BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemajuan teknologi komputer terbukti telah membantu manusia dalam berbagai aspek kehidupan dari hal – hal yang sederhana sampai kepada masalah – masalah yang cukup rumit. Contoh dari kemajuan teknologi komputer adalah kecepatan komputer dalam penyampaian, pertukaran, dan penyimpanan data serta pengamanannya. Bersamaan dengan meningkatnya teknologi informasi, maka meningkat pula kejahatan – kejahatan yang berhubungan dengan sistem informasi. Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting dari suatu sistem informasi, karena suatu informasi akan tidak berguna apabila informasi tersebut tidak autentik lagi sebelum sampai kepada penerima data yang sebenarnya.

Sayang sekali masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem jaringan komunikasi data. Seringkali masalah keamanan berada di urutan kedua, atau bahkan di urutan terakhir dalam daftar hal - hal yang dianggap penting. Apabila menganggu jalannya sistem, seringkali keamanan dikurangi atau ditiadakan. Dalam teknologi informasi, telah dikembangkan berbagai cara untuk mengatasi keamanan data salah satunya adalah dengan algoritma kriptografi yang menggunakan transformasi data sehingga data yang dihasilkan tidak dapat dimengerti oleh pihak ketiga. Transformasi dapat menjadi solusi dalam mengatasi masalah privasi (*privacy*) dan autentikasi (*authentication*) data.

Kriptografi merupakan dasar untuk memahami keamanan pada komputer, khususnya keamanan jaringan. Kriptografi sudah digunakan hampir di segala bidang yang terkait dengan penggunaan jaringan komputer.

Bahkan kehidupan kita saat ini dilingkupi oleh kriptografi antara lain mulai dari transaksi di mesin ATM (*Automatic Teller Machine*), transaksi di bank, transaksi dengan kartu kredit, percakapan melalui telepon genggam, mengakses internet, sampai mengaktifkan peluru kendali pun menggunakan kriptografi. Kriptografi telah menjadi bagian penting dalam dunia teknologi informasi saat ini. Hampir semua penerapan teknologi informasi menggunakan kriptografi sebagai alat untuk menjamin keamanan dan kerahasiaan informasi. Karena itu, kriptografi menjadi ilmu yang berkembang pesat. Untuk memenuhi hal tersebut, dilakukan proses penyandian (enkripsi dan dekripsi) terhadap data yang akan dikirimkan.

Enkripsi dilakukan pada saat pengiriman dengan cara mengubah data asli menjadi data rahasia, sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengubah data rahasia menjadi data asli. Jadi data yang dikirimkan selama proses pengiriman adalah data rahasia, sehingga data asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Data asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia.

Disini enkripsi dapat diartikan sebagai kode atau *cipher*. Sebuah sistem pengkodean menggunakan suatu *tabel* atau kamus yang telah didefinisikan untuk kata dari informasi atau yang merupakan bagian dari pesan, data, atau informasi yang di kirim. Sebuah *cipher* menggunakan suatu algoritma yang dapat mengkodekan semua aliran data (*stream*) bit dari suatu pesan asli (*plaintext*) menjadi *cryptogram* yang tidak di mengerti. Karena sistem *cipher* merupakan suatu sistem yang telah siap untuk di *otomasi*, maka teknik ini digunakan dalam sistem keamanan jaringan komputer.

National Institute of Standard and Technology (NIST) untuk pertama kalinya mengumumkan suatu algoritma standar penyandian data yang telah dijadikan standard sejak tahun 1977 adalah *Data*

Encryption Standard (DES). DES terbukti menjadi algoritma enkripsi yang aman di dunia selama puluhan tahun. Kekuatan DES ini terletak pada panjang kuncinya yaitu 56-bit. Meski demikian, pada tahun 1990 panjang kunci DES dianggap terlalu pendek dan pada tahun 1998, 70 ribu PC di internet berhasil membobol kunci *DES* dalam tempo 96 hari, tahun 1999 dalam tempo waktu 22 hari. Perkembangan kecepatan perangkat keras dan meluasnya penggunaan jaringan komputer terdistribusi mengakibatkan penggunaan DES dalam beberapa hal, terbukti sudah tidak aman dan tidak mencukupi lagi terutama dalam hal yang pengiriman data melalui jaringan internet. Perangkat keras khusus yang bertujuan untuk menentukan kunci 56-bit DES hanya dalam waktu beberapa jam sudah dapat dibangun. Beberapa pertimbangan tersebut telah menandakan bahwa diperlukan sebuah standard algoritma baru dan kunci yang lebih panjang. *Triple-DES* muncul sebagai alternatif solusi untuk masalah - masalah yang membutuhkan keamanan data tingkat tinggi seperti perbankan, tetapi ia terlalu lambat pada beberapa penggunaan enkripsi.

