ENKRIPSI SELEKTIF VIDEO MPEG DENGAN ALGORITMA RSA

Prati Hutari Gani[1], Maman Abdurrohman S.t[2], M.t[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Tugas Akhir ini membahas perancangan keamanan video dengan menerapkan metode enkripsi selektif dalam mengamankan data video. Pada umumnya, data video memiliki nilai yang lebih rendah dibandingkan dengan data digital lainnya (seperti data rahasia pada sebuah perusahaan, informasi bank, dll). Maka dari itu enkripsi selektif dipilih dalam mengamankan data video karena 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. Enkripsi dilakukan dengan algoritma RSA, 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.

MPEG-1 dan MPEG-2 merupakan format video yang digunakan pada tugas akhir ini, karena kedua format tersebut memiliki struktur bitstream yang hampir sama, sehingga pemrosesannya dapat dilakukan dengan satu algoritma. Data visual yang akan dienkripsi adalah pada lapisan picture yaitu frame I dan frame P. keamanan video dapat dicapai dengan mengenkripsi data ini.

Pada tugas akhir ini akan dibangun sebuah perangkat lunak dengan menggunakan platform Java berdasarkan perancangan. Pengujian yang dilakukan yaitu dengan mengenkripsi dan mendekripsi video dengan format MPEG-1 dan MPEG-2. Hasil pengujian mengujian bahwa keamanan video dapat direalisasikan dengan menggunakan metode enkripsi selektif dan key length pada algoritma RSA yang sesuai untuk diimplementasikan dan sesuai dengan kebutuhan yang dapat dilihat pada parameter Brute Force Attack.

Kata Kunci : Video MPEG, Kriptografi, Selektif, RSA, Brute Force Attack

---

Abstract

This final project discusses the design of video security by applying selective encryption method to secure the video data. In general, the video data has a lower value compared with other digital data (such as confidential data on a company, bank information, etc.). Therefore selective encryption to secure the data selected in the video for selective encryption is one method that can resolve performance problems. Selective encryption is a technique to encrypt a portion of the video data, while other data is left as it is. Encryption uses RSA algorithm, one of the public-key cryptosystem that is very often used to provide privacy to the authenticity of the digital data. Security encryption / decryption of data this model is the difficulty of factoring the modulus n is very large.

MPEG-1 and MPEG-2 are the video format used in this final project, since both formats have bitstream structures are virtually identical, so that the processing can be done with a same single algorithm. Visual data to be encrypted is the layer of the picture frame I and frame P. Video security can be achieved by encrypting the data.

In this final project will be built a software using the Java platform based design. Tests conducted is to encrypt and decrypt video with MPEG-1 and MPEG-2. Test results video examines the security can be realized by using selective encryption method and key length corresponding to the RSA algorithm to be implemented and in accordance with the needs that can be seen on the parameters of Brute Force Attack.

Keywords : MPEG Video, Cryptography, Selective, RSA, Brute Force attack

---

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.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan analisis dan pengujian yang telah dilakukan dapat ditarik beberapa kesimpulan sebagai berikut.

1. Metode enkripsi selektif dengan menggunakan algoritma RSA dapat diimplementasikan dalam proses kriptografi video MPEG
2. Performansi metode enkripsi selektif dengan algoritma RSA dapat dilihat pada lama waktu proses enkripsi. Terdapat 2 hal yang mempengaruhi lamanya waktu enkripsi, yaitu: jumlah data yang dienkripsi (ratio) dan *key length* (panjang bit kunci). Jumlah data yang dienkripsi (ratio) dipengaruhi oleh jumlah *frame I* dan *frame P* yang akan dienkripsi.
3. Performansi disini dilihat dari kecepatan pemrosesan enkripsi, pada percobaan ini metode enkripsi selektif tidak akan begitu berpengaruh keunggulannya dari sisi kecepatan jika dikombinasikan dengan algoritma RSA dengan panjang kunci diatas 64 bit karena kecepatan pemroresan enkripsi yang dihasilkan sangat lambat.
4. Implementasi enkripsi selektif akan mudah dilakukan jika menggunakan stream cipher daripada block cipher. Karena pada enkripsi selektif membutuhkan informasi dari data yang tersebar pada stream dengan ukuran yang berbeda-beda. Algoritma RSA merupakan stream cipher yaitu tidak memerlukan data yang tetap dalam proses enkripsinya sehingga dapat memperkecil kompleksitas algoritma karena tidak diperlukan proses penggabungan data-data tersebut sebelum enkripsi dilakukan.
5. Algoritma RSA memiliki tingkat keamanan data video yang tinggi, karena dari hasil percobaan dengan menggunakan *brute force attack* dibutuhkan waktu yang cukup lama untuk menembus keamanan algoritma RSA.
6. Dengan menggunakan metode enkripsi selektif data video hasil enkripsi memiliki format yang sama dengan data asli sehingga dapat diputar pada decoder standar, tetapi data-data visualnya tidak dapat dikenali lagi.
7. Enkripsi selektif akan lebih efisien jika diterapkan dalam pengamanan video berformat MPEG-2 dibandingkan dengan video berformat MPEG-1

