BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi di era globalisasi saat ini telah mengalami kemajuan yang pesat. Bidang informasi pun tidak luput dari pengaruh perkembangan saat ini. Kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi baik itu komersial, lembaga pemerintahan, maupun individual (pribadi) [1]. Selaras dengan kemajuan teknologi, tindak kriminal yang marak terjadi adalah *cyber crime* atau kejahatan melalui internet. Beragam kejahatan yang terjadi di dunia maya, seperti yang kita kenal yaitu *hacker, cracker, phreaker* dan sebagainya. Data yang berada di internet pun bermacam-macam kepentingannya, mulai dari sesuatu yang disebarluaskan hingga informasi penting yang hanya orang tertentu yang boleh mengaksesnya, oleh sebab itu keamanan dan kerahasiaan data menjadi aspek penting dalam pertukaran dan pengambilan informasi pada saat ini [2].

Pengamanan data sangat dibutuhkan dalam pertukaran informasi. Informasi yang diambil ataupun ditukar mempunyai bermacam-macam jenis, seperti teks, audio, video maupun gambar. Perkembangan teknologi juga mempengaruhi pertukaran informasi saat yang dapat terjadi dengan sangat cepat dan singkat sehingga sangat rentan terjadi pencurian informasi dan manipulasi data yang kemudian disebarluaskan kembali.

Data - data yang ada di dalam komputer dapat dengan mudah dimanipulasi, jika hanya mengandalkan keamanan dasar dari komputer itu sendiri. Karena itu diperlukan sebuah metode khusus dalam pengamanannya agar dapat meningkatkan kerahasiaan informasinya.

Metode dalam pengamanan data yang dibutuhkan adalah kriptografi. Metode ini sangat sering digunakan dalam pengamanan data yang penting bagi suatu kegiatan tertentu. Seperti halnya pada algoritma kriptografi yang merupakan seni dalam merahasiakan pesan [1]. Dengan pola-pola tertentu, perhitungan-perhitungan matematika yang akurat, dan perkembangannya yang pesat, membuat kriptografi menjadi "seni" utama dalam pengamanan data pada saat ini. Algoritma yang digunakan pada penelitian ini adalah AES (*Advanced Encryption Standard*).

AES atau sering disebut Rijndael ini merupakan standard kriptografi yang ditetapkan oleh NIST (*National Institute of Standards and Technology*) sebagai pengganti DES, karena algoritma DES mempunyai kelemahan yang cukup fatal. Sehingga pada bulan Oktober 2000, NIST menetapkan AES sebagai algoritma standard kriptografi yang bertahan hingga saat ini [2].

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dikemukakan, maka permasalahan yang dapat dirumuskan adalah sebagai berikut :

1. Bagaimana proses algoritma *Advanced Encryption Standard* dalam bahasa pemrograman yang didukung oleh *pc desktop* berbasis Java ?

2. Bagaimana hasil enkripsi dan dekripsi data dari algoritma *Advanced Encryption Standard* ?

1.3 Batasan Masalah

1. Aplikasi ini berjalan pada *notebook* dan *pc desktop* dengan sistem operasi Windows.
2. Pengguna dapat menjalankan aplikasi ini pada komputer dengan sistem operasi minimal Windows XP.
3. Penelitian ini mempunyai batasan pada *Advanced Encryption Standard,* serta hanya melakukan uji coba pada *file* berformat *.docx, *.txt, *.mp4. Penelitian akan diimplementasikan pada aplikasi berbasis Java.

1.4 Maksud dan Tujuan Penelitian

Tujuan dari penelitian ini adalah mengamankan data-data dengan menggunakan algoritma *Advanced Encryption Standard* (AES), serta mempertahankan kualitas data yang di amankan, sehingga data dari pengguna tidak dapat dimanipulasi oleh orang tidak bertanggung jawab.

1.5 Metodologi Penelitian

Metodologi yang digunakan untuk menyelesaikan tugas akhir ini adalah sebagai berikut :

1.5.1 Metode Pengumpulan Data

Dalam penyusunan laporan dan penelitian ini dibutuhkan data maupun informasi yang *real* sesuai penelitian yang dilaksanakan. Data yang digunakan adalah *.docx, *.mp4, *.txt. Data yang diperoleh, yang disesuaikan dengan banyaknya jenis *file* yang digunakan. Sedangkan dalam pengumpulan datanya, penulis mempelajari sumber pustaka yang dapat dijadikan rujukan dari buku atau literatur – literatur dan juga melakukan pengumpulan data berupa rujukan yang bersumber dari internet dan lingkungan sekitar.

1.5.2 Metode *Testing*

Dalam penelitian ini metode pengujian yang digunakan ada 2 yaitu metode *White - Box Testing* dan *Black - Box Testing*.

1.5.2.1 *White - Box Testing*

White - Box Testing adalah cara pengujian dengan melihat kedalam modul ataupun *project* untuk meneliti kode-kode program dan untuk menganalisis apakah ada kesalahan dalam program tersebut atau tidak. Salah satu contoh penerapan *white - box testing* adalah disaat menjalankan *class* apakah dapat berjalan dengan baik atau tidak. Jika terjadi kesalahan dalam penulisan kode program, maka akan keluar pesan *error*.

1.5.2.2 *Black Box Testing*

Black Box Testing, yaitu metode uji coba yang memfokuskan pada keperluan fungsionalitas aplikasi yang dibuat. Karena itu uji coba *Black Box* memungkinkan pengembangan aplikasi ini untuk membuat himpunan kondisi *input* yang akan melatih seluruh syarat - syarat fungsional suatu program. Metode pengujian *Black Box* berusaha untuk menemukan kesalahan dalam beberapa kategori, diantaranya: fungsi-fungsi yang salah atau hilang, kesalahan dalam struktur data atau akses *database* eksternal, kesalahan performa, kesalahan inisialisasi, dan terminasi.

1.6 Sistematika Penulisan

Sistematika Laporan disusun menggunakan dasar – dasar penulisan karya ilmiah. Metode ini dilakukan supaya dalam penyusunan laporan skripsi menjadi lebih rapih dan mudah dipahami. Sistematika penulisan pada skripsi adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi tentang latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, metode penelitian dan sistematika penulisan laporan penelitian.

BAB II LANDASAN TEORI

Bab ini akan dijelaskan tentang landasan teori yang mendasari pembahasan secara detile berupa definisi – definisi yang berkaitan langsung dengan penelitian maupun komponen – komponen yang lain yang digunakan pada penelitian.

BAB III ANALISIS DAN PERANCANGAN

Bab ini menguraikan tentang gambaran penelitian, analisis semua masalah maupun peluang yang ada, apabila disitu terdapat masalah maka akan dicari solusinya dan diselesaikan melalui penelitian, dan apabila ditemukan peluang maka peluang tersebut akan diraih menggunakan penelitian ini.

BAB IV HASIL DAN PEMBAHASAN

Bab ini membahas mengenai gambaran secara umum tentang aplikasi, prosedur operasional, analisis sistem, implementasi desain, hasil *testing*, spesifikasi *hardware* maupun *software* yang digunakan untuk membuat dan menjalankan sistem ini.

BAB V PENUTUP

Bab ini berisi kesimpulan dari keseluruhan isi laporan dan saran – saran yang membangun untuk menambah kesempurnaan aplikasi.