IMPLEMENTASI PENGAMANAN MP3 MENGGUNAKAN ALGORITMA ADVANCED ENCRYPTION STANDARD

SKRIPSI

Disusun Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Komputer
pada Departemen Ilmu Komputer/ Informatika

Disusun oleh:

Ismaya Khusnu Wicaksana

J2F009085

DEPARTEMEN ILMU KOMPUTER / INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO
2016

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini :

Nama : Ismaya Khusnu Wicaksana

NIM : J2F009085

Judul : Implementasi Pengamanan MP3 Menggunakan Algoritma Advanced Encryption Standard

Dengan ini saya menyatakan bahwa dalam tugas akhir/skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Semarang, 27 Juni 2016

(materai)

Ismaya Khusnu Wicaksana

J2F009085

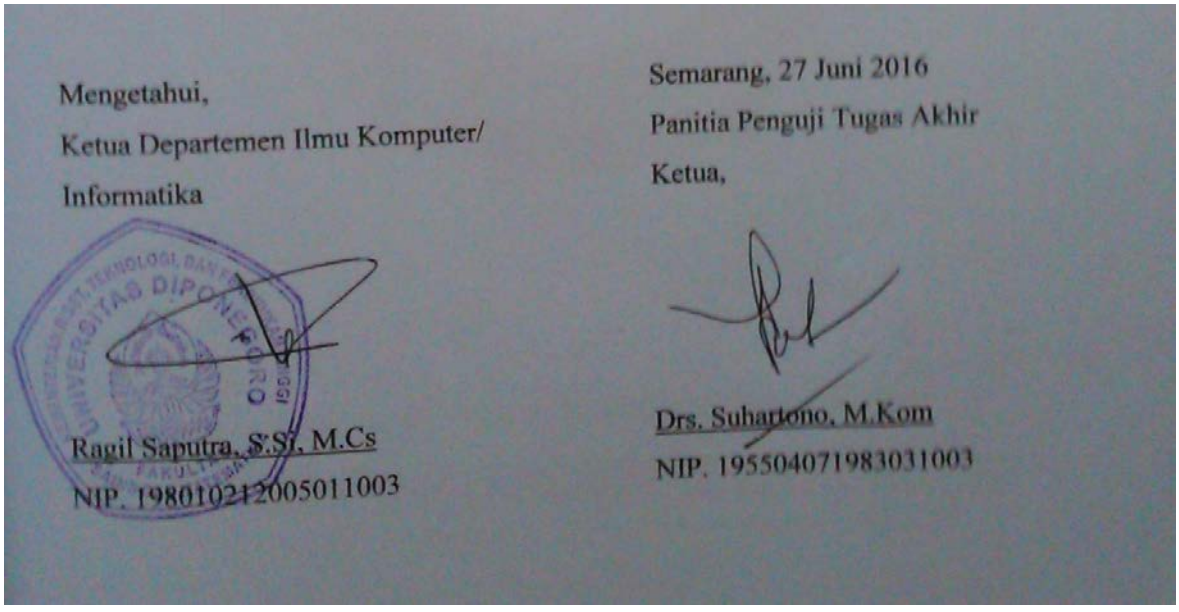
HALAMAN PENGESAHAN

Nama : Ismaya Khusnu Wicaksana

NIM : J2F009085

Judul : Implementasi Pengamanan MP3 Menggunakan Algoritma Advanced Encryption Standard

Telah diujikan pada sidang akhir pada tanggal 23 Juni 2016 dan dinyatakan lulus pada tanggal 27 Juni 2016.



