IMPLEMENTASI KEAMANAN DALAM MELINDUNGI FILE AUDIO DENGAN MENGGUNAKAN *LEFT SHIFTING* PADA STREAM *CIPHER*

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	:	**ARIANSYAH**
NPM	:	**1514370146**
PROGRAM STUDI	:	**SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2021

LEMBAR PENGESAHAN

IMPLEMENTASI KEAMANAN DALAM MELINDUNGI FILE AUDIO DENGAN MENGGUNAKAN *LEFT SHIFTING* PADA STREAM *CIPHER*

Disusun Oleh:

NAMA	**: ARIANSYAH**
NPM	**: 1514370146**
PROGRAM STUDI	**: SISTEM KOMPUTER**

Skripsi Telah Disetujui oleh Dosen Pembimbing Skripsi
Pada Tanggal : 24 Maret 2021

Dosen Pembimbing I	Dosen Pembimbing II
Herdianto, S.Kom., M.T.	Heri Kurniawan, S.Kom., M.Kom.

Mengetahui:

Dekan Fakultas Sains dan Teknologi	Ketua Program Studi Sistem Komputer
Hamdani, S.T., M.T.	Eko Hariyanto, S.Kom., M.Kom.

SURAT PERNYATAAN

ang Bertanda Tangan Dibawah Ini :

	:	ARIANSYAH
M	:	1514370146
at/Tgl.	:	BINJAI / 12/10/1996
at	:	jl. Flores lk. 2 kel. Kebun Lada Kec. Binjai Utara Kota Binjai
P	:	082240739633
Orang Tua	:	RAHMAD TIKA/SONDANG SITORUS
tas	:	SAINS & TEKNOLOGI
am Studi	:	Sistem Komputer
	:	Implementasi Keamanan Dalam Melindungi File Audio Dengan Menggunakan Left Shifting Pada Stream Cipher

na dengan surat ini menyatakan dengan sebenar - benarnya bahwa data yang tertera diatas adalah sudah benar sesuai n ijazah pada pendidikan terakhir yang saya jalani. Maka dengan ini saya tidak akan melakukan penuntutan kepada UNPAB. a ada kesalahan data pada ijazah saya.

anlah surat pernyataan ini saya buat dengan sebenar - benarnya, tanpa ada paksaan dari pihak manapun dan dibuat dalam an sadar. Jika terjadi kesalahan, Maka saya bersedia bertanggung jawab atas kelalaian saya.

Medan, 25 November 2020
Membuat Pernyataan

METERAI TEMPEL
E9AHF793558184
6000
ENAM RIBU RUPIAH

ARIANSYAH
1514370146

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

PERMOHONAN JUDUL TESIS / SKRIPSI / TUGAS AKHIR*

yang bertanda tangan di bawah ini :

a Lengkap	: ARIANSYAH
pat/Tgl. Lahir	: BINJAI / 12 Oktober 1996
or Pokok Mahasiswa	: 1514370146
ram Studi	: Sistem Komputer
entrasi	: Keamanan Jaringan Komputer
ah Kredit yang telah dicapai	: 143 SKS, IPK 3.27
or Hp	: 082240739633

an ini mengajukan judul sesuai bidang ilmu sebagai berikut :

Judul
Implementasi Keamanan Dalam Melindungi File Audio Dengan Menggunakan Left Shifting Pada Stream Cipher

: Diisi Oleh Dosen Jika Ada Perubahan Judul

Yang Tidak Perlu

Medan, 05 Desember 2020

Rektor I,

(Cahyo Pramono, S.E., M.M.)

Pemohon,

(Ariansyah)

Tanggal : .....
Disahkan oleh :
Dekan

(Hamdani, ST., MT.)

Tanggal : 22 Juni 2021
Disetujui oleh :
Dosen Pembimbing I :

(Herdianto, S.Kom., MT)

Tanggal : .....
Disetujui oleh:
Ka. Prodi Sistem Komputer

(Eko Hariyanto, S.Kom, M.Kom)

Tanggal : 22 Juni 2021
Disetujui oleh:
Dosen Pembimbing II:

(Heri Kurniawan, S.Kom, M.Kom)

SURAT KETERANGAN PLAGIAT CHECKER

Dengan ini saya Ka.LPMU UNPAB menerangkan bahwa saurat ini adalah bukti pengesahan dari LPMU sebagi pengesah proses plagiat checker Tugas Akhir/ Skripsi/Tesis selama masa pandemi ***Covid-19*** sesuai dengan edaran rektor Nomor : 7594/13/R/2020 Tentang Pemberitahuan Perpanjangan PBM Online.

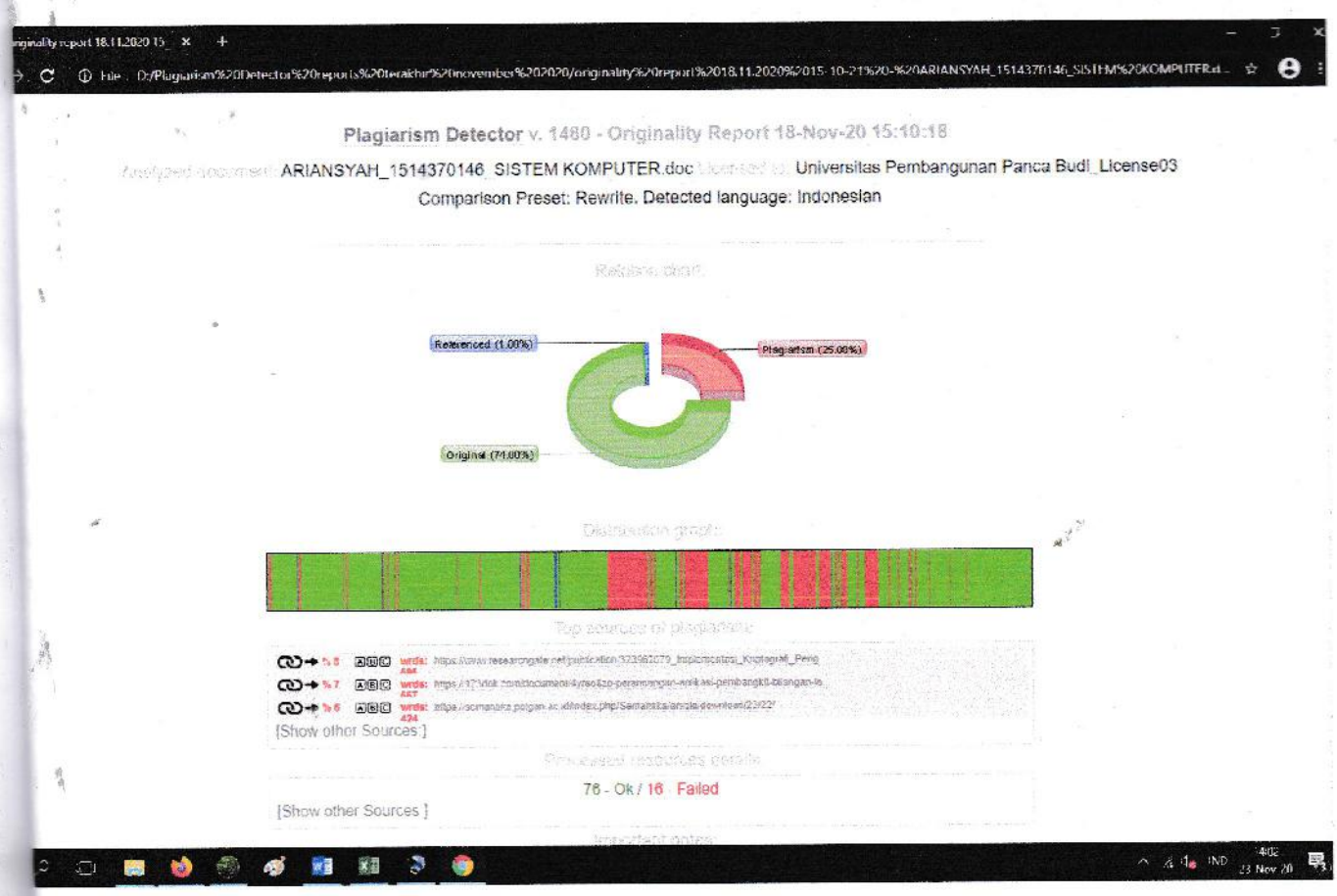
Demikian disampaikan.

NB: Segala penyalahgunaan/pelanggaran atas surat ini akan di proses sesuai ketentuan yang berlaku UNPAB.

Ka.LPMU

Hasmi Muharram Ritonga, BA., MSc

No. Dokumen : PM-UJMA-06-02	Revisi	: 00	Tgl Eff	: 23 Jan 2019


Plagiarism Detector v. 1480 - Originality Report 18-Nov-20 15:10:18
ARIANSYAH_1514370146_SISTEM KOMPUTER.doc
Universitas Pembangunan Panca Budi_License03
Comparison Preset: Rewrite. Detected language: Indonesian
Referenced (1.00%)
Plagiarism (25.00%)
Original (74.00%)
[Show other Sources]
76 - Ok / 16 - Failed
[Show other Sources]

YAYASAN PROF. DR. H. KADIRUN YAHYA

UNIVERSITAS PEMBANGUNAN PANCA BUDI

JL. Jend. Gatot Subroto KM 4,5 PO. BOX 1099 Telp. 061-30106057 Fax. (061) 4514808
MEDAN - INDONESIA
Website : www.pancabudi.ac.id - Email : admin@pancabudi.ac.id

LEMBAR BUKTI BIMBINGAN SKRIPSI

ama Mahasiswa	:	ARIANSYAH
PM	:	1514370146
rogram Studi	:	Sistem Komputer
enjang endidikan	:	Strata Satu
osen Pembimbing	:	Herdianto, S.Kom., MT
udul Skripsi	:	Implementasi Keamanan Dalam Melindungi File Audio Dengan Menggunakan Left Shifting Pada Stream Cipher

Tanggal	Pembahasan Materi	Status	Keterangan
09 Juni 2020	Teks yang dimerahkan perlu untuk dilakukan perbaiki.	Revisi	
2 Juli 2020	Harap dijadikan satu file bab 1 - 5	Revisi	
2 Juli 2020	harap diperbaiki bab 1-5	Revisi	
6 Agustus 2020	ACC seminar Hasil	Revisi	
4 Oktober 2020	Acc sidang meja hijau	Disetujui	
24 Maret 2021	ACC sidang meja hijau	Disetujui	

Medan, 31 Mei 2021
Dosen Pembimbing,

Herdianto, S.Kom., MT

YAYASAN PROF. DR. H. KADIRUN YAHYA

UNIVERSITAS PEMBANGUNAN PANCA BUDI

JL. Jend. Gatot Subroto KM 4,5 PO. BOX 1099 Telp. 061-30106057 Fax. (061) 4514808
MEDAN - INDONESIA
Website : www.pancabudi.ac.id - Email : admin@pancabudi.ac.id

LEMBAR BUKTI BIMBINGAN SKRIPSI

ama Mahasiswa	:	**ARIANSYAH**
PM	:	**1514370146**
rogram Studi	:	**Sistem Komputer**
enjang endidikan	:	**Strata Satu**
osen Pembimbing	:	**Heri Kurniawan, S.Kom., M.Kom**
udul Skripsi	:	**Implementasi Keamanan Dalam Melindungi File Audio Dengan Menggunakan Left Shifting Pada Stream Cipher**

Tanggal	Pembahasan Materi	Status	Keterangan
05 Juni 2020	Periksa lg penulisan bahasa asing	Revisi	
18 Juni 2020	Cek file	Revisi	
30 Juni 2020	Perbaiki penulisan table, judul table pada baris kedua harus dibuat	Revisi	
Juli 2020	Perbaiki format penulisan table	Revisi	
3 Agustus 2020	Acc seminar hasil	Disetujui	
6 Oktober 2020	Acc sidang	Disetujui	
29 Maret 2021	Acc jilid	Disetujui	

Medan, 31 Mei 2021
Dosen Pembimbing,

Heri Kurniawan, S.Kom., M.Kom

YAYASAN PROF. DR. H. KADIRUN YAHYA
PERPUSTAKAAN UNIVERSITAS PEMBANGUNAN PANCA BUDI
Jl. Jend. Gatot Subroto KM. 4,5 Medan Sunggal, Kota Medan Kode Pos 20122

SURAT BEBAS PUSTAKA
NOMOR: 3345/PERP/BP/2020

Perpustakaan Universitas Pembangunan Panca Budi menerangkan bahwa berdasarkan data pengguna perpustakaan
ma saudara/i:

: ARIANSYAH
: 1514370146
/Semester : Akhir
s : SAINS & TEKNOLOGI
n/Prodi : Sistem Komputer

annya terhitung sejak tanggal 07 Desember 2020, dinyatakan tidak memiliki tanggungan dan atau pinjaman buku
s tidak lagi terdaftar sebagai anggota Perpustakaan Universitas Pembangunan Panca Budi Medan.

Medan, 07 Desember 2020
Diketahui oleh,
Kepala Perpustakaan,

Sugiarjo, S.Sos., S.Pd.I

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
Nomor. 1039/BL/LAKO/2020

ertanda tangan dibawah ini Ka. Laboratorium Komputer dengan ini menerangkan bahwa :

	: ARIANSYAH
I.	: 1514370146
at/Semester	: Akhir
tas	: SAINS & TEKNOLOGI
an/Prodi	: Sistem Komputer

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

Medan, 07 Desember 2020
Ka. Laboratorium

Fachrid Wadly, S. Kom., M.Kom.

kumen : FM-LAKO-06-01	Revisi : 01	Tgl. Efektif : 04 Juni 2015

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau

Medan, 07 Desember 2020
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	: ARIANSYAH
Tempat/Tgl. Lahir	: BINJAI / 12/10/1996
Nama Orang Tua	: RAHMAD TIKA
N. P. M	: 1514370146
Fakultas	: SAINS & TEKNOLOGI
Program Studi	: Sistem Komputer
No. HP	: 082240739633
Alamat	: jl. Flores lk. 2 kel. Kebun Lada Kec. Binjai Utara Kota Binjai

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **Implementasi Keamanan Dalam Melindungi File Audio Dengan Menggunakan Left Shifting Pada Stream Cipher**, 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 transkripnya 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.	0
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.**	**1,605,000**

Ukuran Toga : L

Hormat saya

ketahui/Disetujui oleh :

ndani, ST., MT.
kan Fakultas SAINS & TEKNOLOGI

ARIANSYAH
1514370146

tan :

- 1.Surat permohonan ini sah dan berlaku bila :

siswa.pancabudi.ac.id/ta/mohonmejahijau

PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa dalam skripsi ini tidak terdapat karya yang pernah di ajukan untuk memperoleh gelar kesarjanaan disuatu perguruan tinggi, dan sepanjang pengetahauan saya juga tidak terdapat karya atau pendapat yang pernah di tullis oleh orang lain, kecuali yang secara tertulis diacu dalam skripsi ini dan di sebutkan dalam daftar pustaka.

Medan, 31 Juli 2021

(ARIANSYAH)

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

NAMA	: ARIANSYAH
NPM	: 1514370146
Fakultas / program studi	: SAINS DAN TEKNOLOGI / SISTEM KOMPUTER
Judul Skripsi	: IMPLEMENTASI KEAMANAN DALAM MELINDUNGI FILE AUDIO DENGAN MENGGUNAKAN LEFT SHIFTING PADA STREAMCIPHER

Dengan ini menyatakan bahwa :

1. Skripsi ini merupakan hasil karya tulis saya sendiri dan bukan merupakan hasil karya orang lain.
2. Memberi ijin hak bebas royaliti Non-Eksklusif kepada UNPAB untuk menyimpan, mengalih-media/formatkan mengelola, mendistribusikan, dan mempublikasikan karya skripsinya melalui internet atau media lain bagi kepentingan akademis.

Demikian surat pernyataan ini saya perbuat dengan penuh tanggung jawab dan saya bersedia menerima sanksi dan konsekuensi apapun sesuai dengan aturan yang berlaku apabila di kemudian hari di ketahaui terbukti bahwa pernyataaan ini tidak benar.

