BAB VI
KESIMPULAN DAN SARAN

6.1 Kesimpulan

Dari perancangan, pembuatan dan pengujian aplikasi kriptografi video *streaming* menggunakan algoritma VEA dapat diambil kesimpulan yaitu:

1. Algoritma enkripsi video yaitu algoritma VEA dengan menggunakan algoritma enkripsi kunci rahasia fungsi *hash* yaitu *message digest* 5 (MD5) berhasil ditetapkan dan diimplementasikan sesuai dengan hasil pengujian. *Transmitter*, *receiver*, beserta proses enkripsi dan dekripsi video di dalamnya dapat berjalan dengan baik. *Transmitter* mengirimkan paket-paket data video yang tersimpan di komputer *transmitter* dan paket-paket data video tersebut dienkripsi terlebih dahulu sebelum dikirim. *Receiver* menerima paket-paket data video, kemudian mendekripsinya terlebih dahulu sebelum dijalankan di *display* video. Jika kunci untuk mengenkripsi dan mendekripsi paket data tidak sama antara *transmitter* dan *receiver*, *receiver* akan mendekripsi paket-paket data video yang dikirim *transmitter* tersebut namun data tersebut akan terlihat acak atau tidak jelas. Hal ini menunjukkan bahwa model enkripsi video *streaming* yang dirancang dan dibangun ke dalam bentuk perangkat lunak berhasil diimplementasikan.
2. Secara umum, penerapan algoritma VEA terhadap video *streaming* tidak membebani kinerja dari video *streaming*-nya itu sendiri. Pengujian menunjukkan bahwa perbedaan waktu yang dibutuhkan antara model *streaming* video menggunakan VEA dengan model *streaming* video yang tidak menggunakan VEA tidak berbeda jauh hanya berkisar kurang lebih 2 detik.
3. Performansi dari algoritma VEA dan MD5 yang digunakan untuk membangun model *streaming* video tidak terpengaruh oleh panjang kunci yang diberikan. Hasil pengujian berdasarkan panjang kunci pada video mpeg-1 dipeoleh waktu sekitar 11 detik dan pada video mpeg-2 diperoleh waktu sekitar 6 detik. Performansi waktu yang dihasilkan konstan walau dengan panjang kunci yang beragam baik dari panjang kunci yang hanya 1 karakter sampai ribuan karakter.

Oleh karena itu, dapat disimpulkan bahwa penerapan algoritma VEA terhadap video *streaming* memberikan banyak dampak positif, terutama karena pengiriman datanya yang menjadi lebih aman, komputasi ringan, dapat diterapkan kepada *file* video walaupun ukuran *file* video tersebut sangat besar, dan selain itu juga penerapan model *streaming* video menggunakan VEA tidak membebani kinerja *streaming* video.

6.2 Saran

Dalam peranangan dan pembuatan aplikasi ini masih terdapat kekurangan dan kelemahan, oleh karena itu masih diperlukan penyempurnaan untuk pengembangan kedepannya. Berikut adalah beberapa hal yang perlu diperhatikan dan disempurnakan :

1. Perlu ditambahkan algoritm auntuk pause untuk *display* video saat *client* belummendapatkan *byte-byte* yang akan diolah dari *server* saat *streaming* karena permasalahan koneksi.
2. Memanfaatkan algoritma kompresi video untuk pengembangan perangkat lunak berikutnya. Dengan algoritma kompresi video, video *streaming* akan memiliki *bit rate* yang lebih kecil sehingga beban pada jaringan lebih ringan.
3. Pengembangan perangkat lunak untuk video-audio *streaming*.
4. Masih terdapat banyak algoritma enkripsi video lain yang dapat dianalisis dan dibandingkan dengan algoritma enkripsi video yang telah dibahas dalam tugas akhir ini. Untuk algoritma enkripsi videonya sendiri, masih ada MVEA dan RVEA sedangkan algoritma enkripsi kunci rahasia lain misalnya seperti AES, Triple DES, RSA, El-gamal, dan lain-lain.
5. Penggunaan format-format video lain seperti .avi, .rmbv, .flv, dan lain sebagainya terutama yang mendukung format-format video terbaru yang muncul saat ini.
6. Perlu dilakukan pengujian dengan menggunakan komputer yang lebih banyak untuk mengetahui tingkat performan sisistem.

DAFTAR PUSTAKA

[1] Stallings, William. 2005. *Cryptography and Network Security, 4th edition*.

[2] Munir, Rinaldi, M.T. 2006. *Diktat Kuliah IF5054 Kriptografi*. STEI ITB.

[3] Ramsky, Tessa. 2005. *Perangkat Lunak Enkripsi Video MPEG-1 dengan Modifikasi Video encryption algorithm*. Sekolah Teknik Elektro dan Informatika-ITB.

[4] Bhagarva, Bharat. Shi, Changgui. Wang, Sheng-Yih. 2002. *MPEG Video Encryption Algorithms*. USA : Purdue University.

[5] Apostolopoulos, John. Tan, Wai-tian.Wee, Susie. 1999. *MPEG Video Encryption in Real-time Using Secret Key Cryptography*. USA : Purdue University.

[6] Munir, Rinaldi, M.T. 2006. *Fungsi Hash Satu-ArahdanAlgoritma MD5.* STEI ITB.

[7] Anonymous. 2012. *Documentation*. http://libav.org/documentation.html. (diakses tanggal 3 Maret 2012).

[8] Anonymous. 2012. *Sourcemd5*. http://www.flowgroup.fr/download/DemoMD5.zip (diakses tanggal 3 Maret 2012)

[9] Anonymous. 2012. *Gambar Struktur File Format MPEG*. http://www.fh-friedberg.de/fachbereiche/e2/telekom-labor/zinke/mk/mpeg2beg/videobit.gif (diakses tanggal 8 Maret 2012)

[10] Anonymous. 2012. *ffmpeg.* http://dranger.com/ffmpeg. (diakses tanggal 9 April 2012)

[11] Anonymous. 2012. *Tutorial*. http://www.csharp-station.com/Tutorial.aspx (diakses tanggal 21 April 2012)

[12] Anonymous. 2012. *Tabel Struktur Start Code Header MPEG - Tabel Start Code - Tabel Stream ID.* http://dvd.sourceforge.net/dvdinfo/mpeghdrs.html (diakses tanggal 5 Mei 2012)

[13] Anonymous. 2012. *Tabel Minimum Spesifikasi Microsoft Visual Studio 2008.* http://social.msdn.microsoft.com/Forums/en/vssetup/thread/8f1fc4a7-1c2b-4af8-86a6-be7903510e18 (diakses tanggal 9 Mei 2012)