BAB I

PENDAHULUAN

I.1 Latar Belakang

Teknologi komputer sangat dibutuhkan oleh kehidupan manusia terutama personal maupun kelompok (organisasi). Kelompok (organisasi) tersebut sangat membutuhkan adanya komputerisasi dalam setiap kegiatannya. Dari hal penggunaan komputerisasi tersebut, maka dibuatlah sebuah keamanan bagi seluruh aset-asetnya, terutama informasi-informasi dan data-data penting demi menjaga kerahasiaan informasi data tersebut. Dari keamanan data tersebut menimbulkan tuntutan akan tersedianya suatu sistem pengamanan data yang lebih baik agar dapat mengamankan data dari berbagai ancaman yang mungkin timbul. Ini merupakan latar belakang berkembangnya sistem keamanan data yang berfungsi untuk melindungi data yang ditransmisikan atau dikirimkan melalui suatu jaringan komunikasi.

Kerahasiaan dari data atau informasi merupakan informasi yang sangat penting dalam suatu organisasi ataupun suatu perusahaan yang merupakan suatu kelengkapan pelayanan. Dan pada zaman teknologi ini merupakan suatu zaman yang dimana yang menggunakan suatu jaringan komputer yang dimana sutu pihak yang tidak bertanggung jawab dapat mengakses suatu akses jaringan tersebut, Hal tersebut dapat mengakibatkan proses pengiriman data menjadi tidak aman karena dimanfaatkan oleh pihak lain yang tidak bertanggung jawab untuk mengambil data maupun informasi yang bisa merugikan pihak tertentu. Salah satu cara untuk

menjaga keamanan dan kerahasiaaan suatu data tersebut ialah dengan menggunakan metode kriptografi Dalam Bidang Kriptografi terdapat dua konsep yang sangat penting yaitu enkripsi dan deskripsi, Proses pengiriman pesan akan melalui proses enkripsi untuk mengubah teks asli (plaintext) menjadi teks sandi (ciphertext) sehingga tidak dapat dibaca atau dimengerti oleh orang lain dan kerahasiaan data dan Integritas Data tersebut agar tetap aman. maka dibutuhkan sebuah algortima yang dapat memproteksi file dan folder dokumen adalah Dengan Metode keamanan yang tepat dalam permasalahan ini ialah dengan metode Algoritma kriptografi AES (*Advanced Encryption Standard*). untuk enkripsi dan dekripsi data Algoritma *Advanced Encryption Standard* (AES) dipilih karena memiliki suatu tingkat keamanan pertukaran informasi yang cukup bagus, dan pada penelitian ini diuji coba file dan folder dokumen untuk melihat kecepatan waktu yang dibutuhkan selama proses enkripsi dan dekripsi.

Dalam hal ini juga ditambahkan sebuah sistem pendukung pada pengamanan data setelah melakukan teknik kriptografi dalam menjaga keamanan data informasi tersebut yaitu dengan teknik penyembunyian data atau disebut steganografi. Steganografi merupakan seni dan ilmu untuk menyembunyikan pesan dalam sebuah media pesan. Kerahasiaan pesan yang ingin disampaikan merupakan faktor utama dalam steganografi. Dengan demikian, metode *AES* diharapkan akan membuat pengamanan isi data file dan folder memiliki tingkat keamanan yang lebih tinggi khususnya untuk data yang bersifat rahasia pada Kantor KEJATISU sehingga data asli tersebut tidak dapat dibaca dan diterjemahkan oleh orang yang tidak bertanggung jawab

Berdasarkan uraian permasalahan tersebut maka penulis ingin mengambil penelitian dengan judul **"Implementasi Metode AES Pada Pengamanan Data File dan Folder Dokumen Pada KEJATISU".**

I.2 Ruang Lingkup Permasalahan

I.2.1 Identifikasi Masalah

Berdasarkan latar belakang tersebut, penulis mengidentifikasi masalah sebagai berikut :