Medan, 31 Juli 2021

(ARIANSYAH)

ABSTRAK

ARIANSYAH

Implementasi Keamanan Dalam Melindungi File Audio Dengan Menggunakan *Left Shifting* Pada Stream *Cipher*

2021

File merupakan suatu berkas yang dapat menyimpan data-data pribadi atau umum. File audio merupakan salah satu jenis file yang dapat menyimpan rekaman suara dari percakapan pribadi, kegiatan atau perusahaan. File audio sering digunakan dalam menyimpan bukti-bukti autentik yang bersifat sangat rahasia. File audio yang menyimpan informasi rahasia tidak boleh jatuh ke tangan orang yang tidak bertanggung jawab tanpa seizin pemiliknya. Tetapi, ada kalanya file tersebut berhasil curi. Teknik kriptografi sangat penting disematkan dalam usaha penyandian file audio agar tidak dapat dicuri. Teknik *Left Shifting* atau pergeseran bit dapat membantu melakukan proses enkripsi pada file audio sehingga file tersebut aman dari pencurian. File audio akan dienkrip dengan menggunakan kunci yang ditentukan. File audio yang sudah mengalami proses *Left Shifting* akan terjamin kerahasiaannya.

Kata Kunci: algoritma, dekripsi, enkripsi, kriptografi, *Left Shifting*

DAFTAR ISI

KATA PENGANTAR

Puji syukur ke hadirat Allah SWT karena dengan anugerah dan hidayah-Nya penulis masih diberikan kesempatan untuk menyelesaikan skripsi ini dapat diselesaikan dengan baik dan sebagaimana mestinya. Skripsi ini berjudul " **IMPLEMENTASI KEAMANAN DALAM MELINDUNGI FILE AUDIO DENGAN MENGGUNAKAN *LEFT SHIFTING* PADA STREAM *CIPHER***". Penulis mengucapkan banyak terima kasih kepada banyak pihak yang telah membantu dalam penyelesaian penyusunan skripsi ini. Penulis ingin mengucapkan terima kasih kepada:

1. Orang tua saya yang telah mendukung saya untuk menyelesaikan skripsi ini.
2. Bapak Dr. H. Muhammad Isa Indrawan, S.E., M.M., selaku Rektor Universitas Pembangunanan Panca Budi, Medan.
3. Bapak Ir. Bhakti Alamsyah, M.T, Ph.D., selaku Rektor I, Universitas Pembangunan Panca Budi, Medan
4. Bapak Hamdani, S.T., M.T., selaku Dekan Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi, Medan.
5. Bapak Eko Hariyanto, S.Kom., M.Kom., selaku Ketua Program Studi Sistem Komputer Universitas Pembangunan Panca Budi, Medan.
6. Bapak Herdianto, S.Kom., M.T., selaku Dosen Pembimbing I yang telah memberikan arahan dan membimbing dalam penyelesaian skripsi ini.
7. Bapak Heri Kurniawan, S.Kom., M.Kom., selaku Dosen Pembimbing II yang telah memberikan koreksi terhadap tata tulis untuk penyelesaian skripsi ini.
8. Dosen-dosen pada Program Studi Sistem Komputer Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi, Medan.
9. Seluruh staff dan karyawan pada Universitas Pembangunan Panca Budi, Medan.
10. Teman-teman penulis dari program studi Sistem Komputer Fakultas Sains dan Teknologi, Universitas Pembangunan Panca Budi, Medan

Penulis juga menyadari bahwa penyusunan skripsi ini belum sempurna baik dalam penulisan maupun isi disebabkan keterbatasan kemampuan penulis. Oleh karena itu, penulis mengharapkan kritik dan saran yang sifatnya membangun dari pembaca untuk kesempurnaan isi skripsi ini.

Medan, 24 Maret 2021
Penulis

Ariansyah
1514370146

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

File audio memiliki beberapa format, namun saat ini file audio yang popular dan banyak di gunakan adalah file audio yang berformat mp3, Karena ukurannya yang kecil dan memiliki kualitas suara yang cukup bagus. Dan saat Kemajuan Teknologi informasi juga turut menjadi salah satu faktor kenapa Mp3 banyak di gunakan masyarakat, Permasalahan yang ada pada perangkat lunak yang di bangun untuk menjalankan *file audio* hanya dengan format Mp3, Agar dapat mengirim secara daring melaui internet.

Upaya yang di lakukan agar *file audio* dapat berbentuk format Mp3 agar dapat di kirim melalui daring secara internet harus menggunakan perangkat keras terlebih dahulu yaitu menggunakan flash disk, harddisk atau komputer secara langsung, melainkan melalui jaringan internet, sehingga keamanan data sangat dibutuhkan pada saat pengiriman file tersebut. Karena file yang harus dikirim melalui jaringan internet, keamanan informasi tersebut akan rentan terhadap pencurian dan penyalahgunaan data. Perkembangan teknologi media elektronik mengizinkan banyak pihak yang tidak bertanggung jawab berusaha mencari cara dan kelemahan sistem untuk mencuri informasi. Hasil pencurian tersebut dapat digunakan untuk hal-hal yang hanya menguntung satu belah pihak saja.

Program aplikasi dibutuhkan dalam mengaplikasikan teknik ini agar dapat memberikan keamanan pada file audio. Aplikasi akan dibuat dengan

menggunakan bahasa pemrograman Microsoft Visual Basic.Net 2010. Dengan terciptanya aplikasi, diharapkan file audio yang akan dikirim akan terjamin kerahasiaannya. Berdasarkan permasalahan yang sudah diungkapkan sebelumnya, maka penulis mencoba untuk memilih judul "**IMPLEMENTASI KEAMANAN DALAM MELINDUNGI FILE AUDIO DENGAN MENGGUNAKAN *LEFT SHIFTING* PADA STREAM *CIPHER***".

1.2 Rumusan Masalah

Bedasarkan latar belakang masalah yang telah di uraikan di atas maka rumusan masalah pada penelitian ini adalah sebagai berikut:

1. Bagaimana melakukan proses enkripsi dan dekripsi file audio dengan menggunakan *Left Shifting*?
2. Bagaimana tingkat keberhasilan ini dalam meng enkripsi file audio?

1.3 Batasan Masalah

Adapun batasan masalah yang digunakan dalam penulisan Skripsi ini adalah sebagai berikut:

1. File yang diproses adalah file audio berekstensi *.mp3
2. Teknik *Left Shifting* digunakan pada proses dekripsi dengan menggeser karakter ke arah kiri sebanyak kunci.
3. Proses enkripsi menggunakan arah kanan yaitu arah yang berlawanan dari proses dekripsi

4. Bahasa pemrograman yang digunakan adalah Microsoft Visual Basic.Net 2010.
5. Program aplikasi adalah berbasis desktop dan tidak online.

1.4 Tujuan Penelitian

Adapun tujuan penelitian yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut:

1. Untuk merancang proses enkripsi dan dekrips *file audio* dengan menggunakan *Left Shifting*.
2. Untuk mengetahui seberapa besar metode *left shifting* ini dalam mengamankan *file audio*

1.5 Manfaat Penelitian

Adapun manfaat penelitian yang digunakan dalam penulisan Skripsi ini adalah sebagai berikut:

1. Dapat menambah pengetahuan peraktis tentang *file audio* dalam metode ini.
2. Setelah adanya penelitian ini nantinya dapat digunakan sebagai referensi bagi mahasiswa yang ingin menggunakan metode ini.
3. Memberikan pemahaman tentang teknik *Left Shiftin*

BAB II

LANDASAN TEORI

2.1 Pencurian Data

Pencurian data adalah istilah yang digunakan untuk menggambarkan ketika informasi disalin atau diambil secara ilegal dari bisnis atau orang lain. Biasanya, informasi ini adalah informasi pengguna seperti kata sandi, nomor jaminan sosial, informasi kartu kredit, informasi pribadi lainnya, atau informasi rahasia perusahaan lainnya. Karena informasi ini diperoleh secara ilegal, ketika orang yang mencuri informasi ini ditangkap, ia akan dituntut secara hukum sepenuhnya (Yakub, 2012).

Pencurian data adalah transfer ilegal atau penyimpanan informasi apa pun yang bersifat rahasia, pribadi, atau finansial, termasuk kata sandi, kode perangkat lunak, atau algoritme, informasi berorientasi proses, atau teknologi eksklusif. Dianggap sebagai pelanggaran keamanan dan privasi yang serius, konsekuensi dari pencurian data bisa sangat parah bagi individu dan bisnis.

Beberapa hal yang sering secara umum termasuk dalam pencurian data adalah sebagai berikut:

1. *Drive USB* - Menggunakan teknik mengisap jempol, informasi dapat dipindahkan ke thumb drive atau drive USB. Ini dianggap sebagai metode paling mudah pencurian data karena kapasitas penyimpanan perangkat USB meningkat seiring waktu dengan biaya yang menurun.

2. *Hard drive* - Informasi besar dapat ditransfer menggunakan hard drive portabel
3. Perangkat yang menggunakan kartu memori, *PDA* - *Slurping pod* dimungkinkan dengan perangkat yang menggunakan kartu memori dan *PDA*
4. *Email* - Cara populer lain untuk mengirimkan informasi adalah melalui email.
5. Mencetak - Metode lain yang digunakan dalam pencurian data adalah dengan mencetak informasi dan secara ilegal menyimpan atau mendistribusikannya.
6. Berbagi jarak jauh - Menggunakan akses jarak jauh, data dapat ditransfer ke lokasi lain dari mana data dapat didistribusikan.
7. Serangan *malware* - Serangan malware berpotensi mengekstraksi informasi sensitif.

Ada beberapa hal yang dapat dilakukan agara pencurian data dapat dicegah, antara lain:

1. Enkripsi informasi rahasia atau informasi pribadi.
2. Sistem manajemen data memiliki langkah-langkah keamanan yang diperlukan untuk memastikan file perusahaan tidak dipindahkan atau diakses secara ilegal.
3. Tinjauan berkala pada perangkat dan sistem yang dapat menimbulkan risiko tinggi.

4. Penggunaan jaringan terbatas dalam suatu organisasi.
5. Penggunaan terbatas perangkat yang dapat menyimpan data.
6. Penguncian laptop dan langkah-langkah keamanan biometrik.
7. Melindungi informasi rahasia dan pribadi menggunakan kata sandi.
8. Penggunaan perangkat lunak anti-malware.

Pencurian data adalah tindakan mencuri informasi digital yang disimpan di komputer, server, atau perangkat elektronik dari korban yang tidak dikenal dengan maksud untuk membahayakan privasi atau mendapatkan informasi rahasia. Informasi dapat mencakup apa saja dari informasi keuangan, seperti nomor kartu kredit atau rekening bank, hingga informasi pribadi, seperti nomor jaminan sosial, nomor SIM, dan catatan kesehatan. Setelah hanya masalah bisnis besar dan organisasi, pencurian data adalah masalah yang berkembang untuk pengguna komputer sehari-hari (Stallings, 2013).

File audio adalah salah satu file penting yang dapat disalahgunakan. File audio merupakan file hasil rekaman kegiatan atau rekaman pribadi dimana hanya pemilik file tersebut yang boleh mendengar isi percakapan atau isi rekaman yang terkandung pada file tersebut. Sistem keamanan sangat diperlukan dalam menjaga kandungan informasi dari file audio terlebih-lebih pada saat file audio akan dikirimkan melalui jaringan internet. Salah satu cara adalah melakukan penyandian terhadap file audio tersebut sehingga file tersebut tidak dapat lagi didengar oleh orang-orang yang tidak memiliki izin terhadap file tersebut.

Penyandian file sangat penting digunakan pada file audio untuk tetap menjaga kerahasiaan audio. Hal ini bertujuan agar audio hanya dapat didengar oleh penerima pesan saja. Untuk melakukan penyandian file, dibutuhkan teknik kriptografi. Kriptografi stream *Cipher* adalah salah satu metode penyandian yang dapat digunakan. Teknik *Left Shifting* atau pergeseran bit adalah salah satu teknik yang dapat digunakan dalam melakukan penyandian file audio. Teknik ini bekerja dengan cara memutar atau penggeser posisi bit dari *Plaintext* sesuai dengan jumlah pergeseran yang sudah ditentukan. Teknik ini bekerja dengan cepat karena tidak membutuhkan perhitungan matematika yang rumit.

2.1.1 Bagaimana Pencurian Data Terjadi

Pencurian data terjadi melalui berbagai cara. Paling sering, itu terjadi karena seseorang meretas ke dalam sistem komputer untuk mencuri informasi sensitif, seperti kartu kredit atau informasi pribadi Anda, atau seorang karyawan di perusahaan yang salah menangani informasi tersebut. Dengan dunia yang semakin digital, ratusan bisnis dan organisasi yang berbeda menyimpan informasi pribadi Anda, seperti nomor jaminan sosial, alamat surat, tanggal lahir, dan informasi rekening bank Anda.

Bahkan dengan kemajuan teknologi baru, penjahat cyber dapat beradaptasi dan menemukan cara untuk meretas ke dalam sistem untuk mencuri data, terutama perusahaan ritel yang menampung informasi pembayaran. Sebagian besar perusahaan memiliki rencana pelanggaran data, tetapi banyak karyawan tidak tahu

mereka ada atau tidak yakin rencana itu akan berhasil. Sangat penting bahwa semua perusahaan yang menangani data sensitif mendidik dan melatih karyawan tentang cara menangani informasi sensitif.

2.1.2 Menghindari Pencurian Data

Pencurian data adalah masalah nyata dan dapat terjadi pada siapa saja. Meskipun tidak ada cara untuk sepenuhnya mencegah pencurian data, ada beberapa langkah yang dapat diambil hari ini untuk membatasi risiko kehilangan data, antara lain:

1. Bayar menggunakan uang tunai, bukan kartu kredit atau debit.
2. Gunakan kartu kredit atau debit dengan teknologi pin-and-chip.
3. Lindungi komputer Anda dari virus dan malware dengan menginstal, menggunakan, dan memperbarui perangkat lunak *antivirus* dan *anti-spyware* di semua komputer dan perangkat elektronik Anda.
4. Selalu perbarui semua sistem operasi dan program perangkat lunak dengan menginstal pembaruan keamanan, peramban web, sistem operasi, dan program perangkat lunak sesegera mungkin setelah tersedia.
5. Jangan buka surel yang meragukan atau lampiran surel karena bisa berupa surel *phising*.
6. Periksa secara teratur laporan kartu kredit Anda dan laporan kredit untuk biaya tidak sah dan jalur kredit baru.

7. Gunakan kata sandi yang kuat dan unik untuk semua situs web yang membutuhkan login. Ubah ini secara rutin, terutama jika kata sandi akun telah dikompromikan dalam pelanggaran data.
8. Gunakan hanya koneksi *Wi-Fi* yang aman.
9. Buang dokumen dengan benar yang berisi informasi sensitif melalui kertas penghancur kertas dan singkirkan semua data dari perangkat elektronik.
10. Amankan jaringan dan koneksi internet melalui firewall dan kata sandi aman.
11. Jika menjalankan bisnis yang menyimpan informasi sensitif, pastikan karyawan terlatih dalam menangani data dan karyawan memahami kebijakan perusahaan terkait dengan berbagi informasi sensitif.

2.2 Algoritma

Algoritma adalah seperangkat instruksi yang dirancang untuk melakukan tugas tertentu. Ini bisa berupa proses sederhana, seperti mengalikan dua angka, atau operasi yang rumit, seperti memutar file video terkompresi. Mesin pencari menggunakan algoritma kepemilikan untuk menampilkan hasil yang paling relevan dari indeks pencarian mereka untuk permintaan tertentu (Hidayat, 2012).

Dalam pemrograman komputer, algoritma sering dibuat sebagai fungsi. Fungsi-fungsi ini berfungsi sebagai program kecil yang dapat dirujuk oleh program yang lebih besar. Misalnya, aplikasi tampilan gambar dapat menyertakan pustaka fungsi yang masing-masing menggunakan algoritme khusus untuk membuat format file gambar yang berbeda. Program pengeditan gambar dapat

berisi algoritma yang dirancang untuk memproses data gambar. Contoh algoritma pemrosesan gambar termasuk pemangkasan, pengubahan ukuran, penajaman, pengaburan, reduksi mata merah, dan peningkatan warna (Firmansyah, 2012).

