BAB 1

PENDAHULUAN

1.1 LATAR BELAKANG MASALAH

Pesatnya perkembangan teknologi informasi memberikan dampak baik yang bersifat positif maupun negatif bagi kehidupan manusia. Salah satu dampak negatif yang ditimbulkan yaitu adanya eksploitasi terhadap komputer itu sendiri, sehingga menimbulkan sebuah permasalahan baru yang dapat mengancam pengguna komputer lain salah satunya yaitu *privacy*. Pengguna komputer tertentu mengkhawatirkan kerahasiaan informasi yang mereka miliki agar tidak dapat diketahui orang lain seperti data sensitif perusahaan, informasi pribadi dan lain sebagainya. Salah satu solusi yang ditawarkan yaitu dengan mengenkripsi data rahasia mereka.

Enkripsi merupakan sebuah proses dalam mengubah pesan *plain text* (pesan yang dapat dimengerti oleh manusia) menjadi sebuah pesan *cipher text* (pesan acak yang tidak dapat dimengerti oleh manusia) dan dekripsi adalah proses mengubah kembali pesan *cipher text* menjadi *plain text* (Atul Kahate, 2009:59). Enkripsi telah banyak diterapkan dalam berbagai penggunaan fasilitas yang berkaitan dengan komputer salah satunya enkripsi MD5 yang sering diterapkan dalam teknologi berbasis *website* dalam menyimpan informasi.

Terdapat banyak metode enkripsi yang telah diciptakan, contohnya RSA, Blowfish, Rijndael, DES, Serpent, RC4, dll. Masing-masing memiliki cara tersendiri dalam mengenkripsi pesan. Perkembangan pesat *hardware* dan *software* memberikan kecepatan yang memungkinkan komputer dapat menyandikan pesan dalam waktu yang semakin singkat dengan proses yang sangat rumit terjadi dibelakangnya.

Dari berbagai metode enkripsi yang ada, penulis memilih DES dan AES (Rijndael). DES dipilih karena DES merupakan salah satu standar enkripsi yang diterapkan oleh *Federal Information Processing Standard* (FIPS) Amerika Serikat dan menjadi acuan dalam pembuatan enkripsi lainnya. AES dipilih karena AES masih diterapkan hingga saat ini yang ditetapkan oleh *National Institute of Standards and Technology* (NIST).

Berkaitan dengan terus mengembangkan ilmu pengetahuan membandingkan enkripsi DES dan AES guna mendapatkan data tentang performa DES dan AES. Oleh karena itu penulis memutuskan untuk melakukan penelitian dengan judul **"ANALISA ALGORITMA ENKRIPSI SIMETRIS DES (*DATA ENCRYPTION STANDARD*) DAN AES (*ADVANCED ENCRYPTION STANDARD*)".**

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang, maka dapat diambil perumusan masalah sebagai berikut :

1. Bagaimana hasil perbandingan kecepatan DES dan AES dalam mengenkripsi sebuah pesan?
2. Bagaimana cara kerja DES dan AES dalam mengenkripsi sebuah pesan?

1.3 BATASAN MASALAH

Batasan masalah dalam penelitian ini adalah sebagai berikut :

1. Algoritma kriptografi yang digunakan adalah DES dan AES.
2. Data yang digunakan berupa *plaintext.*
3. *Plaintext* pada DES berukuran 64 bit dan kelipatannya.
4. *Plaintext* pada AES berukuran 128 bit dan kelipatannya.
5. *Key* yang digunakan pada AES yaitu sebesar 128 bit.
6. Kegiatan yang dilakukan hanya dalam mengenkripsi suatu pesan tidak termasuk proses dekripsinya.

1.4 TUJUAN DAN MANFAAT PENELITIAN

1.4.1 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah :

1. Membandingkan performa algoritma DES dan AES menggunakan 2 kriteria yaitu kecepatan dan memori yang digunakan dalam mengenkripsi sebuah pesan.
2. Mengetahui cara kerja algoritma DES dan AES dalam mengenkripsi sebuah pesan.

1.4.2 Manfaat Penelitian

Adapun manfaat dari penelitian yang dapat diperoleh adalah :

1. Bagi penulis dapat menambah pengetahuan dengan mengetahui cara kerja DES dan AES serta menambah pengetahuan dibidang keamanan data.
2. Bagi pembaca dapat menambah wawasan dan pengetahuan tentang keamanan data khususnya DES dan AES.

1.5 SISTEMATIKA PENULISAN

Untuk membahas lebih jelas dan terperinci dalam penulisan dan memberikan gambaran terhadap pembaca, maka dengan ini penulis membagi atas beberapa bab yang saling berhubungan satu sama lainnya dan sesuai dengan ruang lingkup judul, sistematika penulisannya antara lain sebagai berikut:

BAB I : PENDAHULUAN

Pada bab ini menguraikan tentang latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian dan sistematika penulisan.

BAB II : LANDASAN TEORI

Pada bab ini terdapat teori-teori mengenai AES dan DES seperti pengenalan,cara kerja serta formula dalam menjalankan DES dan AES itu sendiri secara matematis.

BAB III: METODOLOGI PENELITIAN

Pada bab ini menjelaskan tentang langkah-langkah kerja dan metode yang digunakan dalam analisis untuk menyelesaikan masalah yang dibahas.

BAB IV: ANALISIS DAN PEMBAHASAN

Pada bab ini membahas tentang analisis yang dilakukan terhadap permasalahan berdasarkan topik yang ada.

BAB V: HASIL ANALISIS DAN PEMBAHASAN

Pada bab ini berisi tentang hasil dari analisis dan rekomendasi berdasarkan penelitian yang dilakukan.

BAB VI: PENUTUP

Pada bab ini berisi tentang kesimpulan dan saran yang diajukan agar dapat menjadi bahan pertimbangan.