BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam segala aspek kegiatan manusia sangat bergantung pada pesan atau data sebagai komponen utama informasi. Sehingga kualitas pengiriman pesan sangatlah penting untuk diperhatikan terutama pada segi keamanan dan kecepatan pengiriman pesan (Bagus, 2011).

Kriptografi sebagai suatu ilmu hadir untuk meningkatkan aspek keamanan pesan. Hal ini dilakukan dengan menyandikan pesan ke dalam bentuk acak yang tidak dapat dimengerti lagi maknanya. Akan tetapi, dengan suatu algoritma dan kunci yang sudah ditentukan sebelumnya, bentuk acak tersebut dapat dikembalikan ke pesan semula (Dana, 2011).

Pengamanan data digital dengan kriptografi dapat diimplementasikan pada berbagai bentuk format data digital. Beberapa contohnya adalah implementasi kriptografi pada data teks, gambar, dan audio. Kriptografi pada data teks memang lebih familiar dikenal dikalangan masyarakat luas. Aplikasi-aplikasi yang sudah menerapkan kriptografi pada data teks pun sudah banyak dikembangkan (Dana, 2011).

Selain file teks, file audio juga sangat perlu untuk disandikan terlebih-lebih file audio yang bersifat penting dan rahasia. Sebagai contoh yaitu file audio yang berisi rekaman instruksi perang atau strategi perang dan file audio yang berisi rekaman lagu untuk sebuah ajang kompetisi yang akan dikirim melalui internet. Contoh lainnya yaitu file audio yang berisi rekaman mengenai warisan yang harus disimpan dalam waktu tertentu dan file audio yang berisi rekaman pidato politik yang hanya boleh diketahui oleh internal partai tertentu. File-file audio tersebut sudah seharusnya dijaga kerahasiannya. Sehingga, apabila file tersebut jatuh ke pihak yang tidak bertanggung jawab tidak akan memiliki makna yang berarti baginya. Salah satu cara untuk menjaga kerahasian file audio tersebut adalah dengan menggunakan aplikasi kriptografi, khususnya aplikasi kriptografi file audio (Dana, 2011).

Ada banyak model dan metode enkripsi, salah satu diantaranya adalah enkripsi dengan algoritma *Rivest Code* 6 (RC6). Model ini merupakan salah satu algoritma kunci simetris yang berbentuk *block chipper*. Algoritma ini merupakan pengembangan algoritma sebelumnya yaitu RC5 dan telah memenuhi semua kriteria yang diajukan oleh NIST (Prayudi, 2005).

RC6 menggunakan 4 (empat) *working registers*, dan menyertakan operasi perkalian integer sebagai operasi primitif tambahan. Operasi perkalian meningkatkan penyebaran untuk tiap putarannya sehingga meningkatkan faktor keamanan, mengurangi putaran, dan meningkatkan performa hasil. Tingkat keamanan pada algoritma ini terletak pada kekuatan rotasi yang berdasarkan data, penggunaan *eksklusif* OR yang bergantian, fungsi modulo dan fungsi persamaan yang menggunakan rotasi yang tetap (Subari, 2011).

Oleh karena itu, dengan berkembangnya kemajuan teknologi yang sekarang ini, maka penulis tertarik untuk membangun suatu aplikasi kriptografi yang dapat meng-enkripsi dan deskripsi untuk media audio yang dituangkan dalam penulisan yang berjudul: "PENERAPAN ALGORITMA *RIVEST CODE* 6 (RC6) UNTUK ENKRIPSI DAN DESKRIPSI AUDIO".

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang diatas, maka penulis merumuskan masalah yang ada, yaitu: "Bagaimana menerapkan Algoritma *Rivest Code* 6 (RC6) untuk enkripsi dan deskripsi audio?".

1.3 Batasan Masalah

Batasan masalah yang akan dibahas pada penerapan algoritma *Rivest Code* 6 (RC6) untuk enkripsi dan deskripsi audio antara lain, sebagai berikut:

1. Implementasi enkripsi dan dekripsi hanya untuk media audio yang berformat WAV.
2. Algoritma yang digunakan adalah *Rivest Code* 6 (RC6).
3. Bahasa pemograman yang digunakan adalah *Java*.

