ISSN 2089-8673
Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)
Volume 1, Nomor 2, Juli 2012

PENGEMBANGAN APLIKASI KRIPTOGRAFI FILE AUDIO DENGAN ALGORITMA *DATA ENCRYPTION STANDARD* (DES)

I Wayan Dana Asmara, Made Windu Antara Kesiman, Ketut Agustini
Jurusan Pendidikan Teknik Informatika
Universitas Pendidikan Ganesha
email: dekndu@yahoo.com, eghee2006@gmail.com

ABSTRACT

Data security is one important issue in the era of information technology and communications. One alternative of maintaining data security is to develop applications that implement cryptographic algorithms. This study aims to design and develop a cryptographic application that implements the algorithm of Data Encryption Standard (DES).

This application system is designed by using UML (Unified Modeling Language) with encryption and decryption of WAV files as the main design. Encryption and decryption process use the DES algorithm. DES algorithm is a symmetric cryptographic algorithms that uses the same key for encryption and decryption. DES algorithm takes part on 64 bit data blocks and uses a key length of 64 bits. The processes contained in the DES algorithm includes an internal key generation, the initial permutation, enchipering, and the final permutation.

Implementation of the DES algorithm in audio file cryptographic applications generate an software called a AudioEncryptor. Based on the results obtained by testing the software, AudioEncryptor is able to encrypt the audio files well. The voice that is produced by audio files different from actual sound, so the confidentiality of the information contained in audio files that are encrypted very securely. Besides encryption and decryption, AudioEncryptor also equipped by facilities to record and play the audio files. The software of AudioEncryptor is developed by using Java programming language in Java 2 Standard Edition (J2SE).

Key words: Cryptography, audio files, DES algorithm, WAV

ABSTRAK

Keamanan data merupakan salah satu isu penting di era teknologi informasi dan komunikasi. Salah satu alternatif untuk menjaga keamanan data adalah dengan mengembangkan aplikasi yang menerapkan algoritma kriptografi. Penelitian ini bertujuan

ISSN 2089-8673
Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)
Volume 1, Nomor 2, Juli 2012

untuk merancang dan mengembangkan sebuah aplikasi kriptografi yang mengimplementasikan algoritma *Data Encryption Standard* (DES).

Perancangan sistem aplikasi ini menggunakan UML (*Unified Modeling Language*) dengan enkripsi dan dekripsi file WAV sebagai rancangan utama. Proses enkripsi dan dekripsi ini menggunakan algoritma DES. Algoritma DES merupakan algoritma kriptografi simetri yaitu algoritma kriptografi yang menggunakan kunci yang sama untuk enkripsi dan dekripsi. Algortima DES bekerja pada blok data 64 bit dan menggunakan panjang kunci 64 bit. Proses-proses yang terdapat pada algoritma DES meliputi pembangkitan kunci internal, permutasi awal, *enchipering*, dan permutasi akhir.

Implementasi Algoritma DES pada aplikasi kriptografi file audio menghasilkan sebuah perangkat lunak yang disebut dengan *AudioEncryptor*. Berdasarkan hasil pengujian perangkat lunak diperoleh bahwa *AudioEncryptor* mampu mengenkripsi file audio dengan baik. Suara yang dikeluarkan file audio terenkripsi tidak sama dengan suara sebenarnya, sehingga kerahasiaan informasi yang terkandung dalam file audio yang sudah dienkripsi sangat aman. Selain enkripsi dan dekripsi, *AudioEncryptor* juga dilengkapi dengan fasilitas *record* dan *play* audio yaitu fasilitas untuk merekam dan memutar file audio. Perangkat Lunak *AudioEncryptor* sendiri dikembangkan dengan menggunakan bahasa pemrograman *Java* yaitu pada lingkungan *Java 2 Standard Edition* (J2SE).

