

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan dan kerahasiaan data pada jaringan komputer saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan jaringan komputer saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Sistem-sistem vital, seperti sistem pertahanan, sistem perbankan, sistem bandara udara dan sistem-sistem yang lain setingkat itu, membutuhkan tingkat keamanan yang sedemikian tinggi. Hal ini lebih disebabkan karena kemajuan bidang jaringan komputer dengan konsep open system-nya sehingga siapapun, di manapun dan kapanpun, mempunyai kesempatan untuk mengakses kawasan-kawasan vital tersebut. Untuk menjaga keamanan dan kerahasiaan pesan, data, atau informasi dalam suatu jaringan komputer maka diperlukan beberapa enkripsi guna membuat pesan, data, atau informasi agar tidak dapat dibaca atau dimengerti oleh sembarang orang, kecuali oleh penerima yang berhak.

Pengamanan pesan, data, atau informasi tersebut selain bertujuan untuk meningkatkan keamanan, juga berfungsi untuk:

- a) Melindungi pesan, data, atau informasi agar tidak dapat dibaca oleh orang-orang yang tidak berhak.
- b) Mencegah agar orang-orang yang tidak berhak, menyisipkan atau menghapus pesan, data dan atau informasi.

Salah satu hal yang penting dalam komunikasi menggunakan komputer dan dalam jaringan komputer untuk menjamin kerahasiaan pesan, data, ataupun informasi adalah enkripsi. Keamanan data sangatlah penting karena semakin terbukanya informasi, setiap orang selali ingin mendapatkan informasi yang diinginkan baik dengan cara pasif maupun aktif.

Keamanan dan kerahasiaan data pada jaringan komputer saat ini menjadi isu yang sangat penting, serta selalu berkembang dengan cepat. Dengan adanya algoritma kriptografi yang meliputi proses enkripsi maka pesan , data maupun informasi dapat di kodekan sehingga orang yang tidak berkepentingan tidak dapat membaca informasi tersebut, selain orang yang bisa mengakses dengan kunci (*key*) untuk mendeskripsikannya.

Dengan adanya metode - metode algoritma kriptografi dan berdasarkan latar belakang yang sudah di jabarkan sebelumnya, maka dibuatlah *sistem manajemen file kriptografi untuk keamanan data* dalam sebuah jaringan komputer agar dapat melindungi dan menjaga otentikasi serta keaslian sebuah data.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah di paparkan diatas, dapat di rumuskan permasalahan sebagai berikut :

- a) Bagaimana membangun manajemen file kriptografi untuk keamanan data ?
- b) Bagaimana menjaga kendali akses serta keutuhan data ?
- c) Bagaimana membangun dan mengimplementasi kriptografi untuk keamanan data dalam jaringan dalam ruang lingkup data document file ?

1.3 Batasan Masalah

Dalam penyusunan penelitian ini akan ditentukan beberapa batasan masalah yaitu :

- a) System ini hanya untuk proses encrypt / decrypt data/document file.
- b) Manajemen file hanya dalam bentuk file encrypter.
- c) File yang bisa di amankan hanyalah file office, PDF.

1.4 Tujuan dan Manfaat

Maksud dari penelitian ini adalah memberikan sebuah solusi awal untuk keamanan data dengan menggunakan metode kriptografi yang dapat memfasilitasi para pengguna dan penyedia layanan informasi dalam jaringan computer. Serta manfaat dari system ini antara lain :

- a) Menjaga kendali akses dan kerahasiaan data dalam sebuah database jaringan
- b) Memberikan layanan *entity authentication* dimana layanan ini memberikan kepastian terhadap identitas yang terdapat dalam sebuah komunikasi data,
- c) Serta *data origin authentication* yaitu layanan yang memberikan kepastian sumber sebuah data.

1.5 Metologi dan Sistematika Penelitian

1.5.1 Metologi Penelitian

Langkah yang dilakukan dalam penelitian rancangan ini adalah :

- a. **Study Pustaka.** Identifikasi masalah dilakukan dengan cara studi pustaka pada media perpustakaan jurnal maupun internet bisa menjadi sumber yang berkaitan dengan pembuatan aplikasi tersebut.

- b. **Perumusan Masalah.** Merumuskan masalah menjadi hak yang wajib agar mendapatkan pokok pembahasan serta menemukan jalan keluar permasalahan.
- c. **Studi Literature.** Diperlukan literatur yang berhubungan dengan sistem keamanan data melalui studi pustaka di perpustakaan maupun di kumpulan jurnal serta media internet.
- d. **Perancangan System.** Perancangan sistem yang akan dirancang harus sesuai dengan yang dibutuhkan, proses, interface hingga sistem manajemen database.
- e. **Implementasi Program.** Pada tahap ini merupakan tahapan implementasi dari hasil rancangan sistem.
- f. **Penulisan Laporan.** Pada tahap ini dilakukan penyusunan Laporan yang sudah dijelaskan dalam landasan teori yang telah di tulis serta hasil penelitian berupa implementasi yang telah dibuat.

1.5.2 Sistematika penelitian

Sistematika penulisan laporan tugas akhir yang disusun adalah sebagai berikut :

BAB I : PENDAHULUAN

Bab ini terdiri atas Latar Belakang, perumusan masalah, Batasan Masalah, Tujuan dan Manfaat, serta sistematika penulisan tugas akhir ini.

BAB II : LANDASAN TEORI

Bab ini membahas mengenai beberapa teori dasar yang berhubungan dengan penerapan kriptografi untuk *encryption* dalam

system keamanan data untuk menjaga kerahasiaan dan otentikasi sebuah data.

BAB III : PERANCANGAN SISTEM

Membahas mengenai Rancangan dan Alur Algoritma Sistem yang dibuat, Disain Perangkat Lunak meliputi Desain Proses, Disain Antar Muka, dan Disain Data.

BAB IV : IMPLEMENTASI

Bab ini akan dijelaskan mengenai implementasi pembuatan aplikasi berdasarkan hasil rancangan yang telah dibuat sebelumnya

BAB V : PENUTUP

Bab ini berisi kesimpulan dari tugas akhir ini dan saran-saran untuk pengembangan dan perbaikan dari tugas akhir ini.

(Halaman ini sengaja dikosongkan)