BAB I

PENDAHULUAN

1.1 Latar Belakang

Informasi adalah sesuatu hal yang sangat penting pada era teknologi saat ini, banyak orang berburu informasi melalui berbagai macam cara, seperti melalui media massa maupun elektronik, terutama internet. Ditambah pula saat ini kemudahan dalam mendapatkan informasi semakin bertambah seiring dengan datangnya era kebebasan dalam memperoleh informasi. Hal ini menimbulkan berbagai macam efek, baik itu positif ataupun negatif, oleh karena itulah informasi yang kita anggap penting harus dijaga kerahasiannya serta diupayakan agar aman dari pihak-pihak yang dianggap bisa menyalahgunakan informasi tersebut, dan kriptografi dalam hal ini telah mencoba melakukannya selama bertahun-tahun.

Internet saat ini telah menjadi media utama dalam pertukaran informasi, tidak hanya itu, internet telah pula berubah menjadi media bisnis, pendidikan, dan yang saat ini ramai dibicarakan orang yaitu sebagai media jejaring sosial (*social networking*). Aktivitas yang terjadi di dalamnya pun rentan terhadap keamanan informasi yang akan dikirim maupun diterima, seperti aktivitas yang akan dibahas yaitu, aktivitas dalam kontrak mata kuliah secara *online*, aktivitas yang akan dibicarakan terutama adalah aktivitas dalam mengakses data ke dalam sistem basis data yang ada, dan dilakukan secara *remote* di dalam asitektur sistem berbentuk *client-server*.

Sistem manajemen basis data adalah suatu kumpulan dari data yang saling terhubung dan suatu program yang dapat mengakses data tersebut (Silberschatz, 2002, h. 16). 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.

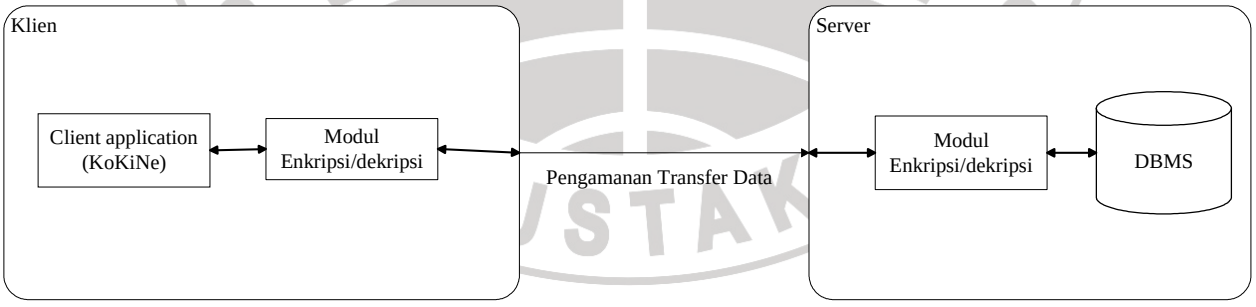
Basis data telah menjadi suatu kebutuhan di beberapa organisasi dan perusahaan komersial pada saat ini. Basis data digunakan secara luas untuk berbagai bidang seperti bisnis, perbankan, pendidikan, kepegawaian, dan lain-lain.

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 (Silberschatz, 2002, h. 16). Ada beberapa level keamanan pada basis data, diantaranya: keamanan sistem operasi, keamanan sistem manajemen basis data, keamanan jaringan, keamanan fisik, dan keamanan segi manusia (Silberschatz, 2002, h.248).

Untuk mengatasi masalah keamanan jaringan maka perlu dibuat suatu sistem yang dapat melakukan pengamanan data selama dalam jaringan, salah satu

caranya yaitu mengimplementasikan kriptografi. Penerapan kriptografi untuk mengatasi keamanan transmisi data *query* dan hasil *query* basis data dapat dilakukan dengan cara melakukan enkripsi data selama data tersebut berada dalam jaringan. Enkripsi data yang berupa hasil *query* basis data dilakukan sewaktu hasil *query* dari basis data tepat sebelum memasuki jaringan dan kembali didekripsi setelah sampai ditempat tujuan atau tempat pengakses yang aman. Secara teknis, penerapan kriptografi ini dilakukan dengan membuat modul pengenkripsi dan pendekripsi pada sumber dan tujuan. Sumber data pada transmisi hasil *query* terdapat pada sistem manajemen basis data dan penerima berupa aplikasi pada *client*.

Implementasi kriptografi dilakukan dengan cara membuat modul kriptografi dijadikan *stored procedure* pada sistem manajemen basis data dan sebagai modul yang terintegrasi dengan aplikasi berbasis *web* pada *client*, dimana dalam hal ini adalah perangkat lunak Kontrak Kuliah *Online* (KoKiNe).



Gambar 1.1 Gambaran Umum Implementasi

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 *plain*teks data sedangkan *stream cipher* beroperasi dengan transformasi waktu pada tiap *byte plain*teks. 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.

Menurut hasil pengetesan kecepatan algoritma kriptografi RC4 adalah 5380,035 *Kbytes*/detik pada *Pentium*133 memori 16 MB pada *Windows* 95 (Budi, S, 1998). Kecepatan dalam pengetesan ini adalah kecepatan enkripsi di memori, pada kenyataanya proses enkripsi *file* melibatkan banyak faktor lain seperti *interface* IO, tipe *hardisk*, dan lain-lain sehingga pada kenyataannya kecepatan enkripsi lebih lambat dari hasil tersebut, karena dipengaruhi faktor lain tersebut. Hasil pengetesan didapat dengan enkripsi 256 *byte* per blok sebanyak 20480 kali, atau setara dengan kurang lebih 5 MB data. Sebagai perbandingan, hasil pengetesan dengan algoritma *Blowfish* pada jenis komputer yang sama yaitu 2300 K*Byte*/detik pada 8 *byte* per blok (Budi, S, 1998). Jadi pengetesan tersebut membuktikan bahwa RC4 sebagai algoritma yang cepat dalam pemrosesan proses enkripsi dan dekripsi.