Pada tahun 2001, *the U.S. National Institue of Standards and Technology* (NIST) mengumumkan bahwa sudah saatnya untuk pembuatan standard algoritma penyandian baru yang kelak diberi nama *Advanced Encryption Standard* (AES). Algoritma AES ini dibuat dengan tujuan untuk menggantikan algoritma DES dan *Triple-DES* yang telah lama digunakan dalam menyandikan data elektronik. Berdasarkan uraian tersebut, dalam penulisan ini penulis mengangkat judul “Pembuatan Aplikasi Enkripsi Dan Dekripsi Dengan Algoritma Kriptografi AES Menggunakan Pemprograman Java“.

1.2 Perumusan Masalah

Dalam pelaksanaan tugas akhir ini terdapat beberapa permasalahan yang menjadi titik utama pembahasan, diantaranya adalah sebagai berikut :

1. Bagaimana algoritma AES melakukan perlindungan terhadap data ?
2. Bagaimana aplikasi enkripsi dapat memberikan perlindungan pada sebuah informasi atau data ?

1.3 Pembatasan Masalah

Batasan masalah dari penulisan tugas akhir ini adalah sebagai berikut :

1. Algoritma yang digunakan adalah algoritma AES
2. Pembuatan aplikasi enkripsi menggunakan Java
3. Tidak mencakup perhitungan matematis dalam algoritma, karena perhitungannya sangat kompleks.
4. Aplikasi algoritma kunci rahasia AES diimplementasikan untuk ekstensi *file*.
5. Aplikasi hanya berjalan pada sistem operasi *windows*.

1.4 Tujuan dan Manfaat

Tujuan dari penulisan tugas akhir ini adalah sebagai berikut :

1. Memberikan gambaran dalam proses enkripsi dan dekripsi pesan atau informasi secara detail.
2. Perencanaan pengimplementasian aplikasi algoritma AES untuk melakukan proses enkripsi dan dekripsi terhadap *file* penting.
3. Menjadi jawaban atas permasalahan keamanan pesan atau informasi saat ini.

Manfaat penelitian ini sebagai berikut :

1. Memperkenalkan teknologi keamanan data atau informasi menggunakan metode enkripsi dan dekripsi
2. Menjaga pesan atau informasi agar tidak dapat dimanipulasi atau dirubah, dihapus.
3. Meningkatkan keamanan terhadap *file* - *file* yang dianggap penting.
4. Menerapkan semua bidang ilmu yang diperoleh selama perkuliahan.

1.5 Metode Penelitian

Dalam penyusunan tugas akhir ini akan digunakan metode penelitian sebagai berikut:

1. Studi Literatur

   Dalam penulisan ini menggunakan studi literature, yaitu penelitian kepustakaan dengan menggunakan bahan – bahan pustaka yang mendukung, baik dari buku maupun narasumber yang terpercaya, termasuk dari internet itu sendiri.

2. Perancangan perangkat lunak

   Perancangan perangkat lunak meliput perancangan fungsi algoritma dan perancangan antarmuka.

3. Pengujian perangkat lunak

   Pengujian yang dilakukan menyangkut tingkat keamanan file yang pesan yang terenkripsi.

4. Perbaikan

   Perbaikan dilakukan terhadap kesalahan - kesalahan yang mungkin terjadi pada program, laporan dan dokumentasi teknis.

1.6 Sistematika Penulisan

Penulisan laporan tugas akhir ini dibagi menjadi lima bab dan masing - masing akan dibahas dalam sub - sub babnya. Adapun sistematika penulisan laporan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Membahas latar belakang, tujuan dan manfaat, perumusan masalah, identifikasi masalah, ruang lingkup masalah, metode penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini akan membahas mengenai teori pendukung yang melandasi dan berhubungan dengan penelitian.

BAB III METODE PENELITIAN

Bab ini mengemukakan tentang cara dan prosedur dalam melakukan penelitian.

BAB IV ANALISIS DAN PEMBAHASAN

Secara umum bab ini membahas tentang langkah - langkah pembuatan program, mulai dari gambaran umum, rancangan desain aplikasi, langkah – langkah dalam pembuatan program.

BAB V KESIMPULAN DAN SARAN

Bab ini membahas mengenai kesimpulan dan saran yang sesuai dengan materi yang dibahas.