BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Seiring dengan perkembangan teknologi dalam dunia bisnis, sistem basis data telah menjadi simbol dari salah satu bentuk aset yang paling berharga. Basis data telah menjadi 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 semakin luasnya penggunaan sistem basis data, perlindungan terhadap informasi yang disimpan dalamnya menjadi sangat diperlukan untuk melindungi dari berbagai macam ancaman diantaranya pembacaan data, manipulasi data dan perusakan data oleh pihak yang tidak berwenang. Ada beberapa tingkatan keamanan pada sistem basis data, diantaranya : keamanan sistem oprasi, keamanan sistem manajemen basis data, keamanan jaringan, dan keamanan segi manusia.

Untuk mengatasi masalah terjadinya penyalahgunaan terhadap hak akses basis data maka peru dibuat suatu sistem yang dapat melakukan pengamanan data, salah satu caranya yaitu mengimplementasikan kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga keamanan informasi. Peran utama kriptografi adalah untuk mengamankan data itu sehingga tidak bisa dibaca, dimanipulasi dan di rusak oleh pihak yang tidak berwenang pada. Peroses penyandian pada kriptografi terdiri atas dua tahap, yaitu enkripsi dan dekripsi. Enkripsi merupakan proses

perubahan *plaintext* menjadi *cipherteks* yang tidak dapat dimengerti, sedangkan dekripsi adalah proses perubahan kembali ciphertext menjadi plainteks.

Penerapan kriptografi untuk mengatasi masalah keamanan sistem basis data dapat dilakukan dengan cara melakukan enkripsi data selama basis data tersebut sedang tidak digunakan. Secara teknis, penerapan kriptografi ini dilakukan dengan membuat modul pengenkripsi dan pendekripsi data pada sistem.

Pengamanan sistem basis data memerlukan suatu proses yang cepat, karena itu algoritma kriptografi simetris adalah suatu algoritma yang tepat diimplementasikan untuk kasus ini. Algoritma kunci simetris terbagi menjadi *block cipher* dan *stream cipher*, perbedaannya yaitu *block cipher* beroprasi dengan transformasi yang sama dengan blok besar dari plainteks data sedangkan *stream cipher* beroprasi dengan transformasi waktu pada tiap *byte* plainteks. Karena itu *stream cipher* memiliki kecepatan dan kebutuhan *hardware* yang lebih rendah dibandingkan dengan *block cipher*. Blowfish merupakan algoritma *block cipher* yang paling tepat dibandingkan dengan algoritma *block cipher* lainnya untuk mengatasi maslaah keamanan sistem basis data. Hal itu di karenakan Blowfish merupakan algoritma kriptografi kunci simetri *block chiper* dengan panjang blok tetap 64 *bit* dan menerapkan teknik kunci berukuran sembarang dengan ukuran kunci antara 32 *bit* hingga 448 *bit* memiliki ukuran default sebesar 128 bit dan juga memanfaatkan teknik pemanipulasian *bit* dan teknik pemutaran ulang dan pengalihan kunci yang dilakukan sebanyak 16 kali. Blowfish atau sering disebut "*OpenPGP.Cipher.4*" merupakan enkripsi yang termasuk dalam golongan *Symmetric Cryptosystem* (Schneier, 1993), yaitu menggunakan kunci yang sama

untuk enkripsi dan dekripsinya.

Blowfish dikembangkan untuk memenuhi kriteria desain sebagai berikut (Schneier, 1993):

1. Cepat, pada implementasi yang optimal Blowfish dapat mencapai kecepatan 26 *clock cycle* per byte.
2. Kompak, Blowfish dapat berjalan pada memori kurang dari 5 KB.
3. Sederhana, Blowfish hanya menggunakan operasi penambahan (*addition*), XOR, dan penelusuran tabel (*table lookup*) pada *operand* 32 bit. Desainnya mudah untuk dianalisa yang membuatnya resisten terhadap kesalahan implementasi.
4. Tingkat keamanan yang variatif, panjang kunci Blowfish dapat bervariasi dan dapat mencapai 448 bit (56 byte).

1.2 Rumusan Masalah

1. Bagaimana menerapkan algoritma blowfish sebagai perlindungan data pada basis data ?
2. Bagaimana merancang aplikasi yang dapat melindungi data pada file basis data ?

