RANCANG BANGUN APLIKASI PENGAMANAN DATA MENGGUNAKAN METODE SYMMETRIC STREAM CHIPHER

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	**: REZTIA RUZIENDY**
NPM	**: 1514370519**
PROGRAM STUDI	**: SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

LEMBAR PENGESAHAN

RANCANG BANGUN APLIKASI PENGAMANAN DATA MENGGUNAKAN METODE SYMMETRIC STREAM CHIPHER

DISUSUN OLEH :

NAMA : REZTIA RUZIENDY

N.P.M : 1514370519

PROGRAM STUDI : SISTEM KOMPUTER

Skripsi telah disetujui oleh Dosen Pembimbing Skripsi
Pada tanggal :

Dosen Pembimbing I	Dosen Pembimbing II
Leni Marlina, S.Kom., M.Kom	**Raja Fuad Nasrul, S.Kom., M.Kom**

Mengetahui,

Dekan Fakultas Sains Dan Teknologi	Ketua Program Studi
Sri Shindi Indira, S.T., M.Sc	**Eko Hariyanto, S.Kom., M.Kom**

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 JUDUL TESIS / SKRIPSI / TUGAS AKHIR*

ya yang bertanda tangan di bawah ini :

ama Lengkap	: REZTIA RUZIENDY
empat/Tgl. Lahir	: Medan / 09 Desember 1997
omor Pokok Mahasiswa	: 1514370519
ogram Studi	: Sistem Komputer
nsentrasi	: Keamanan Jaringan Komputer
mlah Kredit yang telah dicapai	: 141 SKS, IPK 3.40
omor Hp	: 085359590772
engan ini mengajukan judul sesuai bidang ilmu sebagai berikut	:

No.	Judul
1.	Rancang Bangun Aplikasi Pengamanan Data Menggunakan Metode Symmetric Stream Chipher.

an : Diisi Oleh Dosen Jika Ada Perubahan Judul

et Yang Tidak Perlu

Rektor

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

Medan, 26 Maret 2019
Pemohon,

(Reztia Ruziendy)

Tanggal : .....
Disahkan oleh :
Dekan

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

Tanggal : 26-3-2019
Disetujui oleh :
Dosen Pembimbing I :

(Leni Marlina, S.Kom., M.Kom)

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

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

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

(RAJA NASRUL FUAD, S.KOM., M.KOM)

Telah Diperiksa oleh LPMU
dengan Plagiarisme..... 51 %
Medan 17 OKTOBER 2019
AN. KA. LPMU
THARMIZI HAKIM
Cahyo Pramono, SE,MM

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau

Medan, 17 Oktober 2019
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

Telah di terima
berkas persyaratan
dapat di proses
Medan, 18/10/2019
Ka. BPAA
an.
FEGUH WAHYONO, SE., MM

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	: REZTIA RUZIENDY
Tempat/Tgl. Lahir	: Medan / 9 desember 1997
Nama Orang Tua	: RUKMANTO
N. P. M	: 1514370519
Fakultas	: SAINS & TEKNOLOGI
Program Studi	: Sistem Komputer
No. HP	: 085359590772
Alamat	: Jl. Pasar XIII Perumahan Mutiara biru

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul Rancang Bangun Aplikasi Pengamanan Data Menggunakan Metode Symmetric Stream Chipher., 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.	1,605,000
			2.875.000
			~~4.580.000~~
			4.580.000

UK 50%

Wendy 18/10/19

Ukuran Toga : M

Diketahui/Disetujui oleh :
Sri Shindi Indira, S.T.,M.Sc.
Dekan Fakultas SAINS & TEKNOLOGI

Hormat saya
REZTIA RUZIENDY
1514370519

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.

TANDA BEBAS PUSTAKA
No. 905/PERP/BP/2019
Telah diperiksa tidak ada sangkut paut dengan UPT Perpustakaan
Medan 17 OCT 2019
Kepala UPT Perpustakaan
UNIVERSITAS PEMBANGUNAN PANCA BUDI
UNPAB INDONESIA
UPT. PERPUSTAKAAN
M. Muttaqin, S.kom, M.kom

KKM CENTER
PANCA BUDI
18/10-2019

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	:	REZTIA RUZIENDY
N.P.M.	:	1514370519
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, 17 Oktober 2019
Ka. Laboratorium

AN

Fachrid Wadly, S.Kom

Plagiarism Detector v. 1092 - Originality Report:

