DIGITAL RIGHTS MANAGEMENT MENGGUNAKAN ALGORITMA *RIVEST CODE 4* PADA KONTEN AUDIO DIGITAL

SKRIPSI

DINDA YUNITA

1310511027

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI TEKNIK INFORMATIKA

2017

DIGITAL RIGHTS MANAGEMENT MENGGUNAKAN ALGORITMA *RIVEST CODE 4* PADA KONTEN AUDIO DIGITAL

SKRIPSI

Diajukan Sebagai Salah Satu Syarat Untuk Memperoleh Gelar Sarjana Komputer

DINDA YUNITA

1310511027

UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN" JAKARTA

FAKULTAS ILMU KOMPUTER

PROGRAM STUDI TEKNIK INFORMATIKA

2017

PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya sendiri, dan semua sumber yang dikutip maupun yang dirujuk telah saya nyatakan dengan benar.

Nama : Dinda Yunita

NIM : 1310511027

Tanggal : 11 Juli 2017

Bilamana di kemudian hari ditemukan ketidaksesuaian dengan pernyataan saya ini, maka saya bersedia dituntut dan diproses sesuai dengan ketentuan yang berlaku.

Jakarta, 11 Juli 2017

Yang Menyatakan,

(Dinda Yunita)

PERNYATAAN PERSETUJUAN PUBLIKASI SKRIPSI UNTUK KEPENTINGAN AKADEMIS

Sebagai civitas akademik Universitas Pembangunan Nasional "Veteran" Jakarta, saya yang bertanda tangan di bawah ini :

Nama : Dinda Yunita

NIM : 1310511027

Fakultas : Ilmu Komputer

Program Studi : Teknik Informatika

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pembangunan Nasional "Veteran" Jakarta Hak Bebas Royalti Non eksklusif (*Non-exclusive Royalty Free Right*) atas karya ilmiah saya yang berjudul :

***Digital Rights Management* Menggunakan Algoritma *Rivest Code 4* Pada Konten Audio Digital**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti ini Universitas Pembangunan Nasional "Veteran" Jakarta berhak menyimpan, mengalih media/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Skripsi saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta. Demikian penyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta

Pada tanggal : 11 Juli 2017

Yang menyatakan,

(Dinda Yunita)

PENGESAHAN

Skripsi diajukan oleh :

Nama : Dinda Yunita

NIM : 1310511027

Program Studi : Teknik Informatika

Judul Skripsi : Digital Rights Management Menggunakan Algoritma Rivest Code 4 Pada Konten Audio Digital

Telah berhasil dipertahankan di hadapan Tim Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Komputer pada Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Pembangunan Nasional "Veteran" Jakarta.

Dr. Nidjo Sandjojo, M.Sc.
Ketua Penguji

Nurul Chamidah, S.Kom., M.Si.
Penguji I

Henki Bayu S., S.Kom., M.T.I.
Pembimbing I

Dr. Nidjo Sandjojo, M.Sc.
Dekan

Vini Indriasari, S.T., M.Sc., Ph.D.
Ketua Program Studi

Ditetapkan di : Jakarta

Tanggal Ujian : 11 Juli 2017

DIGITAL RIGHTS MANAGEMENT MENGGUNAKAN ALGORITMA RIVEST CODE 4 PADA KONTEN AUDIO DIGITAL

Dinda Yunita

Abstrak

Digital Rights Management (DRM) merupakan salah satu sistem yang dapat melindungi audio digital dari pembajakan. DRM dapat di implementasikan menggunakan algoritma kriptografi simetris. Algoritma kriptografi simetris adalah algoritma yang menggunakan kunci yang sama untuk kegiatan enkripsi dan dekripsi. Penelitian ini dilakukan untuk mengimplementasikan DRM menggunakan algoritma *Rivest Code 4* melalui tahapan *key scheduling algorithm* dan *pseudo random generation algorithm* sehingga menghasilkan audio yang terenkripsi dan dapat di dekripsi kembali melalui tahapan yang sama seperti proses enkripsi. Penelitian ini menghasilkan aplikasi yang dapat digunakan untuk melindungi audio digital dengan cara melakukan proses enkripsi dan dekripsi. Hasil pengujian menunjukkan bahwa audio yang telah di enkripsi tidak dapat didengar dengan jelas, tetapi audio yang telah di dekripsi dapat didengar dengan jelas dan menghasilkan kualitas audio yang sama dengan audio yang asli. Audio yang telah di enkripsi mengalami penurunan intensitas suara terhadap audio aslinya hingga 45,37 %. Ukuran dan panjang audio dapat mempengaruhi durasi yang dibutuhkan untuk proses enkripsi maupun dekripsi. Proses enkripsi dan dekripsi yang dilakukan juga tidak memberikan perubahan terhadap besar ukuran *original audio* maupun *encrypted audio*.

