BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Masalah keamanan merupakan salah satu aspek paling penting dalam dunia teknologi informasi, misalnya : keamanan dokumen. Sekarang ini, sebagian besar dokumen-dokumen menggunakan aplikasi Microsoft Office, karena kemudahan dalam menggunakannya. Di dalam Microsoft Office ada beberapa aplikasi yang dapat digunakan, yaitu Microsoft Word, Microsoft Excel, Microsoft Access,dan Microsoft PowerPoint. Berbagai aplikasi dalam Microsoft Office dapat digunakan untuk mengolah kata dan angka sesuai kebutuhan pengguna.

Keamanan dokumen sangat diperlukan, maka setiap orang memerlukan suatu aplikasi yang dapat mengamankan dokumen rahasia dan penting agar dokumen tersebut hanya dapat di lihat dan di baca oleh orang tertentu saja.

Beberapa cara telah dikembangkan untuk menangani masalah keamanan ini, salah satu teknik untuk pengamanan data adalah dengan menggunakan algoritma penyandian data. Algoritma penyandian data saat ini telah semakin banyak jumlahnya, sejalan dengan berkembangnya ilmu yang mempelajari penyandian data tersebut. Ilmu ini biasa disebut Kriptografi.

Dalam kriptografi terdapat beberapa metode yang cukup penting dalam pengamanan data, untuk menjaga kerahasiaan data salah satunya adalah enkripsi (*encryption*). Enkripsi adalah suatu proses yang dilakukan untuk mengubah pesan asli menjadi *chipertext.* Sedangkan suatu proses yang dilakukan untuk mengubah

pesan tersembunyi menjadi pesan asli disebut dekripsi. Pesan biasa atau pesan asli disebut *plaintex* sedangkan pesan yang telah diubah atau disandikan supaya tidak mudah dibaca disebut dengan *chipertext*.

Untuk mengatasi masalah keamanan dokumen ini, penulis melakukan pendekatan teknologi enkripsi data menggunakan algoritma Blowfish. Enkripsi data merupakan teknologi untuk memastikan bahwa informasi yang mengalir pada suatu sesi tidak disadap atau diubah orang lain. 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 cara kerja algoritma blowfish?
2. Bagaimana menerapkan algoritma blowfish?
3. Bagaimana melakukan pengujian aplikasi yang telah dibuat?

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 *file* berbasis desktop
2. Dokumen yang digunakan adalah dokumen yang di buat menggunakan aplikasi yang terdapat dalam Microsoft Office.
3. File yang digunakan adalah file yang berekstensi .doc, .docx, .rtf, .txt, .xls, .xlsx .mdb, dan .ppt, .pptx.
4. Algoritma kriptografi yang digunakan adalah Blowfish

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai adalah membuat sebuah aplikasi yang mampu mengenkripsi dan dekripsi file pada Microsoft Word (.doc, .docx, .rtf, .txt), Microsoft Excel (.xls, .xlsx), Microsoft Access (.mdb) dan Microsoft PowerPoint (.ppt, .pptx). Setelah file di enkripsi dapat di ubah kembali seperti semula dengan proses dekripsi.

1.5 Manfaat Penelitian

Dapat membantu mengatasi masalah keamanan dokumen pada file pada Microsoft Word (.doc, .docx, .rtf, .txt), Microsoft Excel (.xls, .xlsx), Microsoft Access (.mdb) dan Microsoft PowerPoint (.ppt, .pptx).

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 Kuesioner

Kuesioner merupakan teknik pengumpulan informasi yang memungkinkan penganalisis sistem mempelajari sikap-sikap, keyakinan, perilaku, karakteristik beberapa orang dalam organisasi yang terpengaruh oleh sistem yang diajukan (Kendall & Kendall, 2003). Metode ini diimplementasikan terhadap beberapa orang yang berkompeten di bidang IT sebagai sample penelitian.

c. 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.

d. Metode Eksperimental

Metode eksperimental dilakukan dengan cara uji coba perancangan dan sistem. Objek dalam hal ini penulis menyajikan simulasi enkripsi dan dekripsi data serta hasil dan analisanya.

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 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 2009				Juni - Juli 2009				Agustus-Sept 2009				Okt - Nov 2009				Des - Jan 2009/10			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Literatur	1. Menentukan Permasalahan (latar belakang, rumusan, batasan dan tujuan masalah)																				
		2. Memahami cara kerja Algoritma Blowfish & Algoritma lainnya.																				
		3. Mengumpulkan landasan teori permasalahan.																				
2	Perancangan Sistem	1. Menentukan software yang akan digunakan.																				
		2. Menganalisa masalah perancangan																				
		3. Membuat Perancangan sistem																				
3	Uji Coba Rancangan	1. Simulasi uji coba rancangan & Analisa uji coba rancangan 2. Rancangan yang optimal																				
4	Implementasi	1. Mempelajari masalah Implementasi sistem																				
		2. Implementasi rancangan ke dalam sistem																				
5	Uji Coba Sistem	1. Simulasi uji coba sistem 2. Analisa sistem																				
6	Penyusunan Laporan	1.Dokumentasi penelitian secara lengkap 2. Laporan Skripsi																				