IMPLEMENTASI ENKRIPSI *AUDIO* (*VOICE*) MENGGUNAKAN ALGORITMA *BLOWFISH*

Disusun dan Diajukan untuk Memenuhi Persyaratan Ujian Akhir Memperoleh
Gelar Sarjana Komputer pada Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi
Medan

SKRIPSI

OLEH

NAMA : **SRI WAHYUNI**
N.P.M : **1414370356**
PROGRAM STUDI : **SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

LEMBAR PENGESAHAN

IMPLEMENTASI ENKRIPSI *AUDIO (VOICE)* MENGGUNAKAN ALGORITMA *BLOWFISH*

Disusun Oleh:

NAMA	**: SRI WAHYUNI**
NPM	**: 1414370356**
PROGRAM STUDI	**: SISTEM KOMPUTER**

Skripsi telah disetujui oleh Dosen Pembimbing Skripsi pada tanggal 22 Agustus 2019 :

Dosen Pembimbing I	Dosen Pembimbing II
Zulham Sitorus, S.Kom., M.Kom	**Dr. Muhammad Iqbal, S.Kom., M.Kom**

Mengetahui,

Dekan Fakultas Sains dan Teknologi	Kepala Program Studi Sistem Komputer
Sri Shindi Indira, S.T., M.Sc	**Dr. Muhammad Iqbal, S.Kom., M.Kom**

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama	: Sri Wahyuni
NPM	: 1414370356
Prodi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer (KJK)
Judul Skripsi	: Implementasi Enkripsi *Audio*(*Voice*) Menggunakan Algoritma *Blowfish*

Dengan ini menyatakan bahwa:

1. Tugas Akhir/Skripsi saya bukan hasil Plagiat.
2. Saya tidak akan menuntut perbaikan nilai Indeks Prestasi Komulatif (IPK) setelah ujian Sidang Meja Hijau.
3. Skripsi saya dapat dipublikasikan oleh pihak lembaga dan saya tidak akan menuntut akibat publikasi tersebut.

Demikian pernyataan ini saya perbuat dengan sebenar-benarnya, terima kasih.

Medan, September 2019

Yang membuat pernyataan

Sri Wahyuni

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama	: Sri Wahyuni
NPM	: 1414370356
Prodi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer (KJK)
Judul Skripsi	: Implementasi Enkripsi *Audio*(*Voice*) Menggunakan Algoritma *Blowfish*

Dengan ini mengajukan permohonan untuk ujian sarjana lengkap pada fakultas Sains & Teknologi Universitas pembangunan pancabudi.

Sehubungan dengan hal tersebut, maka saya tidak akan lagi ujian perbaikan nilai di masa yang akan datang.

Demikian pernyataan ini saya perbuat dengan sebenar-benarnya, terima kasih

Medan, September 2019

Yang membuat pernyataan

Sri Wahyuni

TANDA BEBAS PUSTAKA

No. 20/perp/01./2019

Dinyatakan tidak ada sangkut paut dengan UPT. Perpustakaan

Medan, 16 JAN 2019

Ka. UPT. Perpustakaan

Sugiarjo, S.Sos, SIP

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau

Medan, 28 Desember 2018
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

Telah Diperiksa oleh LPMU dengan Plagiarisme 41 %
Medan 16 JANUARI 2019
Ka. LPMU
HUSNI M. RITONGA, BA., MSC.
Calvin Pramono, SE, MM

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	: SRI WAHYUNI
Tempat/Tgl. Lahir	: MEDAN / 19 Desember 1996
Nama Orang Tua	: RAJIAN
N. P. M	: 1414370356
Fakultas	: SAINS & TEKNOLOGI
Program Studi	: Sistem Komputer
No. HP	: 083172583143
Alamat	: JL. BUNGA ASOKA I ASAM KUMBANG

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **Implementasi Enkripsi Audio(Voice) Menggunakan Algoritma Blowfish**, Selanjutnya saya menyatakan :

1. Melampirkan KKM yang telah disahkan oleh Ka. Prodi dan Dekan
2. Tidak akan menuntut ujian perbaikan nilai mata kuliah untuk perbaikan indek prestasi (IP), dan mohon diterbitkan ijazahnya setelah lulus ujian meja hijau.
3. Telah tercap keterangan bebas pustaka
4. Terlampir surat keterangan bebas laboratorium
5. Terlampir pas photo untuk ijazah ukuran 4x6 = 5 lembar dan 3x4 = 5 lembar Hitam Putih
6. Terlampir foto copy STTB SLTA dilegalisir 1 (satu) lembar dan bagi mahasiswa yang lanjutan D3 ke S1 lampirkan ijazah dan transkipnya sebanyak 1 lembar.
7. Terlampir pelunasan kwintasi pembayaran uang kuliah berjalan dan wisuda sebanyak 1 lembar
8. Skripsi sudah dijilid lux 2 examplar (1 untuk perpustakaan, 1 untuk mahasiswa) dan jilid kertas jeruk 5 examplar untuk penguji (bentuk dan warna penjilidan diserahkan berdasarkan ketentuan fakultas yang berlaku) dan lembar persetujuan sudah di tandatangani dosen pembimbing, prodi dan dekan
9. Soft Copy Skripsi disimpan di CD sebanyak 2 disc (Sesuai dengan Judul Skripsinya)
10. Terlampir surat keterangan BKKOL (pada saat pengambilan ijazah)
11. Setelah menyelesaikan persyaratan point-point diatas berkas di masukan kedalam MAP
12. Bersedia melunaskan biaya-biaya uang dibebankan untuk memproses pelaksanaan ujian dimaksud, dengan perincian sbb :

1. [102] Ujian Meja Hijau	: Rp.	100.000
2. [170] Administrasi Wisuda	: Rp.	1,500,000
3. [202] Bebas Pustaka	: Rp.	100,000
4. [221] Bebas LAB	: Rp.	5,000
Total Biaya	: Rp.	1,705,000
S.UK. Termin	Rp	3400.000
	Rp	5.105.000

Diketahui/Disetujui oleh :

Sri Shindi Indira, S.T.,M.Sc.
Dekan Fakultas SAINS & TEKNOLOGI

16/01-19

Hormat saya

SRI WAHYUNI
1414370356

Catatan :

- 1.Surat permohonan ini sah dan berlaku bila ;
  - a. Telah dicap Bukti Pelunasan dari UPT Perpustakaan UNPAB Medan.
  - b. Melampirkan Bukti Pembayaran Uang Kuliah aktif semester berjalan
- 2.Dibuat Rangkap 3 (tiga), untuk - Fakultas - untuk BPAA (asli) - Mhs.ybs.

Telah di terima berkas persyaratan dapat di proses
Medan, 20 FEB 2019
Ka. BPAA

TEGUH WAHYONO, SE., MM.

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI

Jl. Jend. Gatot Subroto Km 4,5 Medan Fax. 061-8458077 PO.BOX : 1099 MEDAN

PROGRAM STUDI TEKNIK ELEKTRO	(TERAKREDITASI)
PROGRAM STUDI TEKNIK ARSITEKTUR	(TERAKREDITASI)
PROGRAM STUDI SISTEM KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI TEKNIK KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI AGROTEKNOLOGI	(TERAKREDITASI)
PROGRAM STUDI PETERNAKAN	(TERAKREDITASI)

PERMOHONAN MENGAJUKAN JUDUL SKRIPSI

yang bertanda tangan di bawah ini :

a Lengkap	: SRI WAHYUNI
pat/Tgl. Lahir	: MEDAN / 19 Desember 1996
r Pokok Mahasiswa	: 1414370356
am Studi	: Sistem Komputer
ntrasi	: Keamanan Jaringan Komputer
h Kredit yang telah dicapai	: 138 SKS, IPK 3.54

n ini mengajukan judul skripsi sesuai dengan bidang ilmu, dengan judul:

Judul Skripsi	Persetujuan
Sistem Pendukung Keputusan Penentuan Jenis Sakit Kepala Dengan Menggunakan Metode Multi Criteria Decision Making (MCDM)	☐
Sistem Pendukung Keputusan Penentuan Pembelian Laptop dengan Metode AHP (Analytical Hierarchy Process) Berbasis Web	☐
Aplikasi Enkripsi ~~Pengiriman Pesan Suara~~ Menggunakan Algoritma ~~Twofish~~ 2 4 C.	☑

VIDEO STREAMING.

l yang disetujui oleh Kepala Program Studi diberikan tanda ☑

Implementasi Enkripsi Audio (Voice) Menggunakan Algoritma BLOWFISH.

Medan, 03 Mei 2018

Pemohon,

(SRI WAHYUNI)

Dekan I,

(Ir. Bhakti Alamsyah, M.T., Ph.D.)

Nomor : .....
Tanggal : .....
Disahkan oleh
Dekan,

(Sri Shindi Indira, S.T., M.Sc.)

Tanggal : 10, 05 - 2018
Disetujui oleh :
Dosen Pembimbing I :

(.....)

Tanggal : 23 Mei 2018
Disetujui oleh:
Ka. Prodi Sistem Komputer

(MUHAMMAD IQBAL, S.Kom.,M.Kom.)

Tanggal : .....
Disetujui oleh:
Dosen Pembimbing II:

(.....)

No. Dokumen: FM-LPPM-08-01	Revisi: 02	Tgl. Eff: 20 Des 2015

FM-BPAA-2012-038

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

Universitas	: Universitas Pembangunan Panca Budi
Fakultas	: SAINS & TEKNOLOGI
Dosen Pembimbing I	: Zulham Sitorus, S.Kom., M.Kom
Dosen Pembimbing II	: Dr. Muhammad Iqbal, S.Kom., M.Kom
Nama Mahasiswa	: SRI WAHYUNI
Jurusan/Program Studi	: Sistem Komputer
Nomor Pokok Mahasiswa	: 1414370356
Jenjang Pendidikan	: Strata 1 (S1)
Judul Tugas Akhir/Skripsi	: Implementasi Enkripsi Audio (Voice) Menggunakan Algoritma Zuc.

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
26/9 18	Revisi penulisan pada BAB I,II,III. Beri catatan belakang supaya penulisan penomoran di lengkapkan kaji ulang, konsep lapangan tentang Zuc, tidak terlihat. Sesuaikan dengan jurnal-jurnal yg ada.	[paraf]	
3/10 18	Acc. BAB. I. Lanjut BAB. II - III.	[paraf]	
5/10 18.	Revisi bab II. BAB I Acc.	[paraf]	

Medan, 26 Mei 2018
Diketahui/Disetujui oleh :
Dekan,

Sri Shindi Indira, S.T.,M.Sc.

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

Universitas	: Universitas Pembangunan Panca Budi
Fakultas	: SAINS & TEKNOLOGI
Dosen Pembimbing I	: Zulham Sitorus, S.Kom, M.Kom
Dosen Pembimbing II	: Dr. Muhammad Zahal, S.Kom., M.Kom
Nama Mahasiswa	: SRI WAHYUNI
Jurusan/Program Studi	: Sistem Komputer
Nomor Pokok Mahasiswa	: 1414370356
Jenjang Pendidikan	: Strata I
Judul Tugas Akhir/Skripsi	: Implementasi Enkripsi Audio (Voice) Menggunakan Algoritma Blowfish.

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
9/10 18.	Revisi penulisan dan kurang jelas pada BAB II. dan III. banyak membaca jurnal..		
22/10 18.	Acc BAB. II Lnjt BAB III. di perbaiki penulisan judul dan tujuannya.		
7/11 18.	Revisi BAB I, II. Ffi sesuaikan dgn apa yg di project..		
10/11 18.	Acc. I, II. Lanjut III IV		
	=> BAB III, IV. di Seminarkan. Dgn analisa masalah.		
3/9 19.	Acc jilid		

Medan, 26 Mei 2018
Diketahui/Disetujui oleh :
Dekan,

Sri Shindi Indira, S.T.,M.Sc.

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

niversitas : Universitas Pembangunan Panca Budi
akultas : SAINS & TEKNOLOGI
osen Pembimbing I : Zulham Sitorus, S.Kom., M.Kom
osen Pembimbing II : Dr. Muhammad Zaki, S.Kom., M.Kom
ama Mahasiswa : SRI WAHYUNI
rusan/Program Studi : Sistem Komputer
mor Pokok Mahasiswa : 1414370356
njang Pendidikan : Strata Satu (S1)
dul Tugas Akhir/Skripsi : Implementasi Enkripsi Audio (Voice) Menggunakan Algoritma Blowfish.

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
29/11 2018	Acc Seminar.		
7/12 18.	Acc Sidang		
19.	Acc jilid Cuk.		

Medan, 29 November 2018
Diketahui/Disetujui oleh :
Dekan,

Sri Shindi Indira, S.T.,M.Sc.

yang tidak perlu

Coret yang tidak perlu

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

Universitas : Universitas Pembangunan Panca Budi
Fakultas : SAINS & TEKNOLOGI
Dosen Pembimbing I : Zulham Sitorus, S.Kom., M.Kom
Dosen Pembimbing II : Dr. Muhammad Isa, S.Kom., M.Kom
Nama Mahasiswa : SRI WAHYUNI
Jurusan/Program Studi : Sistem Komputer
Nomor Pokok Mahasiswa : 1414370356
Jenjang Pendidikan : Strata Satu (S1)
Judul Tugas Akhir/Skripsi : Implementasi Enkripsi Audio (Voice) Menggunakan Algoritma ZUC

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
7/8 -18	~ perbaiki latar belakang		
22/8 -18	~ Acc BAB I		
30/8 -18	~ Acc BAB II		
12/9 -18	~ perbaiki judul gambar		
17/9 -18	~ Acc BAB III		
24/9 -18	~ tambahkan hasil pengujian aplikasi		
26/9 -18	~ Acc BAB IV		
13/11 -18	~ Acc BAB V dan seminar		
27/11 -18	~ Acc sidang		
3/9 18	Acc		

Medan, 26 Mei 2018
Diketahui/Disetujui oleh :
Dekan,

Sri Shindi Indira, S.T.,M.Sc.

Coret yang tidak perlu

Plagiarism Detector v. 1092 - Originality Report:

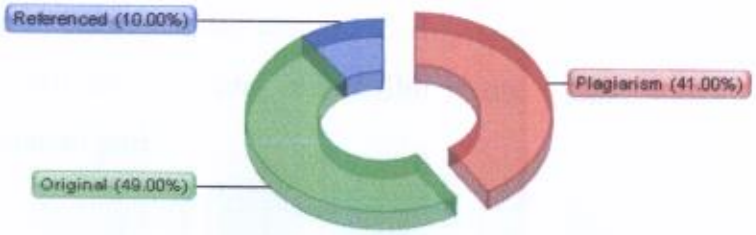
Analyzed document: 30-11-18 3:13:05 PM

"SRI WAHYUNI_1414370356_SISTEM KOMPUTER.docx"

Licensed to: **Universitas Pembangunan Panca Budi_License2**

UNIVERSITAS PEMBANGUNAN PANCA BUDI
Beriman, Berilmu, Berkarya

Relation chart:



Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

Top sources of plagiarism:

% 10	wrds: 713	http://purnama015.blogspot.com/
% 8	wrds: 648	http://ritasari-algoritma-ritasari.blogspot.com/2009/01/algoritma-blowfish.html
% 8	wrds: 576	https://anzdoc.com/enkripsi-pesan-dalam-media-gambar-menggunakan-metode-hibrid-.html

[Show other Sources:]

Processed resources details:

265 - Ok / 63 - Failed

[Show other Sources:]

Important notes:

Wikipedia:	Google Books:	Ghostwriting services:	Anti-cheating:
Wiki Detected!	[not detected]	[not detected]	[not detected]

Excluded Urls:

YAYASAN PROF. DR. H. KADIRUN YAHYA
UNIVERSITAS PEMBANGUNAN PANCA BUDI
LABORATORIUM KOMPUTER
Jl. Jend. Gatot Subroto Km 4,5 Sei Sikambing Telp. 061-8455571
Medan - 20122

KARTU BEBAS PRAKTIKUM

Yang bertanda tangan dibawah ini Ka. Laboratorium Komputer dengan ini menerangkan bahwa :

Nama	:	SRI WAHYUNI
N.P.M.	:	1414370356
Tingkat/Semester	:	Akhir
Fakultas	:	SAINS & TEKNOLOGI
Jurusan/Prodi	:	Sistem Komputer

Benar dan telah menyelesaikan urusan administrasi di Laboratorium Komputer Universitas Pembangunan Panca Budi Medan.

