IMPLEMENTASI ALGORTIMA KRIPTOGRAFI ADVANCED ENCRYPTION STANDARD (AES) DAN DIGITAL RIGHTS MANAGEMENT (DRM) UNTUK MELINDUNGI HAK CIPTA DIGITAL ARTS BERBENTUK FILE AUDIO

Trio Prayogi Marta[1], R. Rumani M [2], Surya Michrandi Nasution[3]

[1]Sistem Komputer, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita dan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data.
Digital Rights Management (DRM) adalah suatu sistem yang ditujukan untuk mengatasi permasalahan yang terkait dengan pengaturan akses dan distribusi materi digital yang menjamin hak dan kewajiban antara pemilik.
Dalam tugas akhir ini dibuat sebuah implementasi yang menggabungkan kriptografi dan DRM untuk file berbentuk digital audio agar file digital audio tersebut tidak dibajak atau didistribusikan secara ilegal. File audio terlebih dahulu dienkripsi lalu diunggah ke cloud lalu menggunakan mp3 player yang telah dibuat khusus agar file audio yang diunduh tidak bisa dimainkan pada mp3 player lainnya.
Algoritma AES 128 bit yang akan diimplementasikan memiliki perfomansi yang baik, hal ini dapat dilihat pada nilai Avalanche Effect yang diberikan berkisar antara 0.40 – 0.53. File audio memiliki perbedaan frekuensi saat sesudah dienkripsi dengan rata-rata perubahan frekuensi 0.24x dari frekuensi semula.

Kata Kunci : Kriptografi, DRM, AES, File Audio

Abstract

Generally cryptography is the science and art of maintaining the confidentiality of news and the study of mathematical techniques related to information security such as data confidentiality, data authenticity, data integrity, and authentication of data.
Digital Rights Management (DRM) is a system intended to overcome the problems associated with setting up the access and distribution of digital material which ensures rights and obligations between the owner.
In this final project is made an implementation that combines cryptography and DRM for digital audio files in order to form a digital audio file can not be pirated or distributed illegally. First audio file is encrypted and uploaded to the cloud and then use a mp3 player that has been made to the audio files that are downloaded can not be played on other mp3 player.
Algorithm AES-128 bit that implemented have a good performance, this can be seen at the given value of Avalanche Effect ranged from 0.40 to 0.53. Audio files have different frequencies while after encrypted with the average change in frequency of 0.24x original frequency.

Keywords : Cryptography, DRM, AES, Audio Files

BAB 1

PENDAHULUAN

1. 1 Latar Belakang

Perkembangan dunia teknologi *digital* saat ini berkembang sangat pesat, yang dulunya adalah masa-masa dimana segalanya serba analog sekarang menjadi dunia *digital*. File, musik, lukisan dll berubah dan bisa dinikmati secara *digital*. Dulunya sebuah musik berupa piringan hitam, pita rekaman berubah menjadi format *digital*. Lukisan yang dulunya berupa goresan kuas diatas kertas kanvas berubah menjadi *digital*.

Karena berbentuk *digital*, maka tindak laku pembajakan juga semakin pesat, pembajakan hak cipta dari pemilik asli sebuah *digital audio* semakin marak saat ini. Oleh karena itu diperlukan enkripsi *digital* untuk melindungi hak cipta dari pemilik sebuah *digital audio*.

Untuk mengatasi masalah tersebut, muncul metode kriptografi dan *Digital Rights Management* (DRM). Aspek utama dari metode ini adalah mengenkripsi data *digital audio* dan membatasi penggunaan lagu tersebut untuk dimainkan pada mp3 player lainnya.

Oleh karena itu, penulis membuat implementasi metode enkripsi dan DRM untuk digital audio. Metode yang digunakan adalah mengenkripsi lagu terlebih dahulu dengan algoritma kriptografi AES lalu membatasi penggunaan lagu yang diunduh pada player lain.

1. 2 Rumusan Masalah

Rumusan masalah yang diangkat penulis, yaitu:

a) Cara membatasi penggunaan lagu pada *mp3 player* lainnya;

b) Proses enkripsi dan dekripsi *file mp3* dengan algoritma kriptografi AES;

c) Melihat spektrum *digital audio* saat sebelum dan sesudah dienkripsi dan pengujian apa saja yang dilakukan.

1. 3 Batasan Masalah

Masalah apa yang akan dibahas :

a) *File audio* yang digunakan adalah format mp3;

b) Algoritma kriptografi yang digunakan adalah AES-128 bit;

c) Diimplementasikan pada *software* berbasis *desktop*.

1. 4 Tujuan

Tujuan penyusunan tugas akhir ini adalah:

a) merancang bagaimana lagu yang diunduh oleh *client* tidak bisa dibajak;

b) melindungi *digital audio* sebelum proses pengiriman data ke *cloud* menggunakan algoritma kriptografi AES-128 bit;

c) Membuat implementasi algoritma kriptografi dengan performa yang baik.

