BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Dewasa ini perkembangan teknologi komputer dan jaringan komputer, khususnya internet sangatlah cepat dan telah menjadi salah satu kebutuhan dari sebagian besar manusia. Dengan kemudahan yang diberikan teknologi tersebut, perpindahan informasi tidak lagi dibatasi, baik oleh jarak maupun waktu. Namun maraknya perkembangan teknologi juga menyebabkan pergeseran fungsi dari teknologi komputer dan jaringan oleh sebagian orang, baik hal yang sengaja maupun tidak. Hal yang cukup membahayakan dari masalah tersebut salah satunya adalah mengurangi sistem keamanan penyimpanan informasi dalam komputer yang terhubung dengan jaringan ke luar komputer sehingga gangguan-gangguan dari pihak luar dalam proses perpindahan informasi sedikit banyak tidak dapat dielakkan. Dengan tujuan meminimalkan efek gangguan tersebut telah mendorong perkembangan teknologi kriptografi dan steganografi.

Kriptografi merupakan studi matematika yang mempunyai hubungan dengan aspek keamanan informasi seperti integritas data, keaslian entitas dan keaslian data. Kriptografi menggunakan berbagai macam cara dalam upaya mengamankan suatu data. Pengiriman data dan penyimpanan data melalui media elektronik memerlukan suatu proses yang dapat menjamin keamanan dan

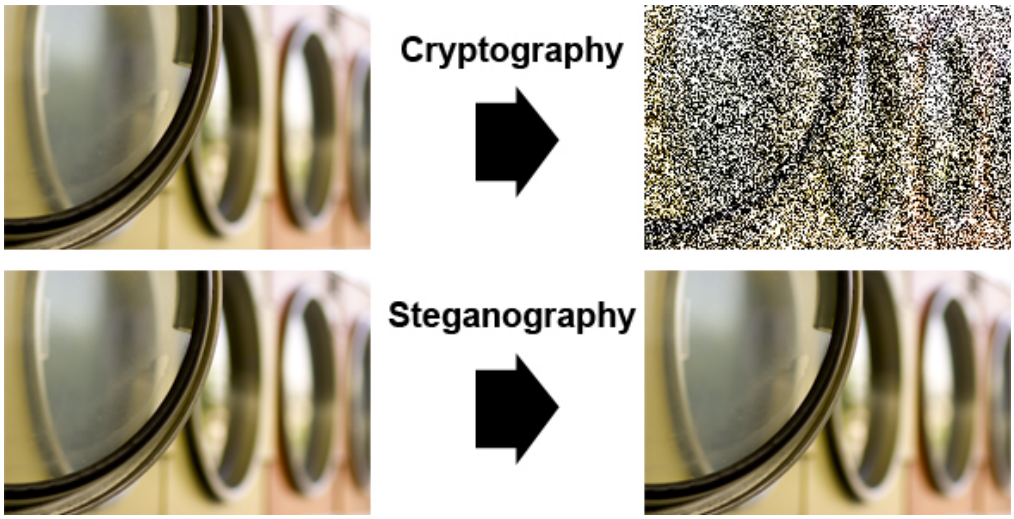
keutuhan dari data yang dikirimkan tersebut. Data tersebut harus tetap rahasia pada saat melalui proses pengiriman, dan harus utuh pada saat data tersebut sampai di tujuan. Untuk memenuhi kebutuhan tersebut, dilakukan teknik enkripsi dan dekripsi terhadap data yang akan dikirimkan.

Enkripsi dilakukan pada saat pengiriman dengan cara merubah data asli menjadi data rahasia, sedangkan proses dekripsi dilakukan pada saat proses penyampaian pesan ke tujuan dengan cara merubah data rahasia tadi kembali ke data asli. Tujuan dari dua proses ini adalah agar pada saat proses pengiriman, data asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Enkripsi dalam hal ini dapat diartikan sebagai kode atau *cipher*. Sebuah sistem pengkodean menggunakan suatu tabel atau kamus yang telah didefinisikan sebelumnya. Pengkodean dilakukan dengan algoritma tertentu untuk mengkodekan semua aliran data *bit* dari suatu pesan asli (*plaintext)* menjadi pesan rahasia *(ciphertext).* Karena sistem ini dapat dilakukan secara otomasi, maka teknik ini dapat digunakan dalam sistem keamanan jaringan komputer.

