



***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 pernyataan 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



Dr. Nidjo Sandjojo, M.Sc.
Dekan



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

Pembimbing I



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

| | |
|-------------------------------------------------------|------|
| HALAMAN JUDUL..... | i |
| PERNYATAAN ORISINALITAS..... | ii |
| PERNYATAAN ORISINALITAS PERSETUJUAN PUBLIKASI | iii |
| PENGESAHAN | iv |
| ABSTRAK..... | v |
| ABSTRACT | vi |
| KATA PENGANTAR | vii |
| DAFTAR ISI | viii |
| DAFTAR TABEL | xi |
| DAFTAR GAMBAR | xii |
| DAFTAR SIMBOL | xiii |
| DAFTAR LAMPIRAN..... | xv |
| | |
| BAB 1 PENDAHULUAN | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 2 |
| 1.3 Ruang Lingkup | 2 |
| 1.4 Tujuan Penelitian | 3 |
| 1.5 Manfaat Penelitian | 3 |
| 1.6 Luaran yang Diharapkan | 3 |
| 1.7 Sistematika Penulisan | 4 |
| | |
| BAB 2 TINJAUAN PUSTAKA..... | 5 |
| 2.1 <i>Digital Rights Management</i> | 5 |
| 2.1.1 Definisi <i>Digital Rights Management</i> | 5 |
| 2.1.2 Tiga Entitas Utama dalam Konsep DRM | 6 |
| 2.1.3 DRM pada Audio Digital | 6 |
| 2.1.4 Keuntungan dan Kerugian DRM | 7 |
| 2.1.5 Cara Kerja DRM | 8 |
| 2.2 Kriptografi | 9 |
| 2.2.1 Definisi Kriptografi | 9 |
| 2.2.2 Komponen Kriptografi | 10 |

| | | |
|---------|----------------------------------------|----|
| 2.2.3 | Algoritma Kriptografi | 12 |
| 2.3 | <i>Rivest Code 4</i> | 14 |
| 2.4 | Audio | 17 |
| 2.4.1 | Jenis Pengolah Audio | 17 |
| 2.4.2 | Penentu Kualitas Audio Digital | 17 |
| 2.4.3 | <i>Waveform Audio Format</i> | 17 |
| 2.5 | Bahasa Pemrograman Matlab | 19 |
| 2.5.1 | Definisi Matlab | 19 |
| 2.5.2 | Bagian-bagian Utama Matlab | 20 |
| 2.5.3 | Kelebihan Matlab | 20 |
| 2.6 | Metodologi Penelitian | 21 |
| 2.6.1 | Metode Pengumpulan Data | 21 |
| 2.6.1.1 | Studi Pustaka | 21 |
| 2.6.1.2 | Studi Literatur | 21 |
| 2.6.2 | Metode Pengembangan Sistem | 21 |
| 2.7 | <i>Unified Modeling Language</i> | 23 |
| 2.7.1 | <i>Use Case Diagram</i> | 23 |
| 2.7.2 | <i>Activity Diagram</i> | 23 |
| 2.7.3 | <i>Sequence Diagram</i> | 23 |
| 2.8 | Studi Literatur | 23 |
| | | |
| BAB 3 | METODOLOGI PENELITIAN..... | 26 |
| 3.1 | Metode Pengumpulan Data | 26 |
| 3.1.1 | Studi Pustaka | 26 |
| 3.1.2 | Studi Literatur | 26 |
| 3.2 | Metode Pengembangan Sistem | 27 |
| 3.2.1 | Fase Perencanaan Syarat-syarat | 27 |
| 3.2.2 | Fase <i>Workshop Design</i> | 27 |
| 3.2.3 | Fase Konstruksi | 28 |
| 3.2.4 | Fase Implementasi..... | 28 |
| 3.3 | Alat Bantu Penelitian | 29 |
| 3.3.1 | Alat Penelitian | 29 |
| 3.3.2 | Objek Penelitian | 29 |
| 3.4 | Jadwal Penelitian | 30 |

| | |
|------------------------------------------|--------|
| BAB 4 HASIL DAN PEMBAHASAN..... | 31 |
| 4.1 Fase Perencanaan Syarat-syarat | 31 |
| 4.1.1 Analisis Kebutuhan | 31 |
| 4.1.2 Menentukan Tujuan | 32 |
| 4.1.3 Menentukan Syarat-syarat | 32 |
| 4.2 Fase <i>Workshop Design</i> | 32 |
| 4.2.1 Perancangan Proses | 32 |
| 4.2.1.1 Proses Enkripsi | 33 |
| 4.2.1.2 Proses Dekripsi | 34 |
| 4.2.2 Perancangan Sistem | 35 |
| 4.2.2.1 <i>Use Case Diagram</i> | 35 |
| 4.2.2.2 <i>Activity Diagram</i> | 38 |
| 4.2.2.3 <i>Sequence Diagram</i> | 41 |
| 4.2.3 Perancangan Antarmuka | 43 |
| 4.2.3.1 Perancangan Form Enkripsi | 43 |
| 4.2.3.2 Perancangan Form Dekripsi | 44 |
| 4.2.3.3 Perancangan Form Help | 45 |
| 4.3 Fase Konstruksi | 45 |
| 4.4 Fase Implementasi | 47 |
| 4.4.1 Cara Penggunaan Aplikasi | 47 |
| 4.4.1.1 Aplikasi Enkripsi | 48 |
| 4.4.1.2 Aplikasi Dekripsi | 51 |
| 4.4.2 Implementasi Algoritma RC4 | 55 |
| 4.4.3 Pengujian Aplikasi | 59 |
| BAB 5 PENUTUP | 65 |
| 5.1 SIMPULAN | 65 |
| 5.2 SARAN | 65 |
| DAFTAR PUSTAKA | 67 |
| RIWAYAT HIDUP | |
| LAMPIRAN | |



