BAB I
PENDAHULUAN

1.1 LatarBelakang

Keamanan data multimedia sangat penting dalam bisnis komersil maupun tidak komersil. Contohnya, pada aplikasi *video on demand*, hanya orang yang membayar yang dapat menonton video tersebut. Selain itu juga pada aplikasi *video conferencing*, hanya orang yang berkepentingan saja yang dapat ikut serta dalam konferens itersebut dan mendapatkan datanya.

Salah satu cara untuk mengamankan aplikasi *distributed multimedia* seperti pada contoh-contoh di atas adalah dengan mengenkripsinya menggunakan algoritma kriptografi seperti DES (*Data Encryption Standar*) atau IDEA (*International Data Encryption Algorithm*). Masalahnya, algoritma kriptografi tersebut memiliki komputasi yang rumit. Implementasi dari algoritma kriptografi ini tidak cukup cepat untuk memproses sejumlah besar data yang dihasilkan oleh aplikasi multimedia. Dua hal yang dapat diperhatikan dari enkripsi data multimedia. Pertama, ukuran data multimedia biasanya sangat besar. Sebagai contoh, ukuran data dari video MPEG-1 berdurasi dua jam kira-kira 1 GB. Kedua, data multimedia harus diproses dengan *delay* sekecil mungkin.

Banyak algoritma enkripsi video yang telah dibangun sampai saat ini, tetapi algoritma yang umum digunakan terutama untuk aplikasi video *streaming* adalah algoritma *Video Encryption*, atau sering disebut juga VEA *(Video Encryption Algorithm)*. Pada algoritma ini *byte-byte* pada *frame* video, di-XOR-kan dengan suatu *byte* kunci tertentu yang telah didefinisikan. Hasil operasi XOR tersebut kemudian diterapkan pada *file* video, sehingga video yang dihasilkan memiliki kualitas gambar tidak sempurna. Video hasil enkripsi dengan VEA itulah yang nantinya diterima oleh *user* yang tidak berhak atau belum memasukkan kunci tertentu yang telah didefinisikan. Alasan banyaknya penggunaan algoritma ini adalah karena tingkat keamanannya yang cukup memuaskan, komputasi yang ringan, dan cocok diimplementasikan di lingkungan video *streaming* karena algoritmanya yang dapat berbasis *stream cipher* maupun *block cipher*, tergantung kebutuhan saat *streaming* video tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan secara jelas diatas, maka rumusan masalah ditekankan pada:

1. Bagaimana proses mengenkripsi dan mendekripsi video *streaming* MPEG dengan algoritma *Video Encryption Algorithm* (VEA).

1.3 Batasan Masalah

Beberapa hal yang menjadi batasan masalah dalam pembuatan program ini yaitu :

1. Tidak mempelajari maupun membuat *encoder* dan *decoder* (*player*) video.
2. File format video yang digunakan hanya Mpeg-1 dan Mpeg-2.
3. Data yang dienkrispi adalah data video tanpa audio.
4. Bahasa pemograman yang digunakan untuk pembuatan aplikasi ini adalah C#.
5. Aplikasi yang digunakan untuk membuat dan menyunting *listing* program adalah *Microsoft Visual Studio* 2008 versi 9.0.21022.8 RTM dan .NET *Framework* versi 3.5 SP1.
6. Menggunakan *library* FFMPEG untuk men-*decode file* video mpeg dan menampilkannya.
7. Komunikasi antar komputer menggunakan protokol TCP/IP dalam jaringan komputer lokal (LAN) yang menggunakan perangkat tambahan jaringan yaitu *switch.*
8. Tipe *streaming* yang digunakan adalah *peer to peer* atau *unicast.*

1.4 Tujuan

Tujuan dari penyusunan skripsi ini adalah merancang dan mengimplementasikan aplikasi untuk kriptografi pada video *streaming* MPEG menggunakan algoritma VEA.

1.5 Manfaat

Manfaat yang diharapkan adalah aplikasi yang dibuat dalam skripsi ini dapat mengamankan video *streaming* MPEG menggunakan algoritma VEA.

1.6 Sistematika Penulisan

Sistematika penulisan laporan skripsi ini adalah sebagai berikut :

BAB I Pendahuluan

Dalam bab ini akan dijelaskan latar belakang, rumusan masalah, batasan masalah, tujuan dan manfaat, metode penelitian dan sistematika penulisan laporan tugas akhir.

BAB II Dasar Teori

Dalam bab ini akan dibahas dan dijelaskan mengenai dasar teoritisyang menjadi landasan dan mendukung pelaksanaan penulisan tugas akhir.

BAB III Metodologi

Dalam bab ini akan membahas tentang metode yang dipakai penulis untuk menyelesaikan laporan tugas akhir.

BAB IV PerancangandanImplementasi

Dalam bab ini menjelaskan langkah-langkah perancangan dan implementasi dari video *streaming* MPEG menggunakan algoritma VEA.

BAB V Pengujian

Dalam bab ini akan disampaikan hasil pengujian dari aplikasi yang telah dibuat.

BAB VI Kesimpulan dan Saran

Dalam bab ini berisi kesimpulan dan saran.