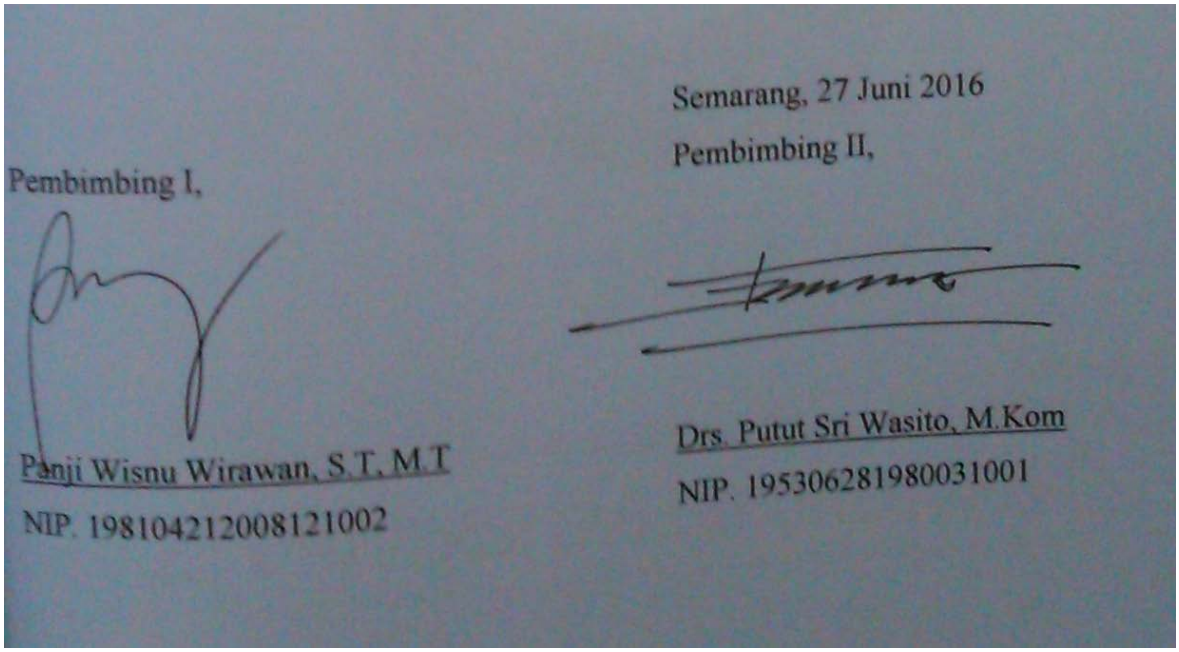
HALAMAN PENGESAHAN

Nama : Ismaya Khusnu Wicaksana

NIM : J2F009085

Judul : Implementasi Pengamanan MP3 Menggunakan Algoritma Advanced Encryption Standard

Telah diujikan pada sidang akhir pada tanggal 23 Juni 2016 dan dinyatakan lulus pada tanggal 27 Juni 2016.



ABSTRAK

Format MP3 merupakan salah satu format suara yang populer. Format ini tidak memiliki implementasi keamanan sehingga dapat menimbulkan beberapa dampak negatif. Salah satu dampak negatifnya adalah resiko terhadap keamanan MP3 yang berisi informasi rahasia. Kelemahan tersebut dapat dihilangkan dengan menerapkan proses enkripsi pada *file* MP3. Algoritma kriptografi Advanced Encryption Standard (AES) dipilih karena pada algoritma ini belum ditemukan celah keamanan, dipelihara dengan baik oleh NIST dan merupakan algoritma yang sering digunakan dalam implementasi keamanan. Implementasi Pengamanan MP3 Menggunakan AES merupakan suatu bentuk implementasi pengamanan dengan melakukan proses enkripsi terhadap *file* MP3 tanpa merusak struktur *file* MP3 sehingga *file* tersebut masih dapat dijalankan pada beragam MP3 *player* dan menghasilkan *noise* saja. *File* MP3 dapat dikembalikan ke bentuk yang sama seperti sedia kala dengan melakukan proses dekripsi. Hasil tersebut dapat dicapai dengan melakukan proses enkripsi selektif terhadap data yang terletak di dalam setiap *frame* pada *file* MP3. Implementasi ini berupa aplikasi yang dibuat dengan menggunakan bahasa pemrograman C++ dengan menggunakan pendekatan Pemrograman Berbasis Objek (PBO) serta penggunaan *framework* Qt. Aplikasi ini diuji dengan menggunakan beberapa MP3 dengan parameter-parameter yang berbeda serta metode pengujian *blackbox testing*. Dari hasil pengujian, aplikasi yang telah dibuat berfungsi sesuai dengan tujuan dan harapan yaitu dapat melindungi *file* MP3 serta mengembalikannya seperti sedia kala. .