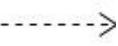



DAFTAR TABEL



| | | |
|------------|------------------------------------------|----|
| Tabel 3.1 | Jadwal Penelitian..... | 30 |
| Tabel 4.2 | Use Case Enkripsi..... | 36 |
| Tabel 4.3 | Use Case Dekripsi..... | 36 |
| Tabel 4.4 | Use Case Help..... | 37 |
| Tabel 4.5 | Kesesuaian Proses Enkripsi | 59 |
| Tabel 4.6 | Kesesuaian Proses Dekripsi | 60 |
| Tabel 4.7 | Hasil Kesesuaian Data | 60 |
| Tabel 4.8 | Pengujian Kualitas Audio | 61 |
| Tabel 4.9 | Pengujian Intensitas Suara | 62 |
| Tabel 4.10 | Pengujian Audio | 63 |
| Tabel 4.11 | Pengujian Ukuran dan Panjang Audio | 64 |




DAFTAR GAMBAR

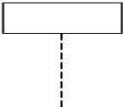


| | | |
|-------------|---------------------------------------------------|----|
| Gambar 2.1 | Arsitektur Digital Rights Management..... | 8 |
| Gambar 2.2 | Proses RC4 | 15 |
| Gambar 3.3 | Metodologi penelitian | 29 |
| Gambar 4.4 | Flowchart Proses Enkripsi | 33 |
| Gambar 4.5 | Flowchart Proses Dekripsi | 34 |
| Gambar 4.6 | Use Case Diagram..... | 35 |
| Gambar 4.7 | Activity Diagram Enkripsi Audio | 38 |
| Gambar 4.8 | Activity Diagram Dekripsi Audio | 39 |
| Gambar 4.9 | Activity Diagram Help..... | 40 |
| Gambar 4.10 | Sequence Diagram Enkripsi | 41 |
| Gambar 4.11 | Sequence Diagram Dekripsi | 42 |
| Gambar 4.12 | Sequence Diagram Help | 43 |
| Gambar 4.13 | Menu Utama Enkripsi | 44 |
| Gambar 4.14 | Menu Utama Dekripsi..... | 45 |
| Gambar 4.15 | Form Help | 45 |
| Gambar 4.16 | Tampilan Form Enkripsi..... | 48 |
| Gambar 4.17 | Tampilan Open File Audio (Plaintext)..... | 49 |
| Gambar 4.18 | Tampilan Input Kunci Enkripsi | 49 |
| Gambar 4.19 | Message Box Enkripsi Berhasil | 50 |
| Gambar 4.20 | Tampilan Save Output | 50 |
| Gambar 4.21 | Message Box Audio Berhasil Disimpan..... | 51 |
| Gambar 4.22 | Tampilan Perbedaan Audio pada Form Enkripsi..... | 51 |
| Gambar 4.23 | Tampilan Utama Form Dekripsi..... | 52 |
| Gambar 4.24 | Tampilan Pilih Lokasi Audio (Ciphertext) | 52 |
| Gambar 4.25 | Tampilan Open File Audio | 53 |
| Gambar 4.26 | Tampilan Input Kunci Dekripsi | 53 |
| Gambar 4.27 | Tampilan Perbedaan Audio pada Form Dekripsi | 54 |
| Gambar 4.28 | Tampilan Form Help | 55 |
| Gambar 4.29 | Grafik Penurunan Intensitas Suara..... | 63 |

DAFTAR SIMBOL

| Simbol Use Case Diagram | | | |
|--------------------------------|-------------------------------------------------------------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------|
| NO | GAMBAR | NAMA | KETERANGAN |
| 1 |  | <i>Actor</i> | Menspesifikasikan himpunan peran yang pengguna mainkan ketika berinteraksi dengan <i>use case</i> . |
| 3 |  | <i>Include</i> | Menspesifikasikan bahwa <i>use case</i> sumber secara <i>eksplisit</i> . |
| 4 |  | <i>Extend</i> | Menspesifikasikan bahwa <i>use case</i> target memperluas perilaku dari <i>use case</i> sumber pada suatu titik yang diberikan. |
| 5 |  | <i>Association</i> | Apa yang menghubungkan antara objek satu dengan objek lainnya. |
| 6 |  | <i>System</i> | Menspesifikasikan paket yang menampilkan sistem secara terbatas. |
| 7 |  | <i>Use Case</i> | 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 |  | <i>Actifity</i> | Memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain |
| 2 |  | <i>Action</i> | State dari sistem yang mencerminkan eksekusi dari suatu aksi |

| | | | |
|---|-----------------------------------------------------------------------------------|----------------------------|----------------------------------------------------------------------|
| 3 |  | <i>Initial Node</i> | Bagaimana objek dibentuk atau diawali. |
| 4 |  | <i>Activity Final Node</i> | Bagaimana objek dibentuk dan dihancurkan |
| 5 |  | <i>Fork Node</i> | Satu aliran yang pada tahap tertentu berubah menjadi beberapa aliran |

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

DAFTAR LAMPIRAN

- Lampiran 1 Grafik Sinyal Audio
- Lampiran 2 Source Code