1. Pengamanan yang kurang optimal dapat mengakibatkan resiko kebocoran data
2. Data pada Kejaksaan Tinggi Sumatera Utara beresiko diakses oleh pihak yang tidak bertanggungjawab

I.2.2 Rumusan Masalah

Rumusan masalah dalam pembahasan dan permasalahan yang akan dihadapi dalam perancangan aplikasi ini :

1. Bagaimana meningkatkan metode pengamanan data yang optimal;
2. Bagaimana melindungi data pada Kejaksaan Tinggi Sumatera Utara melalui sebuah aplikasi enkripsi dan deskripsi data *file* dan *folder* dengan menggunakan Metode AES ?;
3. Bagaimana mengimplementasikan aplikasi *kriptografi* data *file* dan *folder* dengan *Algoritma AES* untuk pengamanan data *file* dan *folder* kedalam pemrograman *PHP*?.

I.2.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini agar tidak menyimpang dari tujuan semula adalah :

1. Studi kasus yang akan diuji cobakan dalam penelitian ini adalah sistem penguncian data *file dan folder* dengan menggunakan kata kunci;
2. Pengamanan data *file dan Folder ini* menggunakan kriptografi dengan Algoritma *Anvanced Encryption Standard (AES)*;
3. Perancangan sistem yang digunakan dengan menggunakan bahasa pemograman *PHP* dengan *database MySQL;*
4. Pemodelan perancangan menggunakan *Unified Modelling Language (*UML). Untuk menggambarkan arus data serta proses pengolahan data yang ada pada sistem yang akan dibuat.
5. sistem pembangunan aplikasi ini adalah dapat mengamankan file-file yang berbentuk ekstensi : “Word”, “Excel”, “Text”, “PPT”, “Pdf”, “xls”, “pptx”
6. File yang dienkripsi tidak dapat bisa lebih besar dibawah 3 mb
7. Hasil dari enkripsi ini bisa dijamin keamanannya selama *symmetry key* encryption tidak bocor ke pihak yang tidak bertanggung jawab

I.3 Tujuan dan Manfaat

I.3.1 Tujuan Penelitian

Adapun tujuan dari penelitian penulis ini adalah :

1. Menambah Pengetahuan penulis mengenai sebuah system aplikasi Kriptografi dengan Algoritma Kriptografi AES (Advanced Encryption Standard)

2. Untuk membangun aplikasi *kriptografi* Modern dengan *Algoritma AES* dalam mengamankan data *File dan Folder*
3. Untuk membuat aplikasi keamanan data *File dan Folder* yang menerapkan *kriptografi* Berbasis *Web*

