BAB I
PENDAHULUAN

I.1. Latar Belakang

Seiring dengan sangat pesatnya perkembangan jaringan data dan kemajuan teknologi informasi khususnya di bidang komputer memungkinkan seseorang untuk berkomunikasi dan bertukar informasi dengan orang lain di dunia maya. Pertukaran informasi di dunia maya atau yang biasa disebut internet. Dalam dunia maya ini bisa mendapat banyak informasi yang kita butuhkan hanya membutuhkan sebuah perangkat yang terhubung ke internet. Informasi yang kita dapatkan bisa bermacam-macam format, diantaranya : *image* (gambar),teks, citra, audio, maupun video. Seiring dengan kemajuan teknologi seperti itu akan menimbulkan beberapa ancaman terhadap informasi yang di dapatkan, hal tersebut membutuhkan sebuah keamanan untuk informasi tersebut.

Pengamanan informasi tersebut sangat dibutuhkan untuk menjaga kerahasiaan dari informasi yang dikeluarkan. Oleh karena itu dibutuhkan sebuah sistem/keamanan data yang dapat mengikuti perkembangan teknologi di dunia maya sehingga data/informasi yang dikirimkan tidak jatuh kepada orang yang tidak berhak atau memodifikasinya. Sekarang ini terdapat sistem/pengamanan data yang biasa dikenal dengan kriptografi. Parameter yang menentukan kunci dekripsi itulah yang harus dirahasiakan. *Image* (gambar) menyajikan informasi secara visual dan informasi yang disajikan secara tekstual. Diantara *file image* yang paling rentan untuk operasi illegal berupa duplikat, modifikasi, bahkan untuk dipalsukan jenis *file image* PNG. Sehingga banyak informasi berupa data *Image* (gambar) yang perlu diamankan dan dijaga kerahasiaanya agar tidak disalah gunakan oleh orang yang tidak berhak untuk

mengetahuinya. Oleh karena itu diperlukan aplikasi yang dapat membantu menjaga kerahasiaan dari data/informasi yang mereka miliki. Untuk menjamin keamanan data berupa *file image* (gambar) jenis PNG yang ditransmisikan, maka *file* dienkripsi dengan AES enkripsi (algoritma enkripsi) menjadi AES image atau gambar yang tidak memiliki arti. Setelah sampai di tujuan, maka AES image didekripsikan kembali menjadi gambar normal yang mudah diterima oleh penerima. Dari sekian banyak jenis kriptografi yang ada, tidak semuanya bisa diterapkan untuk mengenkripsi data *image* (gambar). Namun hal ini bisa di atasi dengan menggunakan metode AES (advanced Encryption Standart. Berdasarkan penjelasan di atas maka penulis tertarik untuk menulis judul **"Impementasi AES (*Advanced Encyrption Standart*) untuk enkripsi dan dekripsi *file image*".**

I.2. Ruang Lingkup Permasalahan

I.2.1. Identifikasi Masalah

Adapun identifikasi masalah dalam penulisan skripsi ini adalah:

1. Pentingnya pengamanan untuk melindungi privasi atau kerahasiaan data.
2. Untuk mengimplementasikan keamanan data berupa *image* menggunakan algoritma AES (*Advanced Encryption Standart*).

I.2.2. Perumusan Masalah

Rumusan masalah yang dapat penulis ambil dari latar belakang yang telah diuraikan tersebut adalah:

1. Apakah dengan mengimpelmentasi metode AES (*Advanced Encryption Standart*) ini akan menghilangkan keaslian *file image*?
2. Bagaimana sistem ini akan bekerja saat proses enkripsi dan dekripsi ?

I.2.3. Batasan Masalah

Adapun batasan masalah dalam mengimplementasikan untuk enkripsi dan dekripsi *file image* adalah sebagai berikut :

1. Aplikasi ini hanya digunakan untuk enkripsi *file* berbasis *image*.
2. Aplikasi ini digunakan untuk *file image* berekstensi PNG.
3. Metode yang digunakan adalah AES (*Advanced Encryption Standart*).

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Berdasarkan perumusan masalah di atas maka tujuan yang ingin dicapai dalam penulisan skripsi ini adalah sebagai berikut :

1. Membuat sebuah aplikasi yang mampu mengamankan *file image* dengan baik.
2. Menghasilkan sebuah sistem keamanan yang dapat berguna bagi orang-orang dalam berkomunikasi (pertukaran informasi)

I.3.2. Manfaat

Manfaat yang diharapkan dari penulisan skripsi ini adalah :

1. Memberikan pengetahuan tentang bagaimana caranya sebuah aplikasi kriptografi dapat mengamankan *file image*.
2. Pengembangan sistem dan aplikasi ini dapat digunakan untuk sistem pengamanan *file* lainnya.
3. Dengan adanya sistem ini dapat membantu dalam ilmu pengetahuan khususnya jaringan dan keamanan informasi.

