BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Dewasa ini media digital, seperti *audio, video*, dan gambar telah menggantikan peran media *analog* dalam berbagai aplikasi. Media digital sudah berkembang sangat pesat dan banyak digunakan sebagai sarana penyampaian informasi. Keberhasilan dalam penerapan media digital karena memiliki beberapa kelebihan yang dimiliki media digital, seperti transmisi bebas derau, penyimpanan yang padat, penyalinan yang sempurna, dan kemudahan dalam melakukan pengeditan. Akan tetapi, di samping kelebihan yang dimiliki dari media digital, terdapat juga kelemahan dari penggunaan media digital, yaitu keamanan informasi yang terkandung di dalamnya (Rumondang, 2006).

Salah satu media digital yang dapat digunakan dalam penyampaian pesan dalam bentuk lambang-lambang auditif adalah*audio* (Sadiman, 2005). Media *audio*dipakai karena mudah dalam penggunaannya dan diikuti dengan kemudahan dalam pengaksesannya. Berbagai macam *File audio* sudah diciptakan mulai dari WAV, MP3, WMA, FLAC, MP4, dan AMR. AMR (*Adaptive Multi Rate*) merupakan file audio kompresi, file ini berukuran kecil yang dihasilkan dari sebuah encoder yang menyesuaikan bit-rate yang sesuai dengan MCU/CPU/Processor yang digunakan. File ini biasanya digunakan untuk hasil rekaman.

Dalam pengiriman pesan melalui media *audio* dan ketika sampai kepada penerima pesan, informasi tersebut harus tetap rahasia dan terjaga keasliannya atau tidak dimodifikasi. Penerima informasi tersebut harus yakin bahwa informasi itu dikirim oleh orang yang tepat, begitu juga sebaliknya, pengirim yakin bahwa penerima pesan adalah orang yang sesungguhnya. Untuk permasalahan berikut diperlukan suatu metode untuk menjaga keamanan suatu informasi. Salah satu metodenya adalah Kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga

keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain(Ariyus, 2006).

Pengamanan suatu pesan dilakukan dengan cara melakukan enkripsi terhadap pesan yang akan dikirim tersebut. Dalam kriptografiterdapat berbagai macam algoritma yang dapat melakukan proses enkripsi terhadap pesan tersebut.Salah satu algoritma yang dapat melakukan enkripsi adalah Algoritma *Data Encryption Standard* (DES). Algoritma DES merupakan algoritma simetri dan tergolong jenis *cipher* blok.Waktu prosess enkripsi dan dekripsi algoritma ini reltif cepat,hal ini karena efisiensi dalam pembangkitan kunci, maka algoritma ini dapat digunakan pada sistem secara real-time. Keamanan algoritma ini terletak pada banyaknya proses enkripsi dan dekripsi yang dilakukan sebanyak 16 kali putaran.

Berdasarkan latar belakang diatas maka diperlukan sebuah aplikasi sistem kriptografi yang dapat menerapkan algoritma DES untuk proses enkripsi dan dekripsi *file audio* AMR.

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang masalah di atas didapatkan suatu perumusan masalah, yaitu bagaimana cara membuat sistem kriptografi *file audio* format AMR dengan menggunakan algoritma DES (*Data Encryption Standard*) ?

1.3 BATASAN MASALAH

Agar fokus penelitian ini terjaga, diberikan beberapa batasan masalah sebagai berikut :

1. Aplikasi yang akan dibangun hanya difokuskan dalam proses enkripsi dan dekripsi *file* AMR.
2. Pada proses enkripsi dilakukan terhadap keseluruhan bit *file* AMR, bukan hanya pada bit datanya saja.
3. Panjang kunci yang digunakan yaitu 64 bit.
4. Hasil dari enkripsi *file* AMR tersebut akan membuat file yang sudah di enkripsi hanya bisa diputar di media pemutar khusus seperti Audacity.