Medan, 16 Januari 2019
Ka. Laboratorium

Fachrid Wadly, S. Kom

ABSTRAK

SRI WAHYUNI

Implementasi Enkripsi *Audio (Voice)* Menggunakan Algoritma *Blowfish*

2019

Perkembangan teknologi membuat manusia menjadi lebih mudah menjalani kehidupan sehari-hari, baik dalam hal berkomunikasi, berbelanja, bepergian bahkan memeriksa kesehatan. Audio merupakan salah satu contoh perkembangan teknologi yang sangat melekat pada saat sekarang ini. Pasalnya, audio merupakan satu format media yang bisa kita rasakan di manapun baik dalam bentuk musik ataupun komunikasi melalui voice message. Salah satu hal yang paling melekat yaitu pengembangan teknologi audio dibidang komunikasi. Dalam bidang komunikasi, audio dapat digunakan sebagai cara bertukar pesan melalui cara baru yaitu dengan melakukan voice message. Dengan voice message, kita dapat bertukar pesan secara instan melalui media audio. Namun semakin berkembangnya teknologi, pemakaian audio dalam komunikasi akan menimbulkan beberapa pertanyaan, seperti apakah audio yang dikirimkan terenkripsi secara baik? Apakah audio tersebut dienkripsi menggunakan teknik yang baik sehingga audio yang dikirim tidak dapat disadap atau dimanipulasi oleh siapapun?

Kata Kunci : *Teknologi, Audio, Enkripsi, Algoritma*

DAFTAR ISI

BAB III ANALISA DAN PERANCANGAN SISTEM

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi membuat proses komunikasi manusia menjadi lebih cepat, instan dan mudah. Dengan berkembangnya teknologi, sistem komunikasi yang dulunya menggunakan surat dan biaya pulsa yang mahal sekarang sudah lebih maju dan mudah dengan hanya menggunakan jaringan internet. Bahkan saat ini, kita sudah dapat bertukar kabar secara instan atau melakukan panggilan video secara jarak jauh hanya dengan menggunakan teknologi internet.

Salah satu contoh berkembangnya teknologi dalam bidang pertukaran informasi dan pertukaran pesan ialah kini kita dapat bertukar pesan instan dalam format file *audio* (*voice message*). Pada *voice message* kita dimungkinkan untuk mengirim pesan dalam format suara singkat ke orang lain hanya dengan menggunakan jaringan internet. Dengan *voice message* pula, kita dapat mengirimkan pesan yang berbentuk file audio ke sesama pengguna lain secara cepat dan tanpa memerlukan biaya tambahan lain.

Dengan berkembangnya teknologi pesan juga membuat semakin berkembangnya celah keamanan terhadap teknologi pertukaran informasi tersebut. Hal ini dapat menyebabkan proses bertukar informasi menjadi tidak aman karena adanya celah yang dapat digunakan para hacker untuk mencuri informasi pesan tersebut secara ilegal. Untuk itulah diperlukan suatu teknik pengamanan data yang

diterapkan pada sistem pertukaran informasi untuk dapat membuat proses pertukaran informasi tersebut lebih aman.

Pada penulisan skripsi ini, penulis mengankat tentang pengamanan data file *audio* menggunakan algoritma *Blowfish*. Algoritma *Blowfish* atau "*OpenPGP.Cipher.4*" merupakan enkripsi yang termasuk dalam golongan *Symetric Cryptosystem*, metode enkripsinya mirip dengan *DES* (*DES-like Cipher*) ditemukan oleh seorang *Cryptanalyst* bernama *Bruce Schneier* Presiden perusahaan *Counterpane Internet Security, Inc* (Perusahaan konsultan tentang kriptografi dan keamanan Komputer) dan dipublikasikan tahun 1994. Di-buat untuk digunakan pada komputer yang mempunyai *microprocesor* besar (32 bit keatas dengan *cache* data yang besar).

Blowfish dikembangkan untuk memenuhi kriteria desain yang cepat dalam implementasinya dimana pada keadaan optimal dapat mencapai 26 *clock cycle* per *byte*, dimana dapat berjalan pada memori kurang dari 5 KB, sederhana dalam algoritmanya sehingga mudah diketahui kesalahannya, dan keamanan yang *variable* dimana panjang kunci bervariasi (minimum 32 bit, maksimum 448 bit, *Multiple* 8 bit, default 128 bit).

Berdasarkan penjelasan dari latar belakang di atas maka penulis mengambil judul yaitu "**IMPLEMENTASI ENKRIPSI *AUDIO (VOICE)* MENGGUNAKAN ALGORITMA *BLOWFISH***".

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana cara menerapkan algoritma *blowfish* untuk mengamankan file *audio* (mp3) ?
2. Bagaimana membuat suatu program yang dapat digunakan untuk0 mengenkripsi dan mendekripsikan suatu file *audio* (mp3) menggunakan algoritma *blowfish* yang dibuat dengan menggunakan bahasa pemograman *VB.NET* ?

1.3 Batasan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka batasan masalah dalam penelitian ini adalah:

1. Program enkripsi dan dekripsi file *audio* (*mp3*) dengan menggunakan algoritma *blowfish* ini akan berbasis *VB.NET* yang dapat di akses secara *offline*.
2. Program ini memiliki 2 (dua) fitur utama yaitu fitur enkripsi untuk mengamankan *audio* (*mp3*) dan fitur dekripsi untuk mendekripsikan file *audio* (mp3) yang telah di enkripsi.
3. Program enkripsi dan dekripsi file *audio* (*mp3*) menggunakan algoritma *blowfish* ini menggunakan 32-bit sampai 408-bit kunci sebagai *output.*

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dijelaskan diatas, berikut merupakan tujuan penelitian dari penulisan skripsi ini yaitu :

1. Untuk menerapkan algoritma *Blowfish* dalam pengamanan file *audio* (*mp3*) sehingga file audio tidak dapat dibuka oleh para pencuri data.
2. Untuk membuat suatu program yang dapat mengenkripsi dan mendekripsi suatu file *audio* (*mp3*) menggunakan algoritma *Blowfish* sehingga audio tersebut tidak dapat didengarkan oleh orang yang tidak berhak.

1.5 Manfaat Penelitian

Manfaat dari penulisan dan penelitan pada skripsi ini yaitu :

1. Untuk menambah pengetahuan terhadap konsep dan cara kerja dari proses enksipsi dan dekripsi menggunakan algoritma *Blowfish* pada file *audio* (*mp3*).
2. Untuk menerapkan algoritma *Blowfish* dalam proses pengamanan data file *audio* (*mp3*) menggunakan bahasa pemrograman *VB .NET*.
3. Untuk menambah pemahaman dan ilmu ke penulis dalam cara algoritma Blowfish serta penerapannya dalam proses enkripsi dan dekripsi.

BAB II

LANDASAN TEORI

1.1 Konsep Dasar Sistem

Sistem merupakan pendekatan prosedur komponen, dengan pendekatan prosedur sistem dapat didefinisikan sebagai kumpulan dari prosedur-prosedur untuk membentuk suatu kesatuan dan tujuan tertentu.

Menurut Romney dan Steinbart (2015:3) “sistem adalah suatu rangkaian yang terdiri dari 2 atau lebih komponen yang saling berhubungan dan saling berinteraksi satu dengan yang lain untuk mencapai tujuan dimana sistem biasanya terbagi dalam sub sistem yang lebih kecil yang mendukung sistem yang besar”.

Menurut Gelinas dan Dull (2012:11), “Sistem merupakan seperangkat elemen yang saling bergantung yang bersama-sama mencapai tujuan tertentu. Dimana sistem harus memiliki organisasi, hubungan timbal balik, integrasi dan tujuan pokok”.

Menurut Mulyadi (2016:4) “Sistem adalah suatu jaringan prosedur yang dibuat menurut pola yang terpadu untuk melaksanakan kegiatan pokok perusahaan”.

Berdasarkan pengertian dan referensi diatas dapat disimpulkan bahwa sistem merupakan gabungan elemen yang saling berkaitan dan berhubungan yang bersama-sama mencapai suatu tujuan tertentu dalam proses yang teratur yang dapat mendukung sistem yang lebih besar dan saling memiliki ketergantungan untuk mencapai tujuan tertentu.

2.2 Pengertian Informasi

Tidak mudah untuk mendefinisikan konsep informasi karena istilah yang satu ini mempunyai banyak aspek, ciri dan manfaat yang satu dengan yang lainnya terkadang sangat berbeda. Informasi merupakan data yang berasal dari fakta lalu membuat pengetahuan yang didapatkan dari pembelajaran, pengalaman ataupun intruksi dan selanjutnya dilakukan pengolahan (proses) untuk menjadi bentuk yang berguna atau bermanfaat bagi si penerima atau pemakainya.

Menurut krismiaji (2015:14), "Informasi adalah data yang telah diorganisasi dan telah memiliki kegunaan dan manfaat".

Hal serupa juga disampaikan oleh Romney dan steinbart (2015:4) : "Informasi adalah data yang telah dikelola dan diproses untuk memberikan arti dan memperbaiki proses pengambilan keputusan keputusan. Sebagaimana perannya, pengguna membuat keputusan yang lebih baik sebagai kuantitas dari peningkatan informasi".

Berdasarkan beberapa pengertian diatas dapat disimpulkan bahwa pengertian informasi adalah data yang di olah dari hasil kesaksian atau rekaman peristiwa atau data. Data itu sendiri adalah kenyataan yang menggambarkan suatu kejadian, sedangkan kejadian itu merupakan peristiwa yang terjadi pada waktu tertentu dan berasal dari fakta yang telah diolah menjadi bentuk yang berguna dan berarti bagi pemakainya dan dapat memberikan ilmu pengetahuan kepada seorang yang menggunakannya serta mempermudah dalam proses mengambil keputusan.

2.3 Pengertian Implementasi

Menurut Nurdin Usman dalam bukunya yang berjudul Konteks Implementasi Berbasis Kurikulum mengemukakan pendapatnya mengenai implementasi atau pelaksanaan sebagai berikut : “Implementasi adalah bermuara pada aktivitas, aksi, tindakan, atau adanya mekanisme suatu sistem. Implementasi bukan sekedar aktivitas, tetapi suatu kegiatan yang terencana dan untuk mencapai tujuan kegiatan”(Usman, 2015:70).

Pengertian implementasi yang dikemukakan di atas, dapat dikatakan bahwa implementasi adalah bukan sekedar aktivitas, tetapi suatu kegiatan yang terencana dan dilakukan secara sungguh-sungguh berdasarkan acuan norma tertentu untuk mencapai tujuan kegiatan. Oleh karena itu implementasi tidak berdiri sendiri tetapi dipengaruhi oleh objek berikutnya. Menurut Guntur Setiawan dalam bukunya yang berjudul Implementasi Dalam Birokrasi Pembangunan mengemukakan pendapatnya mengenai implementasi atau pelaksanaan sebagai berikut “Implementasi adalah perluasan aktivitas yang saling menyesuaikan proses interaksi antara tujuan dan tindakan untuk mencapainya serta memerlukan jaringan pelaksana, birokrasi yang efektif” (Setiawan,2014:39).

2.4 Pengertian Data

Ladjamudin (2013:8), “Data adalah deskripsi dari sesuatu dan kejadian yang kita hadapi (*the description of things and events that we face*). Sementara data bisnis (*business* data) didefinisikan sebagai deskripsi organisasi tentang suatu (*resources*) dan kejadian (*transactions*) yang terjadi (*business data is*

anorganization's description of things (resources) and events (transactions) that it face).

Ibrahim (2015:182), "Data dalam penelitian ini adalah segala bentuk fakta, data dan informasi yang digali dari subjek penelitian".

Dari pengertian diatas, dapat disimpulkan bahwa data merupakan kumpulan fakta mengenai suatu benda, peristiwa atau kegiatan yang disimpan atau dicatat.

2.5 Media *Audio*

Audio adalah suara atau bunyi yang dihasilkan oleh getaran suatu benda agar dapat tertangkap oleh telinga manusia, getaran tersebut harus kuat minimal 20 kali/detik.

Menurut kamus besar bahasa Indonesia edisi ketiga (Tim Penyusun, 2007:76), audio merupakan alat peraga yang bersifat dapat di dengar.

Daryanto (2010: 37), audio berasal dari kata *audible*, yang artinya suaranya dapat di perdengarkan secara wajar oleh telinga manusia.

Menurut Sadiman (2005:49), media audio adalah media untuk menyampaikan pesan yang akan disampaikan dalam bentuk lambing-lambang auditif, baik verbal (ke dalam kata-kata atau lisan) maupun non verbal.

2.6 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani: "*cryptós*" artinya "*secret*" (rahasia), sedangkan "*gráphein*" artinya "*writing*" (tulisan), jadi kriptografi berarti "*secret writing*" (tulisan rahasia). Definisi kriptografi ada beberapa yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat di mengerti lagi maknanya. Definisi ini mungkin cocok pada masa lalu dimana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih dari sekadar *privacy*, tetapi juga untuk tujuan data *integrity*, *authentication*, dan *non-repudiation* (Mollin ,2014).

Kriptografi merupakan ilmu sekaligus seni untuk menjaga keamanan pesan, 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. Kata "seni" di dalam definisi di atas maksudnya adalah mempunyai cara yang unik untuk merahasiakan pesan.Kata "*graphy*" di dalam "*cryptography*" itu sendiri sudah menyiratkan suatu seni (Munir, 2014).

Adapun istilah-istilah yang sering digunakan dalam ilmu kriptgorafi diantara sebagai berikut :

1. *Plaintext*

   Plaintext merupakan pesan asli yang belum disandikan atau informasi yang ingin dikirimkan atau di jaga keamanannya.

2. *Ciphertext*

   Ciphertext merupakan pesan yang telah disandikan (dikodekan) sehingga siap untuk dikirimkan.

3. Enkripsi

   Enkripsi merupakan proses yang dilakukan untuk menyandikan plaintext menjadi ciphertext dengan tujuan pesan tersebut tidak dapat dibaca oleh pihak yang tidak berwenang.

4. Dekripsi

   Dekripsi merupakan proses yang dilakukan untuk memperoleh kembali plaintext dari ciphertext.

5. Kunci

   Kunci yang dimaksud adalah kunci yang dipakai untuk melakukan dekripsi dan enkripsi. Kunci terbagi menjadi dua bagian, diantaranya yaitu kunci pribadi (*private key*) dan kunci umum (*public key*).

6. Kriptosistem

   Kriptosistem merupakan sistem yang dirancang untuk mengamankan suatu sistem informasi dengan memanfaatkan kriptografi.

7. Kriptanalisis

   Kriptanalisis merupakan suatu ilmu untuk mendapatkan plaintext tanpa harus mengetahui kunci secara wajar.

2.7 Tujuan Kriptografi

Berikut merupakan empat tujuan dasar dari aspek kriptografi yang menjadi dasar dari keamanan data, diantaranya yaitu :

1. Kerahasiaan

   Kerahasiaan artinya data yang diamankan hanya dapat diakses oleh pihak-pihak tertentu saja.

2. Otentikasi

   Pada saat mengirim atau menerima informasi, kedua belah pihak perlu mengetahui bahwa pengirim dari pesan tersebut adalah orang yang sebenarnya.