Prosesor	**Memori (MB)**	**Kecepatan (K*Bytes*/detik)**
486/DX4-100	16	557,067
Pentium 100	32	1.079,713
Pentium 166	16	1.792,717

Tabel 1.1 Hasil Pengujian Kecepatan RC4 di *Delphi* 1.0 pada *Windows for Workgroups* 3.11 (Sukmawan, 1998)

Prosesor	**Memori (MB)**	**Kecepatan (K*Bytes*/detik)**
486/DX4-100	16	2.563,846
Pentium 100	16	4.285,714
Pentium 133	32	5.380,035
Pentium 166MMX	32	7.191,522
Pentium 200MMX	32	8.668,172
Pentium Pro 200	64	10.651,872

Tabel 1.2 Hasil Pengujian Kecepatan RC4 di *Delphi* 4.0 pada *Windows* 95, kecuali *Pentium Pro* pada *Windows* NT 4.0 *Server* (Sukmawan, 1998)

Diharapkan dengan mengimplementasikan algoritma kriptografi RC4 dapat meningkatkan keamanan transmisi data dari ancaman penyadap tanpa mengurangi performa perangkat lunak secara signifikan.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dibahas, maka perumusan masalah untuk penelitian ini adalah:

1. Bagaimana mengamankan transmisi data *query* dan hasil *query* dari klien menuju *server*
2. Bagaimana mengimplementasikannya ke dalam sistem yang ada, dalam hal ini adalah Kontrak Kuliah *Online* (KoKiNe)
3. Pembuktian apakah yang dapat menjamin bahwa transmisi data *query* dan hasil *query* yang dikirim sudah dirasa aman

1.2.1 Batasan Masalah

Untuk menghindari melebarnya pembahasan yang ada, maka batasannya adalah :

1. Pengamanan hanya dilakukan terhadap transmisi data *query* dan hasil *query* pada Kontrak Kuliah *Online* (KoKiNe) dari klien menuju *server*, begitu juga sebaliknya, perlu diketahui pula bahwa *query* yang dimaksud bukanlah *query* yang berisikan transaksi basis data, dalam artian *query* yang dilakukan dianggap selalu berhasil (*commit*) dan tidak pernah gagal (tidak terjadi *rollback* transaksi)

2. Pengamanan dilakukan dengan menggunakan algoritma Kriptografi RC4 dan merupakan bagian program dari sistem yang ada.
3. Kontrak Kuliah *Online* (KoKiNe) hanyalah suatu sistem dimana implementasi ini dilakukan, jadi pembahasan mengenai sistem tersebut yang dianggap tidak berpengaruh secara signifikan terhadap implementasi, tidak akan dibahas

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah:

1. Melakukan studi untuk pengamanan transmisi data *query* dan hasil *query* basis data pada sistem yang ada.
2. Mengimplementasikan algoritma kriptografi RC4 terhadap pengamanan tersebut pada sistem yang ada.

1.4 Manfaat Penelitian

Manfaat dari keluaran yang diharapkan adalah:

1. Diharapkan dari hasil studi ini, dapat dijadikan rujukan dalam membangun aplikasi atau sistem yang memiliki karakteristik yang mirip.
2. Diharapkan dari implementasi yang ada, segi keamanan dalam perangkat lunak yang diimplementasikan menjadi lebih meningkat.

1.5 Metodologi Penelitian

1. Metode Pengumpulan Data:

    a. Studi Kepustakaan

    Mempelajari literatur-literatur yang berkaitan dengan teori dan konsep atas masalah yang diteliti agar diperoleh suatu pemahaman yang mendalam serta menunjang proses pembahasan mengenai masalah-masalah yang telah diidentifikasi.

    b. Oberservasi

    Melakukan pengamatan terhadap kenyataan yang ada di lapangan, seperti melihat proses yang ada dalam transaksi kontrak mata kuliah secara manual dan mencoba memetakannya secara *online*

    c. Wawancara

    Mencari apa yang dirasakan pengguna dalam menggunakan kontrak mata kuliah secara manual, baik kekurangan ataupun kelebihan, dan harapan-harapan yang diinginkan pengguna bila kontrak mata kuliah dilakukan secara *online*.

2. Metode Pembangunan Perangkat Lunak

    Metode yang digunakan adalah metode pembangunan perangkat lunak *prototyping*, dengan pendekatan berorientasi objek.

1.6 Sistematika Penulisan

Dalam penyusunan skripsi ini, sistematika penulisan dibagi ke dalam beberapa tahapan, yaitu:

BAB I PENDAHULUAN

Bab ini berisi pembahasan secara umum meliputi latar belakang, perumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi penjelasan secara umum mengenai hal yang berhubungan dengan Kriptografi, Algoritma RC4, basis data, serta keamanan informasi.

BAB III METODOLOGI PENELITIAN

Bab ini berisi penjabaran mengani tahapan penelitian yang dilakukan, metode pengembangan perangkat lunak yang digunakan, serta alat dan bahan penelitian yang digunakan dalam penelitian.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini berisi pembahasan mengenai hasil implementasi Algoritma Kriptografi RC4 pada perangkat lunak Kontrak Kuliah *Online* (KoKiNe)

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan yang diambil dari hasil implementasi yang ada serta saran yang dapat dijadikan dalam penelitian selanjutnya.