I.3.2 Manfaat Penelitian

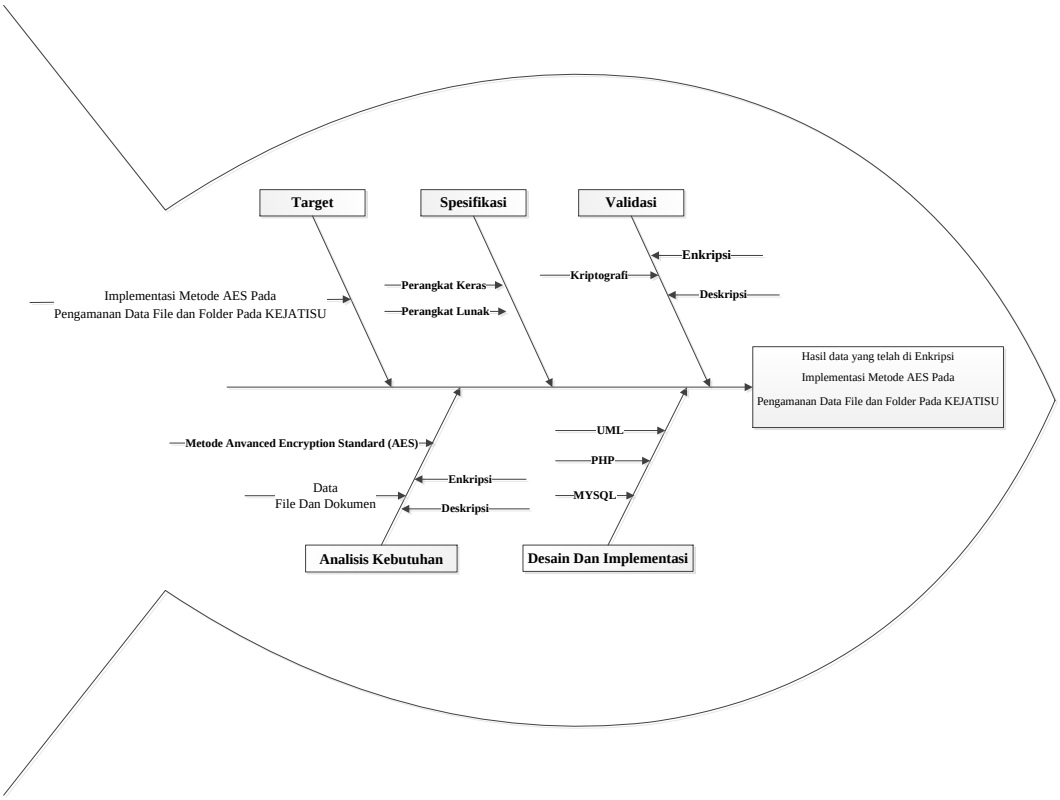
Adapun dilakukannya penelitian ini adalah :

1. Untuk menambah wawasan ataupun pengetahuan kepada pembaca bahwa *kriptografi* dapat digunakan sebagai salah satu cara untuk mengamankan data khususnya *File* maupun folder. Dalam hal ini, penulis berusaha membuat sebuah aplikasi *kriptografi* Modern untuk melakukan Enkripsi dan Dekripsi dengan *Algoritma AES* dalam mengamankan data *File* dan *Folder*.
2. Untuk dapat menambah pengetahuan dan wawasan penulis tentang kriptografi khususnya dalam hal proses enkripsi dan deskripsi didalam pengamanan dan kerahasiaan keamanan data menggunakan kriptografi *Anvanced Encryption Standard* (AES).
3. Melalui penelitian ini, penulis berharap pembaca dapat menerapkan bahkan mengembangkan *Algoritma AES* ini bukan hanya dalam mengamankan data berupa *File* dan *Folder*, tetapi juga dapat mengamankan *file* data dokumen, suara, gambar dan video.

I.4 Metodologi Penelitian

Metode penelitian yang dipakai oleh penulis adalah metode penelitian deskriptif atau disebut juga metode penelitian analitis. Dalam metode penelitian deskriptif ini digunakan teknik-teknik analisis, klasifikasi masalah, *survey*, studi kepustakaan, observasi dan teknik test terhadap masalah-masalah yang berhubungan dengan objek penelitian penulis.

Dalam pengembangan suatu sistem ini peneliti menggunakan model *fishbone* kerena pengaplikasian menggunakan model ini mudah diimplementasikan dimana hal ini menggambarkan pendekatan yang sistematis dan juga berurutan pada pengembangan perangkat lunak. Tahapan metode *fishbone* dapat dilihat pada gambar I.1 di bawah ini.



Gambar I.1 : Model Fishbone

Penjelasan gambar I.1 Perancangan pengamanan data *file* dan folder pada model *fishbone:*

a. Target

Adapun target dari penelitian ini adalah dapat membangun suatu Sistem Keamanan pada file dan folder untuk meningkatkan keamanan pada KEJATISU

b. Analisis Kebutuhan

Dalam tahap ini dilakukan proses enkripsi dan enkripsi pada file dan dokumen pada KEJATISU. Dalam enkripsi dan deskripsi file dan dokumen perlu beberapa pemahaman terkait variable-variabel yang saling berhubungan satu sama lain. Pengimplementasi ini yang tepat dalam pengaman file dan folder pada KEJATISU menggunakan metode *Anvanced Encryption Standard* (AES).