3. Integritas Data

   Tuntutan integritas data berhubungan dengan jaminan setiap pesan yang dikirim sampai pada penerima tanpa ada bagian dari pesan tersebut yang diganti, diduplikasi, diruskan, diubah atau ditambahkan.

4. Ketiadaan penyangkalan

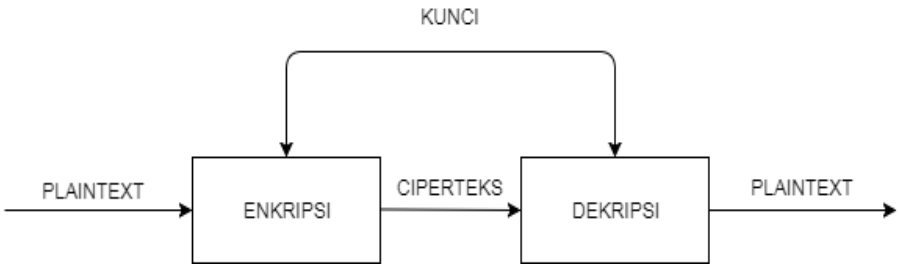
   Ketiadaan penyangkalan mencegah pengirim maupun penerima mengingkari bahwa mereka telah mengirimkan atau menerima suatu pesan atau informasi.

2.8 Algoritma Kriptografi

Algoritma kriptografi atau sering disebut dengan *cipher* adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi (Schneier, 2015). Algoritma kriptografi ada dua macam, diantaranya yaitu :

1. Algoritma Simetris

   Algortima simetris atau disebut juga algoritma konvensional adalah algoritma yang menggunakan kunci yang sama pada proses enkripsi dan dekripsi. Algoritma ini mengharuskan pengirim dan penerima menyetujui satu kunci tertentu sebelum dapat berkomunikasi secara aman. Keamanan algoritma simtri tergantung pada rahasia kunci. Pemecahan kunci berarti memungkinkan setiap orang dapat mengenkripsi dan mendekripsi pesan dengan mudah.

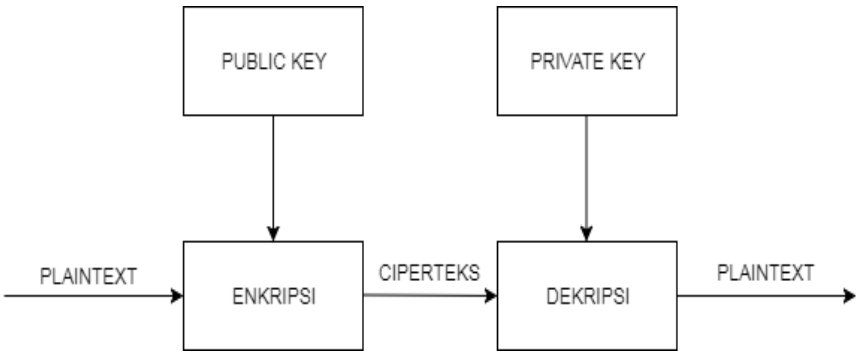


Gambar 2.1 Algoritma Kriptografi Simetris

Sumber: Basri, (2016)

2. Algoritma Asimetris

   Algoritma asimetris merupakan algoritma kriptografi yang salah satu kuncinya digunakan untuk proses enkripsi dan satu lagi digunakan untuk proses dekripsi. Semua orang yang mendapatkan kunci *public* dapat menggunakannya untuk mengenkripsi pesan, sedangkan hanya pengirim dan penerima sajalah yang dapat mendekrip pesan tersebut karena memegang kunci *private*.



Gambar 2.2 Algoritma Kriptografi Asimetris

Sumber: Basri, (2016)

2.9 Keamanan Data

Masalah keamanan merupakan salah satu aspek yang sangat penting dari sebuah sistem informasi. Tapi yang sangat di sayangkan, masalah keamanan ini kurang mendapat perhatian. Seringkali masalah keamanan menjadi urutan kedua atau bahkan urutan yang terakhir dalam daftar hal-hal yang dianggap penting. Apabila mengganggu performansi sistem, masalah keamanan ini sering dikurangiatau bahkan ditiadakan. Kemampuan untuk mengakses untuk menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi, baik yang berupa organisasi komersial (perusahaan), perguruan tinggi, lembaga pemerintahan maupun individual (pribadi) (Syaiful Anwar, 2017).

Hal ini dimungkinkan dengan perkembangan pesat di bidang teknologi komputer dan telekomunikasi. Dahulu jumlah komputer sangat terbatas dan belum digunakan untuk menyimpan hal-hal yang sifatnya sensitif. Penggunaan komputer untuk menyimpan informasi yang sifatnya *classified*, baru dilakukan sekitar tahun 1950-an.

Sangat pentingnya sebuah nilai informasi menyebabkan seringkali informasi di inginkan hanya boleh diakses oleh orang-orang tertentu saja. Jatuhnya informasi ke tangan pihak lain (misalnya pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. Sebagai contoh, banyak informasi dalam sebuah perusahaan yang hanya boleh diakses oleh orang-orang tertentu didalam perusahaan tersebut, seperti misalnya informasi tentang produk yang sedang dibuat, algoritma-algoritma dan teknik yang digunakan untuk menghasilkan produk tersebut. Untuk itu keamanan dari sistem informasi harus terjamin dalam batas yang bisa diterima.

2.10 Enkripsi dan Dekripsi

Enkripsi merupakan sebuah metode penyandian sebuah pesan atau informasi menjadi sebuah teks yang tidak dapat dibaca. Enkripsi berkaitan erat dengan kriptografi, yang merupakan sebuah metode untuk mengamankan sebuah pesan hingga tidak dapat dibaca oleh pihak ketiga. Enkripsi dapat dibagi menjadi dua proses enkripsi yang berbeda yaitu *Block Cipher* dan *Stream Cipher* (Ferguson dkk, 2015).

Dekripsi yaitu proses konversi data yang sudah dienkripsi (*ciphertext*) kembali menjadi data aslinya (*Original Plaintext*) sehingga dapat dibaca atau di mengerti kembali. Pesan yang akan di enkripsi disebut plaintext yang dimisalkan *plaintext* (P), proses enkripsi dimisalkan enkripsi (E), proses dekripsi dimisalkan dekripsi (D), dan pesan yang sudah di enkripsi disebut *ciphertext* yang dimisalkan *ciphertext* (C) (Ferguson dkk, 2015).

2.11 Model-Model Enkripsi

Dalam membahas model-model enkripsi beserta algoritma yang akan dipakai untuk enkripsi ada 2 hal penting yang harus dijabarkan, yaitu enkripsi dengan kunci pribadi dan enkripsi dengan kunci *public* (Ferguson dkk, 2015).

a. Enkripsi Kunci Pribadi

Enkripsi dapat dilakukan jika si pengirim dan si penerima telah sepakat untuk menggunakan metode enkripsi atau kunci enkripsi tertentu.Metode enkripsi atau kuncinya ini harus dijaga ketat supaya tidak ada pihakluar yang mengetahuinya. Kesepakatan cara enkripsi atau kunci dalam enkripsi ini bisa dicapai lewat jalur komunikasi lain yang lebih aman, misalnya dengan bertemu langsung. Cara enkripsi dengan kesepakatan atau kunci enkripsi di atas dikenal dengan istilah enkripsi dengan kunci pribadi, karena cara enkripsi atau kunci yang hanya boleh diketahui oleh dua pribadi yang berkomunikasi tersebut.

Cara enkripsi inilah yang umum digunakan pada saat ini baik untuk kalangan pemerintah maupun kalangan bisnis. Cara enkripsi ini juga dikategorikan sebagai kriptografi simetris, karena dua belah pihak mengetahui kunci yang sama. Selain masalah komunikasi awal untuk penyampaian kunci, cara enkripsi ini juga mempunyai kelemahan yang lain. Kelemahan ini timbul jika terdapat banyak orang yang ingin saling berkomunikasi. Karena setiap pasangan harus menghafal banyak kunci dan harus menggunakannya secara tepat. Sebab, jika tidak, maka si penerima tidak bisa mengartikannya.

b. Enkripsi dengan Kunci Public

Cara enkripsi ini mempunyai banyak kelebihan, salah satunya adalahtiap orang hanya perlu memiliki satu set kunci, tanpa peduli berapa banyak orang yang akan diajak berkomunikasi. Selain itu, cara enkripsi ini tidak membutuhkan saluran yang aman untuk pengiriman kunci, sebab kunci yang dikirimkan ini harus diketahui oleh public. Cara enkripsi sangat praktis sehingga masyarakat umum pun dapat dengan mudah memakainya. Cara kerja enkripsi ini secara singkat dapat diterangkan sebagai berikut. Setiap orang yang menggunakan enkripsi ini harus mempunyai dua buah kunci, satu disebut kunci rahasia yang hanya boleh diketahui oleh dirinya sendiri dan yang lain disebut kunci public yang disebarkan ke orang lain.

Kedua kunci ini dibuat secara acak dengan menggunakan rumus matematika tertentu. Jadi, kedua kunci ini berkaitan erat secara matematika. Jika si A hendak mengirim pesan kepada si B, si A perlu mengenkrip pesan itu dengan kunci public milik si B. Pesan si A yang telah dienkrip dengan menggunakan kunci public si B hanya bisa dibuka dengan kunci public itusendiri. Si B wajib untuk menjamin keamanan kunci rahasianya.Karena kunci rahasia ini tidak perlu diketahui pihak si pengirim berita, kunci ini tidak akan pernah dikirim lewat jalur umum. Hal ini membuat cara ini jauh lebih aman daripada enkripsi dengan kunci pribadi. Misalkan si C dapat mengirim ke B dengan menggunakan kunci public si B yang sama. Walaupun mengetahui kunci public si B, pesan

yang telah dienkrip dengan itu sangat sulit untuk dibuka. Cara enkripsi ini dikategorikan dalam kriptografi asimetris, karena kunci yang dipakai untuk mengenkrip dan untuk membuka enkrip adalah dengan menggunakan dua kunci yang berbeda (Wahana Komputer, dkk, 2014:94).

2.12 Algoritma *Blowfish*

(Faldy, 2016). Algoritma *Blowfish* mempunyai nama lain *OpenPGP.Cipher.4* yang merupakan enkripsi golongan *Symmetric Cryptosystem*, metode enkripsinya mirip dengan *DES (DES-like Cipher)* diciptakan oleh seorang *Cryptanalyst* bernama *Bruce Schneier*. *Blowfish* termasuk dalam enkripsi *block Cipher* 64-bit dangan panjang kunci yang bervariasi antara 32-bit sampai 448-bit. Algoritma *Blowfish* terdiri atas dua bagian, yaitu:

1. *Key-Expansion*

   Berfungsi untuk merubah kunci (minimum 32-*bit*, maksimum 448-*bit*) menjadi beberapa array sub kunci (sub *key*) dengan total 4168 *byte*.

2. Enkripsi Data

   Terdiri dari iterasi fungsi sederhana (*fastel network*) sebanyak 16 kali putaran. Setiap putaran terdiri dari permutasi kunci denpendent dan subsitusi kunci data denpendent.

Langkah kerja algoritma *blowfish* terdiri atas 2 bagian, yaitu (Kurnia, 2016):

a. Proses Ekspansi Kunci (*Key Expansion*)

1) Inisialisasi P-array yang pertama dan juga empat S-box, berututan, dengan string yang telah pasti.String tersebut terdiri dari digit-digit heksadesimal dari phi, tidak termasuk angka tiga di awal.

   Contoh :

   P1

   P = 0x243f6a882

   P = 0x85a308d33

   P = 0x13198a2e4

   dan seterusnya sampai dengan S-box yang terakhir atau P = 0x03707344

2) Kemudian P1 di XOR dengan 32-bit awal kunci, P2 di XOR dengan 32-bit berikutnya dari kunci, dan seterusnya untuk semua bit kunci. Jika Panjang kunci ternyata kurang dari jumlah P box, maka siklus perhitungan akan diulangi hingga semua P ter-XOR-kan.

3) Enkripsikan string yang seluruhnya nol (*all-zero string*) dengan algoritma *blowfish*, menggunakan subkunci yang telah didekripsikan pada langkah 1dan 2.

4) Gantikan P1 dan P2.

5) Enkripsikan keluaran langkah 3 menggunakan algoritma *Blowfish* dengan subkunci yang telah dimodifikasi. dengan keluaran dari langkah 3.

6) Gantikan P3 dan P4.

7) Lanjutkan langkah-langkah di atas, gantikan seluruh elemen P-array dan juga gantikan ke-empat S-box secara berurutan, dengan hasil keluaran algoritma Blowfish yang terus-menerus berubah. dengan keluaran dari langkah 5.

b. Proses Enkripsi Data

Proses enkripsi sebelumnya telah dibahas dan digunakan pada proses perluasan kunci. Kali ini akan diterapkan pada plaintext yang berbeda dengan anggapan bahwa proses perluasan kunci telah diselesaikan dengan baik sehingga nilai semua blok P dan S telah diperbaharui. Hal ini penting dikarenakan proses enkripsi dapat dilakukan jika proses perluasan kunci telah selesai.

1) Plaintext yang digunakan adalah “al p 4a ?”, dimana plaintext dalam nilai angka = 263752415256265289. Nilai tersebut dipecah menjadi nilai XL dan XR yang masing-masing berukuran 32 bit, dimana XL merupakan 32 bit pertama dari plaintext dan XR 32 bit kedua dari plaintext. Didapatkan nilai XL= 26375241 dan XR= 52562652.
2) Perulangan dilakukan sebanyak 16 kali dimana disetiap perulangan dilakukan operasi xor XL dengan Pi dimana i menunjukkan jumlah perulangan yang sudah dilakukan. Lalu, nilai xxRR merupakan hasil dari operasi xor antara XL dan XR sendiri. Setelah didapatkan nilai XL dan XR, maka kedua nilai tersebut dipertukarkan satu dengan yang lain. Terdapat hasil sebagaimana terlihat pada gambar dibawah ini.

Indeks Proses	P Indeks Proses	XL	F(XL)	XR
1	8D717830	2373003349	8064871505	6775194193
2	884446F9	4757456040	7702866319	5474697690
3	AE21C62E	8194656244	9891654133	14328245597
4	BF256408	16796272981	3141382032	5692532836
5	FFA3C4B2	7196306646	2190551807	14691853226
6	25BE839C	14194401334	4396058258	2867358276
7	3BE7ED1B	2433714015	8032108102	11019312752
8	C8A843D3	10072956323	5225731923	7087706124
9	988940B3	5351706815	9358013627	1973610776
10	DEC445AC	2875632820	4330329214	1021772993
11	C36BE21B	4287424218	9554018848	11040485012
12	21DBF4AE	11606399546	4282496971	13455633
13	F0F8B6EB	4030064634	11368883188	375978446

Gambar 2.3 Proses Enkripsi Algoritma Blowfish

3) Nilai xxLL dan xxRR dipertukarkan sehingga:

   XL= 2902575082

   XR= 1323743423

4) Dilakukan operasi xor terhadap XR dan kunci P17

   XR = XR $\oplus$ P17

   XR = 1258505066

5) Dilakukan operasi xor terhadap XL dan kunci P18

   XL = XL $\oplus$ P18

   XL = 3371315541

   Masing-masing nilai XR dan XL dilakukan operasi and terhadap bilangan heksadesimal FFFF FFFF agar ukuran nya tepat 32 bit.

   XR = 1258505066 and 4294967295

   XR = 1258505066

XL = (3371315541 and 4294967295)≪32

XL = 3371315541≪32

XL= 14479689993091547136

Hasil dari proses ini adalah XL ⊕ XR = 11759496057487293479.

