BAB I
PENDAHULUAN

1.1 Latar belakang

Jaringan data semakin berkembang sebagai akibat dari aplikasi bisnis yang menggunakan komputer. Mengirimkan dan menerima data atau informasi antar berbagai tempat yang terpisah oleh batas geografis yang jauh kini telah menjadi semakin praktis. Pengiriman data melibatkan minimal dua buah komputer yang terhubung oleh jaringan, baik itu jaringan lokal maupun jaringan yang lebih luas bukanlah menjadi kendala.

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dari suatu informasi. Dalam hal ini sangat terkait dengan betapa pentingnya informasi tersebut dikirim dan diterima oleh orang yang berkepentingan. Informasi akan tidak berguna apabila di tengah jalan informasi itu disadap atau dibajak oleh orang yang tidak berhak.

Untuk menjaga keamanan dan kerahasiaan data informasi, maka diperlukan enkripsi guna membuat data tidak dapat dibaca atau dimengerti oleh sembarang orang, kecuali oleh penerima yang berhak.

Enkripsi merupakan sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti atau dibaca. Enkripsi dapat diartikan sebagai kode. Sebuah sistem pengkodean menggunakan suatu kamus yang telah didefinisikan untuk mengganti kata atau informasi atau yang merupakan bagian dari informasi yang dikirim.

Teknik enkripsi dan dekripsi data terdiri dari dua metoda, yaitu metoda kunci simetri dan metoda kunci asimetri. Terdapat berbagai jenis algoritma dalam masing-masing metoda. Salah satu algoritma kunci simetri adalah algoritma NewDes . Untuk merealisasikan algoritma tersebut menjadi suatu program enkripsi-dekripsi diperlukan suatu bahasa pemrograman. Dalam perancangan kali ini, bahasa pemrograman yang digunakan adalah Visual Basic 6.0.

1.2 Identifikasi Masalah

Bagaimana merealisasikan suatu program yang dapat digunakan untuk melakukan enkripsi dan dekripsi terhadap suatu file dengan menggunakan algoritma Newdes?

1.3 Tujuan

Merealisasikan suatu program enkripsi dan dekripsi file dengan menggunakan algoritma Newdes untuk meningkatkan keamanan dan kerahasiaan data dalam pengirimannya.

1.4 Pembatasan Masalah

1. Program yang dirancang digunakan untuk melakukan enkripsi dan dekripsi terhadap file berukuran lebih kecil dari 1MB.
2. Bahasa pemrograman yang dipergunakan untuk merealisasikan program Enkripsi dan Dekripsi adalah Visual Basic 6.0.

1.5 Sistematika Penulisan

Laporan tugas akhir ini disusun dengan sistematika sebagai berikut:

1. Bab I : Membahas tentang latar belakang, identifikasi masalah, tujuan, pembatasan masalah, dan sistematika penulisan.
2. Bab II : Memberikan penjelasan mengenai kriptografi.
3. Bab III : Membahas cara kerja enkripsi dan dekripsi dengan algoritma Newdes.
4. Bab IV : Membahas hasil-hasil pengujian dari program yang telah dirancang.
5. Bab V : Merumuskan kesimpulan dan saran.