Kata kunci : *Advanced Encryption Standard* (AES), MP3, Keamanan, C++, Kriptografi

ABSTRACT

MP3 format is one of popular audio formats. Having no security implementation, this audio format has a few downsides. One of the downsides are security risk of classified digital audio data in the MP3. Those downsides could be eliminated by applying encryption process to the MP3. Advanced Encryption Standard (AES) encryption algorithm selected because it has no security flaw, well maintained by NIST and it's a more common algorithm used in security implementation. Implementation of MP3 Security using Advanced Encryption Standard (AES) is a form of MP3 security implentation where encryption process preserves the structure of MP3 file itself. It is resulting in an encrypted MP3 file which is still playable on various MP3 players although it only generates noises. The MP3 file can be decrypted to return to its original form. This implementation is taking form of a computer application that has been created using C++ language with Object-Oriented Programming (OOP) approach and using Qt framework. The application was tested with a few MP3 each with different parameters and blackbox testing method. From the testing, its concluded that the application working as expected from encryption process of MP3 data to decryption process.

Keywords : Advanced Encryption Standard (AES), MP3, Security, C++, Cryptography

KATA PENGANTAR

Segala puji syukur bagi Allah SWT atas karunia-Nya yang diberikan kepada penulis sehingga penulis dapat menyelesaikan penulisan laporan tugas akhir yang berjudul "Implementasi Pengamanan MP3 Menggunakan Advanced Encryption Standard ".

Laporan ini disusun untuk melengkapi pengambilan mata kuliah Tugas Akhir (TA). Dalam penyusunan laporan ini tentulah banyak mendapat bimbingan dan bantuan dari berbagai pihak. Untuk itu, pada kesempatan ini penulis mengucapkan rasa hormat dan terima kasih kepada:

1. Ragil Saputra, S.Si, M.Cs, selaku Ketua Jurusan Ilmu Komputer/ Informatika yang telah membantu dalam proses TA.
2. Helmie Arif Wibawa,S.Si, M.Cs, selaku Koordinator TA yang telah membantu dalam proses pengambilan mata kuliah TA.
3. Panji Wisnu Wirawan, S.T, M.T dan Drs. Putut Sri Wasito, M.Kom, selaku dosen pembimbing yang telah membimbing hingga terselesaikannya laporan TA ini.
4. Indra Waspada, ST, MTI, yang telah membantu memberikan semangat dan dukungan untuk kelancaran proses TA.
5. Teman-teman Informatika Undip Angkatan 2009 yang telah memberikan semangat dan membantu dalam banyak hal yang memperlancar proses pembuatan TA.

Penulis menyadari bahwa dalam laporan ini masih banyak kekurangan baik dari segi materi ataupun dalam penyajiannya karena keterbatasan kemampuan dan pengetahuan penulis. Oleh karena itu, kritik dan saran sangat penulis harapkan. Semoga laporan ini dapat bermanfaat bagi pembaca pada umumnya dan penulis pada khususnya.

Semarang, 27 Juni 2016

Penulis,

Ismaya Khusnu Wicaksana

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

1. 1. Latar Belakang

MP3 merupakan salah satu *format* data suara yang populer (International Federation of the Phonographic Industry, 2013). Selain ukurannya yang kecil, MP3 juga mempunyai reproduksi suara yang cukup bagus serta implementasi algoritma yang relatif mudah.

Format MP3 tidak mempunyai implementasi keamanan sehingga menimbulkan beberapa dampak negatif. Salah satu dampak negatifnya adalah resiko mengenai keamanan data suara jika *file* MP3 mengandung informasi yang bersifat rahasia. Dampak lainnya adalah meningkatnya pembajakan file MP3 yang disebabkan mudahnya proses duplikasi *file* ini. Kelemahan tersebut dapat dihilangkan dengan melakukan proses enkripsi pada *file* MP3. Proses enkripsi pada file MP3 merupakan dasar untuk membentuk sebuah sistem berbasis *Digital Rights Management* (DRM).

