BAB I

PENDAHULUAN

I.1. Latar Belakang

Perkembangan teknologi komputer dan telekomunikasi dewasa ini telah mengalami kemajuan yang sangat pesat dan sudah menjadi suatu kebutuhan, karena banyak pekerjaan dapat diselesaikan dengan cepat, akurat, dan efisien. Sejalan dengan perkembangan teknologi tersebut, semakin mengubah cara masyarakat dalam berkomunikasi. Dulu komunikasi jarak jauh masih menggunakan cara yang konvensional, yaitu dengan cara saling mengirim surat, tetapi sekarang komunikasi jarak jauh dapat dilakukan dengan mudah dan cepat yaitu dengan adanya teknologi seperti email, SMS (*Short Messaging Service*), dan internet yang merupakan salah satu teknologi telekomunikasi yang paling banyak digunakan. Internet telah membuat komunikasi semakin terbuka dan pertukaran informasi juga semakin cepat melewati batas-batas negara dan budaya.

Namun tidak semua perkembangan teknologi komunikasi memberikan dampak yang positif dan menguntungkan. Salah satu dampak negatif dalam perkembangan teknologi adalah adanya penyadapan data, yang merupakan salah satu masalah yang paling ditakuti oleh para pengguna jaringan komunikasi. Dengan adanya penyadapan data maka aspek keamanan dalam pertukaran informasi dianggap penting, karena suatu komunikasi data jarak jauh belum tentu memiliki jalur transmisi yang aman dari penyadapan sehingga keamanan

informasi menjadi bagian penting dalam dunia informasi itu sendiri. Di dalam dunia informasi terdapat data-data yang tidak terlalu penting jadi jika publik mengetahui data tersebut pemilik data tidak terlalu dirugikan. Tetapi apabila pemilik data adalah pihak militer atau pihak pemerintah, keamanan dalam pertukaran informasi menjadi sangatlah penting karena data yang mereka kirim adalah data-data rahasia yang tidak boleh diketahui oleh publik.

Kriptografi merupakan salah satu solusi atau metode pengamanan data yang tepat untuk menjaga kerahasiaan dan keaslian data, serta dapat meningkatkan aspek keamanan suatu data atau informasi. Metode ini bertujuan agar informasi yang bersifat rahasia dan dikirim melalui suatu jaringan, seperti LAN atau internet, tidak dapat diketahui atau dimanfaatkan oleh orang atau pihak yang tidak berkepentingan. Kriptografi mendukung kebutuhan dua aspek keamanan informasi, yaitu perlindungan terhadap kerahasiaan data informasi dan perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan.

Berdasarkan hal tersebut diatas maka diangkatlah judul ***"Implementasi Algoritma AES256 Untuk Pengamanan File Pada Aplikasi Manajemen Kearsipan Berbasis Web Mobile".*** Untuk mengetahui apakah suatu algoritma kriptografi dapat mengamankan data dengan baik dapat dilihat dari segi lamanya waktu proses pembobolan untuk memecahkan data yang telah disandikan.

Seiring dengan perkembangan teknologi komputer yang semakin canggih, maka dunia teknologi informasi membutuhkan algoritma kriptografi yang lebih kuat dan aman. Saat ini, AES (*Advanced Encryption Standard*)

merupakan algoritma *cipher* yang cukup aman untuk melindungi data atau informasi yang bersifat rahasia. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (*National Institute of Standard and Technology*) sebagai pengganti algoritma DES (*Data Encryption Standard*) yang sudah berakhir masa penggunaannya. Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit.

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Berikut adalah merupakan hasil identifikasi masalh yang diperoleh dari hasil pengamatan yang telah dilakukan :

1. Banyak orang-orang yang belum menggunakan aplikasi untuk melakukan pengamanan berkas-berkas penting mereka sendiri.
2. Tidak ada penerapan kriptografi proses penyimpanan berkas, sehingga semua *file* tersimpan dalam format yang mudah dibaca.
3. Belum ada penerapan algoritma AES dalam pengamanan *file*.

