BAB I
PENDAHULUAN

1.1 Latar Belakang

Berbagai organisasi, perusahaan, atau pun pihak – pihak lain telah memanfaatkan teknologi komputer untuk menyimpan dan mengelola data organisasi atau perusahaannya. Saat ini, keamanan terhadap data yang tersimpan di dalam komputer sudah menjadi persyaratan mutlak. Pengamanan terhadap jaringan komputer yang terhubung dengan dokumen-dokumen sudah tidak lagi menjamin keamanan data karena kebocoran data dapat disebabkan oleh "orang dalam" atau pihak – pihak yang langsung berhubungan dengan dokumen-dokumen seperti administrator . Hal ini menyebabkan pengguna dokumen harus menemukan cara untuk mengamankan data tanpa campur tangan administrator.

Kriptografi dapat digunakan untuk mengamankan data. Oleh karena itu, pengguna dokumen membutuhkan bantuan untuk memenuhi kebutuhan keamanan akan data yang disimpannya. Penerapan kriptografi pada Tugas Akhir ini akan difokuskan bagaimana kriptografi dapat mengamankan data dengan tiga kunci yang panjang kuncinya berbeda-beda, mulai dari 128, 192 dan 256 byte. Algoritma kriptografi yang akan digunakan ialah kriptografi AES (Anvanced Encryption Standard) dengan algoritma Rinjdael. Teknik kriptografi AES ini dipilih karena keamanannya lebih terjamin di bandingkan dengan algoritma-algoritma yang lain.

Berdasarkan atas informasi di atas, penulis membuat sebuah implementasi dengan menerapkan metode sistem enkripsi dengan menggunakan algoritma Rinjdael untuk membuat aplikasi kriptografi untuk keamanan dokumen-dokumen yang memerlukan pengamanan dari pihak-pihak yang tidak berkepentingan.

Enkripsi dilakukan pada saat pengiriman dengan cara mengubah data asli menjadi data rahasia, sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengubah data rahasia menjadi data asli. Jadi data yang dikirimkan selama

proses pengiriman adalah data rahasia, sehingga data asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Data asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia.

Disini enkripsi dapat diartikan sebagai kode atau *cipher*. Sebuah *system* pengkodean menggunakan suatu tabel atau kamus yang telah didefinisikan untuk kata dari informasi atau yang merupakan bagian dari pesan, data, atau informasi yang di kirim. Sebuah *cipher* menggunakan suatu algoritma yang dapat meng - kodekan semua aliran data (*stream*) bit dari suatu pesan asli (*plaintext*) menjadi *cryptogram* yang tidak di mengerti. Karena *system cipher* merupakan suatu sistem yang telah siap untuk di outomasi, maka teknik ini digunakan dalam sistem keamanan jaringan komputer.

National Institute of Standard and Technology (NIST) untuk pertama kalinya mengumumkan suatu algoritma standar penyandian data yang telah dijadikan standard sejak tahun 1977 adalah Data Encryption Standard (DES). Kekuatan DES ini terletak pada panjang kuncinya yaitu 56-bit. Untuk menanggapi keinginan agar mengganti algoritma DES sebagai standar. Perkembangan kecepatan perangkat keras dan meluasnya penggunaan jaringan komputer terdistribusi mengakibatkan penggunaan DES, dalam beberapa hal, terbukti sudah tidak aman dan tidak mencukupi lagi terutama dalam hal yang pengiriman data melalui jaringan internet. Perangkat keras khusus yang bertujuan untuk menentukan kunci 56-bit DES hanya dalam waktu beberapa jam sudah dapat dibangun. Beberapa pertimbangan tersebut telah manandakan bahwa diperlukan sebuah standard algoritma baru dan kunci yang lebih panjang. Triple-DES muncul sebagai alternative solusi untuk masalah-masalah yang membutuhkan keamanan data tingkat tinggi seperti perbankan, tetapi ia terlalu lambat pada beberapa penggunaan enkripsi.

Pada tahun 1997, the U.S. National Institue of Standards and Technology (NIST) mengumumkan bahwa sudah saatnya untuk pembuatan standard algoritma penyandian baru yang kelak diberi nama Advanced Encryption Standard (AES). Algoritma AES ini dibuat dengan tujuan untuk menggantikan algoritma DES &

Triple-DES yang telah lama digunakan dalam menyandikan data elektronik. Setelah melalui beberapa tahap seleksi, algoritma Rijndael ditetapkan sebagai algoritma kriptografi AES pada tahun 2000.

Algoritma AES merupakan algoritma kriptografi simetrik yang beroperasi dalam mode penyandi blok (block cipher) yang memproses blok data 128-bit dengan panjang kunci 128-bit (AES- 128), 192-bit (AES-192), atau 256-bit (AES-256). Beberapa mode operasi yang dapat diterapkan pada algoritma kriptografi penyandi blok AES di antaranya adalah Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), dan Output Feedback (OFB). Implementasi AES dengan mode operasi ECB, CBC, CFB, dan OFB tentu saja memiliki kelebihan dan kekurangan tertentu dalam aspek tingkat keamanan data.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, Rumusan masalah yang dapat penulis simpulkan adalah bagaimana cara membuat sebuah aplikasi pengamanan dokumen-dokumen dengan menggunakan teknik kriptografi AES Rinjdael. Sehingga dengan adanya aplikasi ini di harapkan dokumen-dokumen yang perlu dilindungi dari pihak-pihak yang tidak berkepentingan dapat terwujud. Rancangan untuk program aplikasi pengamanan basis data ini menggunakan algoritma enkripsi AES-Rinjdael dengan menggunakan bahasa pemrograman visual basic 6.0.

