BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi di bidang komputer maupun informasi telah berkembang dengan cepat. Mengirimkan dan menerima data atau informasi walaupun terpisahkan oleh jarak yang berjauhan dari satu tempat ke tempat lainnya kini telah menjadi sangat praktis. Kegiatan-kegiatan tersebut tentu saja akan menimbulkan resiko bilamana data atau informasi yang berharga tersebut diketahui dan disalah gunakan oleh orang-orang yang tidak berhak atau berkepentingan.

Masalah keamanan dan kerahasiaan data merupakan isu yang sangat penting dan terus berkembang. Sistem-sistem vital seperti sistem pertahanan, sistem perbankan beserta sistem vital yang lainnya memerlukan tingkat keamanan yang sedemikian tinggi. Oleh karena itu diperlukan tindakan-tindakan untuk merealisasikan keamanan dan kerahasiaan data baik yang dikirim melalui jaringan ataupun disimpan dalam suatu media penyimpanan salah satunya dengan adalah dengan teknik enkripsi.

Teknik enkripsi adalah suatu proses yang dilakukan untuk mengamankan sebuah pesan menjadi sebuah pesan yang tersembunyi. Teknik enkripsi sendiri terdiri dari dua metoda, yaitu metoda kunci simetri dan metoda kunci asimetri. Terdapat berbagai jenis algoritma untuk setiap metoda tersebut. Salah satu algoritma kunci simetri adalah algoritma MISTY1.

1.2 Identifikasi Masalah

Bagaimana merancang dan membangun suatu perangkat lunak enkripsi dan dekripsi data dengan menggunakan algoritma kriptografi MISTY1 yang mampu menciptakan keamanan dan kerahasiaan data dalam suatu pengiriman data?

1.3 Tujuan

Merealisasikan suatu perangkat lunak enkripsi dan dekripsi data dengan menggunakan algoritma MISTY1 sebagai salah satu usaha untuk memperoleh keamanan dan kerahasiaan pada proses pengiriman data.

1.4 Pembatasan Masalah

- Metoda yang digunakan untuk melakukan enkripsi dan dekripsi adalah metoda kunci simetri dengan algoritma MISTY1.
- Data masukan untuk dienkripsi hanya berupa file teks (*.txt), file dokumen (*.doc), file *portable document format* (*.pdf), file gambar metafile (*.emf), dan file gambar bitmap (*.bmp).
- Bahasa pemrograman yang digunakan dalam perancangan program enkripsi dan dekripsi ini adalah Borland Delphi 7.

1.5 Sistematika Penulisan

Laporan tugas akhir ini disusun dengan sistematika sebagai berikut:

- Bab I : Membahas tentang latar belakang, identifikasi masalah, tujuan, pembatasan masalah, dan sistematika penulisan.
- Bab II : Membahas penjelasan mengenai kriptografi secara umum beserta algoritma-algoritma yang menunjang pembuatan tugas akhir.
- Bab III : Membahas tentang perancangan dan cara kerja program enkripsi dan dekripsi.
- Bab IV : Membahas hasil-hasil pengujian dan pengamatan dari program yang telah dirancang dan direalisasikan.
- Bab V : Merumuskan kesimpulan dan saran.