I.2.2. Perumusan Masalah

Yang menjadi rumusan masalah dari penelitian ini adalah sebagai berikut :

1. Bagaimana melakukan pengamanan dokumen atau *file* agar tidak mudah diketahui oleh pihak lain yang tidak berkepentingan?

2. Bagaimana menerapkan algoritma AES256 pada sebuah aplikasi manajemen kearsipan?
3. Bagaimana merancang aplikasi kriptografi berbasis web yang dapat melakukan penyandian terhadapan *file*?

I.2.3. Batasan Masalah

Adapun yang menjadi batasan masalah didalam penelitian ini adalah sebagai berikut :

1. Aplikasi akan dirancangan dalam format web mobile, sehingga memiliki tampilan yang *responsive*.
2. Aplikasi yang dirancang akan menggunakan bahasa pemrograman PHP dan HTML 5.
3. Aplikasi yang dirancang tidak menggunakan database, sehingga *file* word ,excel maupun pdf yang telah di enkripsi akan langsung disimpan pada lokasi yang telah ditentukan.

I.3. Tujuan dan Manfaat Penelitian

I.3.1. Tujuan Penelitian

Adapun yang menjadi tujuan dalam penelitian ini adalah :

1. Untuk melakukan pengamanan dokumen dengan penerapan kriptografi.
2. Untuk merancang sebuah Aplikasi kriptografi yang dikhususkan untuk melakukan penyandian terhadap dokumen digital sebelum dilakukan proses pengiriman dokumen dengan menggunakan email.

3. Untuk menerapkan Algoritma AES256 dalam sebuah aplikasi pengamanan dokumen berbentuk word,excel dan pdf.

I.3.2. Manfaat Penelitian

Adapun yang menjadi manfaat dari penelitian ini adalah :

1. Memberi kemudahan dalam melakukan penyandian dokumen penting yang bersifat rahasia.
2. Memberi pemahaman bagaimana proses enkripsi dan deskripsi bekerja dalam sebuah proses penyandian dokumen.
3. Memberi pemahaman bagaimana mengimplementasikan Algoritma AES256 dalam melakukan proses enkripsi dan dekripsi terhadap sebuah dokumen.

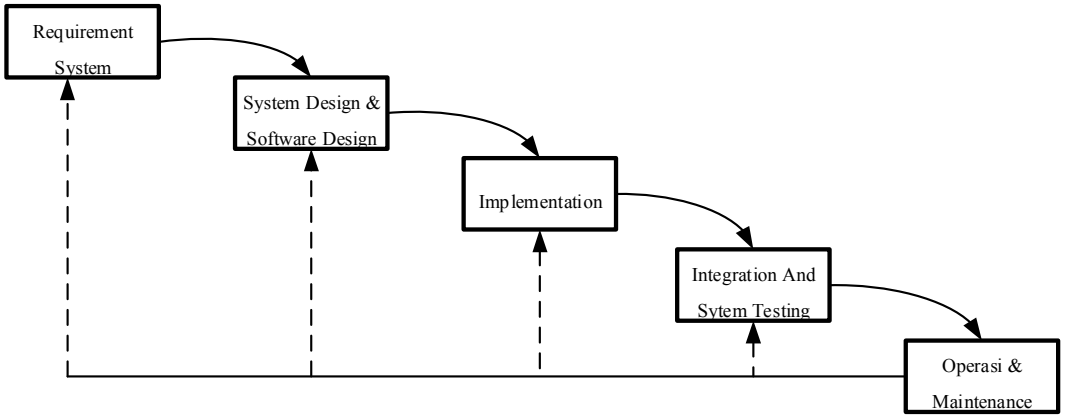
I.3.3. Kontribusi Penilitian

Adapun kontribusi penilitian yang diperoleh dari penelitian ini adalah sebagai berikut :

1. Pemahaman mengenai bagaimana memberikan pengamanan terhadap berkas dokumen word,excel,pdf sehingga isi dari dokumen yang tersimpan tidak mudah diketahui isi dari dokumen.
2. Sebagai referensi untuk penelitian selanjutnya mengenai cara kerja algoritma AES256 dalam melakukan proses enkripsi dan deskripsi pada sebuah dokumen digital.