Kata-kata kunci : Kriptografi, File audio, Algoritma DES, WAV

I. PENDAHULUAN

Teknologi informasi saat ini semakin populer digunakan dalam seluruh aspek kehidupan. Hampir seluruh informasi kini dikelola dalam bentuk digital. Hal ini didukung oleh berbagai keuntungan yang dapat diperoleh seperti kemudahan dalam penyimpanan dan kecepatan dalam pendistribusian. Akan tetapi, penggunaan data digital dalam mengelola pesan bukan berarti meningkatkan keamanan pesan tersebut. Berbagai teknik penyerangan telah muncul sehingga pihak yang tidak bertanggungjawab dapat mengetahui dan menyalahgunakan informasi rahasia yang terkandung dalam pesan. Oleh karena itu, faktor keamanan menjadi salah satu isu penting dalam pengelolaan data digital (Rasyid, 2009).

Kriptografi sebagai suatu ilmu hadir untuk meningkatkan aspek keamanan pesan. Hal ini dilakukan dengan menyandikan pesan ke dalam bentuk acak yang tidak dapat dimengerti lagi maknanya. Akan tetapi, dengan suatu algoritma dan kunci yang sudah ditentukan sebelumnya, bentuk acak tersebut dapat dikembalikan ke pesan semula.

Pengamanan data digital dengan kriptografi dapat diimplementasikan pada berbagai bentuk format data digital. Beberapa contohnya adalah implementasi kriptografi pada data teks, gambar, dan audio. Kriptografi pada data teks memang lebih familiar dikenal dikalangan masyarakat luas. Aplikasi-apikasi yang sudah menerapkan kriptografi pada data teks pun sudah banyak dikembangkan. Beberapa penelitian di bidang kriptografi khususnya yang menggunakan algoritma *DES* yaitu *Simulasi Aplikasi Algoritma DES Pada Transfer Data Uang Bank* (Fitria, 2006) dan *Simulasi Kerahasiaan / Keamanan Informasi Dengan Menggunakan Algoritma DES (Data Encryption Standard)* (Indra Syahputra, 2009).

Namun, pengimplementasian algoritma *DES* pada penelitian ini masih terbatas untuk file teks.

Selain file teks, file audio juga sangat perlu untuk disandikan terlebih-lebih file audio yang bersifat penting dan rahasia. Sebagai contoh yaitu file audio yang berisi rekaman instruksi perang atau strategi perang dan file audio yang berisi rekaman lagu untuk sebuah ajang kompetisi yang akan dikirim melalui internet. Contoh lainnya yaitu file audio yang berisi rekaman mengenai warisan yang harus disimpan dalam waktu tertentu dan file audio yang berisi rekaman pidato politik yang hanya boleh diketahui oleh internal partai tertentu. File-file audio tersebut sudah seharusnya dijaga kerahasiaannya. Sehingga, apabila file tersebut jatuh ke pihak yang tidak bertanggungjawab tidak akan memiliki makna yang berarti baginya. Salah satu cara untuk menjaga kerahasiaan file audio tersebut adalah dengan menggunakan aplikasi kriptografi, khususnya aplikasi kriptografi file audio.

II. KAJIAN PUSTAKA

2.1 Kriptografi

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan (*Cryptography is the art and science of keeping messages secure*) (Rinaldi Munir, 2006), selain itu ada pengertian tentang kriptografi yaitu kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi (Rinaldi Munir, 2006). Kata "seni" di dalam definisi di atas maksdnya adalah mempunyai cara yang unik untuk merahasiakan pesan (kata "*graphy*" di dalam "*cryptography*" itu sendiri sudah menyiratkan sebuah seni). (Rinaldi Munir, 2006).

