BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi jaringan komputer menyebabkan terkaitnya satu komputer dengan komputer yang lainnya. Hal ini membuka banyak peluang dalam pengembangan aplikasi komputer tetapi juga membuat peluang adanya ancaman terhadap pengubahan dan pencurian data (Rifki Sadikin, 2012).

Seiring dengan perkembangan dunia teknologi saat ini, hampir semua hal selalu disajikan dalam bentuk digital dan terkomputerisasi. Seperti halnya buku dan perpustakaan online. Bahkan layanan Bank pun ada di internet yang sebenarnya sangat rawan terjadi tindak kejahatan dunia maya (*Cyber Crime*). Maka dari itu, setiap orang berupaya agar setiap data yang beredar di dunia maya ataupun dalam suatu jaringan tertentu tetap terjaga kerahasiaannya. Banyak cara yang dilakukan orang-orang untuk mengamankan data, salah satu caranya adalah dengan membuat data informasi tersebut tidak dapat dipahami orang lain. Dimulai dari sinilah muncul ilmu baru yang disebut ilmu Kriptografi. Kriptogafi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Dony Ariyus, 2008).

Pada era teknologi sekarang, enkripsi adalah salah satu cara yang paling baik untuk mengamankan pesan. Enkripsi sendiri adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca atau dimengerti.

Setelah data terenkripsi, maka cara agar dapat membaca informasi atau pesan tersebut adalah dengan cara dekripsi, kebalikan dari enkripsi. Dekripsi adalah proses untuk membaca informasi yang sudah dienkripsi.

Ada banyak algoritma kriptografi yang digunakan untuk mengenkripsi pesan, mulai dari yang paling klasik sampai yang paling modern. Semua memiliki karakteristrik sendiri - sendiri. Mengenkripsi sebuah pesan menggunakan algoritma kriptografi sebenarnya bukanlah perkara yang mudah. Karena algoritma kriptografi modern hampir semuanya menggunakan model bit. Oleh karena itu dibutuhkan ketelitian yang luar biasa untuk bisa mengenkripsi sebuah pesan menggunakan algoritma yang bermodelkan bit. Salah satu algoritma yang menggunakan model bit adalah algoritma *Data Encryption Standard (DES)*.

Data Encryption Standard (DES) merupakan salah satu algoritma kriptografi yang cukup sulit dan lama dalam penerapannya. Butuh berkali-kali proses permutasi untuk setiap kunci dan *plainteks* (pesan). Dan apabila proses pengenkripsian dan pendekripsian ini dilakukan secara manual, yang artinya dilakukan tanpa bantuan komputer, maka tingkat kesalahannya luar biasa besar. Salah satu angka saja akan membuat hasil yang sangat berbeda. Bahkan bisa berakibat gagalnya pesan untuk dibaca.

Melihat permasalahan tersebut, tentunya teknologi komputer saat ini dapat kita gunakan untuk pengembangan aplikasi enkripsi dan dekripsi pesan, diharapkan aplikasi enkripsi dan dekripsi pesan ini dapat membatu kita agar lebih mudah mengenkripsi dan mendekripsikan pesan menggunakan algoritma DES. Karena dalam apliksi enkripsi dan dekripsi yang ada sekarang ini, masih terbilang

susah digunakan dan tidak ada penjelasan untuk setiap langkah enkripsi dan dekripsinya.

Berdasarkan latar belakang yang telah dipaparkan inilah penulis mencoba membuat aplikasi yang dapat memudahkan proses enkripsi dan dekripsi pesan menggunakan algoritma DES dan dari penelitian ini penulis mengangkat judul **"Aplikasi Dekripsi dan Enkripsi Pesan dengan Algoritma Data Encryption Standard (DES) berbasis Java".**

1.2. Rumusan Masalah

Memperhatikan latar belakang diatas maka penulis menetapkan rumusan masalah sebagai berikut :

1. Bagaimana alur algoritma kriptografi *Data Encryption Standard (DES)* apabila dikerjakan secara manual (tanpa bantuan *computer*)?
2. Bagaimana melakukan enkripsi dan dekripsi pesan dengan metode DES secara bertahap menggunakan aplikasi yang dibuat?
3. Bagaimana melakukan enkripsi dan dekripsi pesan dengan metode DES secara langsung (*otomastis*) menggunakan aplikasi yang dibuat?
4. Bagaimana melakukan enkripsi dan dekripsi pesan yang berupa kalimat panjang dengan metode DES secara langsung (*otomastis*) menggunakan aplikasi yang dibuat?

1.3. Batasan Masalah

Agar pembahasan lebih terarah, maka penulis memberikan batasan - batasan pembahasan masalah, yaitu :

1. Aplikasi dekripsi dan enkripsi pesan ini dibuat menggunakan bahasa pemrograman Java.
2. Algoritma kriptografi yang digunakan untuk proses enkripsi dan dekripsi pada aplikasi ini adalah algoritma *Data Encryption Standard (DES)*.
3. Hanya sebuah pesan teks tertulis yang akan dienkripsi dan didekripsi kan.
4. Menggunakan kunci kriptografi simetri berupa teks.

1.4. Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah :

1. Melakukan enkripsi dan dekripsi kata atau pesan menggunakan algoritma *Data Encryption Standard (DES)* yang dilakukan secara manual (tanpa bantuan komputer).
2. Membuat aplikasi dekripsi dan enkripsi kata atau pesan menggunakan algoritma *Data Encryption Standard (DES)* berbasis Java.

1.5. Manfaat Penelitian

Dari penelitian ini diharapkan dapat memberikan manfaat yaitu:

1. Memudahkan proses enkripsi dan dekripsi pesan menggunakan algoritma *Data Encryption Standard (DES)*.

2. Dapat menjadi sarana pembelajaran tentang cara pengenkripsian dan pendekripsian pesan menggunakan algoritma *Data Encryption Standard (DES)*.

1.6. Sistematika Penulisan

Dalam penyusunan skripsi ini akan diuraikan dalam bentuk bab, dan masing-masing bab akan dipaparkan dalam beberapa sub bab, diantaranya :

BAB I. Pendahuluan

Dalam bab ini akan menjelaskan latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, sistematika penulisan skripsi dan rencana kegiatan.

BAB II. Landasan Teori dan Tinjauan Umum

Dalam bab ini akan membahas dan menjelaskan mengenai dasar teoritis yang menjadi landasan dan mendukung pelaksanaan penulisan skripsi.

BAB III. Analisis dan Perancangan Sistem

Dalam bab ini akan membahas tentang analisis metode enkripsi dan dekripsi pesan menggunakan algoritma *Data Encryption Standard (DES)* dan perancangan aplikasi *user interface*-nya menggunakan bahasa pemrograman Java.

BAB IV. Implementasi dan Pembahasan

Pada bab ini penulis memaparkan hasil-hasil dari tahapan penelitian, dari tahap analisis, desain, implementasi desain, hasil

uji coba dan implementasinya, serta analisa cara bekerja dari program yang telah dibuat.

BAB V. Penutup

Dalam bab ini akan disampaikan kesimpulan dan saran dari keseluruhan bahasa.