Dalam banyak kasus, ada beberapa cara untuk melakukan operasi tertentu dalam program perangkat lunak. Oleh karena itu, programmer biasanya berusaha membuat algoritma yang seefisien mungkin. Dengan menggunakan algoritma yang sangat efisien, pengembang dapat memastikan program mereka berjalan secepat mungkin dan menggunakan sumber daya sistem minimal. Tentu saja, tidak semua algoritma diciptakan dengan sempurna untuk pertama kalinya. Oleh karena itu, pengembang sering meningkatkan algoritme yang ada dan memasukkannya dalam pembaruan perangkat lunak di masa mendatang. Ketika Anda melihat versi baru dari program perangkat lunak yang telah "dioptimalkan" atau memiliki "kinerja lebih cepat," sebagian besar berarti versi baru mencakup algoritma yang lebih efisien (Edraw, 2019).

2.2.1 Definisi Algoritma

Sebagai metode yang efektif, suatu algoritma dapat diekspresikan dalam jumlah ruang dan waktu yang terbatas dan dalam bahasa formal yang terdefinisi dengan baik untuk menghitung suatu fungsi. Mulai dari keadaan awal dan input awal (mungkin kosong), instruksi menjelaskan perhitungan yang, ketika dijalankan, berlanjut melalui sejumlah terbatas dari negara berturut-turut yang terdefinisi dengan baik, akhirnya menghasilkan "output" dan berakhir pada kondisi akhir akhir (Sumandri, 2017). Transisi dari satu negara ke negara lain

tidak selalu bersifat deterministik; beberapa algoritma, yang dikenal sebagai algoritma acak, memasukkan input acak. Ada empat fitur utama dari algoritma dari definisi:

1. Algoritma bekerja untuk menghasilkan output tertentu.
2. Algoritma bekerja dengan saling terhubung dan berkelanjutan.
3. Algoritma adalah kumpulan dari perintah-perintah kecil untuk mencapai tujuan tertentu.
4. Hasil algoritma akan muncul ketika serangkaian proses sudah terlaksana dengan baik.

Pada prinsipnya, algoritma akan bekerja dengan cara yang masuk akal dan mengerjakan perintah-perintah untuk menghasilkan keluaran yang benar.

2.2.2 Jenis-Jenis Algoritma

Algoritme adalah serangkaian urutan instruksi atau tindakan yang berisi ruang terbatas atau urutan dan yang akan memberikan hasil untuk masalah tertentu dalam jumlah waktu terbatas. Ini adalah pendekatan logis dan matematis untuk memecahkan atau memecahkan masalah menggunakan metode apa pun yang mungkin. Ada banyak jenis algoritme tetapi jenis algoritme yang paling mendasar adalah:

1. Algoritma rekursif

   Ini memecahkan kasus dasar secara langsung dan kemudian berulang dengan input yang lebih sederhana atau lebih mudah setiap kali (Nilai dasar ditetapkan di awal yang diakhiri algoritma). Ini digunakan untuk memecahkan masalah yang dapat dipecah menjadi masalah yang lebih sederhana atau lebih kecil dari jenis yang sama.

2. Algoritma pemrograman dinamis

   Algoritma pemrograman dinamis (juga dikenal sebagai algoritma optimasi dinamis) mengingat hasil masa lalu dan menggunakannya untuk menemukan hasil baru berarti memecahkan masalah kompleks dengan memecahnya menjadi kumpulan subproblem yang lebih sederhana, kemudian menyelesaikan masing-masing subproblem tersebut hanya sekali, dan menyimpannya solusi mereka untuk digunakan di masa depan alih-alih menghitung ulang solusi mereka lagi.

3. Algoritma Backtracking

   Bagaimana kalau belajar mengulang menggunakan contoh katakanlah ada suatu masalah "MONK" dan akan dibagi menjadi empat masalah yang lebih kecil "M, R, A, A". Mungkin masalahnya solusi dari masalah ini tidak diterima sebagai solusi dari " MONK ". Faktanya, tidak tahu yang mana tergantung. Jadi algoritma akan memeriksa masing-masing dari untaian tersebut satu per satu sampai ditemukan solusi untuk "MONK". Jadi pada dasarnya algoritma berusaha memecahkan submasalah tetapi jika tidak mencapai solusi yang diinginkan akan membatalkan apa pun

yang telah dilakukan dan mulai dari awal lagi sampai menemukan solusinya.

4. Algoritma *Divide and Conquer*

   Membagi dan menaklukkan terdiri dari dua bagian, pertama-tama, membagi masalah menjadi sub-masalah yang lebih kecil dari jenis yang sama dan menyelesaikannya secara rekursif dan kemudian menggabungkannya untuk membentuk solusi dari masalah asli.

5. Algoritma *Greedy*

   Algoritma *Greedy* adalah algoritma yang memecahkan masalah dengan mengambil solusi optimal di tingkat lokal (tanpa memperhatikan konsekuensi apa pun) dengan harapan menemukan solusi optimal di tingkat global. Algoritma *Greedy* digunakan untuk menemukan solusi optimal tetapi tidak perlu bahwa akan menemukan solusi optimal dengan mengikuti algoritma ini. Seperti ada beberapa masalah di mana solusi optimal tidak ada (saat ini) ini disebut masalah *NP-complete.*

6. Algoritma *Brute Force*

   Algoritma *Brute Force* hanya mencoba semua kemungkinan sampai solusi yang memuaskan ditemukan. Jenis algoritma seperti itu juga digunakan untuk menemukan solusi optimal (terbaik) karena memeriksa semua solusi yang mungkin. Dan juga digunakan untuk menemukan solusi yang memuaskan (bukan yang terbaik), cukup berhenti segera setelah solusi untuk masalah ditemukan.

7. Algoritma acak

   Algoritma acak menggunakan nomor acak setidaknya sekali selama perhitungan untuk membuat keputusan.

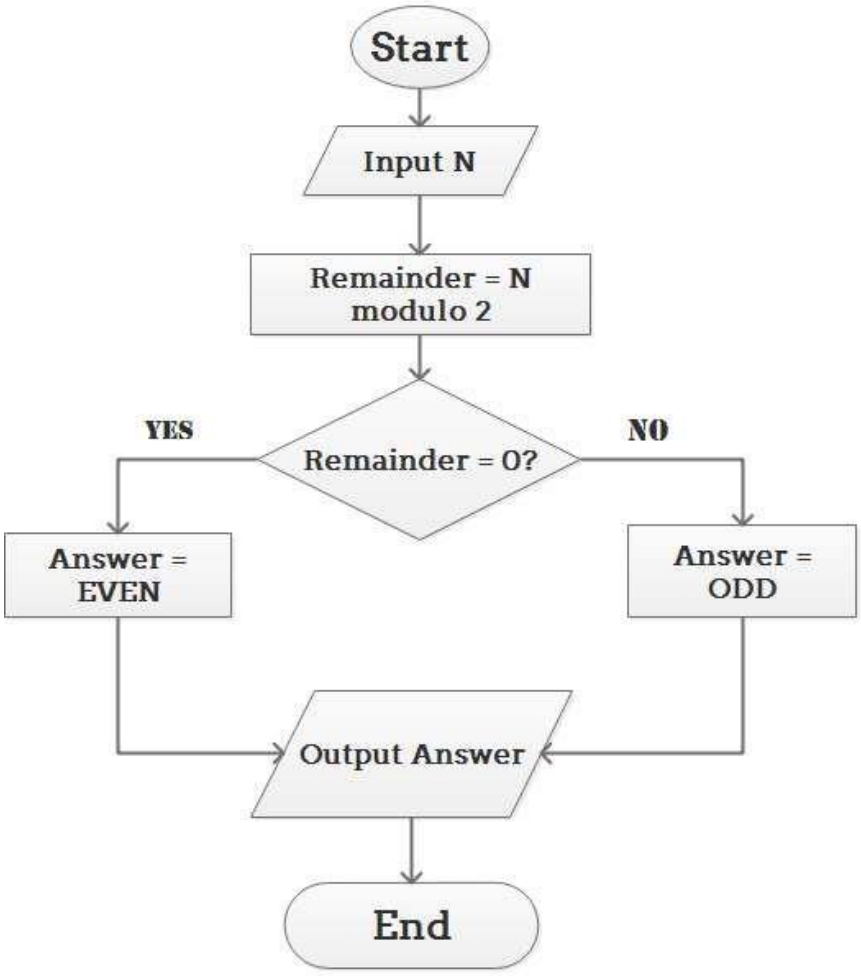
2.2.3 Analisis Kompleksitas Algoritma

Analisis suatu algoritma mengacu pada proses memperoleh estimasi untuk waktu dan ruang yang dibutuhkan untuk menjalankan algoritma. Penting untuk memperkirakan waktu (mis., Jumlah langkah) dan ruang (mis., Jumlah variabel) yang dibutuhkan oleh algoritma. Mengetahui waktu dan ruang yang dibutuhkan oleh algoritma memungkinkan kita untuk membandingkan algoritma yang memecahkan masalah yang sama. Sebagai contoh, jika satu algoritma mengambil n langkah untuk menyelesaikan masalah dan algoritma lainnya mengambil n ^ 2 langkah untuk memecahkan masalah yang sama, kami lebih suka algoritma pertama. Estimasi waktu dan ruang yang diperlukan untuk menjalankan algoritma ini disebut kompleksitas waktu dan ruang dari algoritma.

Waktu yang diperlukan untuk menjalankan suatu algoritma adalah fungsi dari input. Alih-alih berurusan langsung dengan input, parameter digunakan untuk mengkarakterisasi ukuran input. misalnya jika input adalah himpunan yang berisi n elemen, ukuran input n. Ada tiga kasus yang perlu dicatat tentang kompleksitas waktu suatu algoritma karena menentukan kompleksitas waktu yang tepat dari suatu algoritma dalam tugas yang sulit.

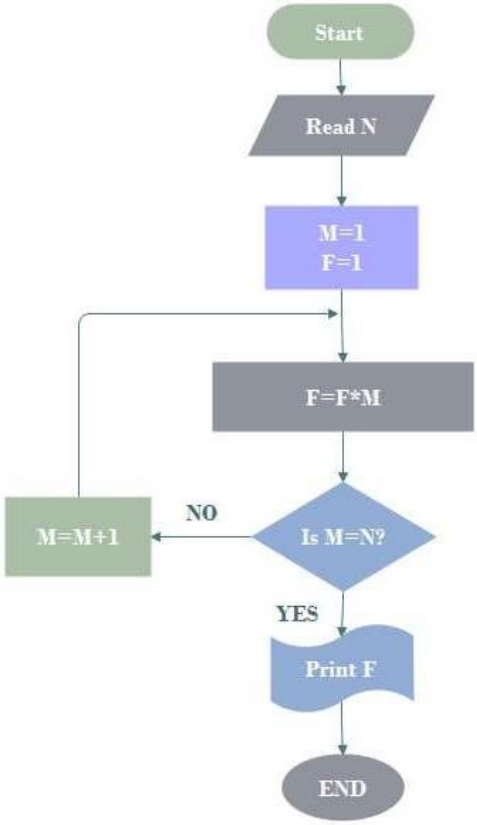
1. Kasus terburuk: f (n) diwakili oleh jumlah maksimum langkah yang diambil pada setiap instance ukuran n.

2. Kasing terbaik: f (n) diwakili oleh jumlah minimum langkah yang diambil pada setiap instance ukuran n.
3. Kasus rata-rata: f (n) diwakili oleh jumlah rata-rata langkah yang diambil pada setiap contoh ukuran n.



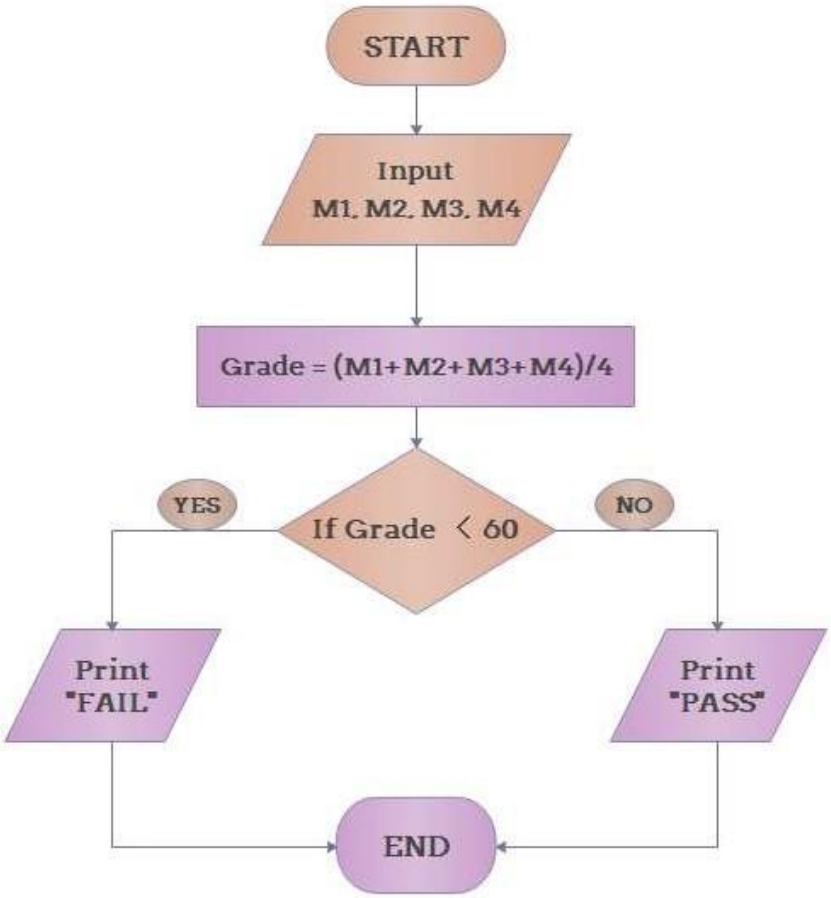
Gambar 2.1 Flowchart algoritma bidang matematika
Sumber: (Edraw, 2019)

Berikut ini adalah contoh flowchart aplikasi algoritma untuk bidang komputer yaitu menentukan hasil faktorial dari bilangan N.



Gambar 2.2 Flowchart algoritma bidang komputer
Sumber: (Edraw, 2019)

Berikut ini adalah contoh flowchart aplikasi algoritma untuk bidang pendidikan formal atau sekolah yaitu menentukan kelulusan mahasiswa.



Gambar 2.3 Flowchart algoritma bidang pendidikan
Sumber: (Edraw, 2019)

Gambar-gambar sebelumnya adalah diagram penggunaan algoritma pada beberapa bidan. Contoh-contoh tersebut memberikan demonstrasi yang jelas dari aplikasi algoritma dalam matematika, pemrograman komputer dan pendidikan.

2.3 Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi (Munir, 2006). Pesan yang akan dienkripsi disebut sebagai *Plaintext* (teks biasa). Disebut demikian karena informasi ini dengan mudah dapat dibaca dan dipahami oleh siapa saja. Algoritma yang dipakai untuk mengenkripsi dan mendekripsi sebuah *Plaintext* melibatkan penggunaan suatu bentuk kunci. Pesan *Plaintext* yang telah dienkripsi (atau dikodekan) dikenal sebagai *Ciphertext* (teks sandi). Di dalam kriptografi kita akan sering menemukan berbagai istilah atau terminologi. Beberapa istilah yang harus diketahui yaitu :

1. Pesan, Plainteks, dan *Cipher*teks

   Pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah (*Plaintext*) atau teks jelas (*cleartext*).

2. Pengirim dan Penerima

   Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sender*) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan.

   Enkripsi dan dekripsi

3. Proses menyandikan plainteks menjadi *Cipher*teks disebut enkripsi (*encryption*) atau *enCiphering* (standard nama menurut ISO 7498-2).

Sedangkan proses mengembalikan *Cipher*teks menjadi plainteks semula disebut dekripsi (*decryption*) atau de*Cipher*ing (standard nama menurut ISO 7498-2).