Ciphertext blowfish : L] ¦F[>di:

c. Proses Dekripsi

Proses dekripsi pada algoritma *blowfish* hampir sama dengan proses enkripsi. Perbedaan terletak pada urutan penggunaan kunci, yaitu kunci dimulai dari indeks paling tinggi menuju indeks 1. Disini akan dilakukan proses dekripsi terhadap ciphertext ” L] ¦F[>di: ”dengan menggunakan kunci yang sudah didekripsi oleh algoritma *RSA* yaitu “9na=36W7_” yang dihasilkan proses enkripsi sebelumnya. Proses Dekripsi dapat dilihat pada gambar dibawah ini.

Indeks Proses	P indeks Proses	XL	F(XL)	XR
1	65F3F6BF	2902575082	11963342236	10772111094
2	5E5FBD5	10870891811	3622815553	2062418091
3	8034E687	4208649772	10029928532	3525326199
4	2215D28D	4030064634	11368883188	10191734232
5	ECB21FE2	11606399546	4282496971	259280945
6	F0F8B6EB	4287424218	9554018848	2327664666
7	21DBF4AE	2875632820	4330329214	8549528228
8	C36BE21B	5351706815	9358013627	10848655375
9	DEC445AC	10072956323	5225731923	159827948
10	988940B3	2433714015	8032108102	15143871461
11	C8A843D3	14194401334	4396058258	6828917197
12	3BE7ED1B	7196306646	2190551807	16317696713
13	25BE839C	16796272981	3141382032	4694688582
14	FFA3C4B2	8194656244	9891654133	7058251936
15	BF256408	4757456040	7702866319	592506491
16	AE21C62E	2373003349	8064871505	4213516537

Gambar 2.4 Proses Dekripsi Algoritma Blowfish

1) Nilai angka dari ciphertext = 11759496057487293479
2) Dilakukan proses perulangan sebanyak 16 kali terhadap nilai XL dan XR.
3) Nilai xxLL dan xxRR dipertukarkan sehingga

   XL = 2373003349

   XR = 4213516537
4) Dilakukan operasi xor terhadap XR dan kunci P17

   XR = XR $\oplus$ P17

   XR= 52562652
5) Dilakukan operasi xor terhadap xxLL dan kunci P18

   XL = XL $\oplus$ P18

   XL = 20581

   Masing-masing nilai XR dan XL dilakukan operasi and terhadap bilangan heksadesimal FFFF FFFF agar ukuran nya tepat 32-*bit*.

   XR = 52562652 and 4294967295

   XR = 52562652

   XL = (20581 and 4294967295)$\ll$32

   XL = 20581$\ll$32

   XL = 88394721918976

   Hasil dari proses ini adalah XL $\oplus$ XR = 263752415256265289.

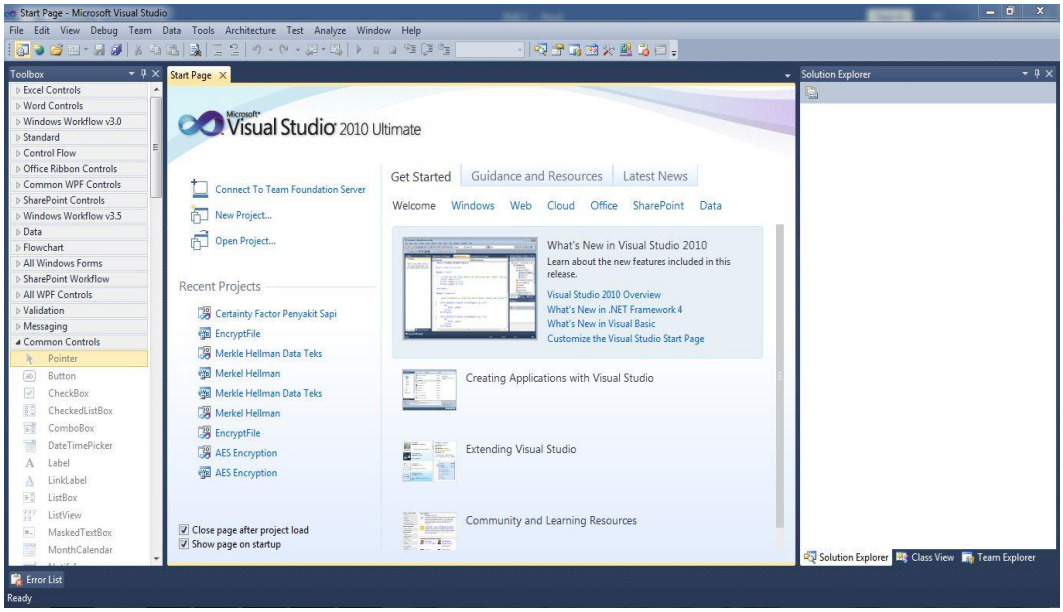
   Plaintext blowfish : al p 4a ?

2.13 *Microsoft Visual Studio* 2010 *Ultimate*

Dalam pembuatan skripsi ini, digunakan aplikasi *Visual Studio 2010 Ultimate* dari *Microsoft* sebagai aplikasi pembuat *software.* Microsoft Visual Studio merupakan sebuah perangkat lunak lengkap (suite) yang dapat digunakan untuk melakukan pengembangan aplikasi, baik itu aplikasi bisnis, aplikasi personal, ataupun komponen aplikasinya, dalam bentuk aplikasi console, aplikasi windows, ataupun aplikasi *web*. *Visual Studio* mencakup kompiler, *SDK*, *Integrated Development Environment* (*IDE*), dan dokumentasi (umumnya berupa *MSDN Library*). Kompiler yang dimasukkan ke dalam paket *Visual Studio* antara lain *Visual C++, Visual C#, Visual Basic, Visual Basic .NET, Visual InterDev*, *Visual J++, Visual J#, Visual FoxPro*, dan *Visual SourceSafe* (Mollin ,2014).

Microsoft Visual Studio dapat digunakan untuk mengembangkan aplikasi dalam native *code* (dalam bentuk bahasa mesin yang berjalan di atas *Windows*) ataupun *managed code* (dalam bentuk *Microsoft Intermediate Language* di atas *.NET Framework*). Selain itu, *Visual Studio* juga dapat digunakan untuk mengembangkan aplikasi *Silverlight*, aplikasi *Windows Mobile* (yang berjalan di atas *.NET Compact Framework*).

Berikut ini merupakan tampilan awal dari *Microsoft Visual Studio 2010 Ultimate*:

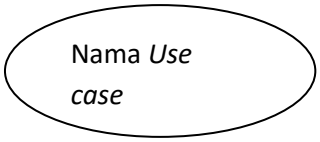


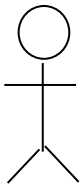
Gambar 2.5 *Microsoft Visual Studio 2010 Ultimate*

2.14 Use Case Diagram

Use case merupakan pendeskripsian sebuah interaksi antara satu atau lebih aktor dengan sistem informasi yang akan dibuat. Secara kasar, *use case* digunakan untuk mengetahui fungsi apasaja yang ada dalam sebuah sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi itu (Rosa & Shalahuddin, 2013).

Tabel 2.1 Table *use case* diagram

Simbol	Deskripsi
Use case 	Fungsionalisasi yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antar unit atau aktor, biasanya dinyatakan dengan menggunakan kata kerja di awal frase nama *use case*.

Aktor  Nama aktor	Orang, proses atau sistem yang lain yang berinteraksi dengan sistem informasi yang akan dibuat diluar sistem yang akan dibuat itu sendiri. Jadi walaupun *symbol* dari aktor adalah gambar orang, tetapi aktor belum tentu menggunakan orang; biasanya dinyatakan menggunakan kata benda di awal frase nama actor
Asosiasi / *Association*	Komunikasi antara aktor dan *use case* yang berpartisipasi pada *use case* atau *usecase* memiliki interaksi dengan actor
Ekstensi / *Extend* <<extend>> 	Kelakuan yang hanya berjalan dibawah kondisi tertentu seperti menggerakkan *handphone*.
Generalisasi 	Elemen yang menjadi spesialisasi elemen lain
Include <<include>> 	Kelakuan yang harus terpenuhi agar suatu *event* dapat terjadi

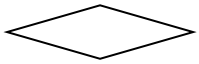
Sumber : Rosa A.S dan M. Shalahudin, 2014:162

2.15 Activity Diagram

Rosa dan M. Shalahudin (2014:161), "Diagram aktivitas atau *activity diagram* menggambarkan *workflow* (aliran kerja) atau aktivitas dari sebuah sebuah sistem atau proses bisnis atau menu yang ada pada perangkat lunak". Yang

perlu di perhatikan disini adalah bahwa diagram aktivitas menggambarkan aktivitas sistem bukan apa yang dilakukan aktor, jadi aktivitas yang dapat dilakukan oleh sistem.

Tabel 2.2 Simbol-Simbol *Activity Diagram*

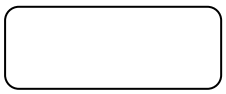
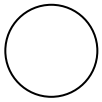
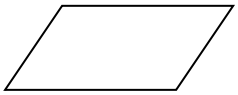
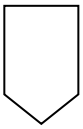
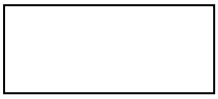
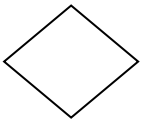
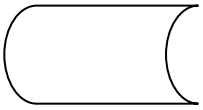
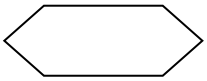
Simbol	Deskripsi
Status awal 	Status awal aktivitas sistem, sebuah diagram aktivitas memiliki sebuah status awal.
Aktivitas 	Aktivitas yang dilakukan sistem, aktivitas biasanya diawali dengan kata kerja.
Percabangan / *decision* 	Asosiasi percabangan dimana jika ada aktivitas pilihan lebih dari satu.
Penggabungan / Join 	Asosiasi penggabungan dimana lebih dari satu aktivitas digabungkan menjadi satu.
Status Akhir 	Status akhir yang dilakukan sistem, sebuah diagram aktivitas memiliki sebuah status akhir.

Sumber : Rosa A.S dan M. Shalahudin, 2014:162

2.16 Flowchart

Indrajani (2015:36), "*Flowchart* adalah penggambaran secara grafik dari langkah-langkah dan urutan prosedur suatu program."Indrajani (2015:38), menjelaskan simbol-simbol dalam *FlowChart* sebagai berikut:

Tabel 2.3 *Flowchart*

Simbol	Maksud	Simbol	Maksud
	Terminal (*START, END*)		Titik sambungan pada halaman yang sama
	*Input / Output (READ, WRITE)*		Tititk konektor yang berada pada halaman lain
	Proses		*Call* (Memanggil subprogram)
	*Decision (YES, NO)*		Dokumen
	*Display*		*Stored Data*
	Alur proses		*Preparation* (Pemberi nilai awal suatu variabel)

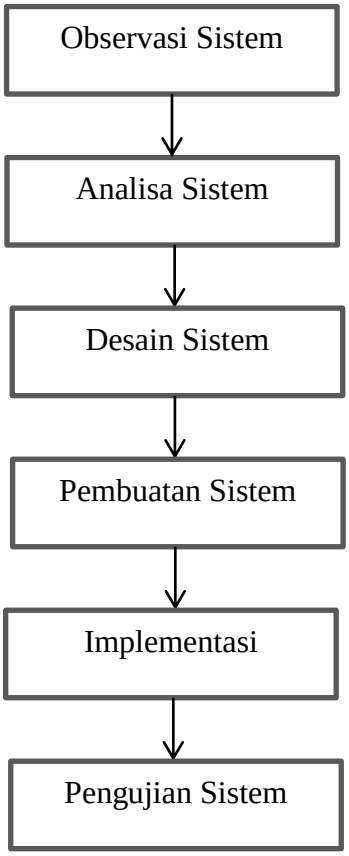
Sumber : Rosa A.S dan M. Shalahudin, 2014:162

BAB III

ANALISIS DAN PERANCANGAN

3.1 Tahapan Penelitian

Adapun tahapan penelitian yang dilakukan oleh penulis dengan judul "Implementasi Enkripsi *Audio* (*Voice*) menggunakan Algoritma *Blowfish*" adalah sebagai berikut:



Gambar 3.1 Tahapan Penelitian

3.2 Metode Pengumpulan Data

Untuk melengkapi penulisan skripsi ini, maka penulis melakukan beberapa metode pengumpulan data antara lain:

1. Studi Pustaka

   Mengumpulkan data dengan cara membaca dan mempelajari buku, jurnal ilmiah dan refrensi mengenai judul yang di angkat.

2. Observasi

   Dalam membuat program, penulis melakukan observasi terhadap tampilan, sistem, cara kerja dan alur kerja dari beberapa program yang sudah menerapkan sistem enkripsi pada pemrosesan datanya.

3.3 Analisa Sistem

Analisis sistem merupakan penjabaran sistem informasi yang utuh kedalam beberapa bagian dengan maksud agar dapat mengidentifikasi dan mengevaluasi berbagai macam masalah dan hambatan sehingga nantinya dapat dilakukan penanggulanggan, perbaikan dan juga pengembangan.

Pada penulisan skripsi ini, penulis membuat sistem enkripsi dan dekripsi audio dengan menggunakan algoritma *blowfish*. Tahap awal dari proses enkripsi dan dekripsi audio yaitu pengguna akan memilih terlebih dahulu file audio yang akan di enkripsi (*.mp3*). Setelah pengguna memilih *file*, barulah terjadi proses enkripsi file audio dimana sistem akan memproses *output stream* (*binary data*) dari file audio dan mengubahnya ke bentuk hasil dari proses algoritma blowfish berdasarkan dari data file audio. Dengan kata lain, pada proses enkripsi sistem

akan membuka isi dari file audio lalu mengubahnya ke bentuk hasil dari proses algoritma blowfish. Hasil dari proses enkripsi ini tidak hanya akan mengubah isi datanya saja melainkan juga mengubah ekstensi dari file audionya sehingga file tersebut tidak dapat dibuka.

Proses dekripsi juga menggunakan alur yang sama dimana file akan terlebih dahulu dibuka secara otomatis oleh sistem lalu didekripsi dengan menggunakan algoritma *blowfish*. Selain mengubah isi data ke bentuk semula, proses dekripsi juga akan merubah ekstensi file ke bentuk semula sehingga file dapat dibuka kembali dan bisa didengarkan.

3.4 Analisa Kebutuhan Perangkat

Dalam merancang program enkripsi dan dekripsi file audio ini, penulis membutuhkan beberapa perangkat di antaranya yaitu :

a. *Hardware* (Perangkat Keras)

   Adapun *Hardware* (Perangkat Keras) yang penulis gunakan dalam pembuatan mesin pencari ini yaitu :

   1) 1 buah laptop dengan spesifikasi yaitu :

      a) RAM 4GB

      b) Processor Intel Core i3

      c) Hard drive 500GB

      d) Display 14”

b. *Software* (Perangkat Lunak)

Penulis juga menggunakan beberapa perangkat lunak untuk membantu dalam proses pembuatan mesin pencari ini. Di anataranya yaitu :

1) *Sistem Opeasi Windows 7*

2) *Microsoft Visual Studio 2010 Ultimate*

3.5 Proses Enkripsi dan Dekripsi Pada Algoritma *Blowfish*

Proses enkripsi dan dekripsi algoritma *blowfish* terdari dari iterasi fungsi sederhana sebanyak 16 kali putaran. Masukkannya adalah 64 bit elemen data X. setiap putaran terdiri dari permutasi kunci dependent dan substitusi kunci dan data dependent. Semua operasi adalah penambahan dan *XOR* pada variabel 32 bit. Operasi tambahan lainnya hanyalah empat penelusuran tabel *array* berindeks untuk setiap putaran.

