BAB I

PENDAHULUAN

1.1. Latar Belakang

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.

Sebagian besar para pengguna sudah terbiasa dengan aplikasi Microsoft Office yang sangat memudahkan siapa saja ketika menggunakan aplikasi ini. Pengolah kata Microsoft Word, begitu mudah digunakansehingga siapapun yang menggunakannya akan merasa nyaman dengan pengolah kata ini. Dalam aplikasi Microsoft Office pengolah kata disimpan sebagai file Microsoft Word, pengolah angka sebagai file Microsoft Excel, dan sebagainya. Memang tidak ada yang aneh dalam sistem penyimpanan seperti ini karena memang sebagian besar di antara masyarakat menggunakan semua aplikasi yang ada pada Microsoft Office.

Sehingga, keamanan dokumen sangat diperlukan untuk membantu mengatasi masalah keamanan data yang dibuat atau disimpan menggunakan aplikasi pada Microsoft Office dari pencurian dokumen-dokumen baik yang tidak penting maupun yang penting dan rahasia. Sehingga orang lain tidak dapat mengetahui isi dari dokumen-dokumen tersebut.

Untuk mengatasi masalah keamanan dokumen ini, topik yang dipilih adalah perancangan aplikasi kriptografi pada file dokumen, menggunakan algoritma AES 256.

1.2. Permasalahan

1.2.1. Rumusan Masalah

a. Bagaimana menyandikan file dokumen menggunakan algoritma AES 256?
b. Apakah file dokumen mengalami perubahan setelah dilakukan proses enkripsi dan dekripsi?

1.2.2. Batasan Masalah

Batasan masalah dalam penelitian ini adalah :

a. Metode Kriptografi yang digunakan yaitu Algoritma AES (*Advance Encryption Standar*).
b. Panjang kunci yang digunakan untuk AES yaitu 256 bit.
c. Kunci yang digunakan hanya kunci Simetri.

1.3. Tujuan dan Manfaat Penelitian

1.3.1. Tujuan Penelitian

Tujuan yang hendak dicapai dalam Tugas Akhir ini adalah, dapat membuat sebuah aplikasi berbasis desktop yang berfungsi untuk menyandikan file dokumen.

1.3.2. Manfaat Penelitian

Manfaat aplikasi ini adalah untuk meningkatkan keamanan untuk file dokumen. Dan juga dibuat untuk digunakan sebagai salah satu alternatif mengamankan data atau pesan menggunakan algoritma kriptografi.

1.4. Cara Penelitian

1.4.1. Metode Penelitian

Metode yang digunakan pada penelitian ini adalah Metode Penelitian dan Pengembangan (*Research and Development*). Penelitian dan Pengembangan atau *Research and Development* (R&D) adalah suatu proses atau langkah-langkah untuk mengembangkan suatu produk baru, atau menyempurnakan produk yang telah ada, yang dapat dipertanggung jawabkan (Sujadi, 2003).

1.4.2. Tahapan Penelitian

Adapun tahapan penelitian yang akan dilakukan dalam proses penelitian ini adalah sebagai berikut :

1. Persiapan Penelitian

   Sebelum masuk ke tahap yang lebih dalam, maka diperlukan persiapan awal dalam melakukan penelitian. Persiapan ini berkaitan dengan hardware dan software yang akan digunakan untuk membangun model Aplikasi. Selain itu juga ada beberapa hal penting yang juga perlu dipersiapkan, yaitu penentuan langkah-langkah yang harus dikerjakan terlebih dahulu agar penelitian tersusun secara terstruktur sehingga memudahkan dalam penyelesaian penelitian dan mendapatkan hasil yang diharapkan.

2. Analisa Sistem

   Tahapan awal dalam membangun model aplikasi ini adalah dengan melakukan analisa terlebih dahulu tentang cara kerja algoritma yang akan digunakan dalam mengenkripsi file dokumen. Di mana algoritma tersebut adalah AES 256.

3. Perancangan Sistem

   Langkah berikutnya adalah membuat perancangan antar muka *(interface)* berupa form-form yang berisi beberapa fungsi yang diperlukan oleh pengguna, menentukan alur program dari form-form tersebut. Rancangan tersebut juga akan diterapkan dalam sebuah sistem dengan bantuan bahasa pemodelan UML(*Unified Modeling Language*).

4. Implementasi

   Selanjutnya adalah menerapkan algoritma AES 256 kedalam form-form yang telah dibuat dalam bentuk *coding*, di mana *coding* tersebut berfungsi sebagai penunjang untuk mengenkripsi dan mendekripsi file dokumen agar dapat melakukan fungsinya sesuai dengan yang diharapkan. Penerapan tersebut berupa tampilan interface dengan menggunakan bahasa pemrograman java.

5. Pengujian Sistem

   Dalam proses pengujian sistem ini peneliti menjalankan sekaligus menguji coba sistem yang telah dibuat dengan melakukan enkripsi maupun dekripsi pada file dokumen. Jika masih ada kesalahan aplikasi atau sistem yang telah dirancang maka dapat dilakukan implementasi ulang pada fitur yang bermasalah.

6. Penyusunan Laporan

   Setelah melakukan semua proses tahapan penelitian yang ada, maka hasil dari penelitian ini disusun dalam bentuk laporan

1.4.3. Teknik Pengumpulan Data

Metode pengumpulan data yang digunakan adalah Metode Studi Pustaka. Dalam penelitian ini peneliti mengacu dari beberapa hasil penelitian yang sudah dilakukan sebelumnya dengan cara melakukan tinjauan pustaka. Dari tinjauan pustaka yang dilakukan, peneliti menemukan beberapa penelitian mengenai kriptografi dan proses

enkripsi/dekripsi dengan algoritma AES, dan bahasa pemrograman yang digunakan. Selain itu, peneliti juga dapat mengetahui hasil penelitian yang telah diperoleh dan kekurangan dari penelitian tersebut. Kemudian mencari beberapa sumber mengenai metode algoritma yang akan digunakan serta software yang diperlukan nantinya.

1.4.4. Alat Yang Digunakan

Bahan/alat yang digunakan dalam proses pembuatan program ini, terdiri dari sebagai berikut :

a. Perangkat Keras

- Processor Intel® Core™ i3-3217U CPU @ 1.80GHz × 4
- Memory RAM 4 GB
- Harddisk 500 GB

b. Perangkat Lunak

- Sistem Operasi Windows 8
- Microsoft Office Word sebagai pengolahan kata
- Bahasa pemrograman JAVA

1.5. Objek dan Waktu Penelitian

1.5.1. Objek Penelitian

Objek yang diteliti dalam enkripsi file dokumen menggunakan algoritma AES yaitu input dan output dari algoritma AES. Jenis file dokumen yang digunakan dalam penelitian ini berupa file dengan ekstensi : doc, docx, xls, xlsx, pdf, ppt, pptx.

1.5.2. Waktu Penelitian

Waktu dalam penelitian dimulai dari bulan April 2015 sampai bulan Juli 2015.

1.6. Jadwal Kegiatan Penelitian

Tabel 1.1 Jadwal Penelitan

Uraian Kegiatan	2015															
	April				Mei				Juni				Juli			
Persiapan Penelitian																
Analisa Sistem																
Perancangan Sistem																
Implementasi																
Pengujian Sistem																
Penyusunan Laporan																