BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era modern saat ini, pertukaran informasi multimedia seperti video melalui media elektronik telah berkembang pesat dan menjadi salah satu hal yang sering dilakukan saat beberapa individu saling berkomunikasi. Akan tetapi perkembangan ini menimbulkan berbagai permasalahan seperti penyalahgunaan akses dan penjiplakan. Tidak semua video yang ada ditujukan untuk umum. Banyak dari video tersebut bersifat pribadi dan hanya dapat diakses oleh kelompok tertentu saja (Ramsky, 2009). Mengingat sebagian video yang ada harus dijaga kerahasiaannya selama proses pengiriman, sementara media komunikasi yang digunakan adalah media umum yang rentan terhadap penyadapan, pemalsuan, dan lain-lain, maka keamanan informasi saat pertukaran informasi video berlangsung perlu diperhatikan. Contohnya, pada aplikasi *video on demand*, hanya orang yang berkepentingan saja yang memiliki akses untuk mendapatkan datanya.

Satu cara yang paling mudah untuk dilakukan untuk melindungi video adalah menutup akses yang tidak sah. Namun, cara ini tidak dapat memastikan video yang ada aman apabila ada yang berhasil mengakses *server* secara langsung. Solusi lain yang dapat dilakukan adalah dengan mengenkripsi seluruh *bit stream* dengan algoritma kriptografi seperti DES (*Data Encryption Standard*) atau IDEA (*International Data Encryption Algorithm*) (Bhagarva, Shi, & Wang, 2002). Masalahnya algoritma kriptografi tersebut memiliki komputasi yang rumit, sehingga tidak cukup cepat untuk memproses sejumlah data besar yang dihasilkan (Apostolopoulos, Tan, & Wee, 1999). Selain itu, implementasi dari algoritma kriptografi ini tidak cukup cepat untuk memproses sejumlah besar data yang dihasikan oleh aplikasi multimedia.

Ada tiga hal yang perlu diperhatikan dari enkripsi data multimedia (Seidel, Socek, & Sramka, 2005). Pertama, ukuran *file* yang sangat besar dibandingkan dengan teks. Kedua, data video harus diproses secara *real-time*. Memproses

sejumlah besar data saat *real-time* dengan algoritma kriptografi yang rumit akan memperberat kinerja komputer serta jaringannya dan juga tidak nyaman untuk orang yang menonton video tersebut secara *real-time* karena dapat menyebabkan *delay*. Ketiga, fungsi *playback* atau *fast-forward* harus tersedia dan dapat berjalan dengan normal. (Seidel, Socek, & Sramka, 2005).

Banyak algoritma enkripsi video yang telah dibangun sampai saat ini. Tetapi, algoritma yang umum digunakan terutama untuk aplikasi video *streaming* adalah algoritma VEA (*Video Encryption Algorithm*). Alasan banyaknya penggunaan algoritma ini adalah karena tingkat keamanannya yang cukup memuaskan, komputasi yang ringan, dan cocok diimplementasikan di lingkungan video *streaming*. (Apostolopoulos, Tan, & Wee, 1999). Algoritma VEA juga digunakan karena merupakan algoritma yang ringan dan unggul dalam hal efisiensi dibanding DES atau IDEA (Seidel, Socek, & Sramka, 2005). Walaupun demikian, algoritma VEA memiliki tingkat keamanan yang relatif rendah (Seidel, Socek, & Sramka, 2005). Untuk meningkatkan keamannya, maka VEA dapat dikombinasikan dengan algoritma kunci rahasia seperti DES atau AES.

1.2 Perumusan Masalah

Permasalahan yang akan diteliti dan diuraikan dalam tugas akhir ini adalah :

1. Bagaimana mengimplementasikan algoritma VEA yang dimodifikasi untuk melakukan enkripsi dan dekripsi video?
2. Bagaimana membangun aplikasi berbasis *web* yang menerapkan algoritma VEA yang telah dimodifikasi untuk enkripsi dan dekripsi video?
3. Bagaimana hasil enkripsi dan *streaming* video yang menggunakan algoritma VEA yang telah dimodifikasi ?

1.3 Batasan Masalah

Penelitian tugas akhir ini dibatasi pada :

1. Video yang digunakan dalam proses enkripsi adalah video dengan format *MPEG4-MP4*.
2. Aplikasi yang dikembangkan berbasis *web*.

1.4 Tujuan Penelitian

Tujuan penelitian tugas akhir ini adalah :

1. Mengimplementasikan algoritma VEA yang telah dimodifikasi untuk melakukan enkripsi dan dekripsi video.
2. Membangun aplikasi berbasis *web* yang menerapkan algoritma VEA yang telah dimodifikasi untuk enkripsi dan dekripsi video.
3. Menganalisa hasil enkripsi dan dekripsi video yang menggunakan algoritma VEA yang telah dioptimasi.

1.5 Manfaat Penelitian

Manfaat penelitian tugas akhir ini adalah mencegah penjiplakan video dalam usaha perlindungan hak cipta dengan cara mengakses *server* secara langsung.

1.6 Sistematika Penulisan Laporan Penelitian

Sistematika penulisan laporan penelitian dibagi menjadi lima bab, yaitu :

1. BAB I PENDAHULUAN

   Bab ini berisi latar belakang diperlukannya enkripsi video, rumusan masalah yang akan diteliti dalam enkripsi video dengan algoritma yang telah ditentukan , batasan masalah, tujuan penelitian, manfaat penelitian, metode serta sistematika penulisan laporan penelitian, serta sistematika penulisan laporan penelitian.

2. BAB II TINJAUAN PUSTAKA

   Bab ini berisi teori-teori yang digunakan dalam perancangan, implementasi dan analisis penelitian. Terdiri dari teori tentang video *streaming*, algoritma *Video Encryption Standard*, kriptografi, algoritma *Advanced Encryption Standard*, optimasi algoritma *Video Encryption Algorithm.*

3. BAB III ANALISIS DAN PERANCANGAN SISTEM

   Bab ini berisi metode penelitian, analisis masalah umum tentang sistem yang akan dibuat, masalah yang ditemukan dari analisis masalah tersebut, spesifikasi kebutuhan sistem,dan juga perancangan sistem.

4. BAB IV IMPLEMENTASI DAN EVALUASI

   Bab ini berisi hasil penelitian, mulai dari proses implementasi sistem yang dibuat, spesifikasi perangkat lunak maupun perangkat keras yang digunakan dalam pembangunan sistem, proses pengujian sistem, penjelasan cara pemakaian sistem serta evaluasi dari sistem yang dibuat

5. BAB V SIMPULAN DAN SARAN

   Bab ini berisi simpulan dan saran, pada bagian simpulan akandiuraikan jawaban atas masalah serta tujuan penelitian yang dipaparkan pada BAB I, beserta informasi yang ditemukan pada penelitian. Sedangkan pada bagian saran, diuraikan hal-hal yang masih dapat diteliti untuk penelitian selanjutnya.