Analyzed document: 13/08/2019 08:40:07

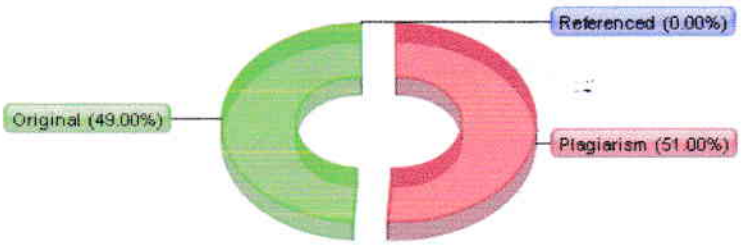
"REZTIA RUZIENDY_1514370519_SISTEM KOMPUTER.doc"

Licensed to: **Universitas Pembangunan Panca Budi_License4**

UNIVERSITAS PEMBANGUNAN PANCA BUDI
Beriman, Berilmu, Berkarya

LEMBAGA PENJAMIN MUTU UNIVERSITAS UNPAB UNIVERSITAS PEMBANGUNAN PANCA BUDI 17/10-19

Relation chart:



Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

Top sources of plagiarism:

% 208	wrds: 23040	http://repository.usu.ac.id/bitstream/handle/123456789/67879/Appendix.pdf?sequence=7&i...
% 57	wrds: 6082	http://www.cyberforum.ru/visual-basic/thread291922.html
% 37	wrds: 3786	https://www.frmtr.com/visual-basic/2961035-dev-paylasim-dosya-saklama-ve-sifreleme.html

Show other Sources:]

Processed resources details:

377 - Ok / 82 - Failed

Show other Sources:]

Important notes:

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

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

ersitas : Universitas Pembangunan Panca Budi
ltas : SAINS & TEKNOLOGI
n Pembimbing I : LENI MARLINA, S.KOM, M.KOM
n Pembimbing II : RAJA NASRUL FUAD, S.Kom., M.Kom
a Mahasiswa : REZTIA RUZIENDY
san/Program-Studi : Sistem Komputer
or Pokok Mahasiswa : 1514370519
ang Pendidikan : S1
l Tugas Akhir/Skripsi : RANCANG BANGUN APLIKASI PENGAMANAN DATA MENGGUNAKAN METODE SYMMETRIC STREAM CHIPHER

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
02. 2019	perbaiki Bab I. penulisan Seminar dgn panduan yg baru.	Leni	
	Acc Seminar proposal.	Leni	
03. 2019	lanjutkan ke Bab II dan III	Leni	
04. 2019	tambahkan teori tdg Data, Aplikasi dan algoritma.	Leni	
	Buat desain/tampilan program.		
04. 2019	perbaiki Bab II	Leni	
05. 2019	perbaiki Bab III	Leni	
05. 2019	lanjut Bab Implementasi.	Leni	
06. 2019	Buat Evaluasi dan aplikasi.	Leni	
	lanjut Bab V dan lengkapi semua.	Leni	
07. 2019	Acc seminar Hasil.	Leni	
10. 2019	Acc Sidang	Leni	
11. 2019	Acc jilid.	Leni	

Medan, 04 Februari 2019
Diketahui/Disetujui oleh :
Dekan,

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

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

ersitas : Universitas Pembangunan Panca Budi
ltas : SAINS & TEKNOLOGI
n Pembimbing I : Leni Marlina, S.Kom, M.Kom
n Pembimbing II : Raja Nasrul Fuad, S.Kom, M.Kom
a Mahasiswa : REZTIA RUZIENDY
san/Program Studi : Sistem Komputer
or Pokok Mahasiswa : 1514370519
ng Pendidikan : S1
l Tugas Akhir/Skripsi : Rancang Bangun Aplikasi Pengamanan Data Menggunakan Metode Symmetric Stream Chipher

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
7/10/19	Acc Sidang		
8/11/19	Acc Jilid		

Medan, 17 Oktober 2019
Diketahui/Disetujui oleh :
Dekan,

UNPAB INDONESIA

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

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

ersitas : **Universitas Pembangunan Panca Budi**
ultas : **SAINS & TEKNOLOGI**
en Pembimbing I : LENI MARLINA, S.Kom., M.Kom
en Pembimbing II : RAJA NASRUL FUAD, S.Kom., M.Kom
a Mahasiswa : **REZTIA RUZIENDY**
san/Program Studi : **Sistem Komputer**
or Pokok Mahasiswa : 1514370519
ang Pendidikan : S1
l Tugas Akhir/Skripsi : RANCANG BANGUN APLIKASI PENGAMANAN DATA MENGGUNAKAN METODE SYMMETRIC STREAM CHIPHER

