BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi telekomunikasi dan penyimpanan data digital dengan menggunakan komputer memungkinkan pengiriman data digital jarak jauh. Berbagai jenis layanan komunikasi tersedia di internet, diantaranya adalah *web*, *e-mail*, *milis*, *newsgroup*, dan sebagainya. Maraknya pemanfaatan layanan komunikasi internet tersebut, menimbulkan banyak masalah, ditambah dengan adanya *hacker* dan *cracker*, sehingga sangat memungkinkan data digital yang dikirim dapat disadap dan diubah oleh pihak lain (Sulistyanto, 2004).

Untuk mengamankan data digital tersebut, salah satu cara dapat diterapkan suatu algoritma kriptografi untuk melakukan enkripsi pada data digital. Ada banyak algoritma kriptografi yang dapat digunakan, berdasarkan sifat kuncinya dibagi menjadi dua yaitu simetris yang hanya memakai satu kunci rahasia dan asimetris (*public key algorithm*) yang memakai sepasang kunci publik dan kunci rahasia (Wibowo, 2009). Kriptografi dapat diimplementasikan pada berbagai bentuk format data digital seperti pada data teks, gambar, video, dan audio. Namun kriptografi pada data teks lebih dikenal dikalangan masyarakat luas.

Selain *file* teks, *file* video juga sangat perlu untuk disandikan terlebih dahulu dikarenakan pesan dari *file* video yang bersifat penting dan rahasia. Sebagai contoh yaitu *file* video film, iklan, *tutorial*, dan video klip musik yang sangat rentan terhadap pembajakan. *File* video tersebut harus dijaga kerahasiannya, karena jika *file* video tersebut jatuh ke pihak yang tidak bertanggung jawab, maka akan terjadi aksi pembajakan yang tentunya akan merugikan si pembuat video tersebut. Salah satu cara untuk menjaga kerahasian *file* video tersebut adalah dengan menggunakan aplikasi kriptografi.

Dari sekian banyak algoritma kriptografi kunci publik yang pernah dibuat, algoritma yang paling populer adalah algoritma RSA. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (*Masschussets Institute of Technology*) pada tahun 1976, yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman. Keamanan Algoritma

RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci pribadi. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritmanya, maka selama itu pula keamanan algoritma RSA tetap terjamin.

Sehingga pada kesempatan ini, penulis mencoba membangun suatu aplikasi kriptografi dengan cara melakukan enkripsi dan dekripsi menggunakan algoritma RSA untuk meningkatkan keamanan data digital khususnya pada *file* video dan penulis mengambil judul **"Penerapan Algoritma Kriptografi Asimetris RSA Pada Pesan Video"**.

1.2 Rumusan Masalah

Berdasarkan pada latar belakang yang telah diuraikan sebelumnya, rumusan masalahnya adalah: "Bagaimana membangun aplikasi enkripsi dan dekripsi menggunakan algoritma RSA agar *file* video digital menjadi aman dari tindakan pembajakan?"

1.3 Batasan Masalah

Dalam penelitian ini penulis memberi batasan, antara lain:

1. Yang akan dienkripsi dan didekripsi adalah *file* video
2. *File* video yang akan dienkripsi dan didekripsi berkapasitas 1MB
3. *File* video yang akan dienkripsi dan didekripsi berekstensi .wmv
4. Algoritma enkripsi dan dekripsi menggunakan algoritma RSA

1.4 Tujuan Penelitian

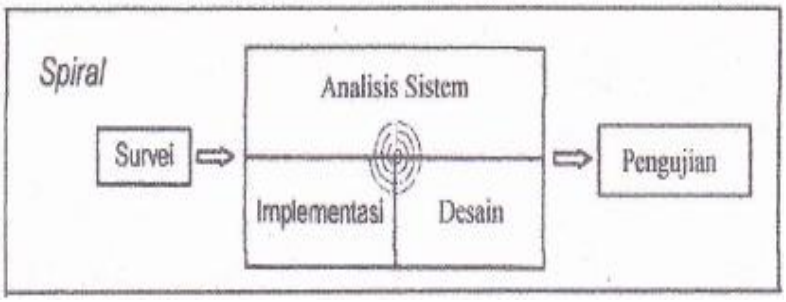
Tujuan penyusunan skripsi ini adalah menghasilkan suatu aplikasi yang dapat digunakan untuk mengenkripsi dan mendekripsi *file* video dengan algoritma RSA agar *file* video tersebut bisa aman dari tindakan pembajakan.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini antara lain:

1. Aplikasi ini dapat digunakan di perusahaan-perusahaan pembuatan film, iklan, *tutorial*, dan pembuatan video klip musik.
2. Dengan adanya aplikasi ini bisa mengurangi tindakan pembajakan pada video digital.
3. Melindungi hak karya cipta pembuat video digital.

1.6 Metodologi Penelitian



Gambar 1.1 Metode *Spiral* (sumber: Sutabri, 2004)

Adapun metodologi penelitian skripsi ini mengikuti metode *spiral* yang tahapan-tahapannya terdiri dari :

1. Survei

   Manfaat dari survei ini adalah untuk menentukan problem-problem atau kebutuhan yang timbul. Survei yang dilakukan oleh penulis antara lain mencari buku-buku dan jurnal-jurnal yang berhubungan dengan judul penelitian yang akan digunakan sebagai referensi di dalam penelitian ini.
2. Analisis Sistem

   Proses pengumpulan data-data yang diperlukan untuk melakukan analisis terhadap hal-hal yang diperlukan dalam pembuatan aplikasi ini, khususnya analis pada *hardware* dan *software*.

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 antara 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 *visual basic 6.0*.

5. Pengujian

   Pada tahap ini akan dilakukan pengujian terhadap sistem yang telah dibangun untuk mengetahui apakah aplikasi ini dapat berfungsi dengan baik. Pengujian yang dilakukan berupa pengujian terhadap aplikasi yaitu menggunakan *blackbox testing* dan *whitebox testing*. Serta akan dilakukan pengujian terhadap waktu proses untuk mengetahui perbedaan waktu proses antara proses enkripsi dengan proses dekripsi pada *file* video dengan kapasitas yang berbeda-beda, dan pengujian keamanan untuk mengetahui kapasitas maksimum *file* video yang dapat dienkripsi.

1.7 Sistematika Penulisan Skripsi

Untuk memberikan gambaran secara garis besar mengenai pembahasan tiap bab yang terdapat dalam skripsi, 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 skripsi, metodologi penelitian, serta sistematika penulisan skripsi.

BAB II LANDASAN TEORI

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

BAB III PERANCANGAN SISTEM

Bab ini menguraikan kebutuhan dasar yang diperlukan selama proses pengembangan perangkat lunak, meliputi pembahasan mengenai algoritma RSA 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.