BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi informasi merupakan salah satu hal penting dalam peradaban manusia untuk mengatasi sebagian masalah derasnya arus informasi. Selain memiliki potensi dalam memfilter data dan mengolah menjadi informasi, teknologi informasi mampu menyimpannya dalam jumlah kapasitas jauh lebih banyak dari cara-cara manual. Salah satu pekerjaan manusia yang akan sangat terbantu dengan hadirnya teknologi informasi, dengan keuntungan yang ditawarkan yaitu pekerjaan manusia dalam mengamankan data (Maradilla, 2009).

Masalah keamanan data merupakan salah satu aspek penting dalam teknologi informasi. Salah satu solusi yang dapat digunakan untuk menjaga keamanan data yaitu dengan melakukan proses enkripsi dan dekripsi guna membuat data ataupun informasi tidak dapat dibaca atau dimengerti oleh orang lain, kecuali untuk penerima yang berhak atau memiliki kunci. Teknik pengamanan data dengan proses enkripsi dan dekripsi dikenal dengan istilah kriptografi (Munir, 2004).

Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi maupun dekripsi data. Teknik ini digunakan untuk merubah data biasa dengan kunci tertentu menjadi data yang tidak diketahui oleh orang lain kecuali bagi orang yang berhak. Kriptografi telah menjadi bagian penting dalam dunia teknologi informasi saat ini. Hampir semua penerapan teknologi informasi menggunakan kriptografi sebagai alat untuk menjamin kemanan data dan kerahasiaan informasi. Karena kriptografi menjadi ilmu yang berkembang pesat, dalam waktu singkat banyak bermunculan algoritma-algoritma baru yang dianggap lebih unggul dari pada pendahulunya, salah satunya adalah algoritma asimetri seperti Algoritma DSA (*Digital Signature Algorithm*), Algoritma RSA (*Rivest Shamir Adleman*), Algoritma DH (*Diffie-Hellman*), Algoritma ECC (*Elliptic Curve Cryptography*), dan Kriptografi Quantum.

Dari sekian banyak algoritma asimetri yang dibuat, algoritma yang paling populer adalah algoritma RSA. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan prima yang relatif besar. Selama belum ada algoritma yang berhasil memecahkan pemfaktoran bilangan prima yang besar, maka selama itu keamanan algoritma RSA tetap terjamin (Alvianto dan Darmaji, 2015).

Untuk membuktikan keamanan algoritma RSA maka diperlukan media sebagai data yang akan diamankan. Pengamanan data dapat dilakukan pada semua *format* multimedia yang ada dalam komputer seperti *format* teks, *format* gambar, *format audio*, dan *format video*. Bahkan untuk *format audio* dan sebagainya asalkan *file-file* tersebut mempunyai bit-bit data yang dapat dimodifikas, maka *file* tersebut dapat diamankan dengan algoritma RSA seperti *format audio* MP3. *Format audio* MP3 adalah salah satu *format audio* yang paling sering digunakan dalam penyimpanan data *audio*, karena data yang disimpan menyerupai data asli saat direkam, dan memiliki ukuran tidak terlalu besar dibandingkan *form*at lain.

Berdasarkan latar belakang di atas maka diperlukan sebuah aplikasi sistem kriptografi yang dapat menerapkan algoritma RSA untuk proses enkripsi dan dekripsi *file audio* MP3. *File audio* MP3 yang telah terenkripsi nantinya masih dapat diputar tetapi suaranya tidak terdengar jelas oleh telinga manusia sehingga diperlukan aplikasi untuk mendekripsi *file audio* MP3 tersebut agar dapat diputar seperti semula.

1.2 Rumusan Masalah

Dengan latar belakang yang telah dipaparkan pada bagian pendahuluan di atas, maka masalah dalam penelitian ini yaitu bagaimana cara membuat aplikasi sistem kriptografi untuk pengamanan *file audio* MP3 dengan menerapkan algoritma RSA (*Rivest Shamir Adleman)*?