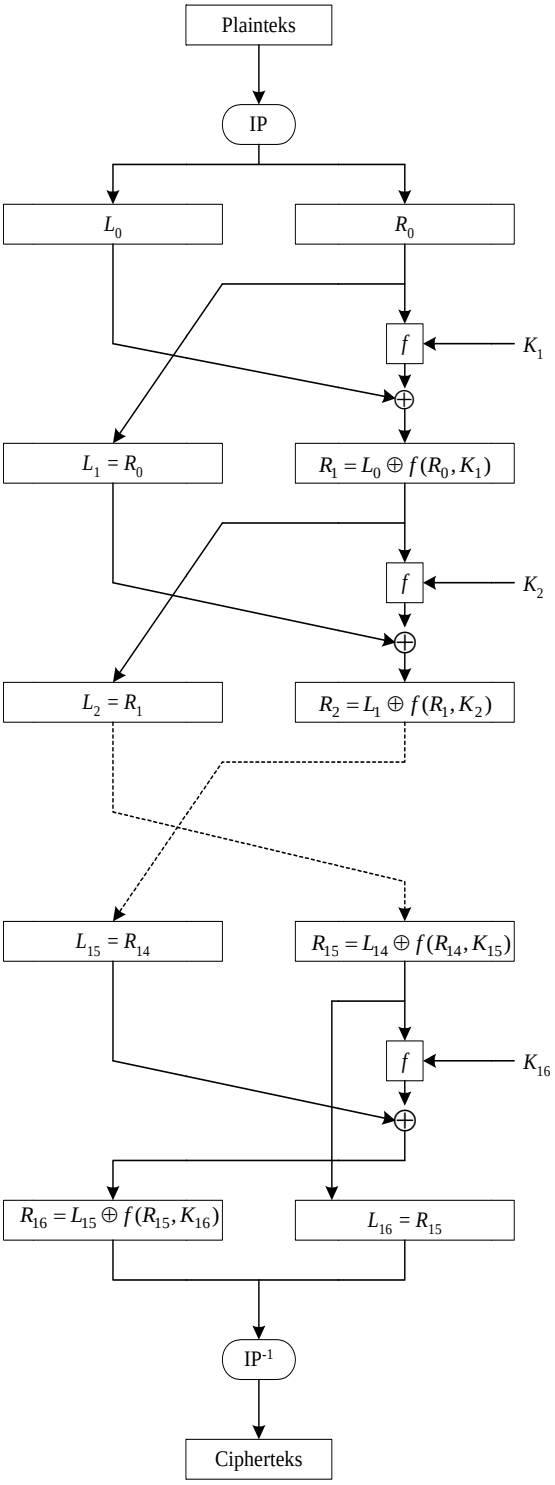
2.2 Algoritma Kriptografi *Data Encryption Standard (*DES*)*

Data Encryption Standard (DES) termasuk ke dalam sistem kriptografi simetri dan tergolong jenis *cipher* blok. DES merupakan algoritma enkripsi yang paling banyak dipakai di dunia, yang diadopsi oleh NIST (*National Institute of Standards and Technology*) sebagai standar pengolahan informasi federal AS. Secara umum DES terbagai menjadi tiga kelompok, yaitu pemrosesan kunci, enkripsi data 64 bit dan dekripsi data 64 bit (Dony Ariyus, 2008).

DES menggunakan algoritma yang sama untuk proses enkripsi dan dekripsi. Jika pada proses enkripsi urutan kunci internal yang digunakan adalah K_1, K_2, …, K_{16}, maka pada proses dekripsi urutan kunci yang digunakan adalah K_{16}, K_{15}, …, K_1. Dengan kata lain, algoritma yang digunakan untuk enkripsi dan dekripsi sebenarnya sama, hanya perbedaannya pada dekripsi penggunaan *kunci internal* yang terbalik.

ISSN 2089-8673
Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)
Volume 1, Nomor 2, Juli 2012