1.4 TUJUAN DAN MANFAAT PENELITIAN

Berdasarkan permasalahan pada penelitian ini, maka tujuan yang diharapkan adalah mendapatkan hasil berupa aplikasi sistem kriptografi *file audio* format AMR menggunakan algoritma DES (*Data Encryption Standard*)

Manfaat yang didapat dari penelitian ini adalah :

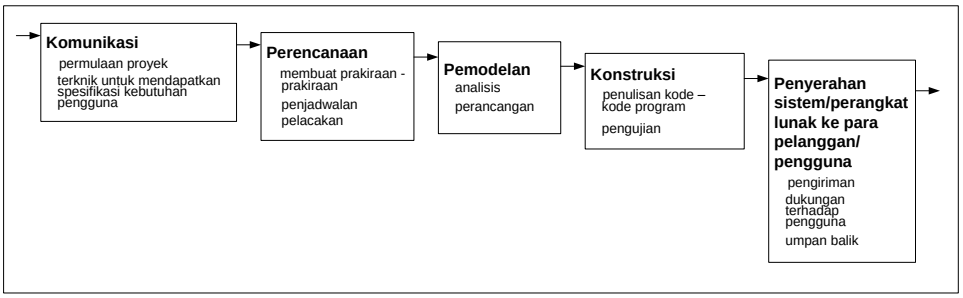
1. Meningkatkan keamanan terhadap *File audio* AMR, sehingga keamanan pesan didalamnya tersebut menjadi relatif aman.
2. Menanggulangi terjadinya manipulasi informasi dari hasil rekaman yang mengandung informasi penting.
3. Memudahkan dalam melakukan proses enkripsi dan dekripsi *file* AMR karena sudah tersedianya aplikasi tersebut.

1.5 METODOLOGI PENELITIAN

Metode yang digunakan dalam penelitian ini adalah sebagai berikut.

a. Metode Pengembangan Sistem

Metode pengembangan sistem yang digunakan yaitu pengembangan sistem dengan menggunakan model air terjun/*waterfall* (Pressman, 2012). Model *waterfall* terdiri dari komunikasi, perencanaan, pemodelan, konstruksi, dan penyerahan sistem/perangkat lunak ke para pelanggan/pengguna. Pengembangan sistem perangkat lunak dengan model *waterfall menurut* Pressman dapat dilihat pada Gambar 1.1.



Gambar 1.1 Model *Waterfall* (Pressman, 2012)

Tahapan pengembangan sistem dalam penelitian ini dapat dilihat pada Tabel 1.1.

Tabel 1.1 Tahapan Pengembangan Sistem

No	Tahap	Kegiatan	Peralatan
1.	**Komunikasi dan Pengumpulan Data**	1. Observasi 2. *Library Research*	
2.	**Perencanaan**	1. Estimasi waktu dan pembuatan jadwal kegiatan secara detail	• Daftar kegiatan • Jadwal kegiatan
3.	**Pemodelan**	1. Analisis sistem 2. Desain sistem dan *software*	• UML • *Flowchart*
4.	**Konstruksi**	1. Pemrograman (*coding*) 2. Pengujian	• *Microsoft Visual Studio 2010* • Kerangka pengujian

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan yang digunakan dalam penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas tentang pendahuluan yang mencakup uraian tentang latar belakang, rumusan masalah, ruang lingkup, tujuan dan manfaat, metodologi penelitian serta sistematika penulisan dijelaskan pada bab ini.

BAB II LANDASAN TEORI

Dalam bab ini dibahas mengenai beberapa teori yang dipakai untuk mendukung penelitian dan penelitian-penelitian sebelumnya yang berkaitan dengan penelitian ini.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini menguraikan kebutuhan dasar yang diperlukan selama proses perancangan perangkat lunak (*software*), meliputi pembahasan mengenai enkripsi dan dekripsi *file* amr dengan algoritma DES (*Data Encryption Standard*) serta menguraikan tentang gambaran secara umum dari desain dan tampilan-tampilan perangkat lunak*(software)* yang dibangun.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini menjelaskan tentang spesifikasi *hardware* dan *software* yang dibutuhkan dalam menjalankan aplikasi, prosedur operasional, rencana implementasi, serta evaluasi dari percobaan yang dilakukan.

BAB V KESIMPULAN DAN SARAN

Bab ini kesimpulan yang telah didapat setelah melakukan proses pembuatan aplikasi sistem, serta saran-saran yang diajukan untuk pengembangan sistem.