1.3 Batasan Masalah

Dari rumusan masalah di atas, maka penulis menentukan batasan masalah. Hal ini sebagai solusi permasalahan, serta untuk membatasi lingkup pembahasan masalah yang telah ditentukan. Yaitu sebagai berikut:

1. Model kriptosistem dirancang dan dibuat sebagai program keamanan data berbasis dekstop.
2. Basis data yang digunakan adalah basis data yang buat menggunakan aplikasi Microsoft SQL Server.
3. Sifat pengamanan data hanya pada pembacaan data oleh orang yang tidak berhak.
4. Algoritma kriptografi yang digunakan adalah Blowfish

1.4 Tujuan Penelitian

Dari permasalah yang ada pada rumusan masalah maka penelitian ini bertujuan untuk membuat sebuah aplikasi yang mampu meningkatkan keamana data pada basis data. Selain itu penelitian ini bertujuan menganalisis kinerja algoritma Blowfish dengan simulasi data terbatas.

1.5 Manfaat Penelitian

Dapat membantu mengatasi masalah keamanan basis data pada file yang dibuat menggunakan aplikasi Microsoft SQL Server.

1.6 Metode Penelitian

Metode penelitian merupakan cara atau teknik yang dilakukan peneliti untuk menyusun suatu karya tulis dan mengumpulkan data-data yang dibutuhkan. Dalam kasus ini penulis menggunakan beberapa metode pengumpulan data, yaitu:

a. Metode Observasi

Metode ini merupakan cara untuk melakukan pengamatan secara langsung terhadap objek penelitian. Mencari dan menyimpulkan masalah yang ada selama ini dan menentukan solusi permasalahan.

b. Metode Wawancara

Metode wawancara merupakan metode pengumpulan data dengan cara mengajukan beberapa pertanyaan kepada beberapa pihak yang mengacu pada bagian-bagian yang berkaitan dengan penelitian yang dilakukan.

c. Metode Dokumentasi

Metode dokumentasi merupakan suatu metode penelitian dimana peneliti mengumpulkan dokumen-dokumen yang berkaitan.

d. Metode Kepustakaan

Metode kepustakaan merupakan studi literatur untuk mengumpulkan data atau informasi yang berhubungan dengan objek penelitian yang dilakukan. Penulis melakukan studi literatur di perpustakaan STMIK AMIKOM Yogyakarta dan melakukan download data dari berbagai macam sumber di internet.

1.7 Sistematika Penulisan Laporan

Sistematika penulisan laporan disusun menggunakan dasar-dasar penulisan ilmiah. Metode ini dilakukan agar penyusunan laporan menjadi lebih teratur dan mudah dipahami. Sistematika laporan dibagi dalam enam bab, yaitu sebagai berikut:

Bab I : Pendahuluan

Bab ini terdiri dari latar belakang masalah, rumusan masalah, batasan masalah, tujuan & manfaat penelitian, metode pengumpulan data dan sistematika penulisan.

Bab II : Dasar Teori

Bab ini berisi tentang dasar-dasar teori yang digunakan dalam penelitian .

Bab III : Analisa dan Perancangan Sistem

Bab ini berisi mengenai analisa permasalahan dan perancangan program. Serta perancangan antar mukanya.

Bab IV : Implementasi dan Analisis hasil Uji Coba Program

Bab ini berisi tentang implementasi rancangan perangkat lunak ke dalam antar muka, pengujian dan hasilnya

Bab V : Penutup

Bab ini merupakan bab yang menyajikan kesimpulan penelitian serta saran.

1.8 Jadwal Penelitian

Tabel 1.1 Tabel Jadwal Penelitian

No	Kegiatan	Target Output	April - Mei 2011				Juni - Juli 2011				Agustus-Sept 2011				Okt - Nov 2011			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Literatur	Menentukan Permasalahan (latar belakang, rumusan, batasan dan tujuan masalah)																
		Memahami cara kerja Algoritma Blowfish & Algoritma lainnya.																
		Mengumpulkan landasan teori permasalahan.																
2	Perancangan Sistem	Menentukan software yang akan digunakan.																
		Menganalisa masalah perancangan																
		Membuat Perancangan sistem																
3	Uji Coba Rancangan	Simulasi uji coba rancangan & Analisa uji coba rancangan																
		Rancangan yang optimal																
4	Implementasi	Mempelajari masalah Implementasi sistem																
		Implementasi rancangan ke dalam sistem																
5	Uji Coba Sistem	Simulasi uji coba sistem																
		Analisa sistem																
6	Penyusunan Laporan	1.Dokumentasi penelitian secara lengkap																
		2. Laporan Skripsi																