Pada tahun 1977, *National Institute of Standard and Technology (NIST)* mengumumkan suatu algoritma standar penyandian data yaitu *Data Encryption Standard (DES).* Kelebihan dari *DES* ini terletak pada panjan kuncinya yaitu 56-*bit*. Sejalan dengan perkembangan perangkat keras dan meluasnya penggunaan jaringan komputer mengakibatkan penggunaan *DES* menjadi tidak aman lagi. Untuk memenuhi kebutuhan akan sistem keamanan yang lebih, maka *National*

Institute of Standard and Technology (NIST) pada tahun 1997 mengumumkan bahwa sudah saatnya membuat standar algoritma penyandian baru yang diberi nama *Advanced Encryption Standard (AES)*. Algoritma *AES* ini dibuat dengan tujuan menggantikan algoritma *DES*. Setelah melalui beberapa tahap seleksi, algoritma *Rijndael* ditetapkan sebagai algoritma kriptografi *AES* pada tahun 2000.

Demi meningkatkan keamanan dari suatu data yang akan dikirim maka data tersebut dapat melalui proses steganografi. Kriptografi dan steganografi merupakan hal yang berbeda. Kriptografi memungkinkan pihak ketiga mengetahui adanya *ciphertext*. Sedangkan steganografi dapat menyembunyikan *ciphertext* tersebut kedalam suatu media penampung baik itu gambar, video, teks ataupun suara sehingga pihak ketiga tidak akan menyadari keberadaan *ciphertext* tersebut. Illustrasi mengenai perbedaan kriptografi dan steganografi dapat dilihat pada gambar 1-1.



Gambar 1.1 Perbandingan Steganografi dan Kriptografi

1.2 Perumusan Masalah

Penelitian ini bertujuan untuk merancang sebuah program aplikasi pengamanan data dengan mengimplementasikan kriptografi dengan metode *Rijndael Advanced Encryption Standard* pada data berupa *plaintext* menjadi *ciphertext.* Kemudian *ciphertext* tersebut akan disamarkan dengan cara menyisipkannya ke dalam sebuah *file* audio.

Program simulasi ini akan menggambarkan bagaimana *plaintext* dapat disimpan dan dapat disimpan kedalam *file* audio tanpa merubah kualitas dari *file* audio itu sendiri.

1.3 Ruang Lingkup Masalah

Pada penelitian ini simulasi dilakukan pada *file* yang akan dirubah menjadi *ciphertext* dengan menggunakan metode *Rijndael Advanced Encryption Standard* 128 *bit,* dan media yang digunakan untuk menampung *ciphertext* tersebut adalah *file* audio dengan format .*wav.*

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Adapun Tujuan dari penelitian ini adalah:

a. Menerapkan metode matematika dalam proses enkripsi dan dekripsi, untuk mengamankan data dari pihak yang tidak berkepentingan.

b. Merancang program simulasi steganografi dalam bentuk suara, dengan metode *Rijndael AES*.

1.4.2 Manfaat

Adapun manfaat dari penelitian ini adalah:

a. Bagi peneliti lain: menambah ilmu pengetahuan di bidang kriptografi, terutama mengenai metode *Rijndael AES*, dan dapat menciptakan algoritma kriptografi yang lebih baik dan optimal.
b. Bagi pengguna program aplikasi: menambah ilmu pengetahuan tentang proses pengamanan data, ke dalam *file* audio.
c. Bagi penulis: menambah ilmu pengetahuan di bidang kriptografi dan keamanan, serta matematika dan teknologi informasi.

1.5 Sistematika Penulisan

Dalam penulisan skripsi, penulis menggunakan susunan bab sebagai berikut:

BAB 1 PENDAHULUAN

Pada bab ini akan diuraikan tentang latar belakang masalah, rumusan masalah, ruang lingkup masalah, tujuan dan manfaat, serta sistematika penulisan.

BAB 2 LANDASAN TEORI

Dalam bab ini akan diuraikan tentang landasan teori yang digunakan dalam penyusunan skripsi seperti pengetahuan mengenai *file* audio berformat .*wav*, kriptografi, steganografi, serta algoritma kriptografi *Rijndael AES.*

BAB 3 ANALISIS DAN PERANCANGAN PROGRAM

Bab ini membahas analisis masalah-masalah yang dihadapi kemudian merancang program simulasi. Analisis program mencakup analisi masalah, usulan pemecahan masalah, serta perancangan program. Perancangan program mencakup model konseptual, bentuk program, perancangan layar, perancangan program dan perancangan menu.

.

BAB 4 IMPLEMENTASI DAN EVALUASI

Bab ini menjelaskan implementasi perangkat lunak, sarana yang dibutuhkan, dan contoh cara pengoperasian perangkat lunak yang dirancang, serta hasil evaluasi dari aplikasi yang sudah berjalan untuk mendukung skripsi ini.

BAB 5 KESIMPULAN DAN SARAN

Pada bab ini diberikan kesimpulan dari hasil penelitian berdasarkan uraian dari bab-bab sebelumnya, dan saran untuk pengembangan lebih lanjut.