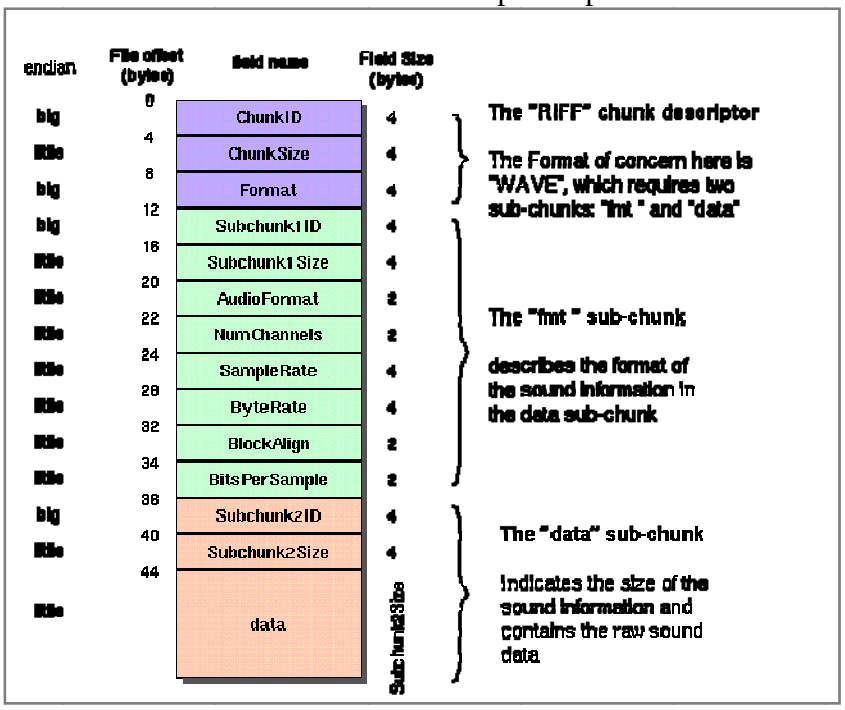
Skema Algoritma DES yang lebih rinci ditampilkan pada Gambar 1.



Gambar 1. Algoritma *Data Encryption Standard* (DES)
(Sumber: Rinaldi Munir, 2006)

2.3 File WAV

Dalam teknologi perangkat lunak dikenal adanya file yang berekstensi WAV. File WAV ini merupakan file audio standar yang digunakan oleh Windows. File WAV ini memungkinkan suara direkam dalam berbagai kualitas, seperti 8-bit atau 16-bit *samples* dengan *rate* 11025Hz, 22050Hz atau 44100Hz. Untuk kualitas yang baik, yaitu: 44100Hz, 16-bit akan memakan kapasitas sekitar 150Kb setiap detiknya. Suara yang berupa digital audio dalam file WAV disimpan dalam bentuk gelombang, karena itulah file ini memiliki ekstensi WAV. File WAV ini dapat dibuat dengan menggunakan berbagai program *wave editor* maupun *wave recorder*. Contoh *wave recorder* adalah *Sound Recorder* milik Windows atau *Sound o'LE* milik *Soundblaster*, sedangkan contoh *wave editor* adalah *Goldwave*, dan *Coolwave*. Struktur file WAV ditampilkan pada Gambar 2.



Gambar 2. *The Canonical Wave File Format*
(Sumber: http://ccrma.stanford.edu/courses/422/projects/waveFormat/)

III. ANALISIS DAN PERANCANGAN

3.1 Analisis Perangkat Lunak

3.1.1 Kebutuhan Perangkat Lunak

Perangkat lunak yang akan dibangun bernama *AudioEnrcyptor*. Adapun proses-proses yang dapat diimplementasikan oleh perangkat lunak *AudioEnrcyptor*, yaitu diantaranya a) membaca dan menyimpan file audio untuk dienkripsi ataupun untuk didekripsi, b) membentuk 16 *internal key* untuk digunakan pada proses enkripsi dan

dekripsi dimana *internal key* dibentuk berdasarkan *key* yang diinputkan oleh user, c) melakukan enkripsi dan dekripsi file audio, d) merekam file audio dalam format WAV, dan e) memutar file audio yang akan dienkripsi dan didekripsi serta file audio yang telah direkam.

3.1.2 Tujuan Pengembangan Perangkat Lunak

Perangkar lunak *AudioEncryptor* merupakan perangkat lunak yang menerapakan algoritma Kriptografi DES untuk mengenkripsi file audio khususnya file audio dengan format WAV. *AudioEncryptor* diharapkan dapat membantu seseorang yang memiliki file audio yang bersifat penting dan rahasia tetap terjaga kerahasiaan informasi yang terkandung di dalamnya.