I.4. Metodologi Penelitian

Untuk memperoleh data-data yang diperlukan dalam penulisan skripsi ini, maka penulis menggunakan beberapa metode, sebagai berikut:

I.4.1. Analisis Tentang Sistem Yang Dirancang

1. Metode Peninjauan Lapangan (*Field Research*)

a. Studi Kepustakaan *(Library Research)*

Penulis melakukan studi pustaka untuk memperoleh data-data yang berhubungan dengan penulisan skripsi.

b. Observasi

Pada tahap ini dilakukan eksplorasi terhadap beberapa perangkat dan konsep yang akan digunakan. Eksplorasi dilakukan pada beberapa perangkat yang akan digunakan untuk membangun aplikasi kriptografi.

c. Studi Literatur

Mencari referensi dan bahan pustaka tentang teori-teori yang berhubungan dengan permasalahan yang akan dikerjakan dalam skripsi ini.

I.4.2. Prosedur Perancangan

Langkah-langkah yang diperlukan untuk mencapai tujuan perancangan, yaitu :

a. Target/Tujuan Penelitian

Target penelitian dilakukan untuk membuat aplikasi enkripsi dan dekripsi *file image* mengamankan supaya orang tidak dapat melihat/membukanya.

b. Analisis Kebutuhan

Untuk mencapai penyelesaian dalam merancang dan mengimplementasikan untuk enkripsi dan dekripsi *file image*, kebutuhan pokok yang diperlukan

adalah memahaminya tentang algoritma dan kriptografi serta kode programnya.

c. Spesifikasi Dan Desain

Dalam membuat skripsi ini, spesifikasi dan desain dari perangkat keras (*Hardware*) dan perangkat lunak (*Software*) yang digunakan adalah sebagai berikut:

1. Perangkat Keras (*Hardware*)

   Perangkat keras yang digunakan antara lain :

   a) Laptop dengan spesifikasi *Intel Core i3 ; Processor 2.35 GHz, Hard disk :* 200 *GB, RAM 2 GB, Monitor LCD 14“, Keyboard* dan *Mouse.*

2. Perangkat lunak (*Software*)

   Software yang digunakan untuk membuat skripsi ini antara lain :

   a) Sistem operasi *Windows* 7

   b) *Microsoft Visual Studio 2010*

d. Implementasi dan Verifikasi

Setelah sistem selesai dirancang, lalu pada tahap ini alat akan dirakit sehingga bisa untuk diuji atau disimulasikan untuk mengetahui hasil kerja dari alat ini.

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 perangkat lunak yang telah selesai kedalam komputer pengguna.

f. Finalisasi

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

1.4.3. Pengujian / Uji coba sistem

Tahap ini merupakan tahap untuk indentifikasi kesalahan yang timbul setelah melakukan pengujian pada sistem perancangan yang telah dibuat. Setelah proses enkripsi dan dekripsi selesai maka akan dilakukan proses pengujian terhadap program yang dihasilkan untuk mengetahui apakah program sudah berjalan dengan benar dan sesuai dengan perancangan yang dilakukan dan hasil/*output* sudah tepat dan akurat.

I.5. Keaslian Penelitian

Adapun penelitian yang pernah dilakukan adalah mengimplementasikan algoritma AES (*Advanced Encryption Standart)* untuk enkripsi dan dekripsi *file image.* Untuk lebih jelas penbandingan-perbandingan dapat dilihat pada tabel I.1 dibawah ini :

Tabel I.1. Tabel keaslihan penelitian

No	Nama Peneliti	Judul	Sistem Yang Dihasilkan
1	Didi Surian, 2006	Algoritma Kriptografi AES Rijandael	Perancangan *file* dekripsi dapat kembali seperti ekstensi *file* sumber karena sistem melakukan proses enkripsi.
2	Mariana,2009	Perbandingan Algoritma Aes Dengan Algoritma Xts-Aes Untuk Enkripsi Dan Dekripsi Teks Sms Berbasis Java Me	Perancangan *file* perbandingan algoritma AES ini mengenkripsi sebuah *teks* SMS menjadi deskripsi.
3	Hendrik Saragih,2015	Implementasi AES untuk enkripsi dan dekripsi *file image*	Perancangan file gambar dengan algoritma AES ini menggunakan gambar untuk di enkripsi dan dekripsi.

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 menjelaskan tentang Latar Belakang, Ruang Lingkup Permasalahan, Tujuan dan Manfaat, Metodologi Penelitian dan Sistematika Penulisan.

BAB II : LANDASAN TEORI

Pada bab ini dibahas mengenai teori-teori yang mendukung pembahasan bab selanjutnya, implementasi untuk enkripsi dan dekripsi *file image* code program yang mendukungnya.

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 yang dirancang, dan kelebihan sistem yang dirancang serta kekurangannya.

BAB V : KESIMPULAN DAN SARAN

Bab ini berisikan bagian penutup yang berisi kesimpulan untuk pemakai dari terbentuknya perancangan sistem simulasi serta saran untuk pengembangan sistem alat selanjutnya.