5.2 Saran

Untuk pengembangan sistem yang lebih baik, terdapat beberapa hal yang dapat dikembangkan, yaitu:

1. Sistem dapat dikembangkan dengan menggunakan algoritma kunci lain untuk meningkatkan performansi dan keamanan
2. Sistem dapat dikembangkan dengan menggunakan *video streaming* sehingga dapat diketahui hal-hal lain yang dapat mengetahui proses enkripsi dan transmisi data
3. Sistem dapat dikembangkan dengan skema enkripsi selektif lainnya

Daftar Pustaka

[1] Firmansah. *Kompresi Video Menggunakan Standar MPEG*. Teknik Elektro Universitas Udayana, Bali. 2011

[2] Furht, Borko dan Darko Kirovski, *Multimedia Encryption and Authentication Techniques and Applications.*Auerbach Publication, New York. 2006

[3] Heriyanto, Tedi. *Pengenalan Kriptografi Edisi 005*.27 Juni 1999

[4] http://www.cs.cf.ac.uk/Dave/Multimedia/node262.html

[5] Iswari, Ni Made Satvika. *Rancangan dan Implementasi Algoritma Pembangkitan Kunci Kombinasi antara Algoritma RSA dan ElGamal.* STEI Institut Teknologi Bandung, Bandung. 2011

[6] J. Meyer dan F. Gadegast. Security Mechanism for Multimedia Data with the Example mpeg-1 Video. Avaible on WWW via http://www.powerweb.de/phade/phade.html.1995.

[7] Kurniawan, Anselmus Krima Adi. *Kriptografi Visual Pada Berkas Video.* STEI Institut Teknologi Bandung, Bandung.

[8] L. Tang, *"Methods for Encrypting and Decrypting MPEGVideo Data Efficiently", Proceedings of the 4'th ACM International Conference on Multimedia*, Boston, MA, 1996, pp. 2 19-229.

[9] Li-Wu, Tsung dan Felix Wu, S. *Selective Encryption and Watermarking of MPEG Video (Extended Abstract).* Computer Science Depertment, North Carolina State University. 1997

[10] Nursanto, Djoko. *Meningkatkan Kecepatan Deskripsi RSA menggunakan Integrasi Metode Montgomery Multification Chinese Remainder Theorem (CRT).* Program Pasca Sarjana Departemen Teknik Elektro, Institut Teknologi Bandung, Bandung. 2003

[11] Nursanto, Djoko. *Tinjauan mengenai aplikasi metode Montgomery Multiflication-Chinese Remainder Theorem (CRT) dalam mempercepat deskripsi RSA.* STEI Intstitut Teknologi Bandung, Bandung. 2003.

[12] Oni, Marvello. *Algoritma Enkripsi pada Video MPEG.* STEI Institut Teknologi Bandung, Bandung.

[13] Pratama, Arief. *Enkripsi Selektif Video MPEG dengan Algoritma Serpent.* STEI Institut Teknologi Bandung, Bandung.

[14] Richardson, Iain E. G. *Video Codec Design. John Wiley & Sons Ltd*. 2002

[15] Rinaldi Munir. *Data encryption standart (des). Technical report*, Program Studi Teknik Informatika Institut Teknologi Bandung., 2005.

[16] T.B. Maples dan G.A. Spanos. *Performace Study of a Selective Encryption Scheme for the Security of Networked, Real-time Video. In Proceedings of 4th International Conference on Computer Communications and Networks*, Las Vegas, Nevada, September 1995.

[17] Uhl, Andreas dan Andreas Pommer. *Image and Video Encryption From Digital Rights Management to Secured Personal Communication*. Springer. 2005

[18] Wikipedia. 2012. *Kriptografi*. http://id.wikipedia.org/wiki/Kriptografi

[19] Wikipedia. 2010. *Kriptoanalisis*. Available At http://id.wikipedia.org/wiki/Kriptoanalisis.

[20] Wikipedia. 2010. *Brute force attack*. http://en.wikipedia.org/wiki/Brute_force_attack.

[21] www.bojacamp.multiply.com/journal/item/

[22] X. Liu and A. M. Eskicioglu, *"Selective Encryption of Multimedia Contents in Distribution Networks: Challenges and New Directions," IASTED*

International Conference on Communications, Internet, and Information Technology (CIIT 2003), Scottsdale, AZ, November 17-19,2003.
[23] Snell & Wilcox, *"MPEG Encoding Basics"*, www.snellwilcox.com.
[24] http://dvd.sourceforge.net/dvdinfo/mpeghdrs.html