4. *Cipher* dan kunci

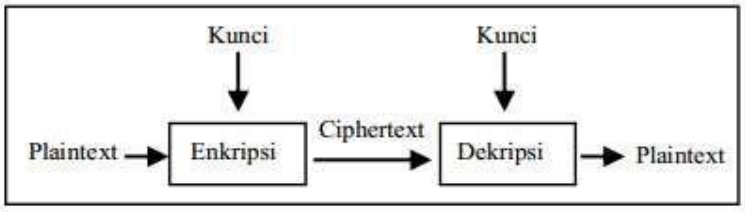
   Algoritma kriptografi disebut juga *Cipher*, yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *Cipher* memerlukan algoritma yang berbeda untuk enkripsi dan dekripsi. Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen-elemen plainteks dan himpunan yang berisi *Cipher*teks. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara dua himpunan tersebut. Misalkan P menyatakan plainteks dan C menyatakan *Cipher*teks, maka :

   E(P) = C ← fungsi enkripsi E memetakan P ke C

   D(C) = P ← fungsi dekripsi D memetakan C ke P

   Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan asal, maka persamaan D(E(P)) = P harus benar. Kriptografi mengatasi masalah keamanan data dengan menggunakan kunci, yang dalam hal ini Algoritma tidak dirahasiakan lagi, tetapi kunci harus tetap dijaga kerahasiaannya. Kunci (*key*) adalah parameter yang digunakan untuk transformasi enkripsi dan dekripsi. Kunci biasanya berupa string atau deretan bilangan. Dengan menggunakan kunci K, maka fungsi enkripsi

dan dekripsi dapat ditulis sebagai skema yang dijelaskan pada Gambar 2.4.



Gambar 2.4 Skema enkripsi dan dekripsi dengan menggunakan kunci
Sumber: (Edraw, 2019)

2.3.1 Sejarah Kriptografi

Kriptografi mempunyai sejarah yang sangat panjang. Kriptografi sudah digunakan 4000 tahun yang lalu, diperkenalkan oleh orang-orang Mesir lewat *hieroglyph*. Jenis tulisan ini bukanlah bentuk standar untuk menulis pesan (Ariyus, 2018).

Gambar 2.5 Tulisan yang menunjukan Heiroglyph
Sumber: (Ariyus, 2018)

Dikisahkan, pada Zaman Romawi Kuno, Pada Suatu saat Jelius Caesar ingin mengirimkan pesan rahasia kepada seseorang jendral di medan perang. Pesan tersebut dikirimkan melalui kurir. Karena pesan tersebut mengandung rahasia, jelius Cesar kemudian memikirkan bagaimana mengatasinya. Ia kemudian mengacak pesan tersbut hingga menjadi suatu pesan yang tidak dapat dipahami oleh siapapun terkecuali oleh jendralnya saja. Tentu pengirim ingin mengenkripsi suatu pesan menggunakan kode *Vigenere* dengan kunci *WARTHOG*.

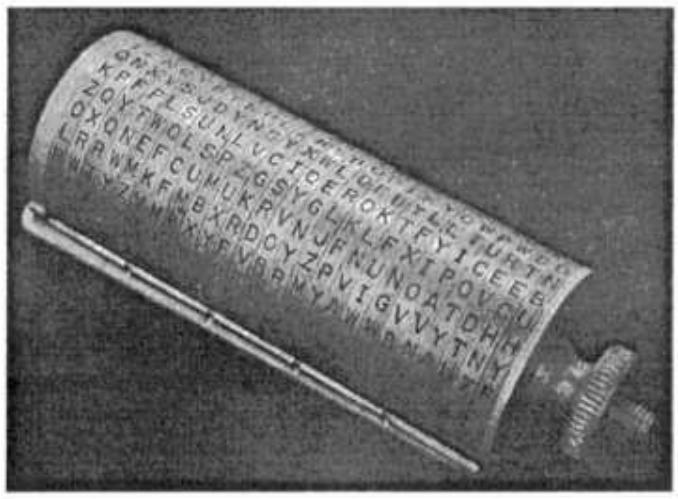
Untuk mengenkripsi huruf pertama, pengirim memutar *W* di potongan silindris dalam hingga berdampingan dengan *a* di silindris luar. Kemudian cari huruf teks-kode di potongan silindris dalam yang cocok dengan huruf teks-asli yang diinginkan di potongan silindris luar.

Selanjutnya mengirim mengenkripsi huruf kedua dengan memutar *A* di potongan silindris dalam hingga berdampingan dengan *a* di potongan silindris luar. Setelah itu cari huruf teks-kode di potongan silindris dalam yang cocok dengan huruf teks-asli yang dinginkan di potongan silindris luar.

Untuk seterusnya, ulang proses untuk huruf R,T,H,O,G dan kemudian ulang lagi dari W hingga seluruh pesan telah terenkripsi (EDUCBA, 2017).

Gambar 2.6 Roda Kaisar
Sumber: (Ariyus, 2018)

Bentuk roda kode sejak versi Jefferson hingga M94 terdiri dari sejumlah potongan silindris yang tersusun di suatu sumbu besi. Setiap potongan silindris memiliki susunan alphabet secara acak di bagaian luar. Potongan-potongan silindris tersebut menjadi dalam mengenkripsi dan mendeskripsi pesan dari pihak penerima dan pengirim. Setiap potongan silindris dapat diputar untuk menyusun alphabet menjadi teks kode ataupun menjadi teks asli. Untuk mengenkripsi suatu pesan, pengirim M94 memiliki bentuk yang hampir sama dengan roda kode jaferson. Bedanya, M94 terbuat dari alumunium. Untuk potongan ke 17, susunan alfabetnya berupa ARMYOFTHEU. Susunan ARMY OFTHEUS menunjukan "Army Orgin of thw M94". M94 memiliki 100 pilihan potongan silindris, walau mungkin yang dipilih untuk digunakan untuk suatu kunci hanya 25 buah. Hal tersebut dapat memperbanyak kemungkinan solusi dari roda kunci.



Gambar 2.7 M-94
Sumber: (Ariyus, 2018)

2.3.2 Kriptografi Simetris

Kriptografi Simetri (Kriptografi Kunci-*Privat*) Pada sistem kriptografi kunci-simetri, kunci untuk enkripsi sama dengan kunci untuk dekripsi, oleh karena itulah dinamakan kriptografi simetri. Keamanan sistem kriptografi simetri terletak pada kerahasiaan kuncinya. Ada banyak algoritma kriptografi modern yang termasuk ke dalam sistem kriptografi simetri, diantaranya adalah :

1. DES (Data Encryption Standard),
2. Blowfish,
3. Twofish,
4. Triple-DES,
5. IDEA,
6. Serpent,
7. AES (Advanced Encryption Standard).

Algoritma kriptografi (*Cipher*) simetri dapat dikelompokkan menjadi dua kategori, yaitu:

1. *Cipher* aliran (stream *Cipher*)

   Algoritma kriptografi beroperasi pada plainteks/*Cipher*teks dalam bentuk bit tunggal, yang dalam hal ini rangkaian bit dienkripsikan/didekripsikan bit per bit.

2. *Cipher* blok (block *Cipher*)

   Algoritma kriptografi beroperasi pada plainteks/*Cipher*teks dalam bentuk blok bit, yang dalam hal ini rangkaian bit dibagi menjadi blok-blok bit yang panjangnya sudah ditentukan sebelumnya.

2.4 *Cipher* Substitusi

Dalam kriptografi, cypher substitusi adalah metode enkripsi dengan mana unit *Plaintext* diganti dengan *Ciphertext*, sesuai dengan sistem tetap; "unit" dapat berupa huruf tunggal (yang paling umum), pasangan huruf, kembar tiga huruf, campuran di atas, dan sebagainya. Penerima menguraikan teks dengan melakukan substitusi terbalik. *Cipher* substitusi dapat dibandingkan dengan *Cipher* transposisi. Dalam sandi transposisi, satuan *Plaintext* disusun ulang dalam urutan yang berbeda dan biasanya cukup kompleks, tetapi satuan itu sendiri tidak berubah. Sebaliknya, dalam *Cipher* subtitusi, unit *Plaintext* dipertahankan dalam urutan yang sama dalam *Ciphertext*, tetapi unit itu sendiri diubah (Wagner, 2003).

Ada sejumlah jenis *Cipher* substitusi yang berbeda. Jika sandi beroperasi pada huruf tunggal, itu disebut sandi substitusi sederhana; sandi yang beroperasi pada kelompok huruf yang lebih besar disebut poligrafi. *Cipher* monoalphabetic menggunakan substitusi tetap atas seluruh pesan, sedangkan *Cipher* polyalphabetic menggunakan sejumlah substitusi pada posisi yang berbeda dalam pesan, di mana unit dari *Plaintext* dipetakan ke salah satu dari beberapa kemungkinan dalam *Ciphertext* dan sebaliknya (Weerasinghe, 2013).

2.1 *Shift Cipher*

Shift Cipher adalah salah satu cryptosystems yang paling awal dan paling sederhana. *Plaintext* yang diberikan dienkripsi ke dalam *Ciphertext* dengan menggeser setiap huruf dari *Plaintext* yang diberikan oleh n posisi. Sebuah *Cipher* Caesar, *Cipher* rotasi atau *Shift Cipher* adalah *Cipher* pengganti sederhana di mana cleartext digeser beberapa kali ke atas atau ke bawah alfabet yang dikenal. *Cipher* Caesar adalah jenis *Shift Cipher*. *Shift Cipher* bekerja dengan menggunakan operator modulo untuk mengenkripsi dan mendekripsi pesan. *Shift Cipher* memiliki kunci K, yang merupakan bilangan bulat dari 0 hingga 25.

PT	**KUNCI**	**CT**
K	1	L
O	-1	N
M	2	O
P	3	S
U	-2	S
T	1	U
E	1	F
R	4	V

Gambar 2.8 Skema Pergeseran Karakter
Sumber: (Mollin, 2001)

Gambar 2.4 adalah skema pertukan *Plaintext* menjadi *Ciphertext*. Setiap karakter akan ditukar posisinya sesuai kunci yang ditentukan pada kolom kunci. Jarak pergeseran ditentukan sesuai dengan nilai kunci. Hasil *Ciphertext* diperoleh dengan cara mengubah posisi bit-bit pada karakter *Plaintext* dengan jarak yang ditentukan. Pergeseran dapat dilakukan ke kanan atas atau ke kiri sesuai dengan kunci yang sudah ditentukan.

2.5 Unified Modelling Language

Unified Modeling Language adalah Metodologi kolaborasi antara metoda-metoda Booch, OMT (*Object Modeling Technique*), serta OOSE (*Object Oriented Software Enggineering*) dan beberapa metoda lainnya, merupakan metodologi yang paling sering digunakan saat ini untuk analisa dan perancangan sistem dengan metodologi berorientasi objek mengadaptasi maraknya penggunaan bahasa "pemrograman berorientasi objek" (OOP) (Wasserkrug et al., 2019).

Beberapa literature menyebutkan bahwa UML menyediakan sembilan jenis diagram, yang lain menyebutkan delapan karena ada beberapa diagram yang digabung, misalnya diagram komunikasi, diagram urutan dan diagram waktu digabung menjadi diagram interaksi (Sukmawati & Priyadi, 2019).

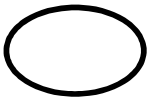
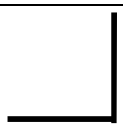
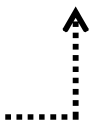
2.5.1 Use Case Diagram

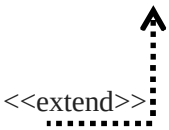
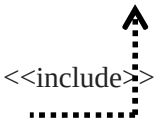
Use Case Diagram adalah abstraksi dari interaksi antara sistem dan aktor. *Use Case Diagram* bekerja dengan cara mendeskripsikan tipe interaksi antara user sebuah sistem dengan sistemnya sendiri melalui sebuah cerita bagaimana sebuah sistem dipakai. *Use Case Diagram* berguna dalam tiga hal:

1. Menjelaskan fasilitas yang ada (*requirement*).
2. Komunikasi dengan klien.
3. Membuat *test* dari kasus-kasus secara umum.

Adapun simbol-simbol dalam *Use Case Diagram* dapat dilihat pada tabel 2.1.

Tabel 2.1 Elemen-Elemen *Use Case Diagram*

SIMBOL	NAMA	KETERANGAN
	*Actor*	Menspesifikan himpunan peran yang pengguna mainkan ketika berinteraksi dengan *use case*
	*Use Case*	Deskripsi urutan aksi-sistem yang menghasilkan suatu hasil yang terukur
	*System*	Menspesifikasian paket yang menampilkan sistem secara terbatas
	*Association*	Simbol yang menghubungkan antara objek satu dengan objek lainnya
	*Dependency*	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri (*independent*) akan mempengaruhi elemen yang

		bergantung padanya elemen yang tidak mandiri
	*Generalization*	Hubungan dimana objek anak (*descendent*) berbagi perilaku dan struktur data dari objek yang ada di atasnya objek induk (*ancestor*)
	*Extend*	Menspesifikasikan bahwa *use case* target memperluas perilaku dari *use case* sumber pada suatu titik yang diberikan
	*Include*	Menspesifikasikan bahwa *use case* sumber secara *eksplisit*

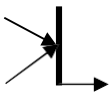
Sumber: (Kurniawan, 2018)

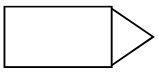
2.5.2 Activity Diagram

Activity Diagram menyediakan analis dengan kemampuan untuk memodelkan proses dalam suatu sistem informasi. *Activity Diagram* dapat digunakan untuk alur kerja model, *use case individual*, atau logika keputusan yang terkandung dalam metode individual. *Activity Diagram* juga menyediakan pendekatan untuk proses pemodelan paralel (Ladjamudin, 2017).

Pada dasarnya, diagram aktivitas canggih dan merupakan diagram aliran data yang terbaru. Secara teknis, diagram aktivitas menggabungkan ide-ide proses pemodelan dengan teknik yang berbeda termasuk model cara, statecharts. *Activity Diagram* mempunyai beberapa elemen dalam memodelkan sebuah sistem, yaitu:

Tabel 2.2 Elemen-Elemen *Activity Diagram*

SIMBOL	NAMA	KETERANGAN
	*Action State*	Menandakan sebuah aktivitas
	*Initial State*	Titik awal untuk memulai suatu aktivitas
	*Final State*	Titik akhir untuk mengakhiri aktivitas
	*Decision*	Pilihan untuk mengambil keputusan
	*Flow Final*	Untuk mengakhiri suatu aliran
	Transition	Menunjukan aktifitas selanjutnya setelah aktivitas sebelumnya
	Synchronization	Dibagi menjadi 2 yaitu fork dan join: Fork digunakan.untuk memecah behaviour menjadi activity atau action yang paralel, sedangkan join untuk menggabungkan kembali activity atau action yang parallel
	Swimlane	Untuk melakukan partisi atau pembagian

	Signal Accept State	Tanda penerimaan
	Signal Send State	Tanda pengiriman

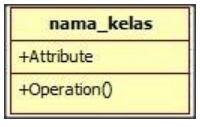
Sumber: (Kurniawan, 2018)

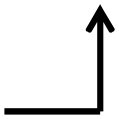
2.5.3 Class Diagram

Tujuan utama dari *Class Diagram* adalah untuk menciptakan sebuah kosa kata yang digunakan oleh analis dan pengguna. *Class Diagram* biasanya merupakan hal-hal, ide-ide atau konsep yang terkandung dalam aplikasi. Misalnya, jika sedang membangun sebuah aplikasi penggajian, diagram kelas mungkin akan berisi kelas yang mewakili hal-hal seperti karyawan, cek, dan pendaftaran gaji.

Class Diagram juga akan menggambarkan hubungan antara kelas. Berikut komponen-komponen yang ada pada *Class Diagram*.

Tabel 2.3 Elemen-Elemen *Class Diagram*

SIMBOL	NAMA	KETERANGAN
	*Class*	Kelas pada struktur sistem
	Association	Relasi antar kelas dengan makna umum, asosiasi biasanya juga di sertai dengan

		multiplicity
	*Directed Association*	Relasi antar kelas dengan makna kelas yang satu digunakan oleh kelas yang lain, asosiasi berarah biasanya juga disertai dengan multiplicity
	*Dependency*	Relasi antar kelas dengan makna kebergantungan antar kelas.

Sumber: : (Kurniawan, 2018)

2.5.4 Sequence Diagram

Sequence Diagram menjelaskan interaksi objek yang disusun berdasarkan urutan waktu. Secara mudahnya *Sequence Diagram* adalah gambaran tahap demi tahap yang seharusnya dilakukan untuk menghasilkan sesuatu sesuai dengan *Use Case Diagram*. Berikut komponen-komponen yang ada pada *Sequence Diagram.*

Tabel 2.4 Elemen-Elemen *Sequence Diagram*

SIMBOL	NAMA	KETERANGAN
	Objek	Menggambarkan objek/orang yang berintraksi di dalam sistem
	Stimulus	Menggambarkan pengiriman pesan
	Self Stimulus	Menyatakan suatu objek mengirimkan pesan untuk menjalankan oprasi yang ada

		pada objek lain.

