BAB I

PENDAHULUAN

1.1 Latar Belakang

Sistem manajemen basis data adalah suatu kumpulan dari data yang saling terhubung dan suatu program yang dapat mengakses data tersebut. Kumpulan data tersebut kemudian lebih dikenal dengan istilah basis data. Basis data mengandung informasi yang sesuai dengan kebutuhan organisasi yang menggunakannya.

Tujuan utama dari sistem manajemen basis data yaitu untuk menyediakan jalan untuk menyimpan dan mendapatkan kembali informasi pada basis data dengan nyaman dan efisien. Sistem basis data didesain untuk menangani jumlah data yang besar, memanajemen data baik struktur penyimpanan maupun mekanisme memanipulasi data. Selain itu basis data harus menjamin keamanan dari informasi yang disimpan, walaupun terjadi *crash* pada sistem dan akses ilegal.

Basis data telah menjadi suatu kebutuhan di beberapa organisasi dan perusahaan komersial pada saat ini. Basis data digunakan secara luas untuk berbagai bidang. Perbankan menggunakan basis data untuk keperluan informasi pelanggan, simpanan, pinjaman dan transaksi perbankan lainnya. Universitas menggunakan basis data untuk menyimpan informasi mahasiswa, informasi pegawai, nilai mahasiswa dan registrasi mata kuliah. Disamping itu basis data juga digunakan untuk menagani administrasi sekolah, Bagian personalia membutuhkan basis data untuk menyimpan data karyawan, gaji karyawan. Selain contoh tersebut masih banyak lagi aplikasi basis data dalam berbagai bidang.

Dengan kebutuhan basis data yang semakin kompleks maka timbul suatu kebutuhan keamanan data dari berbagai macam ancaman diantaranya pembacaan data, modifikasi data dan perusakan data oleh orang yang tidak berhak. Ada beberapa level keamanan pada basis data, diantaranya : keamanan sistem operasi, keamanan sistem manajemen basis data, keamanan jaringan, keamanan fisik, dan keamanan segi manusia.

Untuk mengatasi masalah keamanan jaringan maka perlu dibuat suatu system yang dapat melakukan pengamanan data selama dalam jaringan, salah satu caranya yaitu mengimplementasikan kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan. Sistem kriptografi terdiri dari algoritma kriptografi, plainteks, cipherteks dan kunci. Dimana plainteks adalah data atau informasi yang dapat dimengerti artinya dan cipherteks adalah pesan yang sudah disandikan sehingga tidak bermakna lagi. Algoritma kriptografi adalah aturan untuk melakukan proses enkripsi yaitu proses menyandikan dari plainteks menjadi cipherteks dan proses dekripsi yang merupakan kebalikan dari enkripsi. Algoritma kriptografi ada yang simetris dan asimetris. Algoritma kriptografi simetris yaitu algoritma yang menggunakan hanya satu kunci untuk enkripsi dan dekripsi, sedangkan algoritma kriptografi asimetris yaitu algoritma yang menggunakan kunci publik dan privat dalam proses enkripsi dan dekripsi.

Penerapan kriptografi untuk mengatasi keamanan transmisi hasil *query* basis data dapat dilakukan dengan cara melakukan enkripsi data selama data tersebut berada dalam jaringan. Secara teknis, penerapan kriptografi ini dilakukan dengan membuat modul pengenkripsi dan pendekripsi data pada sistem

Pengamanan transmisi basis data memerlukan suatu proses yang cepat, karena itu algoritma kriptografi simetris adalah algoritma yang tepat diimplementasikan untuk kasus ini. Algoritma kunci simetris terbagi menjadi *block cipher* dan *stream cipher*, perbedaannya yaitu *block cipher* beroperasi dengan transformasi yang sama dengan blok besar dari plainteks data sedangkan *stream cipher* beroperasi dengan transformasi waktu pada tiap *byte* plainteks. Karena itu *stream cipher* memiliki kecepatan yang lebih cepat dan kebutuhan *hardware* yang lebih rendah dibandingkan dengan *block cipher*. RC4 merupakan algoritma *stream cipher* yang paling tepat dibandingkan dengan algoritma *stream cipher* lainnya untuk masalah transmisi hasil *query* basis data seperti ini. Hal itu dikarenakan RC4 memiliki proses enkripsinya yang cukup sederhana dan hanya melibatkan beberapa operasi saja per *byte*-nya.

Diharapkan dengan mengimplementasikan algoritma kriptografi *RC4* dapat meningkatkan keamanan transmisi data dari berbagai ancaman.

1.2 Rumusan Masalah

Dari latar belakang yang telah diuraikan maka dapat dirumuskan beberapa permasalahan yang akan dijadikan dasar dalam penyusunan tugas akhir ini.

Adapun rumusan masalah dapat dideskripsikan sebagai berikut :

1. Bagaimana penerapan algoritma RC4 sebagai perlidungan data pada database dari pembacaan data oleh orang yang tidak berhak.
2. Bagaimana memanagement kunci yang digunakan untuk menkripsi data.