Proses enkripsi pada MP3 menggunakan algoritma Advanced Encryption Standard (AES) dapat melindungi data suara dengan mengacak setiap sampel suara sehingga keamanan data tersebut lebih terjamin. Pemilihan algoritma AES untuk digunakan pada proses enkripsi MP3 didasarkan pada tingkat keamanan yang diberikan oleh algoritma ini.

National Institute of Standards and Technology (NIST) secara terus menerus melakukan analisis dan evaluasi ulang terhadap algoritma AES dan akan melakukan revisi jika ditemukan kelemahan matematis pada algoritma ini (Federal Information Processing Standard Publication, 2001). Jadi algoritma AES merupakan suatu algoritma yang dipelihara dengan baik sehingga tingkat keamanan yang diberikan oleh algoritma ini tetap terjaga.

Dalam jurnal Bismita Gadayanak dan Chittaranjan Pradhan disebutkan bahwa aplikasi pengamanan MP3 yang beliau kembangkan melakukan proses enkripsi pada tahap kompresi. Perbedaan antara metode jurnal tersebut dengan metode pada tugas akhir ini terletak pada tahap enkripsi. Penulis menggunakan pendekatan struktur *file* dan melakukan enkripsi pada setiap *body frame* pada MP3 untuk mempercepat proses enkripsi.

1. 2. Rumusan Masalah

Dirumuskan masalah mengenai bagaimana menggunakan algoritma *Advanced Encryption Standard* (AES) untuk melakukan proses enkripsi maupun dekripsi data suara pada *file* MP3 sehingga *file* hasil enkripsi masih dapat diputar pada berbagai alat pemutar MP3.

1. 3. Tujuan dan Manfaat

Tujuan dari tugas akhir ini adalah menghasilkan sebuah aplikasi yang dapat melakukan proses enkripsi maupun dekripsi pada file MP3 dengan menggunakan algoritma Advanced Encryption Standard (AES) yang dibuat menggunakan bahasa pemrograman C++.

Manfaat yang pembangunan aplikasi pada tugas akhir ini dapat disebutkan sebagai berikut:

1. Mengamankan *file* MP3 dengan melakukan proses enkripsi dengan kunci yang bersifat rahasia.
2. Mengembalikan *file* MP3 yang sudah dienkripsi menjadi file aslinya dengan melakukan proses dekripsi dengan kata kunci yang sesuai.
3. Dapat dikembangkan lebih lanjut untuk pembuatan *Digital Rights Management* pada *file* MP3.

1. 4. Ruang Lingkup

Ruang lingkup implementasi enkripsi MP3 menggunakan Advanced Encryption Standard (AES) dapat diuraikan sebagai berikut :

1. *Input* aplikasi berupa file MP3.
2. *Password* digunakan untuk membentuk kunci yang digunakan pada proses enkripsi dan dekripsi.
3. Proses enkripsi atau dekripsi dijalankan sesuai dengan kondisi file MP3 *input*.
4. Bentuk aplikasi berupa file *executable* dan menggunakan pustaka standard C/C++.

1. 5. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam tugas akhir ini meliputi beberapa pokok bahasan, sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi latar belakang, perumusan masalah, tujuan dan manfaat, ruang lingkup, dan sistematika penulisan dalam pembuatan tugas akhir.

BAB II METODOLOGI

Bab ini berisi kumpulan studi pustaka yang berhubungan dengan topik tugas akhir. Dasar teori yang digunakan dalam tugas akhir ini meliputi MP3, Kriptografi dan AES.

BAB III ANALISIS DAN DESAIN

Bab ini membahas proses pengembangan perangkat lunak pada tahap analisis dan desain.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini membahas proses pengembahan perangkat lunak pada tahap implementasi dan pengujian.

BAB V PENUTUP

Bab ini berisi kesimpulan dan saran yang berkaitan dengan tugas akhir.