Sumber: (Kurniawan, 2018)

2.5.5 Flowchart

Flowchart adalah jenis diagram yang mewakili alur kerja atau proses. Diagram alir juga dapat didefinisikan sebagai representasi diagram dari suatu algoritma, pendekatan langkah demi langkah untuk menyelesaikan suatu tugas. Diagram alur menunjukkan langkah-langkah sebagai kotak dari berbagai jenis, dan urutannya dengan menghubungkan kotak-kotak dengan panah. Representasi diagram ini menggambarkan model solusi untuk masalah yang diberikan. *Flowchart* digunakan dalam menganalisis, merancang, mendokumentasikan, atau mengelola suatu proses atau program di berbagai bidang. *Flowchart* digunakan dalam mendesain dan mendokumentasikan proses atau program sederhana. Seperti jenis diagram lainnya, diagram membantu memvisualisasikan apa yang sedang terjadi dan dengan demikian membantu memahami suatu proses, dan mungkin juga menemukan fitur yang kurang jelas dalam proses tersebut, seperti kekurangan dan hambatan. Ada berbagai jenis diagram alur: masing-masing jenis memiliki set kotak dan notasi sendiri. Dua jenis kotak yang paling umum dalam diagram alur adalah:

1. Langkah pemrosesan, biasanya disebut aktivitas, dan dilambangkan sebagai kotak persegi panjang.
2. Sebuah keputusan, biasanya dilambangkan sebagai berlian.

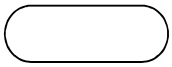
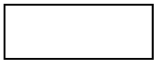
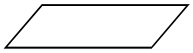
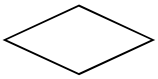
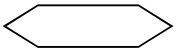
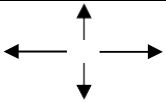
Diagram alir digambarkan sebagai "lintas fungsional" ketika bagan dibagi menjadi bagian vertikal atau horizontal yang berbeda, untuk menggambarkan kontrol unit organisasi yang berbeda. Simbol yang muncul di bagian tertentu berada dalam kendali unit organisasi itu. *Flowchart* lintas fungsional memungkinkan penulis untuk menemukan tanggung jawab untuk melakukan suatu tindakan atau membuat keputusan dengan benar, dan untuk menunjukkan tanggung jawab masing-masing unit organisasi untuk bagian-bagian berbeda dari satu proses tunggal (Nakatsu, 2019).

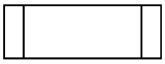
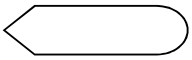
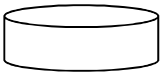
Struktur grafik yang mendasari diagram alur adalah grafik aliran, yang mengabstraksi jenis simpul, isinya, dan informasi tambahan lainnya. Diagram alir menggambarkan aspek-aspek tertentu dari proses dan biasanya dilengkapi dengan jenis diagram lainnya. Misalnya, Kaoru Ishikawa, mendefinisikan diagram alir sebagai salah satu dari tujuh alat dasar kendali mutu, di sebelah histogram, diagram Pareto, lembar periksa, diagram kontrol, diagram sebab-akibat, dan diagram sebaran. Demikian pula, di UML, notasi pemodelan konsep standar yang digunakan dalam pengembangan perangkat lunak, diagram aktivitas, yang merupakan jenis diagram alur, hanyalah salah satu dari banyak jenis diagram yang berbeda.

Diagram Nassi-Shneiderman dan Drakon-chart adalah notasi alternatif untuk aliran proses. Nama alternatif umum termasuk diagram alir, diagram alur proses, diagram alur fungsional, peta proses, diagram proses, diagram proses fungsional, model proses bisnis, model proses, diagram alir proses, diagram alur kerja, diagram alir bisnis. Istilah "diagram alur" dan "diagram alir" digunakan

secara bergantian. Struktur grafik yang mendasari diagram alur adalah grafik aliran, yang mengabstraksi jenis simpul, isinya, dan informasi tambahan lainnya. Adapun simbol-simbol *flowchart* lihat pada tabel sebagai berikut:

Tabel 2.5 Simbol-simbol Flowchart

NO	SIMBOL	FUNGSI
1.		Terminal, untuk memulai atau mengakhiri suatu program
2.		Proses, suatu simbol yang menunjukkan setiap pengolahan yang dilakukan.
3.		Input-Output, untuk memasukkan menunjukkan hasil dari suatu proses
4.		Decision, suatu kondisi yang akan menghasilkan beberapa kemung-kinan jawaban atau pilihan
5.		Preparation, suatu symbol yang menyediakan tempat pengolahan
6.		Connector, suatu prosedur penghubung yang akan masuk atau keluar melalui symbol ini dalam lembar yang sama
7.		Off-Page Connector, merupakan symbol masuk atau keluarannya suatu prosedur pada lembaran kertas lainnya
8.		Arus/Flow, dari pada prosedur yang dapat dilakukan atas ke bawah dari bawah ke atas, ke atas dari kiri ke kanan ataupun dari kanan ke kiri

9.		Predefined Process, untuk menyatakan sekumpulan langkah proses yang ditulis sebagai prosedur
10.		Simbol untuk output, yang ditunjukkan ke suatu device, seperti printer, dan sebagainya
11		Penyimpanan file secara sementara
12		Menunjukkan input / Output Hardisk (media penyimpanan)

Sumber: (Kurniawan, 2018)

2.6 Visual Basic

Visual Basic (VB) adalah bahasa pemrograman yang digerakkan oleh peristiwa dan lingkungan dari Microsoft yang menyediakan antarmuka pengguna grafis (GUI) yang memungkinkan programmer untuk memodifikasi kode hanya dengan menyeret dan menjatuhkan objek dan menentukan perilaku dan penampilan mereka. VB berasal dari bahasa pemrograman BASIC dan dianggap event-driven dan berorientasi objek. VB dimaksudkan agar mudah dipelajari dan cepat untuk menulis kode; Akibatnya, kadang-kadang disebut sistem pengembangan aplikasi cepat (RAD) dan digunakan untuk prototipe aplikasi yang nantinya akan ditulis dalam bahasa yang lebih sulit tetapi efisien (Lee, 2014).

Versi terakhir VB, Visual Basic 6, dirilis pada tahun 1998, tetapi sejak itu telah digantikan oleh VB. NET, Visual Basic for Applications (VBA) dan Visual Studio .NET. VBA dan Visual Studio adalah dua kerangka kerja yang paling

umum digunakan saat ini. VB adalah alat pengembangan berbasis GUI yang menawarkan RAD lebih cepat daripada kebanyakan bahasa pemrograman lainnya. VB juga memiliki fitur sintaksis yang lebih mudah daripada bahasa lain, lingkungan visual yang mudah dipahami dan konektivitas basis data yang tinggi.

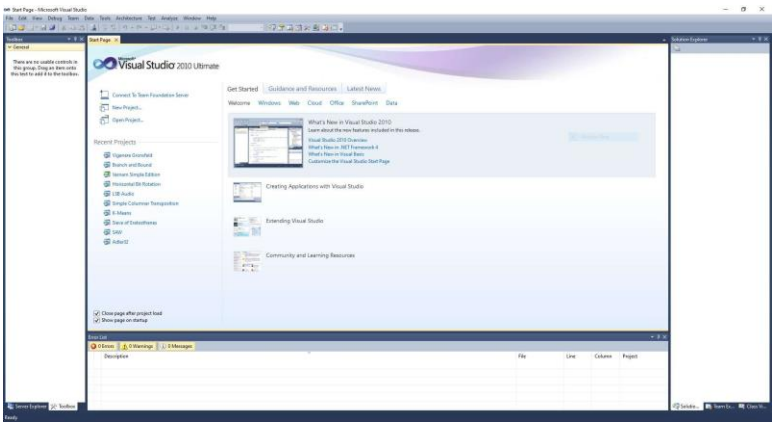
2.6.1 Visual Basic.NET

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.

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).

2.6.2 Antarmuka Visual Basic.NET

Visual Basic.Net memiliki beberapa versi. Berikut ini adalah tampilan dari Visual Basic.Net versi 2010.



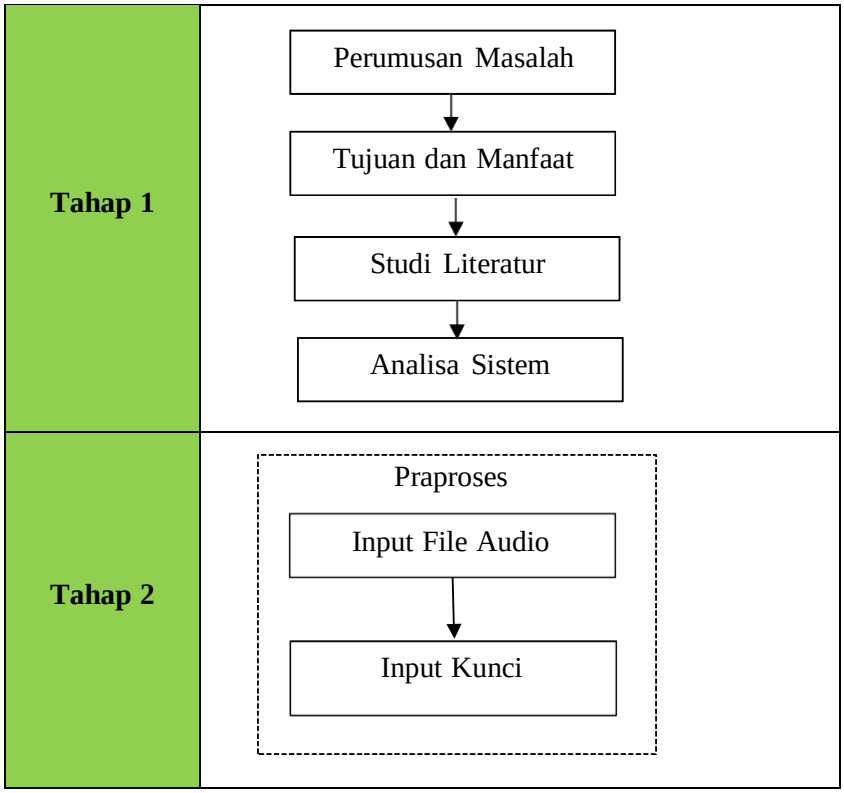
Gambar 2.9 Antarmuka Visual Basic.NET 2010
Sumber: (Rahmel, 2018)

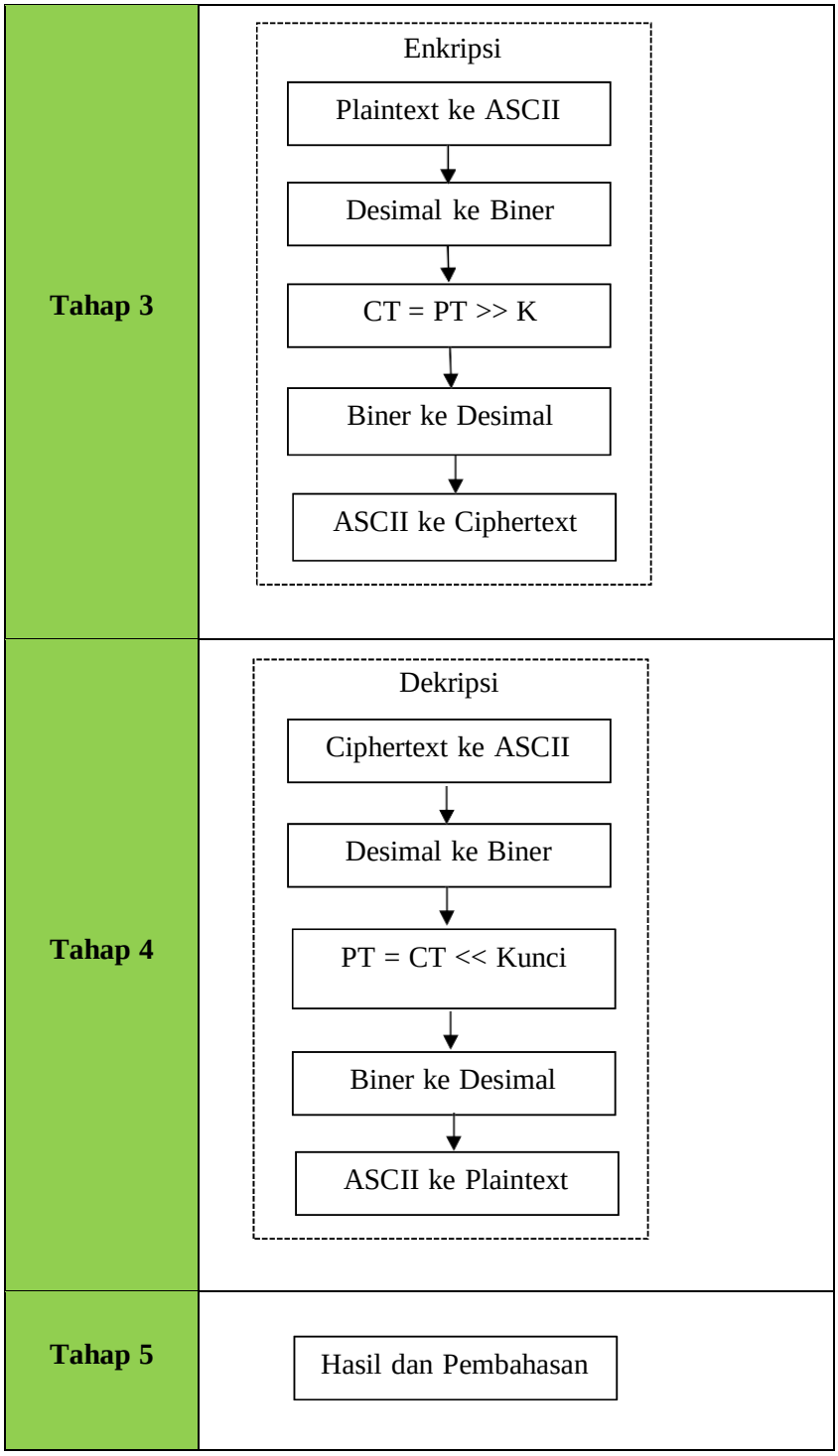
BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Pada bagian ini akan dijelaskan tahapan penelitian yang penulis lakukan dalam melakukan enkripsi dan dekripsi file audio dengan menggunakan teknik *Left Shifting*. Beberapa langkah dilakukan dalam tiap-tiap fase yang sudah ditentukan. Gambar 3.1 adalah kerangka penelitian yang dilakukan.





Gambar 3.1 Tahapan Penelitian

Berikut adalah tahapan penelitian yang dilakukan:

1. Perumusan Masalah

   Rumusan masalah akan dijabarkan terlebih dahulu untuk menentukan masalah yang terjadi dalam proses enkripsi dan dekripsi dengan teknik *Left Shifting.*

2. Tujuan dan Manfaat

   Tujuan dan manfaat akan dijabarkan untuk menentukan arah penelitian dan hasil yang akan dicapai serta manfaatnya terhadap keilmuan.

3. Studi Literatur

   Pencarian referensi dilakukan dengan menentukan studi literatur berdasarkan teori-teori yang diperoleh yang berhubungan dengan ilmu kriptografi. Referensi dapat ditemukan dari internet atau buku-buku.

4. Analisa Sistem

   Proses analisa sistem akan menentukan dan menjelaskan algoritma yang digunakan serta menentukan proses dan cara kerja algoritma tersebut dalam mengatasi masalah.

5. Praproses

   Praproses adalah hal yang dilakukan sebelum proses enkripsi dan dekripsi dilakukan. Bagian ini menentukan file audio dan kunci yang digunakan.

6. Enkripsi

   Melakukan proses enkripsi file yang sudah ditentukan pada praproses. Enkripsi dilakukan berdasarkan jumlah pergeseran bit yang telah ditentukan pada praproses.

7. Dekripsi

   Melakukan proses dekripsi file terenkripsi sehingga kembali menjadi *plaintext* seperti semula.