3.1.3 Masukan dan Keluaran Perangkat Lunak

Berdasarkan proses yang telah dijelaskan sebelumnya, perangkat lunak *AudioEncryptor* memiliki 4 proses utama yaitu *record* file audio, *play* file audio, enkripsi file audio, dan dekripsi file audio.

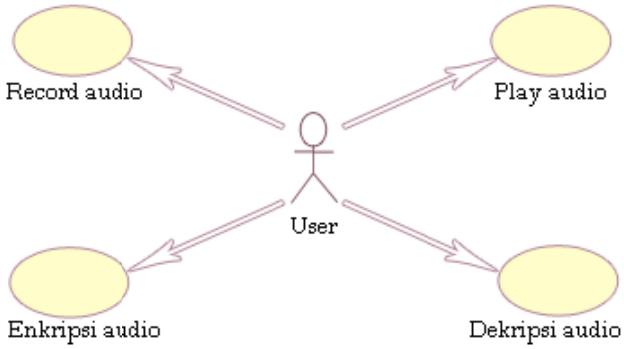
Masukan untuk proses *record* file audio adalah berupa gelombang suara yang dalam hal ini diambil dari kartu suara (*sound card*). Keluaran untuk proses ini adalah file audio dalam format wav. Masukan untuk proses *play* file audio adalah file audio dalam format wav, baik berupa file yang baru direkam pada proses *record* file audio atau file audio yang sudah tersimpan di *data storage*.. Keluaran dari proses *play* file audio adalah berupa suara yang dioutputkan pada *speaker*.

Masukan untuk proses enkripsi file audio adalah file audio asli yang akan dienkripsi dan masukkan berupa *key* untuk digunakan dalam proses enkripsi. Adapun keluaran dari proses ini adalah berupa file audio dengan *sample data* teracak tetapi tetap memiliki format yang sama dengan file audio asli. Sedangkan masukan untuk proses dekripsi adalah berupa file audio yang sudah dienkripsi sebelumnya dan *key*. *Key* yang dimasukkan ketika proses dekripsi harus sama dengan *key* yang dimasukkan ketika proses enkripsi. Keluaran dari proses dekripsi ini adalah file audio asli, yaitu sama dengan file audio sebelum dienkripsi.

3.1.4 Model Fungsional

Pada model fungsional perangkat lunak menjelaskan gambaran umum terhadap proses yang terjadi dalam perangkat lunak. Model fungsional dapat memberikan gambar terhadap proses yang terjadi antara perangkat lunak dengan pengguna luar (*user*). Interaksi antara perangkat lunak dan user dapat memberikan bentuk proses secara jelas yang terjadi pada perangkat lunak seperti masukan dan keluaran dari proses yang dikerjakan. Model fungsional dari perangkat lunak *AudioEncryptor* dideskripsikan menggunakan *Unified Modeling Language* (UML). *User* akan melakukan beberapa proses interaksi yang terdapat pada perangkat lunak seperti pada Gambar 3.

ISSN 2089-8673
Jurnal Nasional Pendidikan Teknik Informatika (JANAPATI)
Volume 1, Nomor 2, Juli 2012



Gambar 3. *Use Case Diagram* Perangkat Lunak *AudioEncryptor*

3.2 Perancangan Perangkat Lunak

Pada perancangan perangkat lunak *AudioEncryptor* ini terdapat beberapa tahapan yang dilalui, yaitu batasan perancangan, perancangan arsitektur, perancangan struktur data, dan perancangan antar muka.

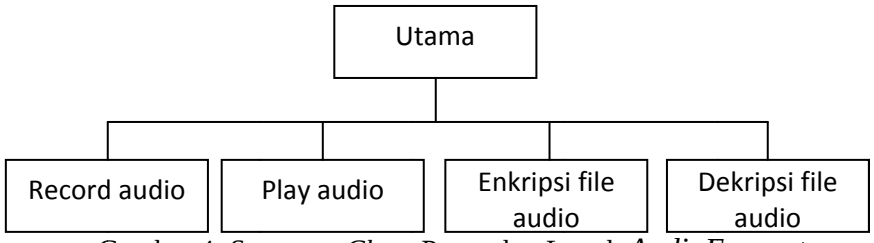
3.2.1 Batasan Perancangan Perangkat Lunak