3.5.1 Proses Enkripsi Pada Algoritma *Blowfish*

Untuk lebih memahami proses enkripsi pada algoritma *blowfish*, maka penulis membuat contoh perhitungan manual yang terjadi pada proses enkripsi. Dalam hal ini, penulis menggunakan parameter sebagai berikut:

1. Bentuk inisial P-array sebanyak 18 buah (P1, P2, ..., P18) masing-masing bernilai 32-bit. P-array terdiri dari 18 kunci dan 32 bit sub kunci.

Tabel 3.1 P-array Konversi ke Biner

P-array	Hexa	Konversi Biner (32-bit)
P1	243F6A88	00100100 00111111 01101010 10001000
P2	85A308D3	10000101 10100011 00001000 11010011
P3	13198A2E	00010011 00011001 10001010 00101110
P4	3707344	00000011 01110000 01110011 01000100
P5	A4093822	10100100 00001001 00111000 00100010
P6	299F31D0	00101001 10011111 00110001 11010000
P7	82EFA98	00001000 00101110 11111010 10011000
P8	EC4E6C89	11101100 01001110 01101100 10001001
P9	452821E6	01000101 00101000 00100001 11100110
P10	38D01377	00111000 11010000 00010011 01110111
P11	BE5466CF	10111110 01010100 01100110 11001111
P12	34E90C6C	00110100 11101001 00001100 01101100
P13	C0AC29B7	11000000 10101100 00101001 10110111
P14	C97C50DD	11001001 01111100 01010000 11011101
P15	3F84D5B5	00111111 10000100 11010101 10110101
P16	B5470917	10110101 01000111 00001001 00010111
P17	9216D5D9	10010010 00010110 11010101 11011001

P18	8979FB1B	10001001 01111001 11111011 00011011

2. Bentuk S-box sebanyak 4 buah masing-masing bernilai 32-bit yang memiliki masukan 256 dalam bentuk hexadecimal yang kemudian dikonversi ke biner.

   S1,0, ..., S1,255

   S2,0, ..., S2,255

   S3,0, ..., S3,255

   S4,0, ..., S4,255

Tabel 3.2 Konversi S-box ke Biner

S-array	Hexa	Konversi biner
S1,0	D1310BA6	11010001 00110001 00001011 10100110
...		
S1,255	6E85076A	01101110 10000101 00000111 01101010
S2,0	4B7A70E9	01001011 01111010 01110000 11101001
...		
S2,255	DB83ADF7	11011011 10000011 10101101 11110111
S3,0	E93D5A68	11101001 00111101 01011010 01101000
...		
S3,255	406000E0	01000000 01100000 00000000 11100000
S4,0	3A39CE37	00111010 00111001 11001110 00110111
...		

S4,255	3AC372E6	00111010 11000011 01110010 11100110

3. Plaintext yang akan dienkripsi diasumsikan sebagai masukan, plaintext tersebut diambil sebanyak 64-bit.

   Plaintext = UPI YPTK

Tabel 3.3 Konversi Plaintext ke Biner

Karakter	ASCII (Hexa)	Biner
U	55	01010101
P	50	01010000
I	49	01001001
<space>	20	00100000
Y	59	01011001
P	50	01010000
T	54	01010100
K	4B	01001011

4. Kemudian plaintext dibagi menjadi 2 bagian, 32 bit pertama disebut XL dan 32 bit yang kedua disebut XR.

   XL = 01010101 01010000 01001001 00100000

   XR = 01011001 01010000 01010100 01001011

5. Pembangkitan sub kunci.

   Kunci = 2905

Tabel 3.4 Konversi Kunci ke biner

Karakter	ASCII (Hexa)	Biner
2	32	00110010
9	39	00111001
0	30	00110000
5	35	00110101

6. XOR kan P1 dengan 32 bit awal kunci, XOR kan P2 dengan 32 bit berikutnya dari kunci dan seterusnya untuk semua bit kunci. Ulangi siklus seluruh bit kunci secara berurutan sampai seluruh P-array ter-XOR kan dengan bit-bit kunci (sampai P18) atau jika disimbolkan:

   P1 = P1 ⊕ K1, P2 = P2 ⊕ K2, P3 = P3 ⊕ K3, . . . P14 = P14 ⊕ K14, P15 = P15 ⊕ K1, . . . P18 = P18 ⊕ K4.

   a. Sub kunci untuk iterasi pertama:

      P1 = P1 ⊕ K1

      P1 = 00100100 00111111 01101010 10001000 XOR

      = 00110010 00111001 00110000 00110101

      P1 = 00010110 00000110 01011010 10111111

   b. Sub kunci untuk iterasi kedua:

      P2 = P2 ⊕ K2

      P2 = 10000101 10100011 00001000 11010011 XOR

      = 00010110 00000110 01011010 10111111

      P2 = 10010011 10100101 01010010 01101100

7. Selanjutnya lakukan operasi XL = XL $\oplus$ Pi dan XR = F(XL) $\oplus$ XR. Dalam hal ini, penulis hanya melakukan 1 iterasi dikarenakan total iterasi proses enkripsi adalah 16 putaran.

   a. Untuk iterasi pertama i = 0 yaitu:

      XL = XL $\oplus$ P1

      XL = 01010101 01010000 01001001 00100000 XOR

      = 00010110 00000110 01011010 10111111

      XL = 01000011 01010110 00010011 10001111

8. Bagi XL menjadi 4 bagian (a, b, c, d) masing-masing 8 bit:

   a = 01000011

   b = 01010110

   c = 00010011

   d = 10001111

9. Fungsi F adalah sebagai berikut:

   F(XL) = $((S1.a + S2.b \bmod 2^{32}) \oplus S3.c) + S4.d \bmod 2^{32})$

   = (11010001 00110001 00001011 10100110. 01000011) +

   (01001011 01111010 01110000 11101001. 01010110) $\bmod 2^{32}$

   = (110110 10111111 11010110 00001100 01110010 +

   = 11001 01011011 00100001 11101110 01000110) $\bmod 2^{32}$

   = 1010000 00011010 11110111 11111010 10111000

   XOR S3.c = 00011010 11110111 11111010 10111000 $\oplus$

(11101001 00111101 01011010 01101000. 11100100)

= 00011010 11110111 11111010 10111000 ⊕

11001111 10111010 10100100 10000100 10100000

= 11001111 10111010 10100100 10000100 10100000 +

S4.d mod 2^{32}

= (11001111 10111010 10100100 10000100 10100000 +

(00111010 00111001 11001110 00110111. 10011111))

mod 2^{32}

= (11001111 10111010 10100100 10000100 10100000 +

100100 00101001 11100111 00010100 00101001

= 11110011 11001010 00111010 10010010 01000001

F(XL) = 11001010 00111010 10010010 01000001

XR = F(XL) ⊕ XR

XR = 11001010 00111010 10010010 01000001 XOR

10010001 01111100 00111001 00111100

XR = 01011011 01000110 10101011 01111101

10. Hasil dari operasi diatas ditukar XL menjadi XR dan XR menjadi XL.

    XL = 01011011 01000110 10101011 01111101

    XR = 01000011 01010110 00010011 10011111

11. Lakukan sebanyak 16 kali, pada perulangan yang ke-16 lakukan kembali proses penukaran XL dan XR.

12. Pada proses ke-17 lakukan operasi untuk XR = XR $\oplus$ P17 dan XL = XL $\oplus$ P18.
13. Proses terakhir satukan kembali XL dan XR sehingga menjadi 64 bit kembali.
14. Nilai biner tersebut dikonversikan ke dalam kode ASCII sehingga menghasilkan ciphertext yaitu: Ü/*oe|9‹

3.5.2 Proses Dekripsi Pada Algoritma *Blowfish*

Untuk lebih memahami proses dekripsi pada algoritma *blowfish*, maka penulis membuat contoh perhitungan manual yang terjadi pada proses dekripsi. Langkah perhitungan manual yang penulis lakukan adalah sebagai berikut:

1. Bentuk inisial P-array sebanyak 18 buah (P1, P2, ..., P18) masing-masing bernilai 32-bit. P-array terdiri dari 18 kunci dan 32 bit sub kunci.

Tabel 3.5 Konversi P-array ke Biner

P-array	Hexa	Konversi Biner (32-bit)
P1	243F6A88	00100100 00111111 01101010 10001000
P2	85A308D3	10000101 10100011 00001000 11010011
P3	13198A2E	00010011 00011001 10001010 00101110
P4	3707344	00000011 01110000 01110011 01000100
P5	A4093822	10100100 00001001 00111000 00100010

P6	299F31D0	00101001 10011111 00110001 11010000
P7	82EFA98	00001000 00101110 11111010 10011000
P8	EC4E6C89	11101100 01001110 01101100 10001001
P9	452821E6	01000101 00101000 00100001 11100110
P10	38D01377	00111000 11010000 00010011 01110111
P11	BE5466CF	10111110 01010100 01100110 11001111
P12	34E90C6C	00110100 11101001 00001100 01101100
P13	C0AC29B7	11000000 10101100 00101001 10110111
P14	C97C50DD	11001001 01111100 01010000 11011101
P15	3F84D5B5	00111111 10000100 11010101 10110101
P16	B5470917	10110101 01000111 00001001 00010111
P17	9216D5D9	10010010 00010110 11010101 11011001
P18	8979FB1B	10001001 01111001 11111011 00011011

2. Bentuk S-box sebanyak 4 buah masing-masing bernilai 32 bit yang memiliki masukan 256 dalam bentuk hexadecimal yang kemudian dikonversi ke biner.

Tabel 3.6 Konversi S-box ke Biner

S-box	Hexa	Konversi biner
S1,0 ... S1,255	D1310BA6 6E85076A	11010001 00110001 00001011 10100110 01101110 10000101 00000111 01101010
S2,0 ... S2,255	4B7A70E9 DB83ADF7	01001011 01111010 01110000 11101001 11011011 10000011 10101101 11110111
S3,0 ... S3,255	E93D5A68 406000E0	11101001 00111101 01011010 01101000 01000000 01100000 00000000 11100000
S4,0 ... S4,255	3A39CE37 3AC372E6	00111010 00111001 11001110 00110111 00111010 11000011 01110010 11100110

3. Ciphertext = Ü/*oe|9‹

Tabel 3.7 Konversi Ciphertext ke Biner

Karakter	ASCII (Hexa)	Biner
Ü	154	10011010
-	45	00101101
/	47	00101111
*	42	00101010
Oe	145	10010001
|	124	01111100

9	57	00111001
<	60	00111100

4. Kemudian plaintext dibagi menjadi 2 bagian, 32 bit pertama disebut XL dan 32 bit yang kedua disebut XR.

   XL = 10011010 00101101 00101111 00101010

   XR = 10010001 01111100 00111001 00111100

5. Pembangkitan sub kunci.

   Kunci = 2905

Tabel 3.8 Konversi Kunci ke biner

Karakter	ASCII (Hexa)	Biner
2	32	00110010
9	39	00111001
0	30	00110000
5	35	00110101

6. XOR kan P18 dengan 32 bit awal kunci, XOR kan P17 dengan 32 bit berikutnya dari kunci dan seterusnya untuk semua bit kunci. Ulangi siklus seluruh bit kunci secara berurutan sampai seluruh P-array ter-XOR kan.

   a. Sub kunci untuk iterasi pertama:

      P18 = P18 $\oplus$ K1

      P18 = 10001001 01111001 11111011 00011011 XOR

            00110010 00111001 00110000 00110101

      P18 = 10111011 01000000 11001011 00101110

b. Sub kunci untuk iterasi kedua:

P17 = P17 $\oplus$ K2

P17 = 10010010 00010110 11010101 11011001 XOR

10111011 01000000 11001011 00101110

P17 = 00101001 01010110 00011110 11110111

7. Selanjutnya lakukan operasi XL = XL $\oplus$ Pi dan XR = F(XL) $\oplus$ XR. Dalam hal ini, penulis hanya melakukan 1 iterasi dikarenakan total iterasi proses enkripsi adalah 16 putaran.

a. Untuk iterasi pertama i = 0 yaitu:

XL = XL $\oplus$ P18

XL = 10011010 00101101 00101111 00101010 XOR

= 10111011 01000000 11001011 00101110

XL = 00100001 01101101 11100100 00000100

8. Bagi XL menjadi 4 bagian (a, b, c, d) masing-masing 8 bit:

a = 00100001

b = 01101101

c = 11100100

d = 00000100

9. Fungsi F adalah sebagai berikut:

F(XL) = $((S1.a + S2.b \bmod 2^{32}) \oplus S3.c) + S4.d \bmod 2^{32})$

= 11010001 00110001 00001011 10100110. 00100001) +

(01001011 01111010 01110000 11101001. 01101101)

$\bmod 2^{32}$

= (00011010 11110111 01010010 10000000 01100110 +
00100000 00100011 00100010 00010011 00110101)
mod2^{32}

= 00111011 00011010 01110100 10010011 10011011

XOR S3.c = 00011010 01110100 10010011 10011011 $\oplus$
(11101001 00111101 01011010 01101000. 11100100)
= 00011010 01110100 10010011 10011011 $\oplus$
11001111 10111010 10100100 10000100 10100000

= 11001111 10100000 11010000 00010111 00111011+
S4.d mod 2^{32}

= (11001111 10100000 11010000 00010111 00111011 +
00111010 00111001 11001110 00110111. 00000100)
mod 2^{32}

= (11001111 10100000 11010000 00010111 00111011 +
11101000 11100111 01110001 11011100)
mod 2^{32}

= 1101000 10001001 10110111 10001001 00010111

F(XL) = 10001001 10110111 10001001 00010111

XR = F(XL) $\oplus$ XR

XR = 10001001 10110111 10001001 00010111 XOR
10010001 01111100 00111001 00111100

XR = 00011000 11001011 01101001 00101011

10. Hasil dari operasi di atas ditukar XL menjadi XR dan XR menjadi XL.

XL = 00011000 11001011 01101001 00101011

XR = 00100001 01101101 11100100 00000100

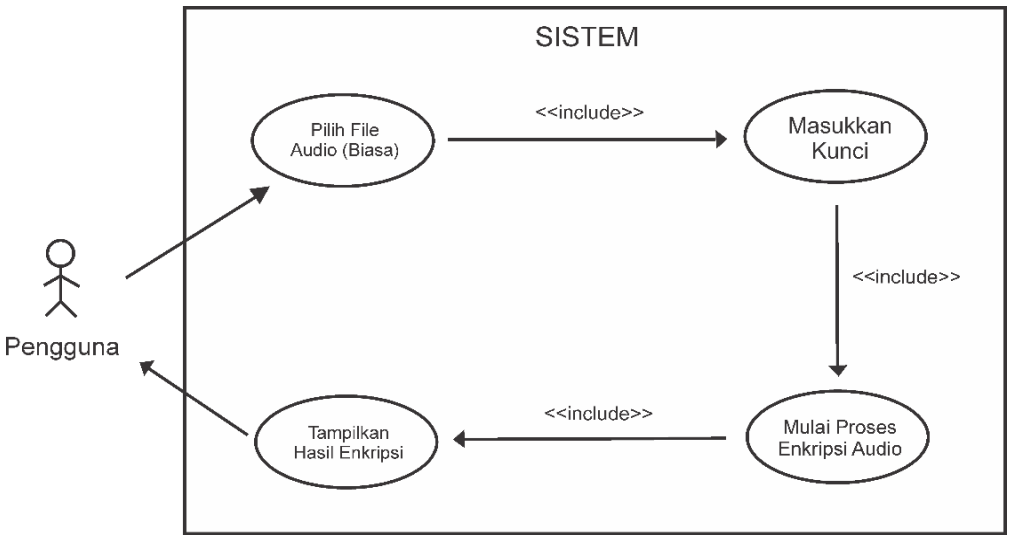
11. Lakukan sebanyak 16 kali, pada perulangan yang ke-16 lakukan kembali proses penukaran XL dan XR.
12. Pada proses ke-17 lakukan operasi untuk XR = XR $\oplus$ P2 dan XL = XL $\oplus$ P1.
13. Proses terakhir satukan kembali XL dan XR sehingga menjadi 64 bit kembali.
14. Nilai biner tersebut dikonversikan ke dalam kode ASCII sehingga menghasilkan ciphertext yaitu: UPI YPTK