1.3 Batasan Masalah

Batasan masalah pada program aplikasi pengamanan basis data dengan algoritma AES (Advanced Encryption Standard) yaitu:

a. Rancangan program aplikasi ini dibuat untuk mengamankan pesan, tetapi rancangan program ini tidak dibandingkan dengan program sejenis sebelumnya

yang telah dibuat sehingga tidak diketahui program ini lebih baik atau tidak dari program sejenis sebelumnya.

b. Ukuran teks yang dapat dienkripsi senilai 2000 karakter, teks berupa angka, huruf dan tombol lain yang tersedia pada keyboard, hal ini dikarenakan keterbatasan bahasa pemograman yang digunakan yaitu visual basic 6.0.
c. Rancangan aplikasi pengamanan basis data ini hanya dapat mengenkripsi dan mendekripsi data yang berupa teks atau tulisan, bukan suara maupun gambar.

1.4 Tujuan Penelitian

Adapun tujuan dari ini adalah :

a. Mempelajari teknik pengamanan enkripsi sebagai lanjutan dari ilmu yang telah dipelajari di bangku kuliah.
b. Menambah pengetahuan penulis mengenai sebuah sistem aplikasi kriptografi dengan algoritma AES (Advanced Encryption Standard).
c. Menerapkan dan memperdalam ilmu pengetahuan penulis tentang pengamanan data dengan menggunakan teknik kriptografi yang telah didapat selama di bangku perkuliahan.

1.5 Metode Penelitian

Dalam penyusunan skripsi ini sangat diperlukan sumber-sumber data dan informasi yang benar dan akurat sehingga dapat menjadi masukkan yang berguna. Data yang diperlukan dalam penyusunan karya tulis ini berkelompok menjadi 2 bagian, yaitu :

a. Riset lapangan

   Riset lapangan dimaksudkan untuk memperoleh informasi secara langsung dari para pakar dan juga dunia internet. Adapun teknik pengumpulan data yang digunakan adalah:

1. Wawancara

   Metode ini dilakukan dengan mewancarai pakar yang mengerti tentang keamanan suatu aplikasi program misalnya programmer. Metode ini digunakan untuk mengetahui tentang bentuk-bentuk sistem keamanan dengan menggunakan enkripsi

2. Peninjauan dan Pengamatan

   Pengamatan dengan langsung terjun kelapangan. Metode ini digunakan untuk mengetahui aplikasi ilmu yang diperoleh dibangku kuliah dengan aplikasi dalam praktek yang nyata.

b. Studi Kepustakaan

   Pada Studi Kepustakaan dilakukan berdasarkan pengetahuan yang telah diterima penulis selama masa perkuliahan, serta membaca buku-buku perpustakaan yang ada dengan hubungannya dengan penelitian ini.

c. Metode perencanaan dan pembuatan aplikasi

   Setelah data-data yang dibutuhkan untuk membuat sistem aplikasi enkripsi ini sudah memadai, maka langkah selanjutnya yang dilakukan yaitu :

   1. Mencoba-coba logika yang akan digunakan dalam pembuatan aplikasi yang sesuai dengan data-data yang telah diperoleh sesuai spesifikasi aplikasi yang diingikan.
   2. Melaksanakan perencanaan tiap-tiap blokdiagram dari hasil coba-coba yang dianggap rangkaian paling efektif yang kemudian digabungkan sehingga menjadi satu sistem aplikasi

d. Mempersiapkan komponen yang diperlukan

   Adapun komponen yang diperlukan yaitu :

   1. Laptop atau PC
   2. Sistem operasi window 7
   3. Program aplikasi Microsoft office, Microsoft office Word akan dibutuhkan untuk tempat menyimpan data

4. Program aplikasi Microsoft Visual Studio 6.0 , Microsoft Visual Basic 6.0 akan dibutuhkan untuk pengkodean

e. Pembuatan aplikasi

Pengkodean tiap-tiap blok dan penggabungan tiap-tiap blok menjadi satu sistem aplikasi.

f. Pengujian aplikasi

Pengujian program aplikasi dilakukan untuk mengetahui apakah aplikasi yang dibuat telah bekerja dengan baik. Pengujian dilakukan pada tiap-tiap blok, kemudian dilakukan pengujian sistem secara keseluruhan.

1.6 Sistematika Penulisan

Pembahasan skripsi ini dibagi ke dalam bab per bab untuk mempermudah dalam pembahasan sistem. Tiap bab masih merupakan satu kesatuan, dengan beberapa perincian sebagai berikut:

BAB I : PENDAHULUAN

Pada bab ini dibahas mengenai latar belakang pembuatan skripsi, rumusan masalah, batasan masalah yang dibahas, tujuan yang diharapkan untuk mengatasi permasalahan, metode penelitian yang dilakukan penulis, dan sistematika penulisan skripsi.

BAB II : LANDASAN TEORI

Pada bab ini dibahas tentang teori-teori dasar yang berkaitan dengan pembuatan aplikasi pada skripsi ini, mulai dari pengertian kriptografi, sejarah kriptografi, taksonomi, tujuan kriptografi, pola-pola penyaringan data, sejarah AES, dan algoritma AES.

BAB III : PERANCANGAN DAN PEMBUATAN APLIKASI

Pada bab ini dibahas tentang perancangan dan pembuatan aplikasi pangamanan basis data dengan menggunakan teknik kriptografi AES (Advance Enkryption Standard).

BAB IV : PENGUJIAN DAN IMPLEMENTASI

Dalam bab ini pembahasannya mengenai pengujian dari modul-modul yang ada di dalam aplikasi yang dibuat dan implementasinya.

BAB V : PENUTUP

Pada bab ini berisi kesimpulan-kesimpulan yang bisa ditarik dari bab-bab sebelumnya juga beberapa saran yang bisa diberikan untuk dapat memperbaiki kekurangan dalam pembuatan skripsi ini.