

BAB I

PENDAHULUAN

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

1.1 Latar Belakang

Kemajuan teknologi di bidang komputer dan telekomunikasi saat ini berkembang sangat pesat. Kemajuan teknologi ini semakin memberikan kemudahan lalu lintas pengiriman data dan informasi dari satu tempat ke tempat lainnya, meskipun tempat tersebut letaknya berjauhan. Data tersebut dapat dikirimkan melalui jaringan lokal maupun jaringan internet. Keamanan dan kerahasiaan informasi yang dikirimkan merupakan suatu faktor yang perlu diperhatikan.

Masalah keamanan merupakan suatu aspek penting dalam pengiriman data maupun informasi melalui jaringan. Hal ini disebabkan karena kemajuan di bidang jaringan komputer dengan konsep *open system*-nya sehingga memudahkan seseorang untuk masuk ke dalam jaringan tersebut. Hal tersebut dapat mengakibatkan proses pengiriman data menjadi tidak aman dan dapat saja dimanfaatkan oleh orang maupun pihak lain yang tidak bertanggung jawab, untuk mengambil data ataupun informasi ditengah jalan. Oleh karena itu, dibutuhkan suatu sistem keamanan yang dapat menjaga kerahasiaan suatu data maupun informasi, sehingga data tersebut dapat dikirimkan dengan aman. Salah satu cara untuk menjaga keamanan dan kerahasiaan suatu data maupun informasi adalah dengan teknik enkripsi dan dekripsi guna membuat pesan, data, maupun informasi agar tidak dapat di baca atau di mengerti oleh sembarang orang, kecuali untuk penerima yang berhak.

Teknik enkripsi dan dekripsi data terdiri dari dua metoda, yaitu metoda kunci publik dan metoda kunci simetri. Berbagai jenis algoritma terdapat dalam kedua metode tersebut. FEAL merupakan salah satu algoritma enkripsi dan dekripsi yang menggunakan metode kunci simetri. Untuk merealisasikan

algoritma tersebut menjadi suatu program enkripsi dan dekripsi diperlukan suatu bahasa pemrograman yang dalam perancangan menggunakan 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 FEAL?

1.3 Tujuan

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

1.4 Pembatasan Masalah

- Program yang dirancang digunakan untuk melakukan enkripsi dan dekripsi terhadap file teks(.txt), file dokumen(.doc), file adobe(.pdf), file gbr(.jpg).
- Metoda enkripsi dan dekripsi yang dipergunakan untuk proteksi data adalah metoda kunci simetri dengan algoritma FEAL
- 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:

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