3.6 Perancangan Alur Sistem

Perancangan atau pemodelan merupakan suatu proses untuk mendapatkan informasi mengenai alur dari sistem yang akan dibuat. Pada bagian ini, penulis akan menjelaskan tentang alur dari sistem mesin pencari yang dibuat.

a. *Use Case Diagram Enkripsi*

Berikut merupakan penjelasan dari *use case diagram* enkripsi sistem file audio yang akan dibuat :

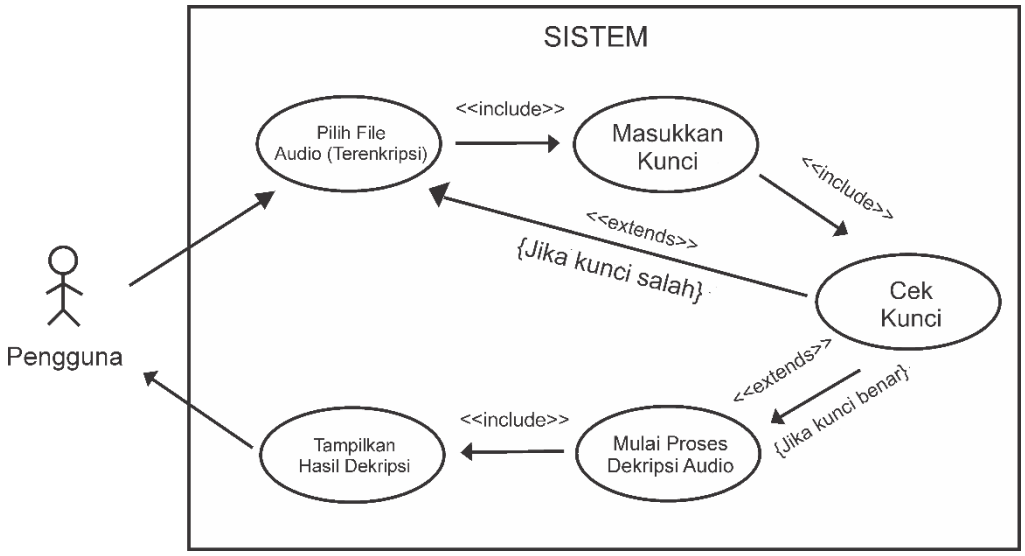


Gambar 3.2 *Use Case Diagram* Enkripsi

Diagram diatas merupakan diagram proses terjadinya enkripsi file audio. Tahap awal dimulainya enkripsi yaitu pengguna memilih terlebih dahulu memilih file audio yang ingin ia enkripsi. Setelah pengguna memilih file audio yang ingin mereka enkripsi, tahap selanjutnya yaitu pengguna akan memasukkan kunci yang digunakan untuk mengenkripsi file audio. Setelah pengguna memasukkan password, sistem akan memulai proses enkripsi dimana sistem akan membuka file audio tersebut lalu mengenkripsi isi file audio tersebut dengan menggunakan algoritma *blowfsh*. Setelah proses enkripsi berhasil, sistem akan memunculkan file hasil dari proses enkripsi tersebut yang nantinya pengguna dapat mengunduh file tersebut.

b. *Use Case Diagram* Dekripsi

Berikut merupakan penjelasan dari *use case diagram* dekripsi sistem file audio yang akan dibuat :

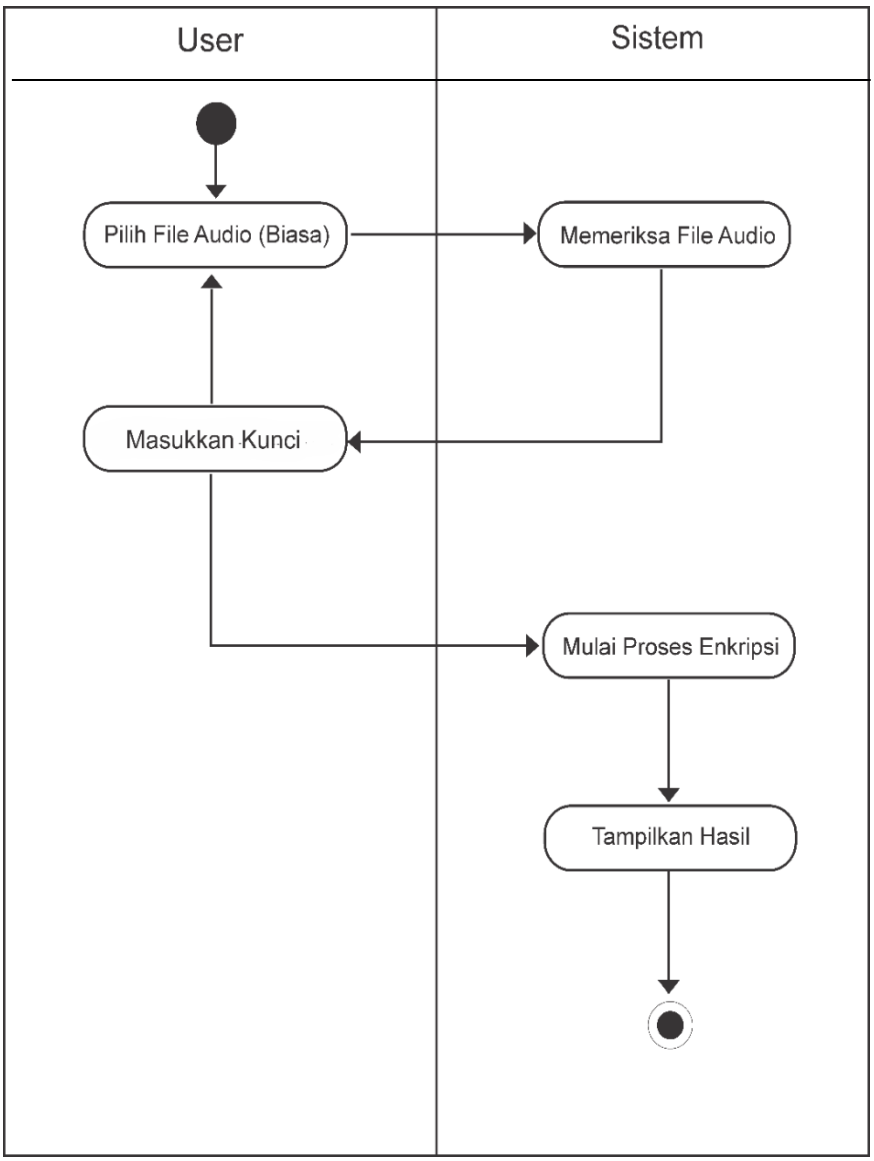


Gambar 3.3 *Use Case Diagram* Dekripsi

Diagram diatas merupakan proses terjadinya dekripsi file audio pada sistem. tahap pertama yaitu pengguna memilih file audio yang terenkripsi. Setelah pengguna memilih file audio yang terenkripsi, pengguna akan diminta untuk memasukkan kunci dari file enkripsi tersebut. Jika kunci yang dimasukkan salah, maka sistem akan meminta untuk memasukkan kunci ulang. Namun jika kunci yang dimasukkan benar, maka sistem akan memulai proses dekripsi file audio. Proses dekripsi file audio ini sama seperti proses enkripsi dimana sistem akan membuka file audio yang terenkripsi tersebut lalu mendekripsinya menggunakan algoritma *blowfish*. Setelah proses dekripsi selesai, sistem akan menampilkan hasil file audio yang terdekripsi tersebut sehingga pengguna dapat mengunduh file tersebut.

c. *Activity Diagram* Enkripsi

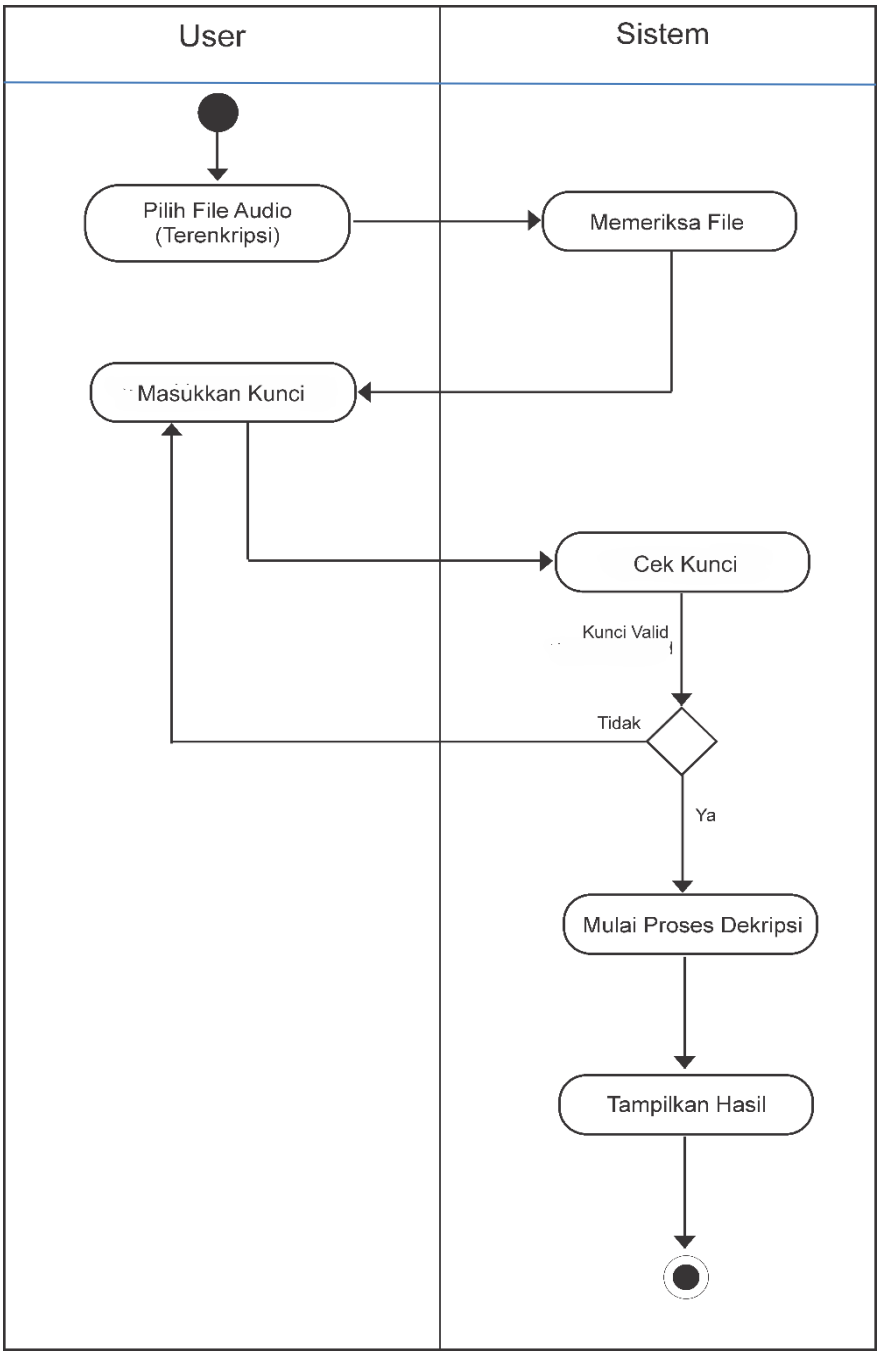
Activity diagram merupakan gambaran dari aktifitas-aktifitas yang terjadi di dalam suatu aplikasi dimulai dari aktifitas pertama sampai aktifitas berakhir. Berikut merupakan gambaran dari activity diagram pada proses enkripsi file audio.



Gambar 3.4 *Activity Diagram* Enkripsi

d. *Activity Diagram* Dekripsi

Berikut merupakan activity diagram dari proses dekripsi file audio :

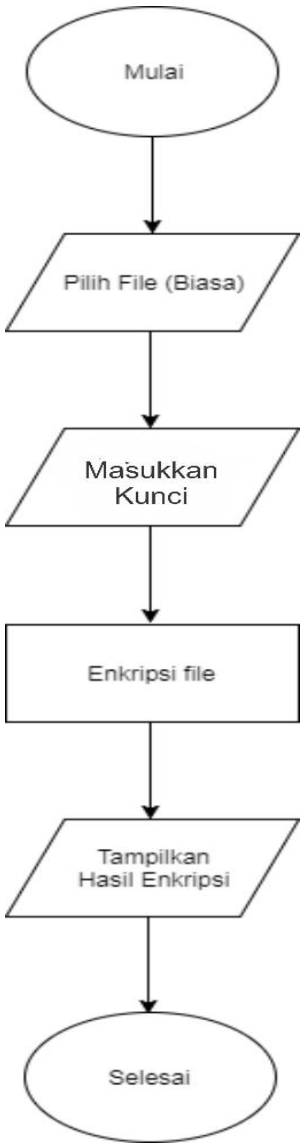


Gambar 3.5 *Activity Diagram* Dekripsi

3.7 *Flowchart* Sistem

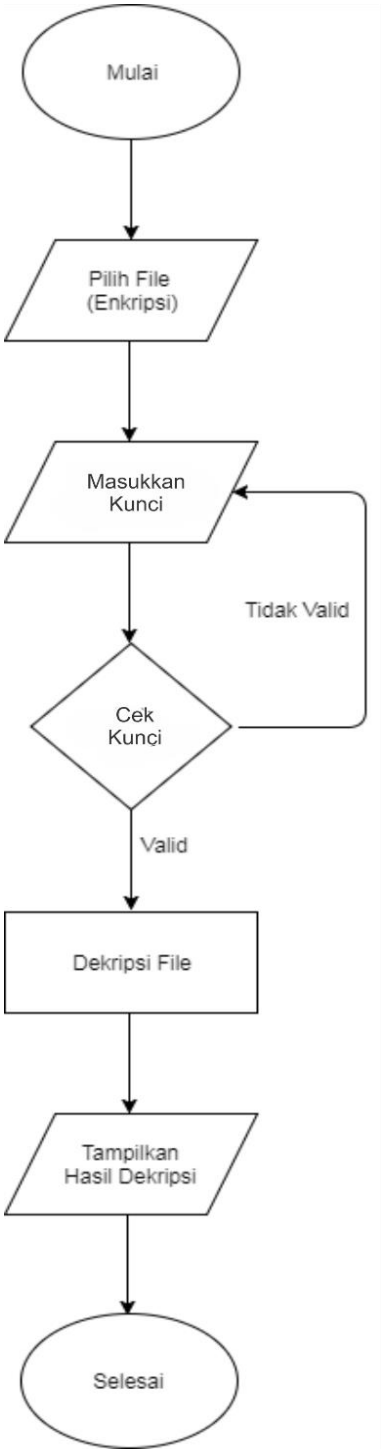
Flowchart merupakan diagram yang menggambarkan alur logika dari data yang akan diproses oleh program dari awal sampai akhir. Berikut merupakan *flowchart* dari sistem enkripsi dan dekripsi file audio yang akan penulis buat :

a. *Flowchart* Enkripsi



Gambar 3.6 *Flowchart* Enkripsi

b. *Flowchart* Dekripsi

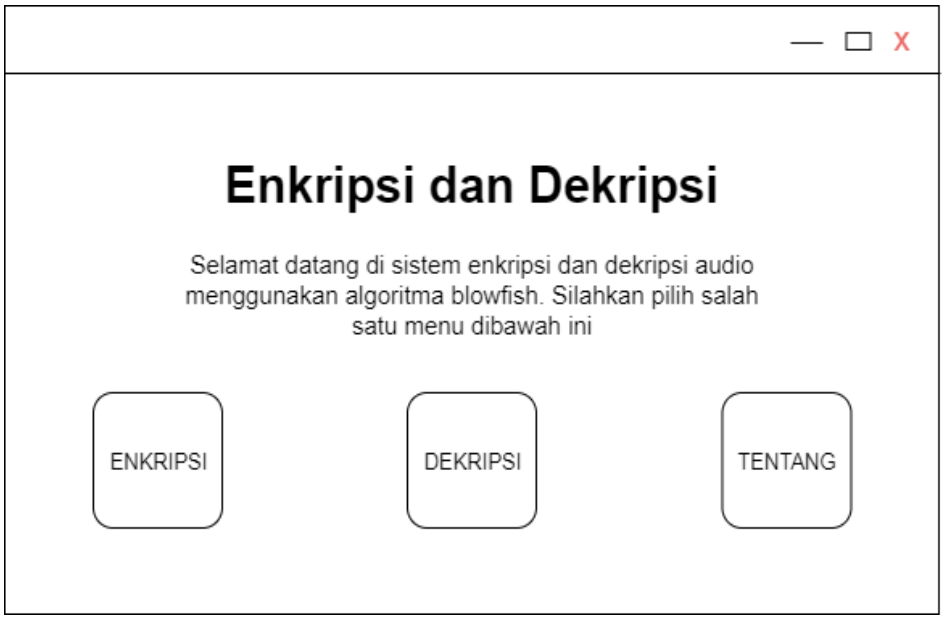


Gambar 3.7 *Flowchart* Dekripsi

3.8 Perancangan Antar Muka

Perancangan antar muka merupakan gambaran (*mockup*) dari tampilan aplikasi yang akan dibuat.

