

BAB I

PENDAHULUAN

1.1 Latar Belakang

Berbagai macam layanan komunikasi tersedia di Internet diantaranya adalah web, e-mail, milis, newsgroups, dan sebagainya. Dengan semakin maraknya orang memanfaatkan layanan komunikasi di Internet tersebut, maka permasalahan pun bermunculan apalagi ditambah dengan munculnya para peretas. Masalah yang pertama yaitu tentang kerahasiaan (*confidentiality*), yaitu bagaimana agar pesan atau file yang ingin dikirimkan tidak dapat dibaca oleh orang lain yang tidak berhak. Masalah yang kedua yaitu tentang keaslian pesan (*authentication*), yaitu pesan yang dikirimkan benar berasal dari seseorang dan bukan dari orang lain yang sedang menyamar.

Masalah keamanan data sangatlah penting jika ingin berkomunikasi melalui internet yang terpenting adalah bagaimana seseorang dapat mengamankan data tersebut agar tidak mudah dilihat atau dibajak oleh orang lain yang tidak berhak atau berwenang. Jika hal tersebut terjadi maka data-data yang dikirimkan rusak bahkan bisa saja hilang serta dapat menimbulkan kerugian bagi seseorang yang telah melakukan komunikasi melalui dunia maya tersebut.

Banyak orang menyiasati bagaimana cara mengamankan informasi yang dikomunikasikannya atau menyiasati bagaimana mendeteksi keaslian dari informasi yang diterimanya. Salah satunya dengan menggunakan penyandian pesan atau sering disebut kriptografi, dengan adanya kriptografi ini bertujuan agar seseorang dapat merasa aman jika berkomunikasi dengan orang lain.

Oleh karena itu dibuatlah sebuah aplikasi yang dapat menyandikan sebuah pesan agar pesan tersebut dapat dirahasiakan oleh pemiliknya. Aplikasi yang dibuat ini merupakan program enkripsi dan dekripsi pesan file dengan metode triple DES menggunakan Visual Basic 2005, hal ini dimaksudkan agar program tersebut dapat digunakan untuk merahasiakan sebuah pesan dari pihak yang tidak berwenang.

1.2 Tujuan Penelitian

Tujuan penulisan laporan proyek akhir ini adalah:

1. Merancang dan membuat aplikasi pengamanan data berbasis file dengan menggunakan algoritma Triple DES.

1.3 Perumusan Masalah

Rumusan masalah dari penulisan proyek akhir ini adalah sebagai berikut :

1. Bagaimana cara membuat sebuah aplikasi pengamanan data menggunakan Triple DES.
2. Bagaimana prinsip kerja perancangan programnya, logika algoritma Triple DES.
3. Bagaimana cara menganalisis hasil dari pengujian kedalam bahasa pemrograman.

1.4 Pembatasan Masalah

1. Membuat aplikasi pengamanan data berbasis file menggunakan Triple DES dan lebih difokuskan lagi pada proses enkripsi dan dekripsi file saja.
2. Program menggunakan visual basic 2005.
3. Diagram *Unified Modeling Language* (UML) yang digunakan hanya dua buah diagram yaitu diagram use case dan diagram konteks.

1.5 Metodologi dan Penelitian

Metode yang digunakan untuk penyusunan laporan tugas akhir ini adalah sebagai berikut:

1. Studi literatur, merupakan metode pengumpulan data dengan cara mengumpulkan bahan-bahan yang didapat dari buku-buku, modul ataupun sampel program yang berkaitan dengan tema penulisan.
2. Metode Rekayasa sistem pengamanan data berbasis enkripsi dan dekripsi ini menggunakan visual basic 6.0.

1.6 Sistematika Penulisan

Untuk mempermudah dalam penyusunan laporan tugas akhir ini terbagi menjadi 5 (lima) bab, yaitu:

BAB I : PENDAHULUAN

Bab ini membahas mengenai latar belakang, maksud dan tujuan, metode penulisan, batasan masalah, dan sistematika penulisan.

BAB II : TEORI DASAR TRIPLE DES

Bab ini berisi tentang materi yang mendukung laporan tugas akhir juga sebagai dasar acuan agar penelitian yang dilakukan tidak menyimpang dari latar belakang masalah yang ada dan sesuai dengan tujuan yang dicapai.

BAB III : ANALISA DAN PERANCANGAN

Bab ini berisi tentang hal-hal yang berhubungan dengan analisa program dan hal-hal yang berhubungan dengan Triple DES.

BAB IV : PERANCANGAN PENGAMANA DATA

BERBASIS FILE DENGAN MENGGUNAKAN TRIPLE DES

Bab ini berisi tentang perancangan terhadap program aplikasinya, diantaranya perancangan aplikasi Aplikasi pengamanan data berbasis file menggunakan triple DES.

BAB V : PENUTUP

Pada bab ini merupakan kesimpulan dan pembahasan pada penulisan proyek akhir ini beserta saran-saran untuk kesempurnaan program aplikasi ini secara keseluruhan.