Adapun batasan yang terdapat dalam perancangan perangkat lunak *AudioEncryptor* adalah sebagai berikut.

a) *AudioEncryptor* menyediakan fasilitas *record*, *play*, enkripsi, dan dekripsi file audio.
b) *AudioEncryptor* hanya dapat merekam, memutar, mengenkripsi dan mendekripsi file audio dengan format WAV.
c) Besarnya ukuran file audio yang dapat direkam, diputar, dienkripsi dan didekripsi tergantung dari besarnya memori yang tersedia pada komputer *user*.

3.2.2 Perancangan Arsitektur Perangkat Lunak

Pada perancangan arsitektur perangkat lunak menggambarkan bagian-bagian modul, struktur ketergantungan antar modul, dan hubungan antar modul dari perangkat lunak yang dibangun.



Gambar 4. *Structure Chart* Perangkat Lunak *AudioEncryptor*

Pada Perangkat lunak *AudioEncryptor* terdapat 6 Class utama yang digunakan untuk merekam, memutar, mengenkripsi, dan mendekripsi file audio.

a) *Class Main*, adalah *class* untuk pembuatan antar muka perangkat lunak (*GUI*).

b) *Class recordAudio*, adalah *class* untuk merekam suara dan menyimpannya dalam format WAV.
c) *Class playAudio*, adalaha *class* untuk memutar file audio khusus file audio dengan format WAV.
d) Class wavIO, adalah *class* untuk membaca dan menyimpan file audio.
e) *Class internalKey*, adalah *class* untuk meng-*generate* 16 *sub-key* yang akan digunakan pada proses enkripsi.
f) *Class enkripsiByDES*, adalah *class* yang menangani proses enkripsi dan dekripsi.

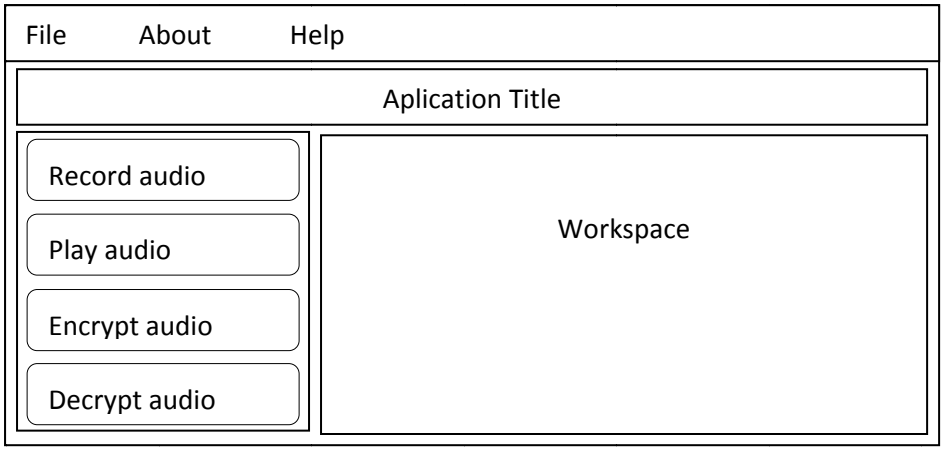
3.2.3 Perancangan Struktur Data

Perangkat lunak ini dibangun pada area pemrograman berorientasi objek, oleh karena itu struktur data yang digunakan adalah objek dan jenis tipe data primitif lainnya. Struktur data utama yang sering digunakan dalam perangkat lunak *AudioEncryptor* ini adalah struktur data untuk objek *String*, *integer*, dan *array byte*. Struktur data untuk objek *String* berfungsi untuk melakukan manipulasi nilai bit yang digunakan untuk mengubah *sample data* file audio menjadi nilai biner. Nilai biner yang terdiri dari nilai 0 dan 1 dibentuk menggunakan objek *String* dan untuk memanipulasinya, menggunakan operasi biner yang disesuikan oleh operasi pada objek *String*. Struktur data untuk objek *integer* berfungsi untuk menyimpan *size* dari sebuah file audio. Sedangkan struktur data untuk objek *array byte* berfungsi untuk menyimpan nilai *sample data* dari sebuah file audio.