Kata Kunci : *Digital Rights Management*, Kriptografi, *Rivest Code 4*, Audio Digital

DIGITAL RIGHTS MANAGEMENT USING RIVEST CODE 4 ALGORITHM IN AUDIO DIGITAL CONTENT

Dinda Yunita

Abstract

Digital Rights Management (DRM) is one of system that can protect audio digital from the piracy. DRM can be implemented using a symmetric cryptography algorithm. A symmetric cryptography algorithm is an algorithm that uses the same key for encryption and decryption activities. This study was conducted to implement DRM using Rivest Code 4 algorithm through the stages of the key scheduling algorithm and the pseudo random generation algorithm to produce the encrypted audio and can be decrypted again through the same stages as the encryption process. This study produces application that can be used to protect audio digital by doing the process of encryption and decryption. The test results show that the encrypted audio can not be heard clearly, but the decrypted audio can be heard clearly and produce the same audio quality as the original audio. The encrypted audio has decreased the sound intensity up to 45.37%. The size and length of the audio can affect the duration required for encryption and decryption process. The encryption and decryption process also does not give any size change of the original audio or the encrypted audio.

Keywords : Digital Rights Management, Cryptography, Rivest Code 4, Audio Digital

KATA PENGANTAR

Puji dan syukur penulis panjatkan ke hadirat Allah SWT atas segala karunia-Nya, sehingga skripsi ini berhasil diselesaikan. Penulisan skripsi ini dapat diselesaikan dengan baik dan lancar karena tak lepas dari bantuan berbagai pihak. Oleh karena itu penulis ingin mengucapkan terima kasih kepada :

1. Bapak Henki Bayu Seta, S.Kom., M.T.I selaku dosen pembimbing yang telah banyak memberikan saran yang bermanfaat dalam proses penyusunan skripsi ini.
2. Bapak Dr. Nidjo Sandjojo. M.Sc selaku Dekan Fakultas Ilmu Komputer.
3. Ibu Vini Indriasari, S.T., M.Sc., Ph.D. sebagai Kepala Program Studi Teknik Informatika.
4. Ayah, Ibu, dan Kakak tercinta, terima kasih tak terhingga atas doa, semangat, kasih sayang, dan ketulusannya dalam mendampingi penulis selama ini.
5. Vita, Amelia, dan Apriany, terima kasih telah menjadi sahabat terbaik yang selalu ada dalam kondisi apapun.
6. Brigita Ferlina, Olga Dara, Shifa Femia, Amallia Rafsanjani, Riqmah Fairus, Nabila Khairunnisa, Agung Dwi, Mochamad Fikri, Agung Septian, dan Adittiya Veriawan, terima kasih atas kebersamaan selama hampir 4 tahun yang begitu berwarna, kalian lebih dari sekedar teman masa perkuliahan.
7. Teman-teman BEMF-IK dan SMF-IK 2015/2016, terima kasih atas kenangan yang begitu berharga dan tak terlupakan.
8. Teman-teman TI angkatan 2013, terutama TI lokal A.

Penulis menyadari bahwa tugas akhir ini masih jauh dari sempurna. Oleh karena itu kritik dan saran sangat diharapkan. Penulis berharap tugas akhir ini dapat memberi manfaat bagi kita semua.

Jakarta, 11 Juli 2017

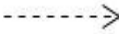
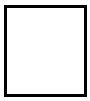
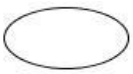
Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR SIMBOL

Simbol Use Case Diagram			
NO	**GAMBAR**	**NAMA**	**KETERANGAN**
1		*Actor*	Menspesifikasikan himpuan peran yang pengguna mainkan ketika berinteraksi dengan *use case*.
3		*Include*	Menspesifikasikan bahwa *use case* sumber secara *eksplisit*.
4		*Extend*	Menspesifikasikan bahwa *use case* target memperluas perilaku dari *use case* sumber pada suatu titik yang diberikan.
5		*Association*	Apa yang menghubungkan antara objek satu dengan objek lainnya.
6		*System*	Menspesifikasikan paket yang menampilkan sistem secara terbatas.
7		*Use Case*	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu aktor

Simbol Actifity Diagram			
NO	**GAMBAR**	**NAMA**	**KETERANGAN**
1		*Actify*	Memperlihatkan bagaimana masing-masingkelas antarmuka saling berinteraksi satu sama lain
2		*Action*	State dari sistem yang mencerminkan eksekusi dari suatu aksi

3		*Initial Node*	Bagaimana objek dibentuk atau diawali.
4		*Actifity Final Node*	Bagaimana objek dibentuk dan dihancurkan
5		*Fork Node*	Satu aliran yang pada tahap tertentu berubah menjadi beberapa aliran

Simbol Sequence Diagram			
NO	**GAMBAR**	**NAMA**	**KETERANGAN**
1		*LifeLine*	Objek *entity*, antarmuka yang saling berinteraksi.
2		*Message*	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi
3		*Message*	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi

DAFTAR LAMPIRAN