1. 5 Metodologi Penelitian

Langkah yang ditempuh untuk menyelesaikan tugas akhir ini adalah:

a) Studi literature, mengumpulkan bahan referensi dari buku, jurnal, *ebook* dll yang berhubungan dengan tugas akhir ini;

b) Merancang diagram alir atau *flow chart* untuk implementasinya;

c) Melakukan uji coba menggunduh file audio yang terenkripsi saat transfer data dan didekripsi pada *mp3 player*;

d) Menganalisa hasil uji coba dari segi performa AES-128bit.

1.6 Sistematika Penulisan

Tugas akhir ini dibagi dalam beberapa topik bahasan yang disusun secara sistematis dan terdiri dari:

BAB 1 PENDAHULUAN

Berisi latar belakang, rumusan masalah, tujuan, batasan masalah, metodologi penelitian, dan sistematika penulisan.

BAB 2 DASAR TEORI

Berisi teori-teori dasar mengenai *digital* audio, kriptografi, algortima kriptografi AES.

BAB 3 PERANCANGAN DAN IMPLEMENTASI

Berisi konfirugarsi umum sistem, perancangan sistem, keluaran yang dihasilkan, dan analisis performansi.

BAB 4 PENGUJIAN SISTEM DAN ANALISIS

Berisi data hasil pengujian terhadap file audio yang sudah terenkripsi apakah berhasil terenkripsi atau tidak.

BAB 5 KESIMPULAN DAN SARAN

Berisi kesimpulan dari penelitian yang sudah dilakukan dan saran pengembangan dan perbaikan selanjutnya.

BAB 5
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dilihat dari hasil pengujian, dapat ditarik kesimpulan sebagai berikut.

1. Perbedaan ukuran *file* lagu dapat mempengaruhi waktu enkripsi dan dekripsi file audio. Penambahan 1MB ukuran file akan menambah 0.38 detik waktu enkripsi dan 0.19 detik waktu dekripsi.
2. Dari 10 lagu yang diuji pada 3 *mp3 player* lainnya, hanya ada 1 lagu yang bisa dimainkan tapi tidak ada suara yang dihasilkan. DRM membatasi penggunaan lagu pada mp3 player lainnya jika ada pendistribusian lagu secara ilegal.
3. Bentuk gelombang *digital audio* memiliki perbedaan saat sebelum dan sesudah enkripsi, dengan rata-rata perubahan frekuensi menjadi 0.24x dari frekuensi semula
4. Algoritma kriptografi AES-128bit yang dibuat menghasilkan performa yang baik. Dari hasil yang diberikan ada perubahan 52 bit – 67 bit pada keluaran dengan merubah 1 bit data masukan.

5.2 Saran

Aplikasi yang telah dibuat untuk mengimplementasikan algoritma kriptografi AES-128bit dan DRM ini tentu saja masih perlu pengembangan agar bisa melindungi hak cipta lebih baik lagi. Saran yang dapat diajukan untuk pengembangan lebih lanjut sebagai berikut.

Menggunakan format *audio* lainnya seperti WAV/AAV/M4A. Menggunakan algoritma AES-192 bit atau AES-256 bit untuk dinilai performanya serta mengembangkan antarmuka *mp3 player* yang lebih baik dan dapat berjalan di perangkat *mobile*.

DAFTAR PUSTAKA

[1] Pohlmann, K. (2010). *Principles of Digital Audio, Sixth Edition.*

[2] Andriansyah, M. (2009). Privacy Engineering dalam Teknologi Digital Right Management untuk Keamanan Produsen, Distributor dan Konsumen. *Jurnal Teknik Informatika Universitas Gunadarma* .

[3] Layton, J. (2008). *How Digital Rights Management Works*. Retrieved November 8, 2012, from howstuffworks?: http://computer.howstuffworks.com/drm.htm

[4] Prayudi, Y. (2010). Digital Right Management (DRM) Berbasis XrML. *Jurnal Teknik Informatika Universitas Islam Indonesia* .

[5] Alfred J. Menezes, P. C. (2010). *Handbook of Applied Cryptography.*

[6] Sadikin, R. (2012). *Kriptografi Untuk Keamanan Jaringan.* Yogyakarta: Penerbit ANDI.

[7] (2009, July 01). Retrieved November 8, 2012, from T.E.G.U.H | Yes. Just t.e.g.u.h: http://teguh.blogdetik.com/tag/drm/

[8] *Top 10 Music Player.* (n.d). Retrieved June 13, 2014, from Softonic:http://en.softonic.com/s/top-10-music-player-software-free-download-2014/downloads

[9] Pressman, R. (2014*). Software Engineering: A Practitioner's Approach*. McGraw-Hill Science/Engineering/Math

[10] Munir, R. (2010). *Algortima dan Pemograman dalam Bahasa Pascal dan C*. INFORMATIKA