8. Hasil dan Pembahasan

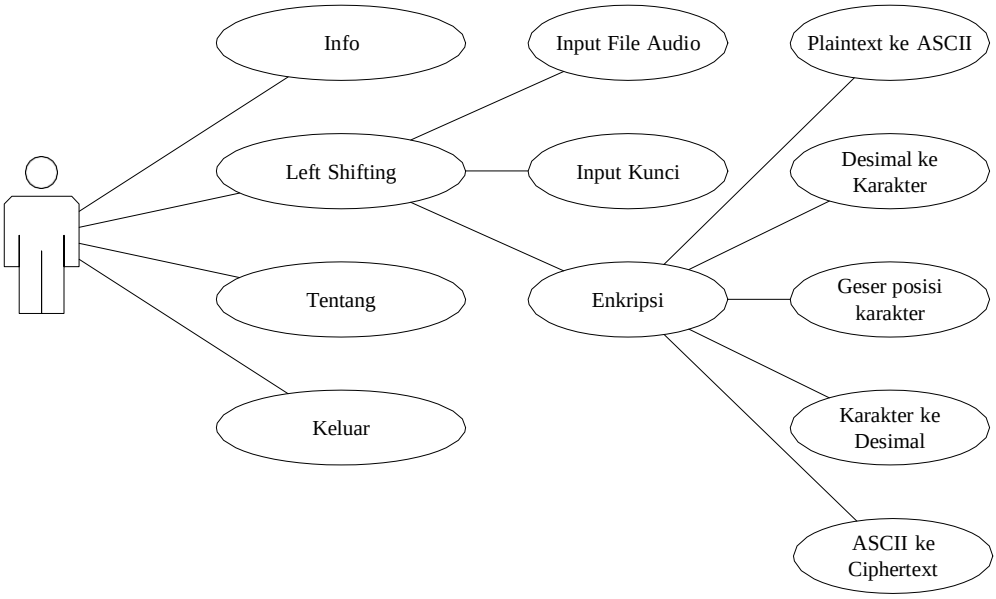
   Bagian ini dilakukan pengujian dan pembuktian akan program aplikasi yang telah dibuat agar tujuan dan manfaat yang sebelumnya tercapai dengan baik dan benar.

3.2 Rancangan Penelitian

Sebelum penelitian dikemas menjadi sistem yang diimplementasikan dalam bentuk program aplikasi, maka penelitian ini memerlukan perancangan agar hasil yang diperoleh lebih baik dan terstruktur. Program aplikasi akan dibuat menggunakan *Microsoft Visual Studio 2010*. Untuk melihat lebih jelas alur kerja dari sistem, berikut ini akan dijelaskan beberapa diagram yang digunakan.

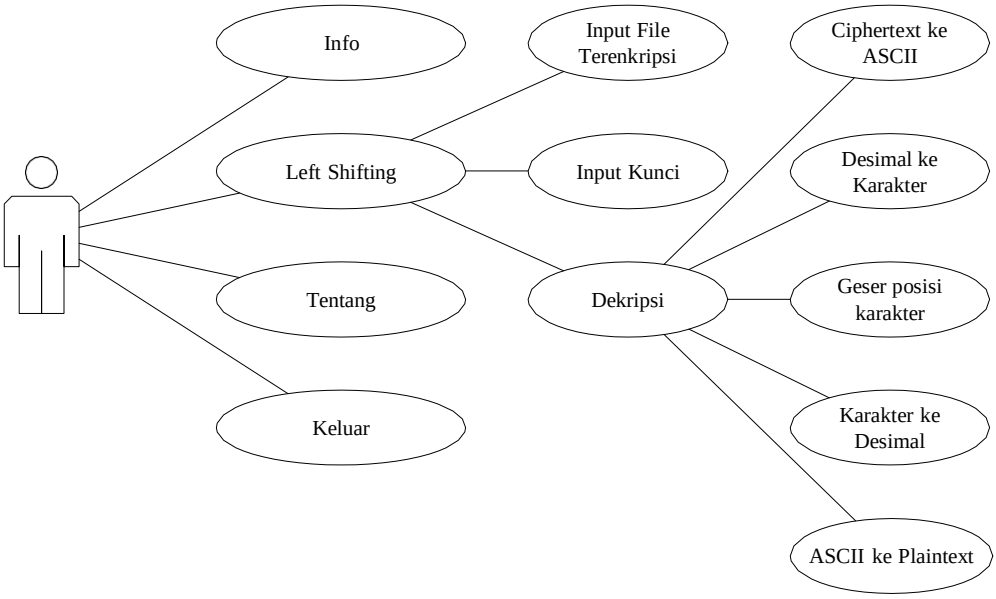
3.2.1 Use Case Diagram

Use Case Diagram menjelaskan tentang alur yang digunakan dalam membuat program aplikasi. Beberapa interaksi antara pengguna dan sistem akan digambarkan pada diagram ini. Diagram ini merupakan gambaran dari fungsi sistem tersebut. Gambar 3.2 adalah perancangan *Use Case* untuk enkripsi program aplikasi *Left Shifting*.



Gambar 3.2 Use Case Diagram Enkripsi

Gambar diagram tersebut menjelaskan proses enkripsi terjadi setelah file audio dan kunci pergeseran bit dimasukkan. Enkripsi akan melakukan pergantian tiap-tiap karakter pada file audio menjadi karakter lain atau dengan teknik substitusi. Kunci merupakan jumlah pergeseran pada karakter file audio. Hasil pergeseran akan dikonversikan kembali menjadi karakter dan menyusun deretan karakter tersebut menjadi file kembali. Hasil enkripsi sudah tidak dapat diputar kembali menggunakan media pemutar suara karena sudah mengalami proses enkripsi.

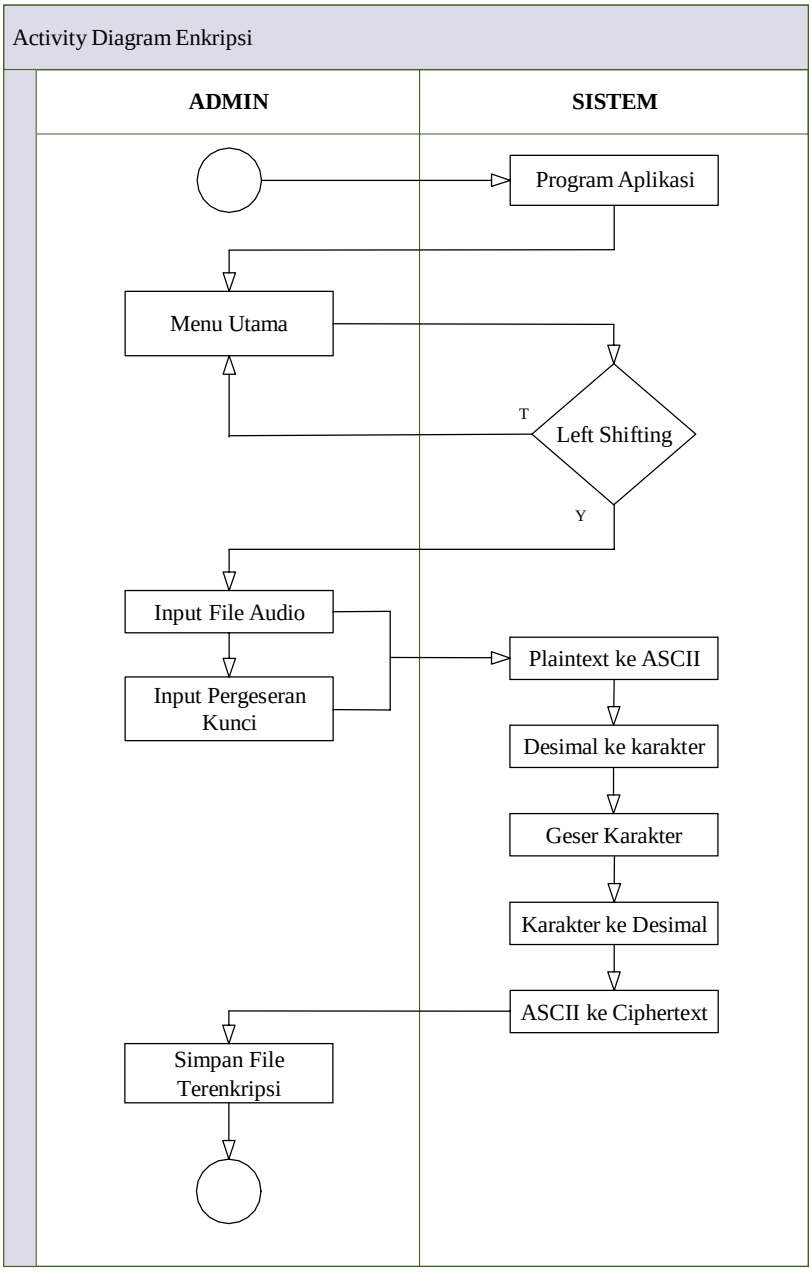


Gambar 3.3 Use Case Diagram Dekripsi

Dekripsi melakukan proses yang sama dengan enkripsi. Perbedaannya adalah pada proses dekripsi, pergeseran bit akan dilakukan dengan arah yang berlawanan. Apabila pada saat enkripsi, perputaran dilakukan ke arah kiri, maka pada dekripsi akan dilakukan perputaran ke arah kanan. Kunci yang digunakan harus sama dengan pada proses enkripsi. Hasil dekripsi dapat diputar kembali dengan menggunakan media pemutar suara.

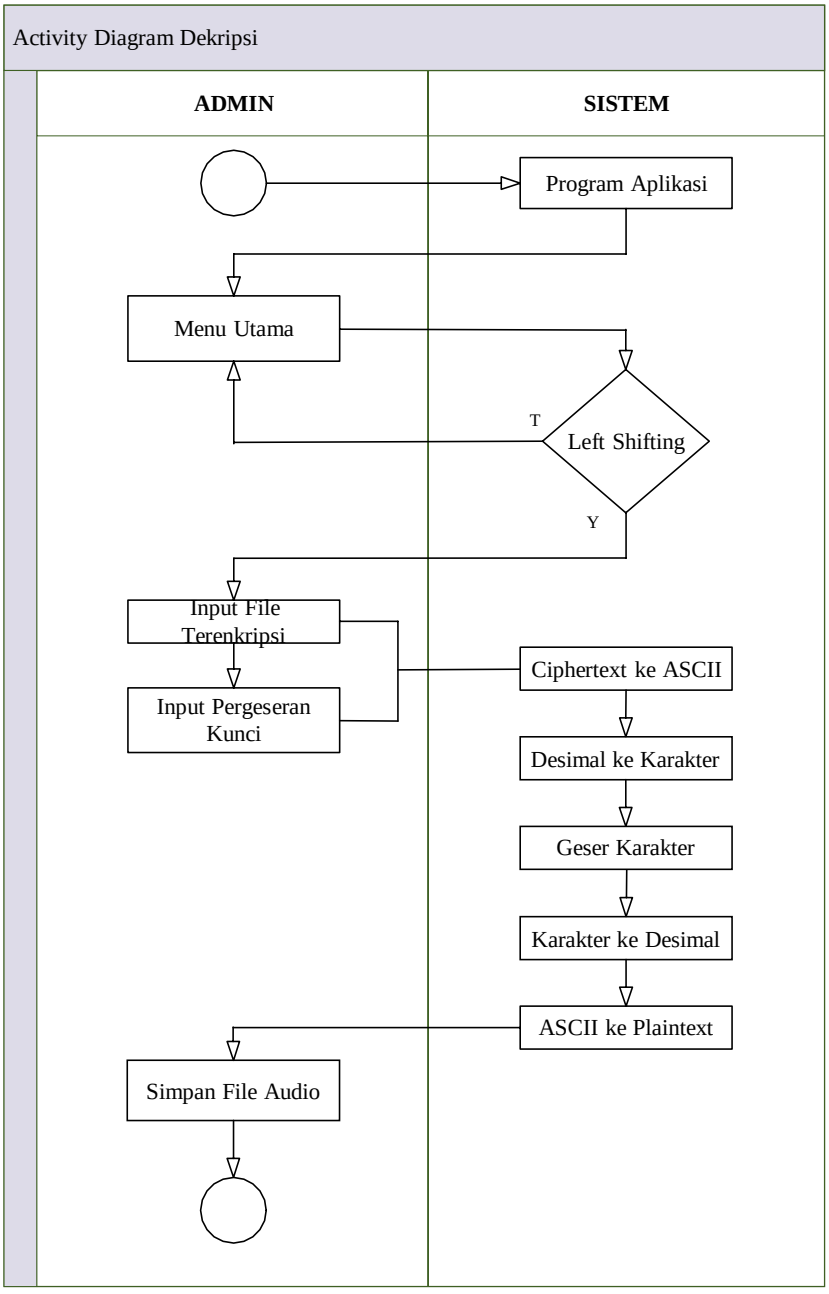
3.2.2 Activity Diagram

Activity diagram menggambarkan alur aktifitas dari system pada penelitian ini. Gambar 3.4 akan menjelaskan *Activity diagram* dari teknik *Left Shifting* pada proses enkripsi.



Gambar 3.4 Activity Diagram Enkripsi

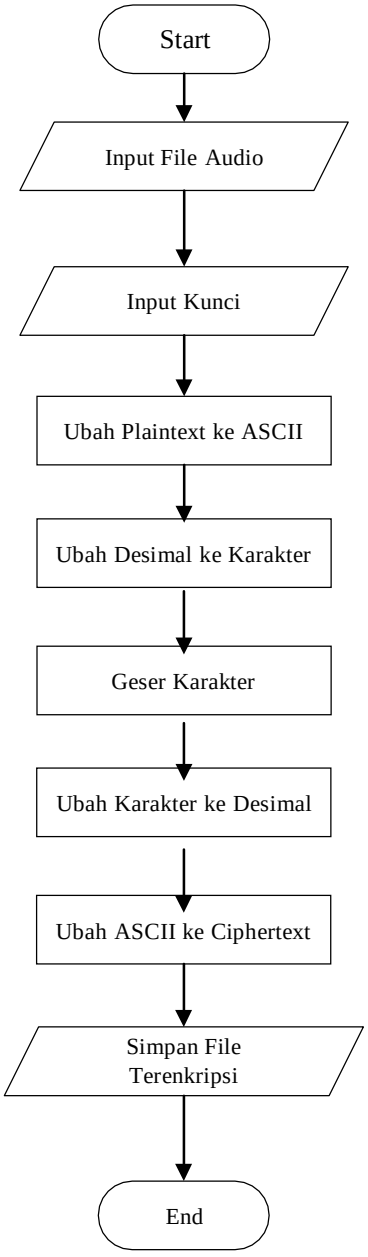
Gambar 3.5 akan menjelaskan *Activity diagram* dari teknik *Left Shifting* pada proses dekripsi.



Gambar 3.5 Activity Diagram Dekripsi

3.2.3 Flowchart Enkripsi

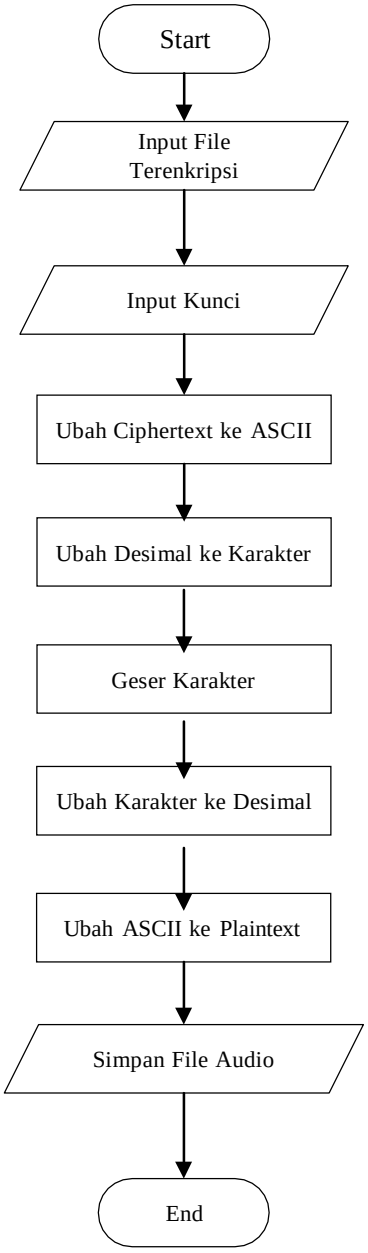
Flowchart enkripsi akan menerangkan alur proses enkripsi dengan teknik *Left Shifting*. *Flowchart* dapat dilihat pada gambar 3.6.



