1. Pendahuluan

1.1 Latar Belakang Masalah

Perkembangan multimedia yang sangat pesat diberbagai bidang mengakibatkan berbagai permasalahan seperti penyalahgunaan akses dan penjiplakan yang telah menimbulkan dampak yang serius terhadap permasalahan legal, social dan ekonomi. Jika ada pihak ketiga yang ingin mengakses video tanpa otoritas, mereka hanya akan mendapatkan video yang datanya telah terenkripsi. Tidak semua video yang ada dibuat untuk konsumsi public. Banyak dari video tersebut bersifat pribadi/*privacy*, yang hanya ditujukan untuk kelompok tertentu saja. Tantangan terbesar dalam enkripsi file multimedia yaitu ukuran file yang relative besar dan aspek *real-time*.

Pada umumnya, data multimedia memiliki nilai yang lebih rendah dibandingkan dengan data digital lainnya (seperti data rahasia pada sebuah perusahaan, informasi bank, dll). Teknologi baru telah meningkatkan kebutuhan akan keamanan multimedia serta perlindungan hak cipta. Pengimplementasian kebutuhan akan keamanan bisa saja nilai nya lebih mahal dibandingkan dengan nilai dari data multimedia yang akan diamankan tersebut dalam hal ini video. Hal ini dapat mengakibatkan pemborosan dana. Untuk itu diperlukan suatu teknik enkripsi yang dapat memenuhi dua faktor penting dalam enkripsi video yaitu efisiensi dan tingkat keamanan. Enkripsi selektif adalah salah satu metode yang dapat mengatasi permasalahan performansi. Enkripsi selektif merupakan sebuah teknik untuk mengenkripsi sebagian porsi dari data video, sedangkan data lainnya dibiarkan sebagaimana adanya. Pada transmisi video, enkripsi selektif sangatlah berguna agar aspek *real-time* terpenuhi. Pada enkripsi selektif, algoritma *chipper* apapun dapat digunakan. Algoritma RSA adalah salah satu dari *public-key cryptosystem* yang sangat sering digunakan untuk memberikan privasi terhadap keaslian suatu data digital. Keamanan enkripsi/dekripsi data model ini terletak pada kesulitan untuk memfaktorkan modulus n yang sangat besar.

1.2 Perumusan Masalah

Permasalahan yang akan diangkat dalam tugas akhir ini adalah :

1. Merancang keamanan video MPEG dengan menggunakan enkripsi selektif dengan algoritma RSA

2. Membangun perangkat lunak enkripsi dan deskripsi video MPEG dengan menggunakan platform java
3. Melakukan pengujian terhadap perangkat lunak tersebut
4. Menganalisis hasil implementasi yang telah dilakukan dengan pengukuran parameter : waktu prosses, *rasio*, *bitrate* dan analisis keamanan (*brute force attack)*
5. Perangkat lunak ini merupakan aplikasi berbasis desktop dan data yang digunakan terbagi 2, yaitu data yang terenkripsi atau yang terdeskripsi

1.3 Tujuan

Berdasarkan rumusan masalah di atas, maka tujuan akhir tugas akhir ini adalah:

1. Menganalisis dan mengimplementasikan metode enkripsi selektif dengan menggunakan algoritma RSA untuk menunjukkan keamanan video dapat direalisasikan dengan menggunakan metode tersebut
2. Menganalisis performansi sistem enkripsi dan dekripsi video MPEG yang telah dibangun

1.4 Hipotesis

Penggunaan metode enkripsi selektif pada kasus video MPEG dengan menggunakan algoritma RSA akan dapat memenuhi faktor penting pada enkripsi file multimedia yaitu tingginya efisiensi pemrosesan (waktu proses dan *bitrate*) dan terjaminnya tingkat keamanan (kekuatan chipper, waktu dalam memecahkan kunci).

1.5 Metodologi Penyelesaian Masalah

Metodologi penyelesaian masalah yang akan digunakan adalah :

1. Studi Literatur

   Pada tahap ini akan dilakukan pemahaman konsep tentang metoda enkripsi selektif, algoritma RSA, format data visual pada video MPEG dan cara kerja java
2. Analisis kebutuhan dan perancangan sistem

   Pada tahap ini dilakukan analisis dan perancangan terhadap sistem yang akan dibangun serta menganalisis metode yang akan digunakan untuk menyelesaikan permasalahan, termasuk menentukan arsitektur sistem, bahasa pemrograman yang digunakan, fungsionalitas, dan antarmuka aplikasi.
3. Implementasi dan pembangunan sistem

Pada tahap ini dilakukan penerapan hasil rancangan desain dan analisisi yang terdiri dari:

a. Pengkodean metode enkripsi selektif dengan algoritma RSA
b. Pembuatan antarmuka/interface aplikasi.

4. Pengujian dan Analisis Hasil

   Pengujian dan analisi dilakukan dengan cara :

   a. Melakukan analisis perbandingan efisiensi enkripsi selektif antara video berformat MPEG-1 dengan MPEG-2 secara objektif
   b. Melakukan analisis perbandingan parameter-parameter yang telah ditetapkan antara video MPEG-1 dengan MPEG-2
   c. Melakukan analisis pengaruh enkripsi selektif terhadap efisiensi pemrosesan keamanan
   d. Melakukan analisis keamanan dengan menggunakan algoritma RSA dengan parameter *brute force attack*

5. Pengambilan kesimpulan dan pembuatan laporan Tugas Akhir

   Pada tahap ini akan diambil kesimpulan berdasarkan hasil pengujian dan analisis dan penyusunan laporan hasil penelitian berupa buku Tugas Akhir.

1.6 Sistematika Penulisan

Tugas akhir ini disusun dengan sistematika penulisan sebagai berikut :

BAB I Pendahuluan

Bab ini berisi latar belakang, perumusan masalah, tujuan dan batasan masalah dari tugas akhir, metodologi yang digunakan dalam menyelesaikan tugas akhir ini serta sistematika penulisan buku tugas akhir.

BAB II Dasar Teori

Bab ini berisi penjelasan singkat mengenai konsep-konsep yang mendukung dikembangkannya sistem ini. Konsep-konsep yang digunakan untuk mendukung sistem ini adalah uraian mengenai keamanan informasi dengan Kriptografi, metode enkripsi selektif, Algoritma RSA dan Kriptoanalisis dengan *Brute Force Attack*.

BAB III Analisis dan Perancangan Sistem

Bab ini berisi analisis kebutuhan sistem serta rancangan sistem secara terstruktur yang tertuang dalam bentuk *Unified Modeling Language (UML)*.

BAB IV Implementasi dan Analisis Hasil Pengujian

Bab ini berisi hasil implementasi dan pengujian metode selektif dengan algoritma RSA serta analisis perbandingan dari hasil pengujian tersebut.

BAB V Kesimpulan dan Saran

Bab ini berisi tentang kesimpulan yang didapat dari pelaksanaan tugas akhir ini dan saran-saran yang diperlukan untuk perbaikan maupun pengembangannya lebih lanjut.