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
0.02.2019	Perbaiki latar belakang		
26.03.2019	Acc Seminar		
5.04.2019	Lanjut Bab II & buat D. Pustaka		
3.04.2019	Acc Bab II.		
03.05.2019	Perbaiki Bab III		
4.05.2019	Acc Bab III		
5.06.2019	Lanjut Bab IV		
05.07.2019	Acc Bab IV Lanjut Bab V dan lengkapi semua		
6.07.2019	Acc Seminar Hasil		

Medan, 04 Februari 2019
Diketahui/Disetujui oleh :
Dekan,

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

yang tidak perlu

PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di perguruan tinggi, dan sepanjang pengetahuan saya juga terdapat karya atau pendapat yang pernah ditulis atau diterbitkan orang lain, kecuali yang secara tertulis diacu dalam skripsi ini dan disebutkan dalam daftar pustaka.

Medan, 20 November 2019

Reztia Ruziendy
1514370519

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama	: Reztia Ruziendy
NPM	: 1514370519
Prodi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer
Judul Skripsi	: RANCANG BANGUN APLIKASI PENGAMANAN DATA MENGGUNAKAN METODE SYMMETRIC STREAM CHIPHER

Dengan ini menyatakan bahwa :

1. Tugas Akhir/Skripsi saya bukan hasil Plagiat
2. Sayat tidak akan menuntut perbaikan nilai indeks Prestasi Kumulatif (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, 14 November 2019

Yang membuat pernyataan

ABSTRAK

REZTIA RUZIENDY

Rancang Bangun Aplikasi Pengamanan Data Menggunakan Metode *Symmetric Stream Chipher*

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika pengirimannya dilakukan melalui jaringan publik, apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan diketahui isi informasinya oleh orang yang tidak berhak. Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan sistem kriptografi yaitu dengan menyandikan isi informasi *(plaintext)* tersebut menjadi isi yang tidak dipahami melalui proses enkripsi dan untuk memperoleh kembali informasi yang asli, dilakukan proses dekripsi, disertai dengan menggunakan kunci yang benar. Penelitian ini bertujuan untuk menghasilkan aplikasi kriptografi pengamanan data dengan menerapkan metode *symmetric stream cipher*. Aplikasi kriptografi dibuat menggunakan bahasa pemrograman *Visual Basic Net* dan di bantu dengan bantuan *Visual Basic Editor Visual Studio* 2010 maka dapat dihasilkan sebuah perangkat aplikasi kriptografi pengamanan data dengan menerapkan metode *symmetric stream chipher*.

Kata Kunci : Aplikasi, Kriptografi, *Symmetric Stream Chipher*

DAFTAR ISI

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika pengirimannya dilakukan melalui jaringan publik, apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan diketahui isi informasinya oleh pihak-pihak yang tidak berhak. Data asli yang akan dikirim atau disimpan disebut *plaintext*, merupakan data yang dapat dibaca dan dimengerti baik oleh orang atau komputer. Sedangkan data yang tidak terbaca, baik oleh manusia atau mesin disebut cipher teks. Sebuah sistem atau produk yang menyediakan enkripsi dan dekripsi disebut kriptografi.

Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan sistem kriptografi yaitu dengan menyandikan isi informasi (*plaintext*) tersebut menjadi isi yang tidak dipahami melalui proses enkripsi dan untuk memperoleh kembali informasi yang asli, dilakukan proses dekripsi, disertai dengan menggunakan kunci yang benar. Namun, sejalan dengan perkembangan ilmu penyandian atau kriptografi, usaha-usaha untuk memperoleh kunci tersebut dapat dilakukan oleh siapa saja, termasuk pihak yang tidak sah untuk memiliki informasi tersebut. Oleh karena itu, penelitian tentang kriptografi akan selalu berkembang untuk memperoleh algoritma

kriptografi yang makin kuat, sehingga usaha-usaha untuk memecah kode kriptografi secara tidak sah menjadi lebih sulit (Dedek dan Ginting, 2017).

Berdasarkan latar belakang diatas, penulis mengangkat tema penelitian dengan judul "**Rancang Bangun Aplikasi Pengamanan Data Menggunakan Metode *Symmetric Stream Chipher***".