c. Spesifikasi

Spesifikasi kebutuhan perangkat lunak adalah sebuah dokumen yang berisi pernyataan lengkap dari apa yang dapat dilakukan oleh perangkat lunak. Adapun spesifikasi kebutuhan dalam membangun sistem yang akan dirancang adalah sebagai berikut :

1. Spesifikasi Perangkat Keras

   Spesifikasi perangkat keras yang dibutuhkan adalah :

   - Laptop *Intel 2core*
   - RAM 2 *Gigabyte*
   - *Hard disk 500 Gigabyte*

2. Spesifikasi Perangkat Lunak

- Sistem operasi Windows 10
- *PHP* dan *Database MySQL Server*

d. Desain dan Implementasi

Perancangan dapat didefinisikan sebagai proses untuk mengaplikasikan berbagai macam teknik dan prinsip untuk tujuan pendefinisian secara rinci suatu perangkat, proses atau sistem agar dapat direalisasikan dalam suatu bentuk fisik. Perancangan menggunakan model UML untuk menggambarkan sistem. Sedangkan implementasi merupakan tahap pengkodean yang merupakan suatu proses translasi. Rancangan detil ditranslasikan ke dalam suatu bahasa pemrograman. Dalam hal ini implementasi menggunakan bahasa pemrograman *PHP* dan *database MySQL Server*.

e. Validasi

Validasi merupakan proses untuk menunjukkan seberapa besar nilai keakuratan program terhadap kondisi-kondisi saat pemakaian sebenarnya. Proses ini menjalankan skenario berdasarkan data dan lingkungan yang merepresentasikan dunia nyata dengan menggunakan mesin percobaan. Verifikasi program merupakan suatu metode yang digunakan untuk menjamin kebenaran suatu program. Verifikasi program melakukan simbolisasi masukan sehingga jaminan diberikan untuk semua data yang berlaku sebagai masukan.

f. Finalisasi

Pada tahapan ini adalah tahapan hasil dari sistem yang sudah dirancang dan berjalan sesuai rencana.

I.5. Kontribusi Penelitian

Adapun yang menjadi kontribusi penelitian ini pada sistem yang dirancang oleh penulis dapat dilihat sebagai berikut :

1. Diharapkan sistem yang akan dibangun ini, Perusahaan dapat lebih mudah lagi dalam mengamankan sebuah data file dan folder dari orang yang tidak bertanggung jawab.
2. Diharapkan pada penelitian ini dapat menjadi sumbangan pemikiran mengenai perkembangan ilmu pengetahuan dan juga dapat bermanfaat bagi pihak-pihak yang membutuhkan dan tidak menutup kemungkinan untuk mengadakan penyempurnaan terhadap hasil pengamatan ini.
3. Diharapkan pada penelitian ini dapat memberi kemudahan bagi perusahaan dalam mengamankan data yang bersifat penting agar dapat menjaga kerahasiaan pada perusahaan.

I.6. Sistematika Penulisan

Sistematika penulisan skripsi ini dibagi menjadi lima bab yang merangkum tiap tahapan yang penulis lakukan, antara lain :

BAB I : PENDAHULUAN

Bab ini menguraikan tentang latar belakang masalah, ruang lingkup masalah, tujuan dan manfaat skripsi, serta metodologi skripsi.

BAB II : TINJAUAN PUSTAKA

Pada bab ini menguraikan tentang beberapa penjelasan dan pengertian yang berdasarkan dengan judul.

BAB III : ANALISIS DAN DESAIN SISTEM

Pada bab ini berisikan analisa permasalahan dan kebutuhan alat, serta pemodelan sistem secara fungsional.

BAB IV : HASIL DAN UJI COBA

Bab ini berisikan tentang tampilan hasil yang dirancang, pembahasan uji coba dari sistem, dan kelebihan serta kekurangannya.

BAB V : KESIMPULAN DAN SARAN

Bab ini berisikan bagian penutup yang berisi kesimpulan serta saran untuk pengembangan sistem alat selasnjutnya.