Selain struktur data tersebut, perangkat lunak *AudioEncryptor* juga memanfaatkan struktur data lain seperti objek file karena *AudioEncryptor* pada prinsipnya bekerja pada level operasi file seperti membaca, mengelola, dan menyimpan file. Sedangkan struktur data pendukung yang lainnya yaitu objek *Image* dan *Icon*. Objek *Image* dan *Icon* ini digunakan untuk memperindah tampilan GUI dari perangkat lunak *AudioEncryptor*.

3.2.4 Perancangan Antarmuka

Antarmuka perangkat lunak terdiri atas *Form* menu utama sebagai berikut.



Gambar 5. Form Utama Aplikasi Kriptografi *AudioEncryptor*

IV. IMPLEMENTASI PERANGKAT LUNAK

Dari analisis dan perancangan yang telah dilakukan, langkah selanjutnya adalah melakukan implementasi perangkat lunak.

4.1 Implementasi Modul

Tabel 1. Tabel Pemetaan Terhadap *Class* Implementasi

Class Perancangan	Class Implementasi	Penjelasan Class Implementasi
Main	*Main.java*	*Class* yang berisi *method* untuk membuat GUI.
recordAudio	*recordAudio.java*	*Class* yang berisi *method* untuk merekam audio.
playAudio	*playAudio.java*	*Class* yang berisi *method* untuk memutar audio.
wavIO	*wavIO.java*	*Class* yang berisi *method* untuk baca dan simpan file audio.
internalKey	*internalKey.java*	*Class* yang berisi *method* untuk meng-*generate* 16 *sub-key*.
enkripsiByDES	*enkripsiByDES.java*	*Class* yang berisi *method* untuk menangani proses enkripsi dan dekripsi.

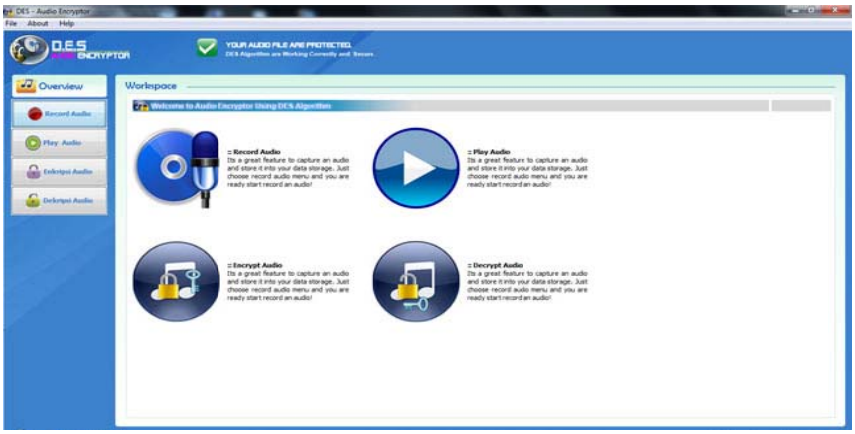
4.2 Implementasi Struktur Data

Sesuai dengan rancangan struktur data yang telah dibuat, dapat diimplementasikan struktur data pada lingkungan pengembangan perangkat lunak. Perangkat lunak ini dibangun berdasarkan orientasi objek sesuai dengan lingkungan pengembangan perangkat lunak yaitu *Java*. Dalam *java*, tipe data dikelompokkan menjadi dua jenis tipe data, yaitu tipe data primitif dan tipe data referensi. Berdasarkan lingkungan pengembangan tersebut, struktur data yang diimplementasikan merupakan struktur data yang berupa tipe data primitif seperti tipe data *integer*, *boolean*, dan *long* serta penggunaan tipe data referensi yang berupa objek yang telah tersedia seperti objek *String* dan objek *array*.