1.3 Batasan Masalah

Untuk memfokuskan dan menjelaskan ruang lingkup penelitian ini, maka dalam pengerjaan proyek ini ditentukan batasan-batasan sebagai berikut :

1. *File audio* MP3 yang dienkripsi mengalami perubahan kapasitas dari 1 MB menjadi 2 MB kemudian setelah didekripsi akan kembali ke kapasitas semula.
2. *File audio* MP3 yang dienkripsi yaitu keseluruhan *bit file* sehingga *file audio* MP3 yang dienkripsi tidak dapat diputar.
3. Hasil dari enkripsi *file audio* MP3 yaitu tidak dapat diputar di media pemutar musik biasa diperlukan media pemutar musik khusus untuk memutarnya.

1.4 Tujuan dan Manfaat Penelitian

Adapun tujuan dan manfaat dari penelitian ini yaitu sebagai berikut :

1.4.1 Tujuan

Berdasarkan permasalahan penelitian ini, tujuan yang diharapkan yaitu mendapatkan hasil berupa aplikasi sistem kriptografi untuk menerapkan algoritma RSA pada *file audio* MP3.

1.4.2 Manfaat

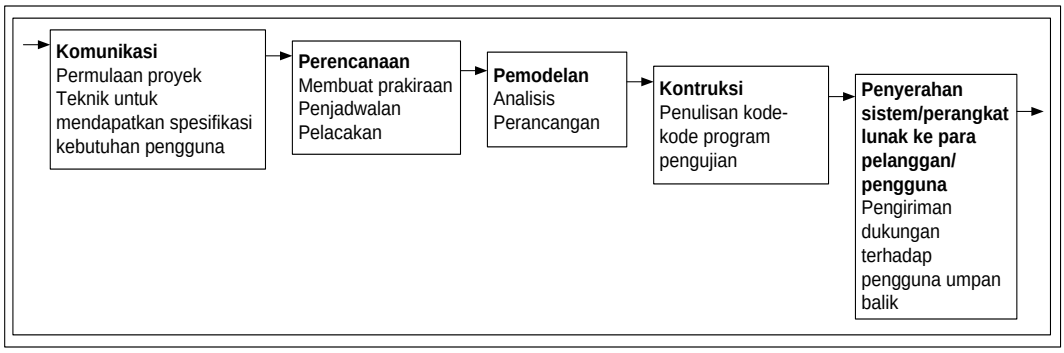
Manfaat dari penelitian ini yaitu :

1. Dengan adanya aplikasi ini diharapkan dapat membuktikan bahwa algoritma RSA dapat diterapkan untuk proses enkripsi dan dekripsi pada *file audio* MP3.
2. Memudahkan proses enkripsi dan dekripsi pada *file audio* MP3 karena sudah tersedia aplikasi tersebut.
3. Dapat mengamankan *file audio* MP3 dengan penerapan algoritma RSA pada aplikasi tersebut.
4. Dapat mengembangkan ilmu pengetahuan terutama pada ilmu pengetahuan mengenai keamanan data dengan kriptografi menggunakan algoritma RSA serta pengalaman membuat sebuah aplikasi.
5. Memenuhi salah satu syarat dalam menempuh gelar S1 (Strata 1).
6. Membantu pemahaman tentang kriptografi terutama pada algoritma RSA untuk enkripsi dan dekripsi data.
7. Dapat dijadikan bahan acuan bagi penelitian lain yang berminat mengkaji permasalahan atau topik yang sama.

1.5 Metodologi Pengembangan Sistem

Metode pengembangan sistem yang digunakan yaitu pengembangan sistem dengan menggunakan model *waterfall*. Model *waterfall* adalah model klasik yang bersifat sistematis, berurutan dalam mengembangkan *software* (Pressman, 2012).