I.4. Metodologi Penelitian

Adapun prosedur penelitian dan pembangunan aplikasi yang lakukan adalah menggunakan metode *waterfall* seperti yang terlihat pada gambar berikut :



Gambar III.1. Prosedur Perancangan (Metode Waterfall)

Adapun tahap-tahap metode pengembangan dalam perancangan aplikasi ini diantara lain adalah sebagai berikut :

1. *Requirement System*, pada tahap ini dilakukan pengumpulan kebuthan sistem secara lengkap, kemudian dilakukan analisis dan melakukan pendefinisian terhadap kebutuhan yang harus dipenuhi oleh aplikasi yang akan dibangun. Adapun hal-hal yang harus dipenuhi pada aplikasi yang akan dibangun adalah memiliki kemampuan untuk melakukan proses enkripsi dan dekripsi dengan menggunakan algoritma AES256 dan dapat melakukan penyandian terhadap beberapa jenis dokumen digital seperti *MS.Word* dan *MS. Excel.*

2. *System Design* dan *Software Design* , pada tahapan ini akan dilakukan proses desain terhadap *user interface*, basis data, penerapan algoritma dan logika dari aplikasi.
3. *Implementation,* pada bagian ini dilakukan proses implementasi terhadap algoritma AES265 yang akan diterapkan kedalam aplikasi.
4. *Integration & System Testing,* ditahap ini akan lakukan proses ujicoba terhadap aplikasi yang telah selesai dirancang, hal ini dilakukan untuk mengetahui apakah aplikasi sudah berjalan sesuai dengan alur kerja yang telah ditetapak ataukah masih terdapat kesalahan-kesalahan yang mengakibatkan aplikasi tidak dapat berjalan dengan baik.
5. *Operation & Maintenance,* Tahapan ini adalah merupakan tahapan akhir dari seluruh rangkaian kegiatan perancangan aplikasi, dimana dalam tahap ini aplikasi dianggap sudah selesai secara keseluruhan dan sudah dapat beroperasi dengan baik pada perangkat desktop maupun mobile.

I.5. Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini menjelaskan tentang Latar Belakang, Ruang Lingkup Permasalahan yang meliputi: Identifikasi Masalah, Perumusan Masalah serta Batasan Masalah, Tujuan Penelitian, Manfaat Penelitian, Metodologi Penelitian, Kontribusi Penelitian dan Sistematika Penulisan.

BAB II LANDASAN TEORI

Bab ini berisikan tentang teori-teori yang berkaitan langsung dengan permasalahan yang dibahas dan memberikan pemahaman serta menyampaikan informasi yang berkaitan dengan aplikasi yang akan dibuat.

BAB III ANALISIS DAN DESAIN SISTEM

Bab ini berisikan tentang Analisis Masalah, Metode Yang Digunakan (jika ada), Perancangan Desain Sistem meliputi: *Use Case* Diagram, *Class* Diagram, *Activity* Diagram, *Sequence* Diagram, Desain Database meliputi: Normalisasi, Desain Tabel.

BAB IV HASIL DAN UJI COBA

Bab ini berisikan tentang tampilan hasil sistem/perangkat lunak yang telah selesai dibangun dengan implementasi rancangan sistem baru, yang meliputi Sekenario Pengujian, serta Hasil.

BAB V KESIMPULAN DAN SARAN

Bab ini berisikan tentang kesimpulan dan saran yang berkaitan dengan analisa dan optimalisasi sistem berdasarkan yang telah diuraikan pada bab-bab sebelumnya.