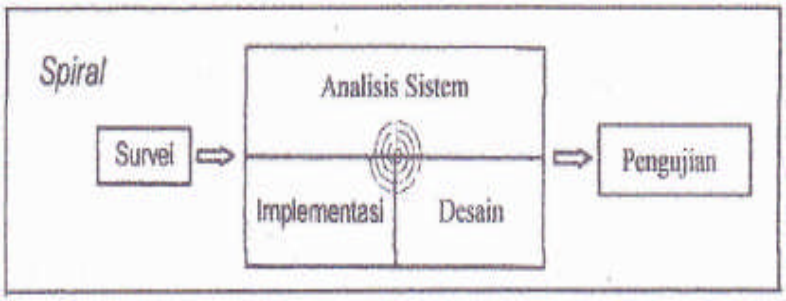
1.4 Tujuan dan Manfaat Penelitian

Tujuan yang ingin dicapai pada penelitian ini adalah membuat aplikasi untuk penerapan algoritma *Rivest code* 6 (RC6) untuk enkripsi dan deskripsi audio.

Sedangkan manfaat dari penelitian ini adalah:

1. Diharapkan dengan adanya aplikasi ini bisa meningkatkan keamanan informasi dalam hal ini adalah informasi dalam bentuk audio.
2. Meminimalisir resiko manipulasi informasi audio oleh pihak-pihak yang tidak bertanggung jawab.

1.5 Metodologi Penulisan Skripsi



Gambar 1.1 Metoda *Spiral*

Adapun metodologi penelitian skripsi ini dengan mengikuti metode *spiral* adalah sebagai berikut (Sutabri, 2004):

1. Survei

   Manfaat dari fase penyelidikan ini adalah untuk menentukan problem-problem atau kebutuhan yang timbul. Hal itu memerlukan pengembangan sistem secara menyeluruh ataukah ada usaha lain yang dapat dilakukan untuk memecahkannya.
2. Analisis Sistem

   Proses pengumpulan data-data yang diperlukan untuk melakukan analisis terhadap hal-hal yang diperlukan dalam pembuatan aplikasi ini.
3. Desain Sistem

   Pada tahap ini hal yang dilakukan adalah menentukan alur sistem dan bahasa pemograman yang akan digunakan dalam perancangan sistem. Perancangan

yang akan dilakukan pada skripsi ini anatar lain perancangan data yang berupa arsitektur, dan antarmuka struktur.

4. Implementasi Sistem

   Pada tahap ini melakukan penerjemahan spesifikasi desain ke kode komputer dengan menggunakan bahasa pemograman *java*.

5. Pengujian

   Pada tahap ini akan dilakukan pengujian terhadap sistem yang telah dibangun untuk mengetahui apakah aplikasi ini dapat berfungsi dengan baik.

1.6 Sistematika Penulisan Skripsi

Untuk memberikan gambaran secara garis besar mengenai pembahasan tiap bab yang terdapat dalam skripsi ini, berikut akan diuraikan secara singkat sistematika penulisannya, antara lain :

BAB I PENDAHULUAN

Pada bab ini, membahas mengenai latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat seminar tugas akhir, metodologi penelitian, serta sistematika penulisan seminar tugas akhir.

BAB II LANDASAN TEORI

Dalam bab ini dibahas mengenai beberapa teori yang dipakai untuk mendukung penulisan skripsi.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini menguraikan kebutuhan dasar yang diperlukan selama proses pengembangan perangkat lunak, meliputi pembahasan mengenai algoritma RC6 serta prosedur kerjanya, serta menguraikan tentang gambaran secara umum dari desain dan tampilan-tampilan perangkat lunak yang dibangun.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini, berupa penjelasan mengenai tahap realisasi setiap prosedur yang telah dirancang ke dalam bentuk program, serta pengujian yang dilakukan terhadap perangkat lunak yang dibangun.

BAB V PENUTUP

Bab ini berisi kesimpulan secara umum dan saran yang diharapkan dapat membangun di masa yang akan datang.