BAB I
PENDAHULUAN

1.1 Latar Belakang

Ilmu teknologi yang semakin berkembang dan diperbaharui secara bertahap khususnya dalam bidang komputer, sangat membantu manusia dalam mendapatkan informasi. Perkembangan ilmu teknologi bidang komputer dapat dilihat dari semakin canggihnya perangkat keras komputer maupun perangkat lunak. Perkembangan itu juga berpengaruh terhadap keamanan penggunaan komputer maupun layanan publik yang semakin meningkatkan keamanan dalam pengambilan informasi.

Dalam penggunaan teknologi sehari-hari, manusia tidak terlepas dari yang namanya internet sebagai kebutuhan untuk saling bertukar informasi. Salah satu informasi yang sering dicari ataupun dikirim adalah dokumen. Di dalam dokumen banyak mengandung informasi-informasi penting di dalamnya. Keamanan dokumen tentu menjadi sangat penting agar tidak adanya pihak-pihak yang tidak berwenang meretas atau memanipulasi informasi dari dokumen tersebut. Ada cara untuk mengamankan suatu informasi agar informasi itu tidak bocor kepada pihak yang tidak berwenang, yaitu dengan menggunakan kriptografi.

Dalam kriptografi terdapat banyak algoritma, salah satunya adalah algoritma AES (Advanced Encryption Standard). Algoritma AES memiliki panjang blok 128 bit dan mampu mendukung panjang kunci 128, 192, dan 256 bit. Algoritma AES digunakan untuk mengenkripsi dan deskripsi informasi, yang menggunakan proses yang berulang yang disebut ronde. Selain itu AES lebih efisien dari segi biaya dan lebih mudah diimplementasikan pada memori berukuran kecil.

Berdasarkan penguraian sebelumnya untuk mengatasi permasalahan diatas, perlu dibangun sebuah aplikasi kriptografi dengan menggunakan metode AES (Advanced Encryption Standard) untuk mengenkripsi dan juga dapat mendekripsi file dokumen agar dapat mengurangi ataupun menghindari tercurinya informasi-informasi penting yang ada didalamnya.

Dengan mempertimbangkan semua hal di atas, penulis membuat laporan akhir yang berjudul "**APLIKASI SISTEM KEAMANAN DATA DENGAN METODE AES BERBASIS WEB**".

1.2 Rumusan Masalah

Adapun rumusan masalah berdasarkan uraian latar belakang yang telah dibahas adalah bagaimana cara membuat aplikasi yang dapat mengamankan dan melindungi suatu data maupun informasi penting dari orang yang tidak berhak terhadap informasi tersebut.

1.3 Batasan Masalah

Dalam pembuatan aplikasi ini ruang lingkup atau batasan masalah yang diuraikan sebagai berikut:

1. Menggunakan sistem operasi Microsoft Windows.
2. Menggunakan aplikasi Macromedia Dreamweaver 8.
3. Menggunakan bahasa pemrograman *PHP*.
4. Menggunakan metode AES (*Advance Encryption Standard*).
5. Menggunakan media transmisi nirkabel (*wireless*).

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Tujuan utama yang ingin dicapai dari dibuatnya laporan akhir ini yaitu membangun suatu aplikasi aplikasi sistem keamaanan data dengan menggunakan algoritma AES (Advanced Encryption Standard) berbasis web yang dapat mengamankan data - data penting.

1.4.2 Manfaat

Adapun manfaat dibuatnya laporan akhir ini adalah :

1. Data – data penting lebih terjaga keamanannya.
2. Data – data penting tidak dapat diambil atau diubah oleh orang yang tidak bertanggung jawab.