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

Berkat perkembangan teknologi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi/data secara jarak jauh. Antar kota antar wilayah antar negara bahkan antar benua bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran data. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Begitu banyak pengguna seperti departemen pertahanan, suatu perusahaan atau bahkan individu-individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain atau kompetitornya atau negara lain. Oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi.

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal.

Camellia merupakan algoritma kriptografi *simetris blok cipher*. Dalam Camellia proses enkripsi dan dekripsi dilakukan pada blok data berukuran 128-bit dengan kunci yang dapat berukuran 128-bit, 192-bit, 256-bit. Algoritma Camellia dikembangkan oleh :

- Kazumaro Aoki (NTT - Nippon Telegraph and Telephone Corp.)
- Tetsuya Ichikawa (Mitsubishi electric Corp.)
- Masayuki Kanda (NTT – Nippon Telegraph and Telephone Corp.)
- Mitsuru Matsui (Mitsubishi electric Corp.)
- Shiho Moriai (NTT – Nippon Telegraph and Telephone Corp.)
- Junko Nakajima (Mitsubishi electric Corp.)
- Toshio Tokita (Mitsubishi electric Corp.)

1.2 Identifikasi Masalah

Bagaimana membuat program enkripsi dan dekripsi menggunakan algoritma Camellia ?

1.3 Tujuan

Merealisasikan suatu perangkat lunak berdasarkan teknik enkripsi dan dekripsi Camellia.

1.4 Pembatasan Masalah

1. Perangkat lunak Enkripsi Camellia diimplementasikan dalam bahasa pemrograman Borland Delphi.
2. Tidak membahas transmisi data.
3. Data masukan berupa teks atau file teks (*.txt).

1.5 Spesifikasi Hardware

Program diuji dengan menggunakan Pentium(R) 4 CPU 2.40 GH Mhz dengan memory sebesar 256 MB.

1.6 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 Camellia, yaitu antara lain : teori dasar kriptografi, algoritma simetrik dan asimetrik, mode enkripsi blok cipher, algoritma Camellia, dan komponen penyusun Camellia.

BAB III PERANCANGAN DAN REALISASI

Bab ini berisi perancangan dan realisasi dari program enkripsi dan dekripsi algoritma Camellia.

BAB IV HASIL PENGAMATAN

Bab ini berisi tentang data hasil pengamatan dari proses enkripsi dan dekripsi algoritma Camellia.

BAB V KESIMPULAN DAN SARAN

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