Gambar 3.6 Flowchart Enkripsi *Left Shifting*

3.2.4 Flowchart Dekripsi

Flowchart dekripsi akan menjelaskan alur dari proses dekripsi dengan teknik *Left Shifting*. *Flowchart* ini dapat dilihat pada gambar 3.7.



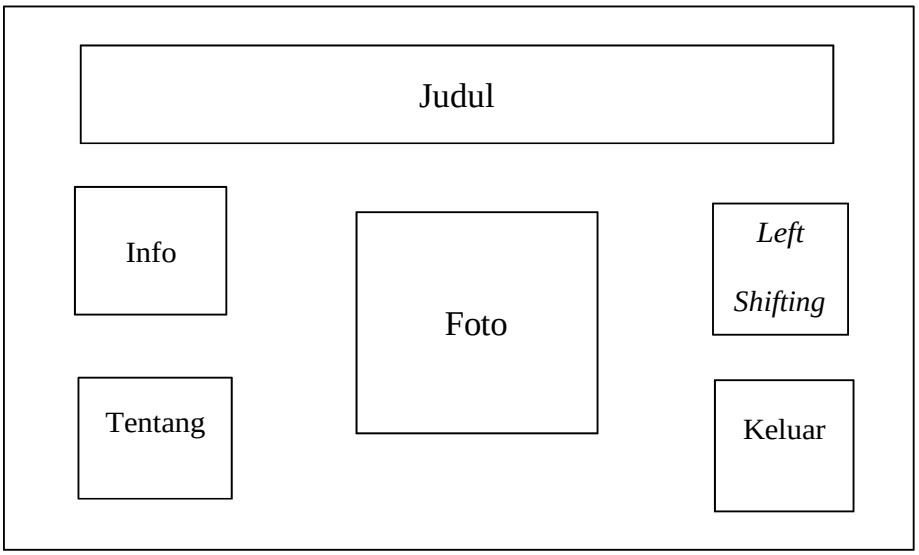
Gambar 3.7 Flowchart Dekripsi *Left Shifting*

3.3 Desain Antarmuka

Pembentukan antarmuka sangat penting dilakukan untuk menghubungkan antara pengguna dan sistem. Penggunaan antarmuka yang baik akan mengurangi kesalahan yang akan terjadi. Beberapa bagian akan terlibat pada desain antarmuka pada program aplikasi ini. Ada empat buah *form* yang akan digunakan pada pembuatan program aplikasi.

3.3.1 Desain Menu Utama

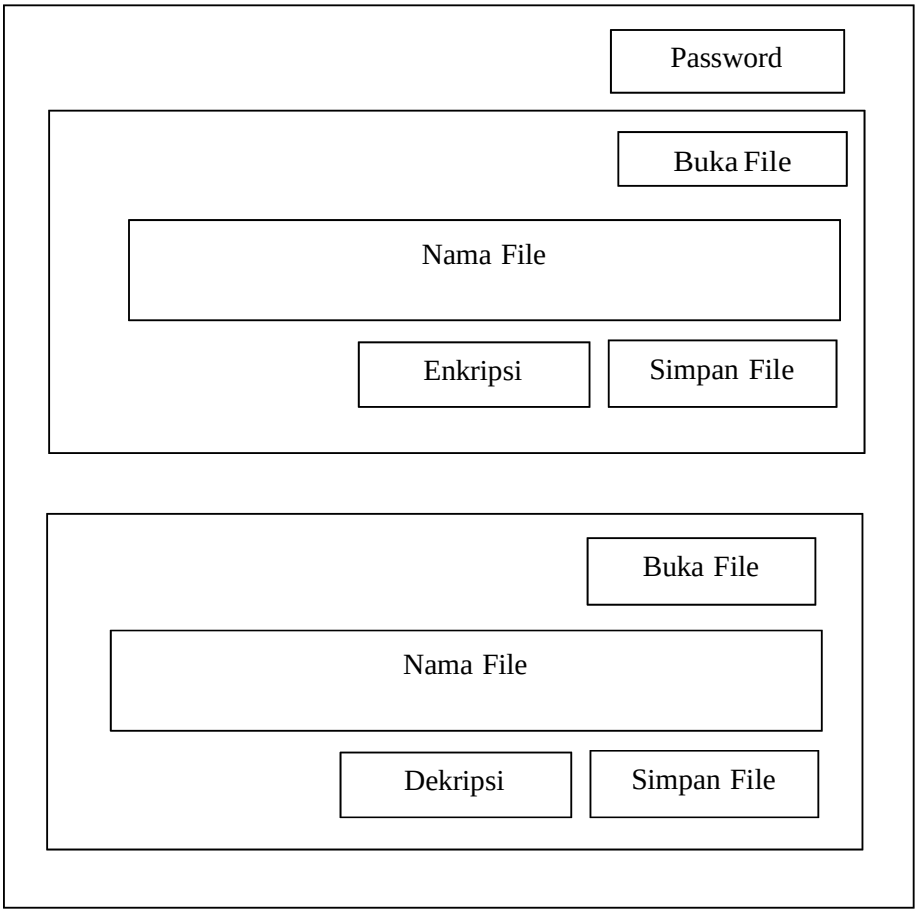
Desain menu utama adalah rancangan tampilan untulk yang pertama sekali akan digunakan dalam program aplikasi untuk melakukan interaksi antara pengguna dan program aplikasi kriptografi dengan teknik *Left Shifting*. Gambar 3.8 adalah hasil desain Menu Utama.



Gambar 3.8 Desain Menu Utama

3.3.2 Desain *Left Shifting*

Desain *Left Shifting* adalah bentuk tampilan antarmuka yang nanti digunakan dalam melakukan proses enkripsi dan dekripsi dengan teknik *Left Shifting*. Gambar 3.9 adalah tampilan desain algoritma *Left Shifting*.



Gambar 3.9 Desain Kriptografi *Left Shifting*

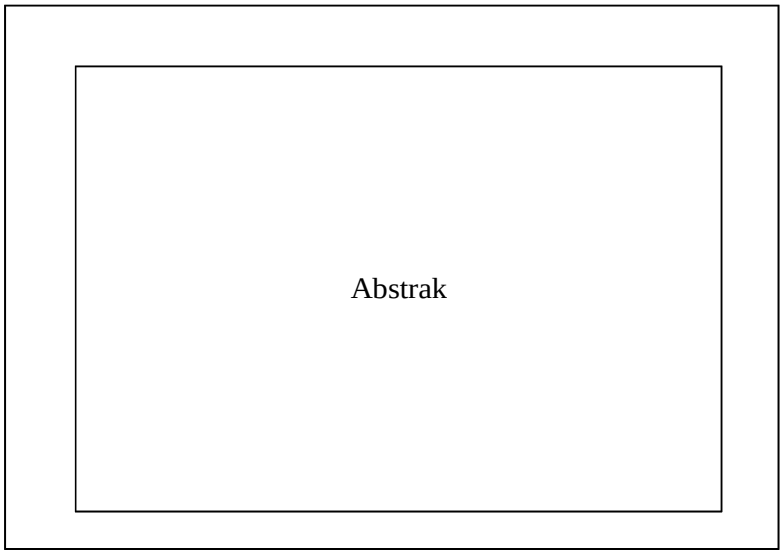
Menu algoritma *Left Shifting* memiliki beberapa bagian antara lain:

- Enkripsi
- Dekripsi

- Password
- Tombol Enkripsi
- Tombol Dekripsi
- Nama File
- Tombol Buka File
- Tombol Simpan File

3.3.3 Desain Info

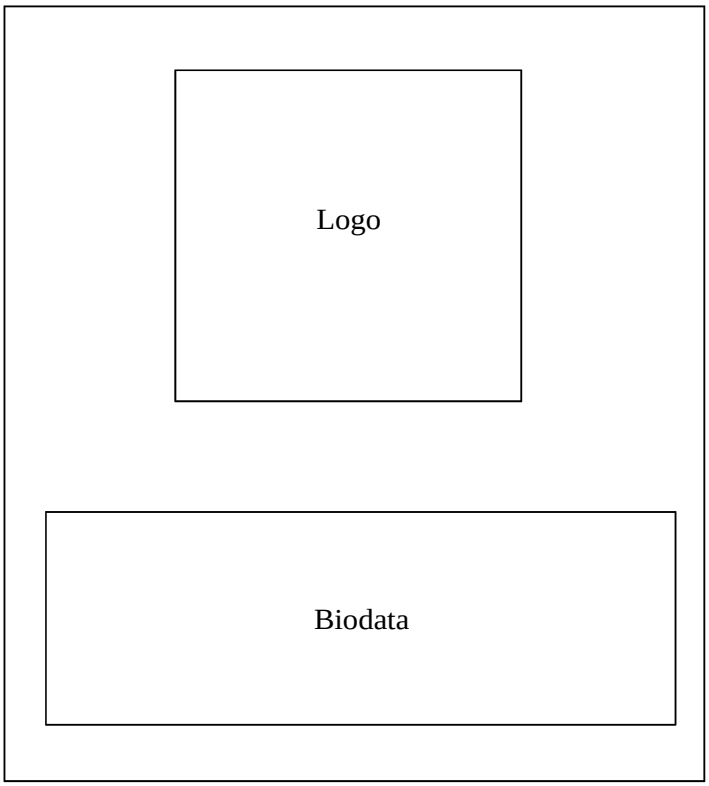
Menu ini menampilkan tentang abtrak penelitian yang dilakukan. Perancangan antarmuka info terdiri dari sebuah objek label untuk menampilkan tentang isi abstrak tersebut. Gambar 3.10 adalah hasil perancangan desain Info.



Gambar 3.10 Desain Info

3.3.4 Desain Tentang

Menu ini menampilkan keterangan atau biodata tentang penulis. Perancangan ini terdiri dari logo Universitas Pembangunan Panca Budi dan beberapa informasi singkat. Perancangan ini memiliki dua objek, *picturebox* dan *label*. Gambar 3.11 adalah hasil desain Tentang.



Gambar 3.11 Desain Tentang

BAB IV

HASIL DAN PEMBAHASAN

Hasil ditentukan berdasarkan perancangan yang sudah dilakukan pada bagian sebelumnya. Untuk mendapatkan hasil yang baik, maka perencanaan pembuatan program aplikasi harus dikerjakan dengan baik dan matang. Hal ini dilakukan untuk menghindari terjadinya kesalahan atau *error* pada program aplikasi pada saat melakukan proses enkripsi dan dekripsi menggunakan algoritma *Left Shifting*. Dalam menunjang kelancaran pembuatan program aplikasi ada beberapa kebutuhan sistem yang harus dipenuhi.

4.1 Kebutuhan Sistem

Sistem merupakan kesatuan penting yang saling berintegrasi dalam menentukan hasil yang akan diperoleh. Kebutuhan sistem merupakan hal yang harus dipenuhi dalam membuat program aplikasi. Kebutuhan sistem dibagi menjadi dua bagian, antara lain:

1. Kebutuhan perangkat keras
2. Kebutuhan perangkat lunak

Kedua kebutuhan tersebut harus dapat saling bekerja sama dan sinkron dalam membuat dan program aplikasi dan menyelesaikan penelitian ini.

4.1.1 Kebutuhan Perangkat Keras

Setiap program aplikasi membutuhkan perangkat keras begitu juga dalam pembuatan penelitian ini yang sangat membutuhkan perangkat keras yang memadai. Tabel 4.1 adalah spesifikasi perangkat keras yang dibutuhkan dalam melakukan penelitian ini.

Tabel 4.1 Spesifikasi perangkat keras

No.	Nama Komponen	Spesifikasi
1	Processor	Intel Core i5 2.4 GHz
2	RAM	4096 MB
3	Storage	500 GB
4	Display	14 inches

4.1.2 Kebutuhan Perangkat Lunak

Tidak terlepas dari kebutuhan perangkat keras, perangkat lunak juga sangat dibutuhkan dalam menunjang hasil yang dicapai terlebih-lebih hasil dalam membuat program aplikasi nanti. Tabel 4.2 adalah spesifikasi perangkat lunak yang digunakan pada penelitian ini.

Tabel 4.2 Spesifikasi perangkat lunak

No.	Nama Komponen	Spesifikasi
1	Sistem Operasi	Windows 10 64 Bit
2	IDE Pemrograman	Microsoft Visual Basic.NET 2010
3	Tangkap Gambar	Snipping Tool
4	Data Editor	Microsoft Excel

4.2 Antarmuka Program Aplikasi

Program aplikasi dibuat menggunakan *Microsoft Visual Basic.NET 2010.* Program aplikasi harus dapat melakukan proses enkripsi dan dekripsi file audio dengan metode *Left Shifting*. Program aplikasi memiliki beberapa antarmuka yang memiliki peranan dan fungsi masing-masing.

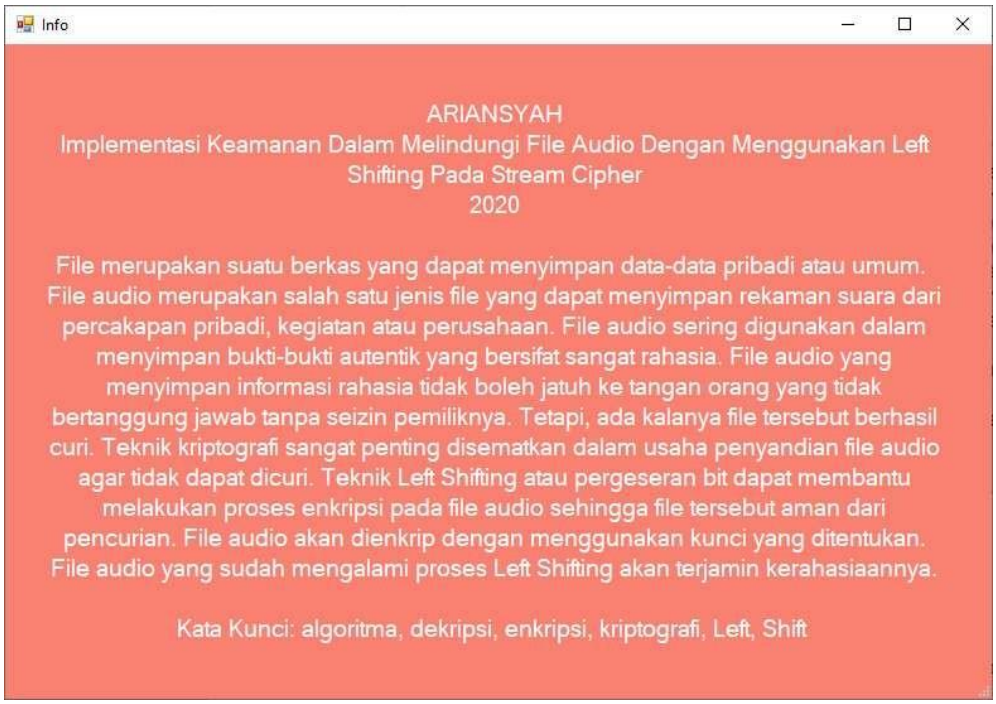
4.2.1 Implementasi Menu Utama

Menu utama akan tampil pada saat pengguna melakukan uji coba pada program aplikasi. Tampilan ini adalah tampilan yang akan dihadapkan kepada pengguna pada pertama sekali. Gambar 4.1 adalah hasil implementasi Menu Utama.

Gambar 4.1 Implementasi Menu Utama

4.2.2 Implementasi Info

Info akan menampilkan abstrak yang penulis berhasil rangkum berdasarkan penelitian yang sudah dilakukan. Gambar 4.2 adalah hasil implementasi dari Info.