1.2 PerumusanMasalah

Adapun perumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana merancang aplikasi pengamanan data dengan menerapkan metode *symmetric stream chipher*?
2. Bagaimana proses kerja *Symmetric Stream Chipher*?

1.3 BatasanMasalah

Karena keterbatasan waktu dan pengetahuan penulis, maka ruang lingkup permasalahan dalam merancang perangkat lunak ini antara lain :

1. Panjang kunci dibatasi minimal 5 karakter dan maksimal 43 karakter.
2. Panjang PCC *(private crypto code)* dibatasi maksimal 22 karakter.
3. Kunci, *Plaintext* dan *chiphertext* yang berfungsi sebagai data *input* bertipe data *string* (*text*).
4. Bahasa pemrograman yang digunakan untuk membuat aplikasi pengamanan data teks adalah dengan menggunakan *Visual Basic Net.*

5. Data yang diamankan berupa data pesan.
6. Kapasitas data pesan yang diamankan maksimal besarnya sekitar 1 megabyte.

1.4 Tujuan Penelitian

Tujuan yang diambil dari penulisan skripsi ini adalah :

1. Untuk mengetahui proses kerja *Symmetric Stream Chipher*.
2. Untuk merancang aplikasi proses penyandian data teks dengan menerapkan metode *Symmetric Stream Chipher*.

1.5 ManfaatPenelitian

Manfaat yang diambil dari penulisan skripsi ini adalah :

1. Untuk melindungi proses penyandian data agar tidak dapat di baca oleh orang-orang yang tidak berhak..
2. Mencegah agar orang-orang yang tidak berhak, mengubah atau menghapus data penyandian.

BAB II

LANDASAN TEORI

2.1 Pengertian Aplikasi

Secara istilah pengertian aplikasi adalah suatu program yang siap untuk digunakan yang dibuat untuk melaksanankan suatu fungsi bagi pengguna jasa aplikasi serta penggunaan aplikasi lain yang dapat digunakan oleh suatu sasaran yang akan dituju. Menurut kamus computer eksekutif, aplikasi mempunyai arti yaitu pemecahan masalah yang menggunakan salah satu tehnik pemrosesan data aplikasi yang biasanya berpacu pada sebuah komputansi yang diinginkan atau diharapkan maupun pemrosesan data yang di harapkan. Pengertian aplikasi menurut Kamus Besar Bahasa Indonesia, "Aplikasi adalah penerapan dari rancang sistem untuk mengolah data yang menggunakan aturan atau ketentuan bahasa pemrograman tertentu **(Juansyah, 2015 : 2)**.

2.2 Pengertian Data

Data adalah sebagai bahan keterangn tentang kejadian nyat atau fakta-fatkat yang dirumuskan dalam sekelompok lambang tertentu yang tidak acak yang menunjukan jumlah, tindakan, atau hal". Data dapat perupa catatan-catatan dalam kertas, buku, atau tersimpan sebagai file dalam basis data **(Hermansyah, 2012 : 14)**.

2.3 Pengertian Logika dan Algoritma

Pengertian algoritma sangat lekat dengan kata logika, yaitu kemampuan seorang manusia untuk berfikir dengan akal tentang suatu permasalahan menghasilkan sebuah kebenaran, dibuktikan dan dapat diterima akal, logika seringkali dihubungkan dengan kecerdasan, seseorang yang mampu berlogika dengan baik sering orang menyebutnya sebagai pribadi yang cerdas. **(Tumpal, 2016 : 85-86)**.

Logika identik dengan masuk akal dan penalaran.Penalaran adalah salah satu bentuk pemikiran.Pemikiran adalah pengetahuan tak langsung yang didasarkan pada pernyataan langsung pemikiran mungkin benar dan mungkin juga tak benar.Definisi logika sangat sederhana yaitu ilmu yang memberikan prinsip-prinsip yang harus diikuti agar dapat berfikir valid menurut aturan yang berlaku.Pelajaran logika menimbulkan kesadaran untuk menggunakan prinsip-prinsip untuk berfikir secara sistematis.Logika berasal dari dari bahasa Yunani yaitu LOGOS yang berarti ilmu. Logika dapat diartikan ilmu yang mengajarkan cara berpikir untuk melakukan kegiatan dengan tujuan tertentu. Algoritma berasal dari nama seorang Ilmuwan Arab yang bernama Abu JafarMuhammad Ibnu Musa Al Khuwarizmi penulis buku berjudul Al Jabar Wal Muqabala. Kata Al Khuwarizmi dibaca orang barat menjadi Algorism yang kemudian lambat laun menjadi Algorithm diserap dalam bahasa Indonesia menjadi Algoritma.