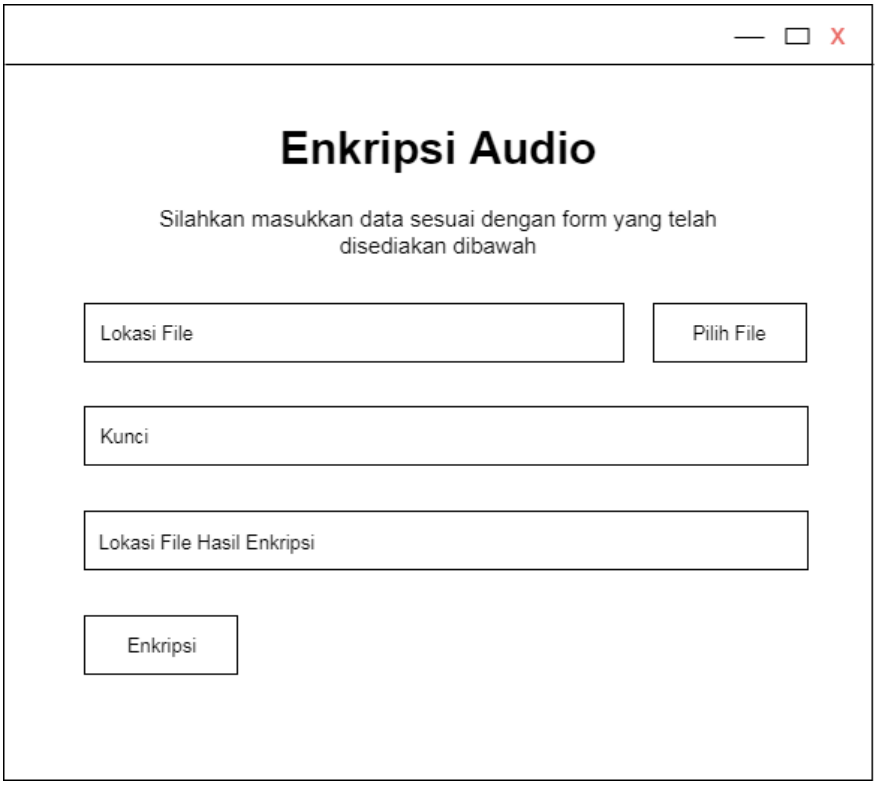
a. Rancangan Tampilan Awal



Gambar 3.8 Rancangan Tampilan Awal

Gambar diatas merupakan rancangan tampilan awal dari sistem enkripsi dan dekripsi file audio menggunakan algoritma *blowfish*. Tampilan diatas merupakan tampilan yang akan dilihat pengguna pada saat mengakses sistem. pada tampilan awal, teradapat dua pilihan yang dapat langsung dipilih pengguna untuk melakukan dekripsi dan enkripsi.

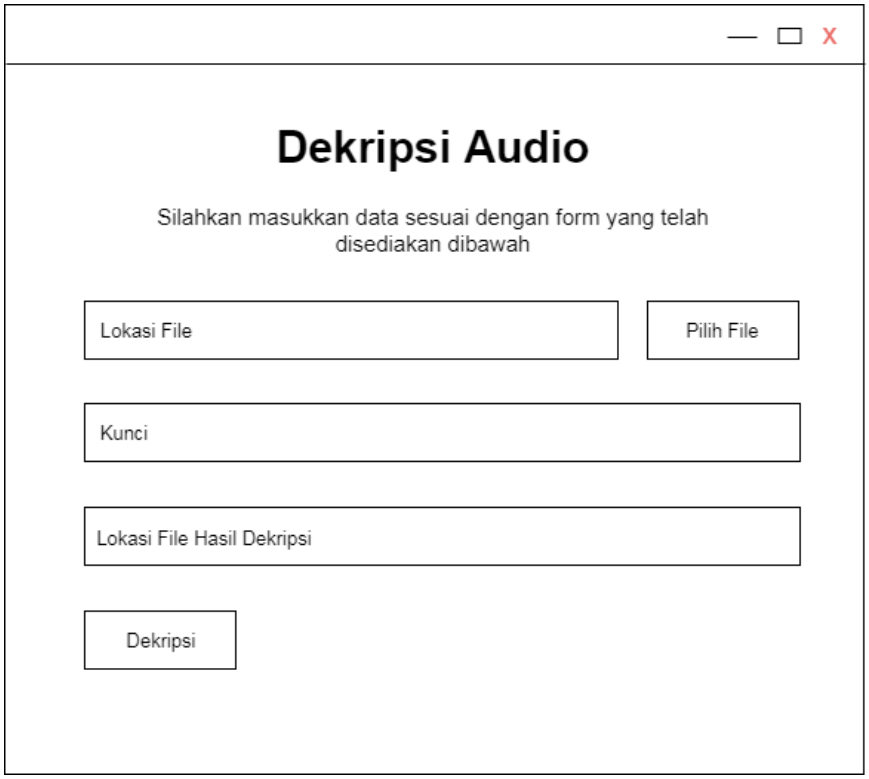
b. Rancangan Tampilan Form Enkripsi



Gambar 3.9 Rancangan Tampilan Form Enkripsi

Gambar diatas merupakan tampilan dari form enkripsi file audio. Pada tampilan ini pengguna akan terlebih dahulu memilih file audio yang akan dienkripsi. Setelah itu pengguna akan memasukkan kunci yang akan digunakan untuk memasukkan mengenkripsi file audio tersebut. jika file sudah terpilih dan kunci telah dimasukkan, pengguna harus menekan tombol enkripsi untuk memulai proses enkripsi. Jika proses telah selesai, hasil file enkripsi akan terlihat pada bagian hasil enkripsi file.

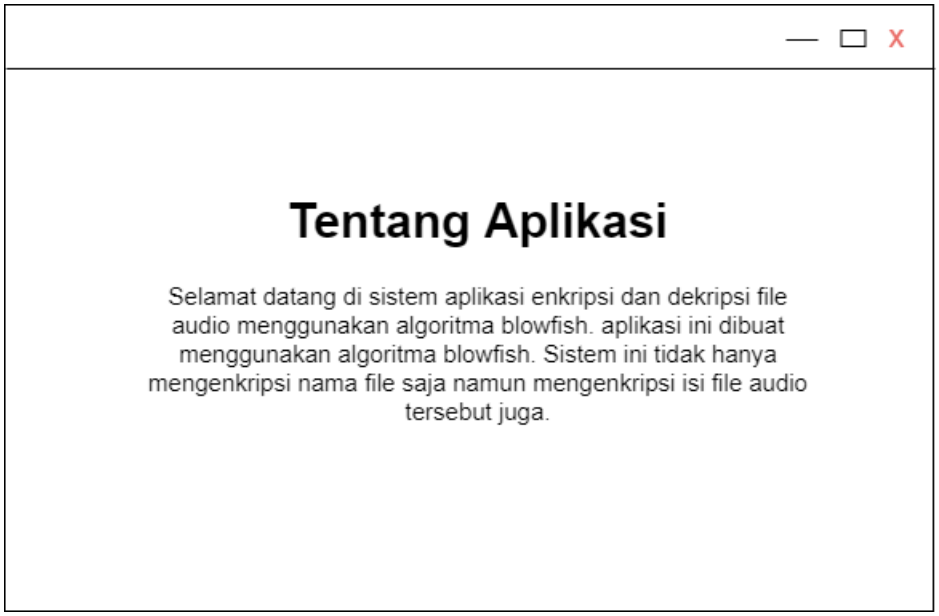
c. Rancangan Tampilan Form Dekripsi



Gambar 3.10 Rancangan Tampilan Form Dekripsi

Gambar diatas merupakan rancangan tampilan form dekripsi. Pada tampilan ini, pengguna harus terlebih dahulu memilih file audio yang telah terenkripsi untuk didekripsi kembali. Setelah memilih file, pengguna harus memasukkan kunci yang sama pada saat digunakan untuk mengenkripsi file audio tersebut. jika sudah memilih file dan memasukkan kunci, tahap selanjutnya ialah menekan tombol dekripsi untuk memulai proses dekripsi. Jika proses dekripsi selesai, hasil dari proses dekripsi akan ditampilkan dibagian lokasi file hasil dekripsi.

d. Rancangan Tampilan Tentang Aplikasi



Gambar 3.11 Rancangan Tampilan Tentang Aplikasi

Gambar diatas merupakan rancangan dari tampilan tentang aplikasi. Pada tampilan ini, pengguna akan melihat penjelasan dari aplikasi dan bagaimana menggunakannya untuk mengenkripsi atau mendekripsi file audio.

BAB IV

IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1 Implementasi Sistem

Bab ini akan menjelaskan hasil implementasi dalam membangun sistem enkripsi dan dekripsi audio menggunakan algoritma *blowfish*. Tahap ini akan menjelaskan apakah setiap proses dapat berjalan dengan baik dan mampu memberikan hasil yang diharapkan.

Pada bab ini, penulis akan menerangkan hasil dari sistem yang telah dibuat beserta fungsi-fungsi yang ada ditampilannya. Mulai dari proses pengambilan file sampai pada proses selesainya enkripsi dan dekripsi.

Seluruh proses perancangan di implementasikan ke software yang dibuat menggunakan *Microsoft Visual Studio 210 Ultimate*. Adapun alat yang digunakan untuk mengimplementasikan sistem enkripsi dan dekripsi file audio ini yaitu :

a. Laptop dengan *processor intel core i3, RAM 4GB, Harddisk 500GB, Mouse*.
b. Software Visual Studio 2010 Ultimate

4.2 Hasil Tampilan Sistem

Berikut merupakan hasil dari tampilan dari sistem yang telah berhasil dibuat, antara lain:

a. Tampilan Halaman Utama

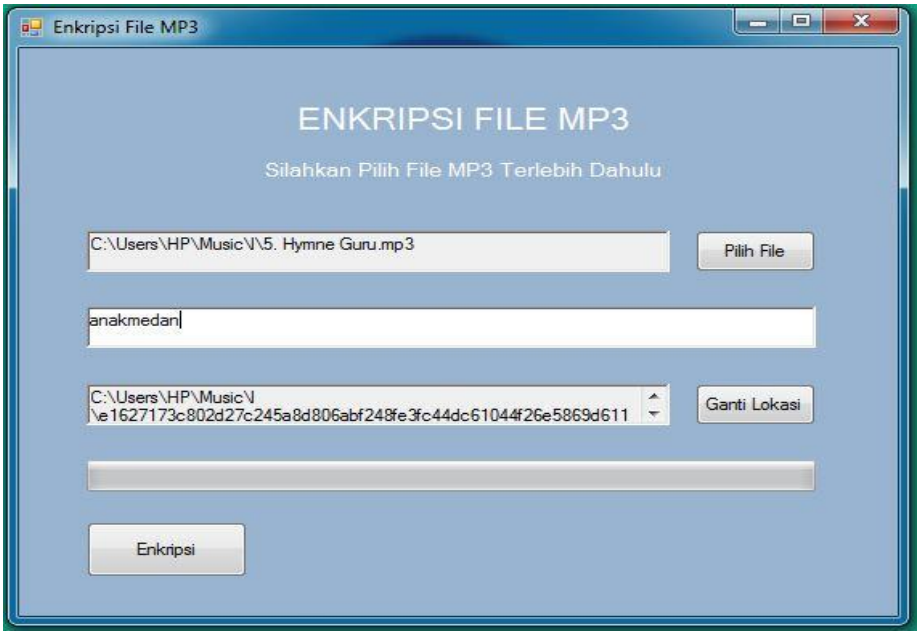
Gambar 4.1 Tampilan Halaman Utama

Gambar diatas merupakan tampilan awal dari sistem yang telah dibuat. Pada tampilan ini, pengguna dapat memilih tiga menu yang telah disediakan diantaranya yaitu menu enkripsi, dekripsi dan tentang aplikasi.

b. Tampilan Halaman Enkripsi

Gambar di bawah ini merupakan tampilan dari halaman enkripsi. Pada tampilan ini, pengguna dapat memulai proses enkripsi file audio dengan memilih file yang akan dienripsi terlebih dahulu. Untuk memilih file, pengguna dapat menekan tombol pilih file. Setelah pengguna berhasil memilih file, informasi lokasi file akan ditampilkan pada input lokasi file.

Setelah memilih file juga, sistem akan secara otomatis meng-*generate* lokasi file hasil enkripsi yang akan ditampilkan pada input lokasi hasil enkripsi. Pengguna juga dapat mengganti lokasi dari hasil file enkripsi. Tahap selanjutnya ialah memasukkan kunci yang akan digunakan untuk mengenkripsi file. Setelah semua form terisi, pengguna cukup menekan tombol enkripsi untuk memulai proses enkripsi file audio. Terdapat juga indikator progres yang akan memberitahu pengguna tentang berapa lama proses enkripsi akan selesai.

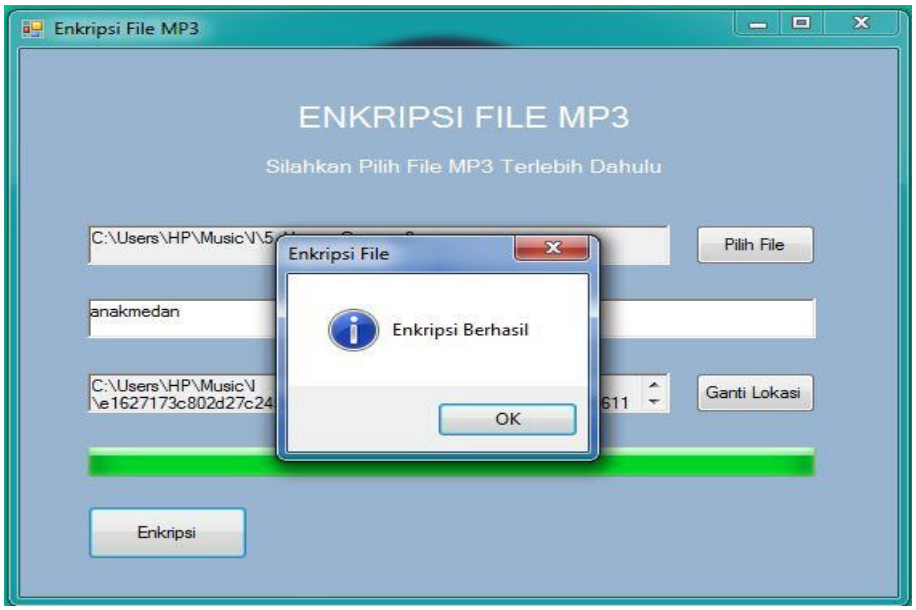


Gambar 4.2 Tampilan Menu Enkripsi

c. Tampilan Berhasil Proses Enkripsi

Gambar dibawah ini merupakan tampilan dari berhasilnya proses enkripsi. Jika proses enkripsi berhasil, maka sistem akan memunculkan popup enkripsi berhasil. Namun jika proses enkripsi gagal, maka sistem

akan menampilkan popup enkripsi gagal. Popup lain juga akan muncul jika pengguna tidak memasukkan kunci atau pengguna tidak memilih file audio yang akan dienkripsi.