3. Bagaimana merancang aplikasi yang dapat mengakses database pada network LAN.

1.3 Tujuan Penelitian

Dari permasalahan yang ada pada rumusan masalah maka penelian pada tugas akhir ini bertujuan :

1. Mempelajari cara untuk melakukan penggunaan algoritma kriptografi untuk pengamanan transmisi hasil *query* basis data.
2. Mengimplementasikan algoritma kriptografi pada sistem yang berfungsi untuk mengamankan transmisi hasil *query* basis data.
3. Merancang sistem pengolahan data yang dapat diakses secara jaringan (LAN).

1.4 Manfaat Penelitian

Manfaat yang dapat dipetik dari penilitan ini adalah :

1. Dengan penerapan algoritma kriptografi maka integritas data yang tersimpan akan terjaga.
2. Dapat digunakan untuk merancang pengolahan data sistem administrasi pendidikan.

1.4 Batasan Masalah

Dalam pelaksanaan tugas akhir ini ditetapkan batasan-batasan yang akan dijadikan pedoman dalam pelaksanaan tugas akhir :

1. Sistem ini hanya melakukan enkripsi dan deskripsi terhadap data yang akan disimpan pada database.

2. Pembahasan hanya mengenai pengamanan data bukan pada design tampilan.
3. Sifat pengamanan data hanya pada pembacaan data oleh orang yang tidak berhak.

1.5 Metodologi

Dalam pelaksanaan tugas akhir ini aktivitas yang dilakukan didalamnya antara lain: mengadakan eksplorasi terhadap kakas konsep yang akan digunakan dalam pembangunan sistem ini, melakukan analisis terhadap permasalahan yang ada, melakukan perancangan sistem berdasarkan hasil analisis tersebut, melakukan implementasi sistem tersebut dengan kakas yang telah ditentukan dan yang terakhir adalah mengadakan testing terhadap sistem tersebut.

Metodologi pembangunan perangkat lunak yang akan digunakan dengan tahapan sebagai berikut :

1. Eksplorasi.

   Pada tahap ini dilakukan eksplorasi terhadap beberapa kakas dan konsep yang akan akan digunakan dalam membuat tugas akhir ini. Eksplorasi dilakukan pada beberapa kakas yang akan digunakan untuk membangun sistem dalam tugas akhir ini.

   Eksplorasi konsep dilakukan dengan cara studi literatur yaitu dengan studi dari berbagai macam buku teks, diktat kuliah, jurnal, karya tulis ilmiah, tugas akhir dan tesis yang berkaitan dengan masalah yang akan dibahas.

2. Analisis Sistem.

Pada tahap ini dilakukan analisis terhadap rumusan masalah dan batasan yang ada dalam tugas akhir ini. Analisis ini juga dilakukan untuk melakukan analisis spesifikasi sistem yang akan dibuat sesuai dengan batasan yang ada.

3. Perancangan Sistem.

   Pada tahap ini dilakukan proses perancangan sesuai hasil analisis. Pada tahap perancangan ini dilakukan beberapa perancangan diantaranya : perancangan arsitektur sistem, perancangan antarmuka, perancangan modul lainnya yang akan berintegrasi dalam suatu sistem.

4. Implementasi Sistem.

   Pada tahap ini dilakukan implementasi sesuai dengan hasil perancangan. Implementasi ini dilakukan dengan menggunakan kakas yang sudah dieksplorasi pada tahap sebelumnya. Pada proses implementasi ini dilakukan pembuatan modul-modul dalam bahasa pemrograman tertentu.

5. Testing Sistem.

   Pada tahap ini dilakukan beberapa tes terhadap sistem yang telah diimplementasikan. Testing dilakukan dengan memasukkan data pengujian tertentu.

1.6 Sistematika Pembahasan

Sistematika Pembahasan dalam tugas akhir ini adalah sebagai berikut :

1. Bab I Pendahuluan, menguraikan hal-hal yang menjadi latar belakang pelaksanaan tugas akhir, perumusan masalah, penentuan tujuan, ruang

lingkup dan batasan masalah, metodologi penyusunan tugas akhir dan sistematika pembahasan dalam laporan tugas akhir.

2. Bab II Dasar Teori, menguraikan teori-teori yang digunakan dan teori yang berkaitan dan mendukung pelaksanaan tugas akhir.
3. Bab III Analisis Masalah, Bab ini berisi tentang analisis kebutuhan sistem, sistem yang diusulkan dan perancangan sistem secara umum.
4. BAB IV Implementasi, menguraikan bagian pembuatan program dan implementasi fungsi yang digunakan.
5. BAB V Uji Coba dan Analisa Hasil, menguraikan hasil uji coba terhadap sistem yang dibangun.
6. BAB VI Kesimpulan, menguraikan kesimpulan terhadap penelitian dan saran sebagai acuan untuk pengembangan dari penelitian.