Gambar 4.2 Implementasi Abstrak

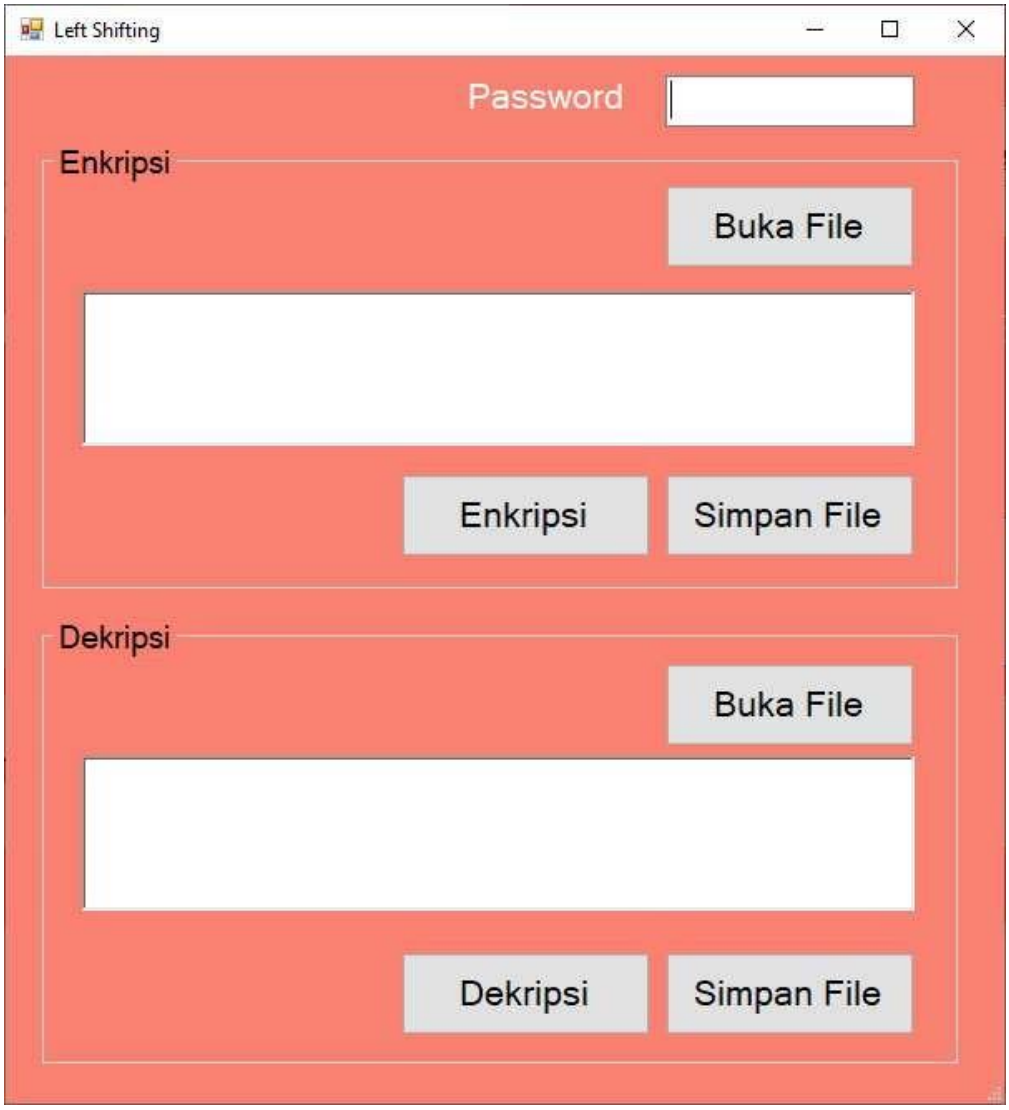
4.2.3 Implementasi Menu Tentang

Halaman tentang adalah antarmuka yang berhubungan dengan biodata penulis. Halaman ini menampilkan nama, NPM, fakutas, program studi dan universitas. Gambar 4.3 adalah tampilan dari implementasi Tentang.

Gambar 4.3 Implementasi Tentang

4.2.4 Implementasi *Left Shifting*

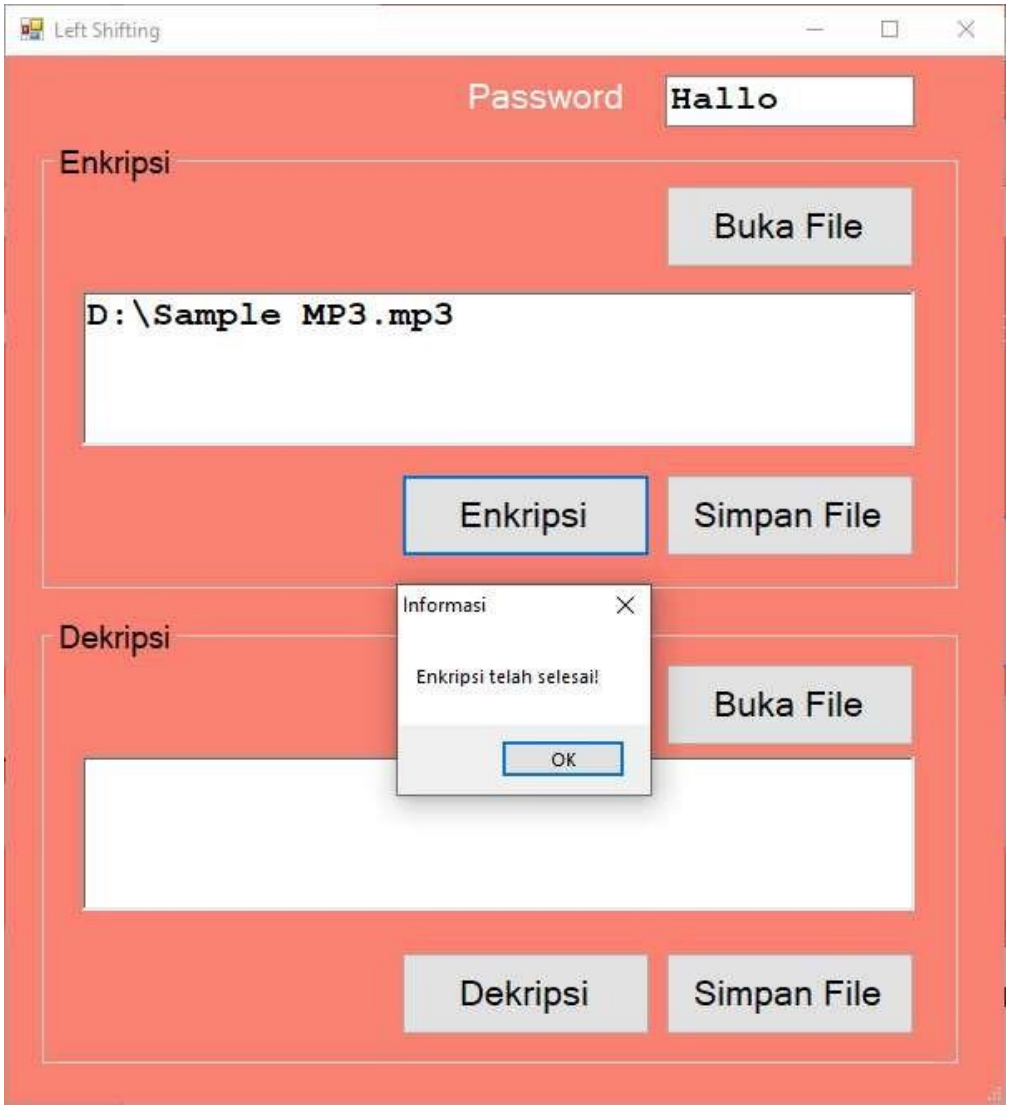
Antarmuka *Left Shifting* merupakan bagian dari program aplikasi yang berfungsi untuk melakukan enkripsi dan dekripsi file audio. Tampilan ini terdiri dari beberapa tombol yang akan melakukan fungsi masing-masing. Gambar 4.4 adalah hasil tampilan dari implementasi *Left Shifting*.



Gambar 4.4 Implementasi Left Shifting

4.2.5 Hasil Enkripsi *Left Shifting*

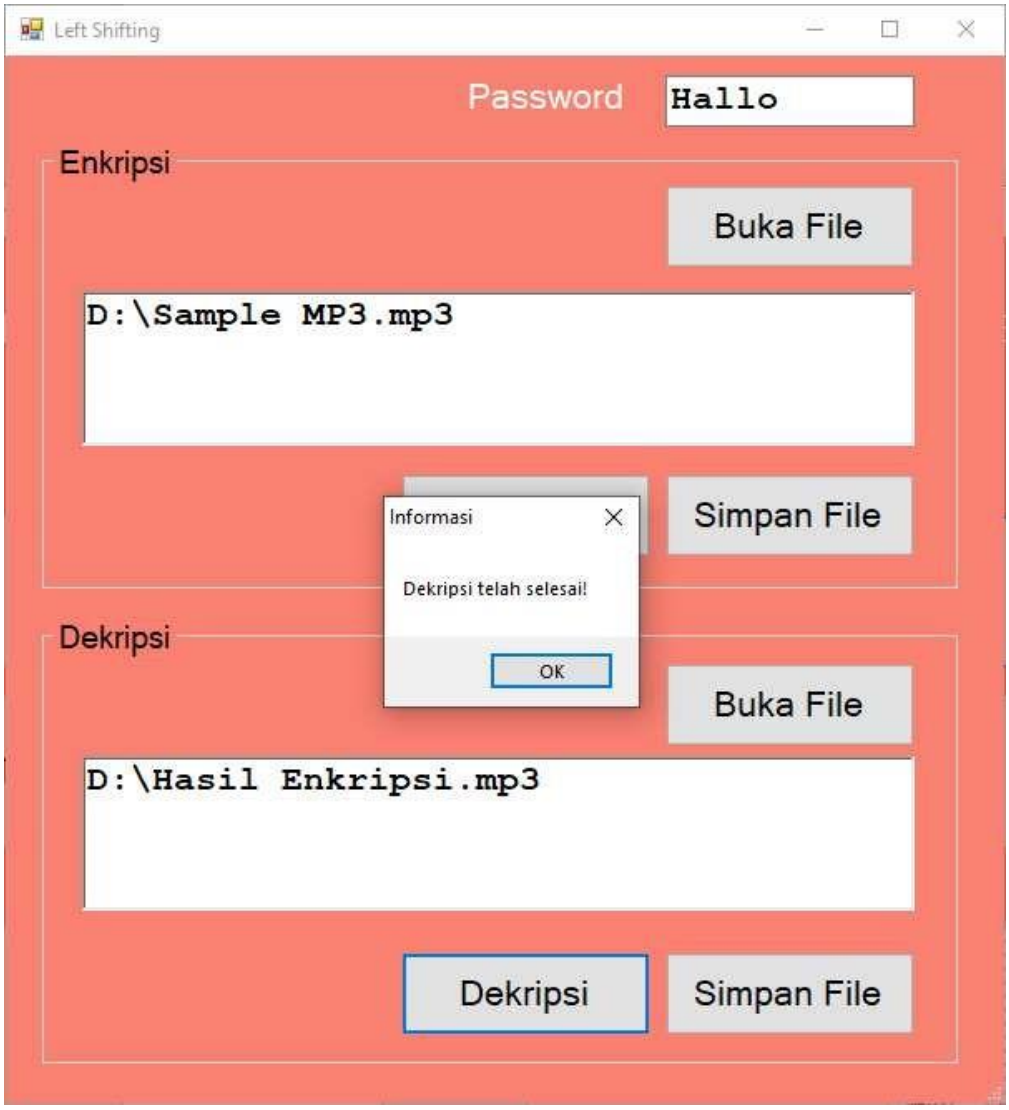
Gambar 4.5 adalah tampilan dari proses enkripsi dengan menggunakan *Left Shifting*. Pengguna dapat memasukkan *password* dan membuka file audio yang akan kemudian dienkripsi. Pengguna menekan tombol Enkripsi dan file hasil enkripsi dapat disimpan.



Gambar 4.5 Hasil perhitungan enkripsi Left Shifting

4.2.6 Hasil Dekripsi *Left Shifting*

Gambar 4.6 adalah tampilan dari proses dekripsi dengan menggunakan *Left Shifting*. Pengguna dapat memasukkan *password* dan membuka file terenkripsi yang akan kemudian didekripsi. Pengguna menekan tombol Dekripsi dan file hasil enkripsi dapat disimpan.



Gambar 4.6 Hasil dekripsi *Left Shifting*

BAB V

PENUTUP

5.1 Kesimpulan

Penulis menarik beberapa kesimpulan yang berhasil diambil dari hasil penelitian. Adapun kesimpulan yang diperoleh adalah antara lain:

1. *Left Shifting* melakukan pergeseran karakter pada file audio pada saat proses enkripsi dan dekripsi.
2. Password merupakan kunci yang dapat digunakan untuk membuka file audio yang sudah terenkripsi.
3. File audio yang dapat diproses adalah maksimal sebesar 5 MB.

5.2 Saran

Penulis juga mengajukan beberapa saran untuk mengembangkan penelitian ini. Adapun saran tersebut adalah antara lain:

1. Hendaknya file yang dapat diproses lebih dari 5MB.
2. Program aplikasi hendaknya dapat digunakan secara *online* dan berbasis *web* dan *mobile*.
3. Hendaknya file yang dapat diproses adalah selain file .MP3.

DAFTAR PUSTAKA

Andriani, Y., Ramli, N. M., Syamsumir, D. F., Kassim, M. N. I., Jaafar, J., Aziz, N. A., ... & Mohamad, H. (2019). Phytochemical analysis, antioxidant, antibacterial and cytotoxicity properties of keys and cores part of Pandanus tectorius fruits. Arabian Journal of Chemistry, 12(8), 3555-3564.

Ambrina Kundyanirum, Kodrat Iman Satoto, Oky Dwi Nurhayati. 2015. "*Sistem Informasi Geografis Pariwisata Kota Semarang"*. Jurnal Ilmiah Mahasiswa Universitas Diponegoro.

Dedi, dkk, 2015. "*Sistem Pendukung Keputusan Pemberian Beasiswa Untuk Menentukan Mahasiswa Berprestasi Berbasis Web dengan Metode AHP"*. Jurnal Dosen STMIK Bina Sarana Global Tanggerang – Banten.

Fachri, B., & Surbakti, R. W. (2021). Perancangan Sistem Dan Desain Undangan Digital Menggunakan Metode Waterfall Berbasis Website (Studi Kasus: Asco Jaya). JOURNAL OF SCIENCE AND SOCIAL RESEARCH, 4(3), 263-267.

Fahmy, Umar. 2015. "*Sistem Pendukung Keputusan Pemilihan Laptop Metode Fuzzy Database Model Tahani Berbasis Web"*. Jurnal Mahasiswa Jurusan Teknik Informatika STMIK PPKIA Pradnya Paramita.

Jogiyanto, Hartono. 2015. "*Analisis & desain sistem informasi : pendekatan terstruktur teori dan praktek aplikasi bisnis"*. Yogyakarta : Penerbit Andi.

Katen, Drs. 2014. "*Sistem Pendukung Keputusan Penentuan Beasiswa (PPA dan BBM) Dengan Metode Simple Additive Weighting (Study Kasus AKBID Kholisaturrahmi Binjai)"*. Jurnal Ilmiah Mahasiswa STMIK Kaputama Binjai.

Maulina, D., Sumitro, S. B., Amin, M., & Lestari, S. R. (2019). Lectin Protein Spodoptera litura Activity After Exposured by Biopesticide from Mirabilis jalapa. International Journal of Applied Biology, 3(1), 62-69.

Minarni. 2015. "*Sistem Informasi Inventory Obat Pada Rumah Sakit Umum Daerah (RSUD) Padang"*. Jurnal Jurusan Teknik Informatika.

Novita, Nanda. 2016. "Metode Fuzzy Tsukamoto Untuk Menentukan Beasiswa". Jurnal & Penelitian Teknik Informatika Universitas Sumatera Utara.

Prayogi, Agus 2018. "Sistem Pendukung Keputusan Untuk Penentuan Jumlah Produksi Nanas Menggunakan Metode Fuzzy Tsukamoto (Studi kasus PT.Great Giant Pineapple)". Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Brawijaya.

Putra, R. R., Hamdani, H., Aryza, S., & Manik, N. A. (2020). Sistem Penjadwalan Bel Sekolah Otomatis Berbasis RTC Menggunakan Mikrokontroler. Jurnal Media Informatika Budidarma, 4(2), 386-395.

Rulia, Puji Hastanti, dkk. 2013. "*Sistem Penjualan Berbasis WEB (E-Commerce) pada Tato Distro Kabupaten Pacitan"*. Jurnal Mahasiswa Ilmu Komputer Universitas UNSA Surakarta Solo.