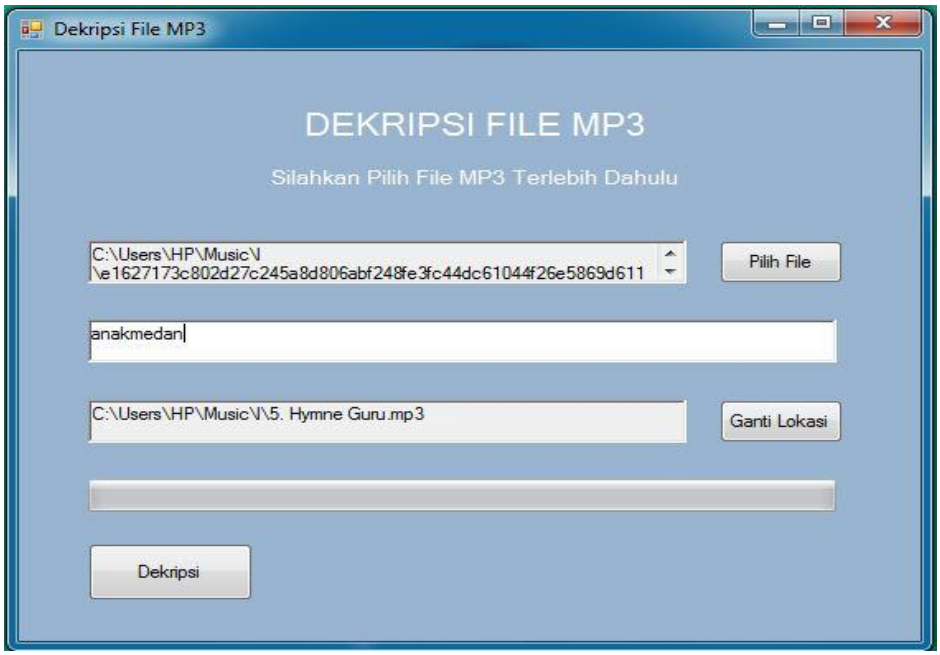


Gambar 4.3 Tampilan Berhasil Proses Enkripsi

d. Tampilan Halaman Dekripsi

Gambar dibawah ini merupakan tampilan dari halaman dekripsi. Pada tampilan ini, pengguna dapat mendekripsi file audio yang telah berhasil dienkripsi sebelumnya. Tahap awal dari proses enkripsi ini ialah pengguna terlebih dahulu memilih file audio yang telah berhasil dienkripsi sebelumnya dengan cara menekan tombol pilih file. Setelah pengguna memilih file tersebut, sistem akan secara otomatis mendekripsi nama file dari audio tersebut lalu menampilkan informasi lokasi file hasil dekripsinya ke input hasil lokasi dekripsi. Tahap selanjutnya ialah memasukkan kunci yang dipakai pada saat mengenkripsi file audio tersebut. setelah semua

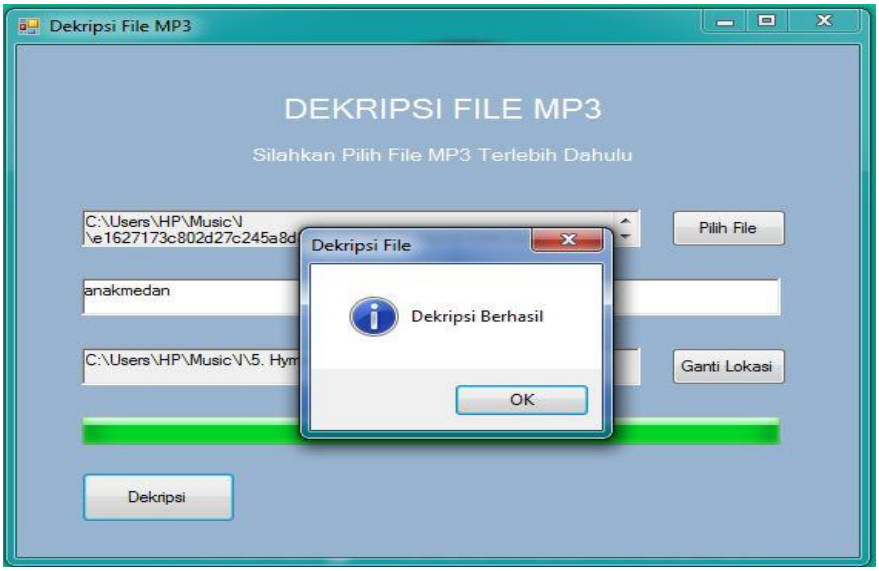
dimasukkan, pengguna dapat menekan tombol dekripsi untuk memulai proses dekripsi file audio.



Gambar 4.4 Tampilan Halaman Dekripsi

e. Tampilan Berhasil Dekripsi

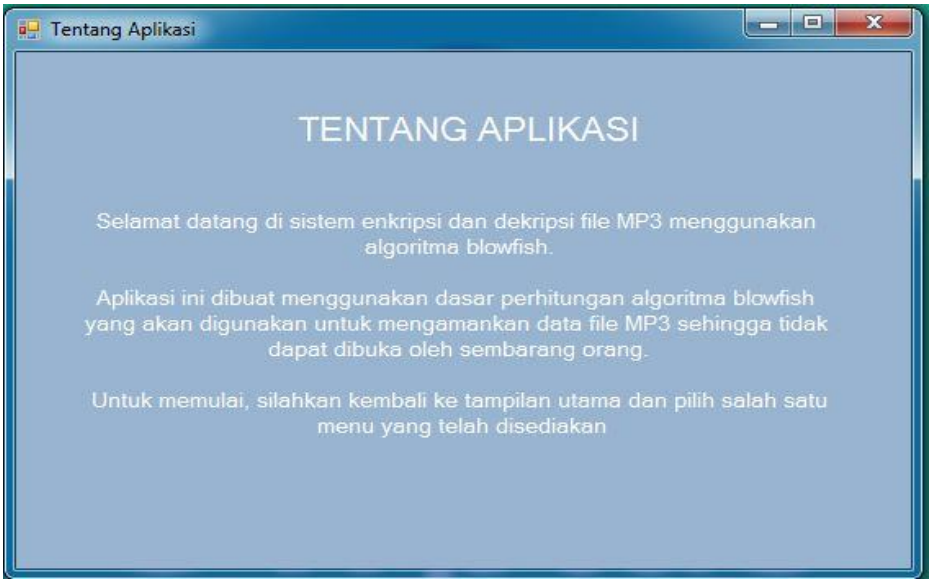
Gambar di bawah ini merupakan tampilan dari berhasilnya proses dekripsi file audio. Pada tampilan ini, pengguna dapat melihat popup yang menyatakan bahwa proses dekripsi file audio telah berhasil. Pengguna juga dapat melihat lokasi dari file audio yang telah berhasil didekripsi pada input lokasi dekripsi file.



Gambar 4.5 Tampilan Berhasil Dekripsi

f. Tampilan Halaman Tentang Aplikasi

Gambar di bawah ini adalah tampilan dari halaman tentang aplikasi. Pada tampilan ini, pengguna dapat melihat detail singkat tentang aplikasi sistem enkripsi dan dekripsi file audio menggunakan algoritma *blowfish*.



Gambar 4.6 Tampilan Tentang Aplikasi.

4.3 Pengujian Sistem

Tabel 4.1 Pengujian Sistem

No	Bulir Pengujian	*Output* yang diharapkan	*Output* yang keluar	Keterangan
1	Pilih File audio	Sistem dapat memilih file audio dari *file explorer*	Sistem berhasil memilih file audio dari *file explorer*	Sesuai
2	Enkripsi File audio	Sistem mampu mengenkripsi file audio sesuai dengan perhitungan algoritma *blowfish*	Sistem berhasil mengenkripsi file audio sesuai dengan perhitungan algoritma *blowfish*	Sesuai
3	Dekripsi file audio	Sistem dapat mendekripsi file audio dengan menggunakan perhitungan algoritma *blowfish*	Sistem berhasil mendekripsi file audio dengan menggunakan perhitungan algoritma *blowfish*	Sesuai
4	Deteksi kesalahan system	Sistem dapat mendeteksi kesalahan seperti pengguna tidak memasukkan kunci, file audio belum dipilih, kunci untuk proses dekripsi salah.	Sistem berhasil mendeteksi kesalahan seperti pengguna tidak memasukkan kunci, file audio belum dipilih, kunci untuk proses dekripsi salah.	Sesuai

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan uraian yang telah dipaparkan bab demi bab dari pengamatan penulis dalam pembuatan dan penyelesaian skripsi ini, maka dapat disimpulkan sebagai berikut:

1. Sistem enkripsi dan dekripsi file audio menggunakan algoritma *blowfish* merupakan aplikasi yang dapat membatu dalam pengamanan file audio sehingga file audio tersebut tidak dapat dibuka oleh para pencuri data.
2. Sitem enkripsi dan dekripsi file audio dengan mrnggunakan algoritma *blowfish* ini berbasis *VB.net* yang dapat diakses secara *offline.*
3. Algoritma *Blowfish* atau "*OpenPGP.Cipher.4*" merupakan enkripsi yang termasuk dalam golongan *Symetric Cryptosystem*, metode enkripsinya mirip dengan *DES* (*DES-like Cipher*).
4. Hasil dari proses enkripsi tidak hanya mengubah isi datanya saja melainkan juga mengubah ekstensi dari file audionya sehingga, file tersebut tidak dapat dibuka. Sedangkan proses dekripsi selain mengubah isi data ke bentuk semula, juga akan merubah ekstensi file ke bentuk semula sehingga file dapat dibuka kembali dan bisa didengarkan.

5.2 Saran

Berdasarkan kesimpulan yang telah dikemukakan diatas, penulis ingin memberikan saran sebagai berikut:

1. Untuk penggunaan program aplikasi yang membutuhkan data file yang cukup besar, disarankan untuk menggunakan perangkat keras atau *hardware* dengan spesifikasi yang lebih tinggi, terutama dalam hal *processor* dan *memory* komputer.
2. Perlu diperhatikan bahwa kunci atau *key* yang digunakan dalam proses enkripsi maupun dekripsi file data harus di ingat baik-baik agar data tersebut dapat dikembalikan seperti semula.
3. Proses enkripsi dan dekripsi dapat lebih dikembangkan lagi untuk file-file data bertipe lain sehingga penggunaannya dapat lebih luas.
4. Proses enkripsi dan dekripsi dapat dibuat lebih efisien baik dalam penggunaan variabel, tipe data maupun yang lainnya sehingga penggunaan *resource* dapat lebih dimaksimalkan.
5. Menambah fitur-fitur lain sehingga program aplikasi lebih bersifat fungsional dan dapat lebih bermanfaat.

DAFTAR PUSTAKA

A.S, Rosa dan Shalahuddin M, (2013). *Rekayasa Peragkat Lunak*. Bandung : Informatika.

A.S, Rosa dan Shalahuddin M, 2014. *Modul Pembelajaran Rekayasa Perangkat Lunak* (*Terstruktur dan Berorientasi Objek*), Modula : Bandung.

Basri.2016. "Kriptografi Simetris Dan Asimetris Dalam Perspektif Keamanan Data Dan Kompleksitas Komputasi." Jurnal Ilmiah Ilmu Komputer, vol. 2. no. 2, 17 – 23.

Dony Ariyus, Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi. Yogyakarta: ANDI, 2008.

Erika, Winda, Heni Rachmawati, and Ibnu Surya. "Enkripsi Teks Surat Elektronik (E-Mail) Berbasis Algoritma Rivest Shamir Adleman (RSA)." *Jurnal Aksara Komputer Terapan* 1.2 (2012).

Gellinas, U. J., Dull, R.B (2012) . *Accounting information systems*, 9th ed. USA: South-Western Cengage Learning.

Hartanto, S. (2017). Implementasi fuzzy rule based system untuk klasifikasi buah mangga. *TECHSI-Jurnal Teknik Informatika*, *9*(2), 103-122

Harumy, T. H. F., & Sulistianingsih, I. (2016). Sistem penunjang keputusan penentuan jabatan manager menggunakan metode mfep pada cv. Sapo durin. In *Seminar Nasional Teknologi Informasi dan Multimedia* (pp. 6-7).

Herdianto, H. (2018). Perancangan Smart Home dengan Konsep Internet of Things (IoT) Berbasis Smartphone. Jurnal Ilmiah Core IT: Community Research Information Technology, 6(2).

Lawrence A. Gordon, Martin P. Loeb, William Lucyshyn, and Robert Richardson, CSI/FBI Computer Crime And Security Survey.: Computer Security Institute, 2005.

Ladjamudin, Al-Bahra Bin. 2013. *Analisis dan Desain Sistem Informasi*. Yogyakarta : Graha Ilmu.

Manku, Saikumar and Vasanth,K. 2015. "Blowfish Encryption Algorithm For Information Security." ARPN Journal of Engineering and Applied Sciences, vol. 10. no. 10, 4717 – 4719.

Muttaqin, muhammad. "analisa pemanfaatan sistem informasi e-office pada universitas pembangunan panca budi medan dengan menggunakan metode utaut." *jurnal teknik dan informatika* 5.1 (2018): 40-43.

Putri, R. E., & Siahaan, A. (2017). Examination of document similarity using Rabin-Karp algorithm. *International Journal of Recent Trends in Engineering & Research*, *3*(8), 196- 201.

Perwitasari, I. D. (2018). Teknik Marker Based Tracking Augmented Reality untuk Visualisasi Anatomi Organ Tubuh Manusia Berbasis Android. *INTECOMS:Journal of Information Technology and Computer Science*, *1*(1), 8-18.

Rahman Chumaidi, "Studi dan Implementasi Algoritma Blowfish Untuk Enkripsi Email," Institut Teknologi Sepuluh Nopember, Surabaya, Makalah Tugas Akhir 2009.

Romney, M.B., Steinbart, P. J. (2015). *Accounting information systems*, 13th edition. UK: *Pearson Educated Limited*.

Rizal, Chairul. "Pengaruh Varietas dan Pupuk Petroganik Terhadap Pertumbuhan, Produksi dan Viabilitas Benih Jagung (Zea mays L.)." ETD Unsyiah (2013).

Ramadhani, S., Suherman, S., Melvasari, M., & Herdianto, H. (2018). Perancangan Teks Berjalan Online Sebagai Media Informasi Nelayan. *Jurnal Ilmiah Core IT: Community Research Information Technology*, *6*(2).

Sidik, A. P. (2018). Algoritma RSA dan Elgamal sebagai Algoritma Tambahan untuk Mengatasi Kelemahan Algoritma One Time Pad pada Skema Three Pass Protocol.

Suriski Sitinjak, Yuli Fauziah, and Juwairiah, "Aplikasi Kriptografi File Menggunakan Algoritma Blowfish," in Seminar Nasional Informatika 2010 (semnasIF 2010), Yogyakarta, 2010, pp. C-85.