCANGAN DAN REALISASI

Bab ini berisi perancangan dan realisasi dari program enkripsi dan dekripsi algoritma CAST-128

BAB IV HASIL PENGAMATAN

Bab ini berisi tentang data hasil pengamatan dari proses enkripsi dan dekripsi algoritma CAST-128.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran yang mungkin berguna dalam penggunaan program enkripsi dan dekripsi menggunakan algoritma CAST-128.