Berikut ini adalah fase-fase dalam model *waterfall* menurut referensi Pressman yang dapat dilihat pada Gambar 1.1



Gambar 1.1 Model *Waterfall* (sumber : Pressman, 2012)

Penjelasan fase-fase yang dilakukan dalam penggunaan model *waterfall* dalam melakukan pengembangan sistem perangkat lunak adalah sebagai berikut:

a. Komunikasi

   Langkah ini merupakan analisis terhadap kebutuhan *software*, dan tahap untuk mengandalkan pengumpulan data dengan melakukan studi pustaka dan studi literatur baik yang ada di jurnal, artikel, maupun dari internet. Pada langkah ini dapat melakukan komunikasi secara tertulis, mencatat semua informasi yang sudah dikumpulkan.

b. Perencanaan

   Proses perencanaan merupakan lanjutan dari proses komunikasi *(analysis requirement)*. Tahapan ini akan menghasilkan data yang berhubungan dengan data pembuatan *software*, termasuk rencana yang dilakukan. Pada langkah ini dapat merencanakan berapa lama pengerjaan dari aplikasi yang akan dibuat dengan membuat jadwal untuk pengerjaan aplikasi tersebut.

c. Pemodelan

Proses pemodelan ini akan menerjemahkan syarat ke sebuah perencanaan *software* yang dapat diperkirakan sebelum dibuat *coding*. Proses ini berfokus pada rancangan struktur data, arsitektur *software*, representasi *interface*, dan detail (algoritma) prosedural. Tahapan ini akan menghasilkan dokumen yang disebut *software requirement*. Pada langkah ini dapat menggunakan *Balsamiq mockups* untuk proses pemodelan.

d. Konstruksi

Konstruksi merupakan proses membuat kode. Pengkodean merupakan penerjemah desain dalam bahasa yang bisa dikenali oleh komputer. *Programmer* akan menerjemahkan transaksi yang diminta. Tahapan inilah yang merupakan tahapan secara nyata dalam mengerjakan suatu *software*, artinya penggunaan komputer akan dimaksimalkan dalam tahapan ini. Setelah pengkodean selesai maka akan dilakukan *testing* terhadap sistem yang telah dibuat. Tujuan *testing* adalah menemukan keslahan-kesalahan terhadap sistem tersebut untuk kemudian bisa diperbaiki. Pada langkah ini dapat menggunakan *Microsoft visual studio* 2010 untuk proses pengkodean.

e. Penyerahan Sistem

Tahapan ini bisa dikatakan final dalam pembuatan sebuah *software* atau sistem. Setelah melakukan analisis, desain dan pengkodean maka sistem yang sudah jadi dapat digunakan. Kemudian *software* yang telah dibuat harus dilakukan pemeliharaan secara berkala, tetapi dalam penelitian ini tidak melakukan penyerahan *software* karena hanya untuk penelitian.

Adapun alasan dan pertimbangan digunakannya model *waterfall* dalam penelitian ini ialah model *waterfall* ini melakukan setiap kegiatannya secara terstruktur dari tahap satu ke tahap berikutnya, dan dilakukan dengan pendekatan sistematis serta berurutan pada pengembangan perangkat lunak. Proses tersebut dimulai dengan spesifikasi kebutuhan pengguna dan berlanjut melaluit tahapan-tahapan komunikasi, perencanaan, pemodelan, konstruksi, serta penyerahan sistem/perangkat lunak ke para pelanggan/pengguna, yang diakhiri dengan dukungan berkelanjutan pada perangkat lunak lengkap.

1.6 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam penelitian ini adalah sebagai berikut:

BAB 1 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 2 LANDASAN TEORI

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

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Bab ini menguraikan kebutuhan dasar yang diperlukan selama proses perancangan perangkat lunak (*software*), meliputi pembahasan mengenaisistem pengamanan *file audio* MP3 dengan algoritma RSA (*Rivest Shamir Adleman*) serta menguraikan tentang gambaran secara umum dari disain dan tampilan-tampilan perangkat lunak (*software*) yang dibangun.

BAB 4 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 5 KESIMPULAN DAN SARAN

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