Objek String digunakan untuk mengubah dan mengolah bilangan biner yang digunakan ketika enkripsi dan dekripsi file audio. *Objek array* yang digunakan adalah *integer* dan *array byte*. Struktur data *integer* berfungsi untuk menyimpan *size* dari sebuah file audio. Sedangkan *objek array byte* digunakan untuk menampung nilai *sample data* dari sebuah file audio.

4.3 Implementasi Antarmuka

Rancangan layar antarmuka perangkat lunak *AudioEncryptor* diimplementasikan menggunakan *class-class* yang terdapat pada *package java.awt* dan *java.swing*. Implementasi layar antarmuka perangkat lunak *AudioEncryptor* ini menggunakan *NetBeans IDE 6.0.1* sebagai editor. Untuk implementasi antarmuka *Form* Menu Utama dapat dilihat pada Gambar 6.



Gambar 6. Implementasi Layar Antarmuka *Form* Menu Utama

V. PENUTUP

Berdasarkan penelitian yang telah dilakukan yaitu "Pengembangan Aplikasi Kriptografi File Audio dengan Algoritma *Data Encryption Standard* (DES)" adapun simpulan yang didapat antara lain.

a) Rancangan sistem aplikasi kriptografi file audio digambarkan menggunakan *Unified Modeling Language* (UML) yang dapat menggambarkan arus data dalam sistem dengan jelas dan sebagai alat dokumentasi yang baik. Penggambaran UML Pengembangan Aplikasi Kriptografi File Audio dengan Algoritma DES terdiri dari *usecase diagram*, *activity diagram*, *sequence diagran*, dan VOPC *diagram*.
b) Implementasi Algoritma DES pada aplikasi kriptografi file audio menghasilkan sebuah perangkat lunak yang mampu mengenkripsi file audio dengan *size* file audio hasil enkripsi dan file audio hasil dekripsi yang tetap sama dengan *size* file audio sebelum dienkripsi. Suara yang dikeluarkan oleh file audio hasil enkripsi tidak sama dengan suara sebenarnya, sehingga kerahasiaan informasi yang terkandung dalam file audio yang sudah dienkripsi sangat aman.

VI. DAFTAR PUSTAKA

Ariyus, Dony. 2008. *Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi*. Yogyakarta: CV. Andi Offset.

Fitria, Faiz Sungkar. 2006. "Simulasi Aplikasi Algoritma Des Pada Transfer Data Uang Bank". Jurnal Informatika, Vol.6, No.1. STMIK Darmajaya.

Hermawan, Benny. 2004. *Menguasai Java 2 & Object Oriented Programming.* Yogyakarta: Andi Publisher.

Indra Syahputra. 2009. Simulasi Kerahasiaan / Keamanan Informasi Dengan Menggunakan Algoritma DES (Data Encryption Standard). Skripsi (tidak diterbitkan). Universitas Sumatera Utara.

Rasyid, Muhamad Fajrin. 2009. ”Kriptografi Audio dengan Teknik Interferensi Data Non Biner”. http://digilib.itb.ac.id (diakses tanggal 20 Desember 2010).

Rinaldi Munir. 2006. ”Bahan Kuliah 1, IF 5054 Kriptografi Pengantar Kriptografi”. http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/kripto2006.htm (diakses tanggal 20 Desember 2010).

Rinaldi Munir. 2006. ”Bahan Kuliah, IF 5054 Cipher Block”. http://www.informatika.org/~rinaldi/Kriptografi/2006-2007/kripto2006.htm (diakses tanggal 20 Desember 2010).

Rinaldi Munir. 2006. ”Data Encryption Standard (DES)”. *http://kur2003.if.itb.ac.id/file/DES.doc* (diakses tanggal 20 Desember 2010).

Scott Wilson. 2003. “WAVE PCM soundfile format”. https://ccrma.stanford.edu/courses/422/projects/WaveFormat/ (diakses tanggal 4 Desember 2010).

William Stallings. 2003. *Network Security Essentials – Appications and Standard*. New Jersey: Prentice Hall.

William Wilson. 2007. “Steganography”. http://www.dreamincode.net/forums/topic/27950-steganography (diakses tanggal 20 Desember 2010).