BAB I
PENDAHULUAN

1.1 Latar Belakang

Saat ini media digital, seperti video, audio, dan gambar, telah menggantikan peran media analog dalam berbagai aplikasi. Keberhasilan dari penerapan media digital ini disebabkan karena beberapa kelebihan yang dimiliki media digital, seperti transmisi yang bebas derau, penyimpanan yang padat, penyalinan yang sempurna, dan kemudahan untuk melakukan pengeditan. Di samping semua kelebihan yang dimiliki media digital seperti yang telah dipaparkan sebelumnya, terdapat kelemahan dari penggunaan media digital (Rumondang,2006).

Teknologi informasi saat ini semakin popular digunakan dalam seluruh aspek kehidupan. Hampir seluruh informasi kini dikelola dalam bentuk data digital. Akan tetapi, penggunaan data digital belum tentu meningkatkan keamanan pesan tersebut. Berbagai teknik penyerangan muncul sehingga pihak yang tidak bertanggung jawab dapat mengetahui informasi rahasia yang terkandung dalam pesan. Oleh karena itu, faktor keamanan menjadi salah satu isu penting dalam pengelolaan data digital.

Hingga saat ini aplikasi yang menerapkan prinsip kriptografi audio sangat banyak dikembangkan. Aplikasi kriptografi audio yang ada hanya dapat membagi informasi yang terdapat pada berkas audio biner, yaitu berkas suara yang terdiri atas dua jenis suara, yaitu suara panjang dan suara pendek (seperti kode Morse) atau suara tinggi dan suara rendah. Dengan demikian, informasi yang ingin dirahasiakan harus berupa data biner.

Berkas audio yang digunakan adalah berkas WAV karena berkas ini merupakan format paling umum digunakan dan dapat diputar oleh hampir seluruh perangkat multimedia. Berkas audio WAV, atau WAV, merupakan standard format berkas audio yang digunakan oleh IBM dan *Microsoft* dalam menyimpan

aliran data audio pada PC. Berkas audio WAV menerapkan teknik *Linear Pulse Code Modulation (LPCM)* dalam merepresentasikan data. *LPCM* merupakan salah satu jenis PCM yang menggunakan metode *lossless* dan tanpa kompresi, yaitu metode yang menyimpan seluruh *sample* audio, sehingga berkas WAV merupakan berkas mentah (sesuai dengan aslinya) (Rasyid,2009).

Kriptografi pada algoritma pengkodean data informasi yang mendukung dari dua aspek keaman informasi yaitu *secrecy* (perlindungan terhadap kerahasian data informasi) dan *authenticity* (perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan). Ada banyak model, dan model enkripsi , salah satu diantaranya adalah enkripsi dengan algoritma *Rivest Code 4* (*RC4*). *RC4* menggunakan panjang kunci dari 1 sampai 256 bit yang digunakan untuk menginisialisasikan table sepanjang 256 bit. Tabel ini digunakan untuk generasi yang berikutnya dari *pseudo random* yang menggunakan *XOR* dengan *plaintexs* untuk menghasilkan *chipertexs* dan masing-masing elemen tabel saling ditukarkan minimal satu kali (Rumondang ,2006).

Dalam penelitian ini, peneliti akan menerapakan suatu algoritma kriptografi *RC4*. Dengan kriptografi, data dapat diubah menjadi sandi-sandi yang tidak dimengerti serta mengembalikannya kembali ke semula, proses ini disebut Enkripsi dan Dekripsi data. Penelitian ini akan membahas bagaimana menerapkan algoritma *RC4* enkripsi dan dekripsi pada file suara bertipe WAV.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah diatas maka rumusan masalah yang akan dibahas adalah bagaimana menerapkan algoritma *RC4*, untuk enkripsi dan dekripsi file suara bertipe WAV.

1.3 Batasan Masalah

Dalam penulisan tugas akhir ini ,penulis akan membatasi beberapa hal berikut ini :

1. Algoritma yang di gunakan adalah algoritma *RC4*.
2. Enkripsi dan dekripsi pada file audio bertipe WAV.

1.4 Tujuan

Tujuan dari penulisan tugas akhir ini adalah menerapkan algoritma *RC4* enkripsi dan dekripsi file suara bertipe WAV.

1.5 Manfaat

Adapun manfaat yang diharapkan dengan dilakukannya penelitian ini adalah:

1. Dapat mengamankan sebuah data jika pesan tersebut bersifat rahasia.
2. Mampu memberikan solusi untuk meningkatkan kehandalan dari proses keamanan data yang disimpan menggunakan algoritma *RC4*.

1.6 Metodologi Penelitian

Model pengembangan sistem yang digunakan adalah model *waterfall*. Tahapan-tahapan dari model *waterfall* adalah (Pressman,2002):

1. Analisis

   Pada tahapan ini dilakukan pengumpulan data-data yang berhubungan dengan aplikasi yang akan dibuat. Kemudian data-data tersebut dianalisis.
2. Desain

   Pada tahapan ini akan dilakukan desain perangkat lunak meliputi desain *interface*, desain lingkungan perangkat lunak dan lain-lain.
3. Generasi kode

   Pada tahapan ini desain yang telah dibuat, diterjemahkan ke dalam bahasa pemrograman. Alat bantu yang digunakan adalah *Microsoft Visual Basic 2008.NET*.
4. Pengujian

   Setelah aplikasi dibuat, kemudian akan dilakukan pengujian. Metode pengujian yang digunakan adalah metode *black box testing.*

1.7 Sistematika Penulisan

Untuk memberikan gambaran secara garis besar isi dari laporan penulisan, akan diuraikan secara singkat sistematika penulisannya sebagai berikut:

BAB I PENDAHULUAN

Memberikan gambaran mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini akan dibahas penjelasan mengenai istilah-istilah, penelitian-penelitian terdahulu dan beberapa poin penting lain yang berguna dalam penelitian ini.

BAB III ANALISIS DAN DESAIN

Pada bab ini akan membahas tentang analisis sistem yang akan digunakan, spesifikasi proses menggunakan *Data Flow Diagram*, desain *input* dan *output*, serta desain menu dan model yang akan digunakan.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Pada bab ini akan membahas mengenai implementasi program yang di telah dibuat.

BAB V PENUTUP

Berisi simpulan umum dan saran yang membangun untuk masa mendatang.