Logika identik dengan masuk akal dan penalaran.Penalaran adalah salah satu bentuk pemikiran. Pemikiran adalah pengetahuan tak langsung yang didasarkan pada pernyataan langsung pemikiran mungkin benar dan mungkin juga

tak benar.Definisi logika sangat sederhana yaitu ilmu yang memberikan prinsip-prinsip yang harus diikuti **(Tumpal, 2016 : 85-86)**.

2.4. 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. 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 terminology **(Pabokory, 2015 : 22)**.

Beberapa istilah yang harus diketahui yaitu :

1. Pesan, Plainteks, dan Cipherteks

   Pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah (*plaintext*) atau teksjelas (*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.

3. Enkripsi dan dekripsi Proses menyandikan plainteks menjadi *cipherteks* disebut enkripsi (*encryption*) atau *enciphering* (standard nama menurut ISO 7498-2). Sedangkan proses mengembalikan *cipherteks* menjadi *plainteks* semula disebut dekripsi (*decryption*) atau *deciphering* (standard nama menurutISO 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 yangberbeda 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 *cipherteks*. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara dua himpunan tersebut.

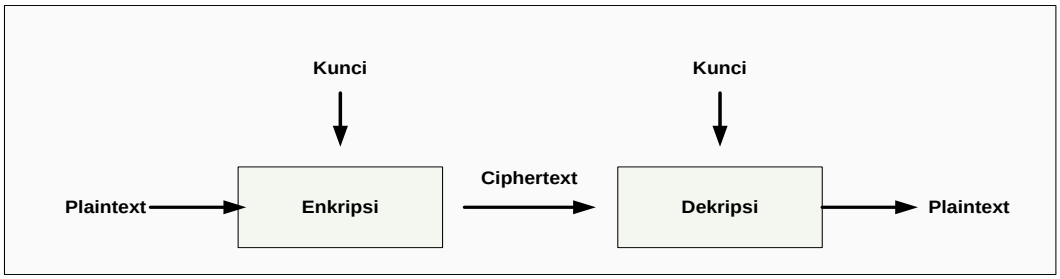
   Misalkan P menyatakan plainteks dan C menyatakan cipherteks,maka :

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

   D(C) =P →fungsi dekripsi Dmemetakan C ke P

   Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesanasal, maka persamaan D(E(P)) = P harusbenar.Kriptografi mengatasimasalah keamanan data dengan menggunakankunci, yang dalam hal inialgoritma tidak dirahasiakan lagi, tetapi kunci harus tetap dijagakerahasiaannya. 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 diperlihatkan pada Gambar 2.1.



Gambar 2.1.Skema enkripsi dan dekripsi dengan menggunakan kunci.
Sumber : (Pabokory, 2015 : 22)

2.5. Sejarah Kriptografi

Sejarah kriptografi sebagian besar merupakan sejarah kriptografi klasik, yaitu metode enkripsi yang menggunakan kertas dan pensil atau mungkin dengan bantuan alat mekanik sederhana. Secara umum algoritma kriptografi klasik dikelompokkan menjadi dua kategori, yaitu algoritma transposisi (*transposition cipher*) dan algoritma substitusi (*substitution cipher*). *Cipher* transposisi mengubah susunan huruf-huruf di dalam pesan, sedangkan *cipher* substitusi mengganti setiap huruf atau kelompok huruf dengan sebuah huruf atau kelompok huruf lain **(Pabokory, 2015)**.

2.6. Tujuan Kriptografi

Dari paparan awal dapat dirangkumkan bahwa kriptografi bertujuan untuk member layanan keamanan. Yang dinamakan aspek-aspek keamanan:

1. Kerahasiaan (*confidentiality*)

   Adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.

2. Integritas data (*data integrity*) adalah layanan yang menjamin bahwa pesan masih asli atau belum pernah dimanipulasi selama pengiriman.
3. Otentikasi (*authentication*) adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak - pihak yang berkomunikasi(*user autehentication*).
4. *Non-repudiation*adalah layanan untuk menjaga entitas yang berkomunikasi melakukan penyangkalan **(Pabokory, 2015: 22)**.

2.7. Jenis-jenis Algoritma Kriptografi

Algoritma kriptografi dibagi dua, yaitu algoritma simetri (menggunakan satu kunci), algoritma asimetri (menggunakan dua kunci berbeda untuk proses enkripsi dan dekripsi)

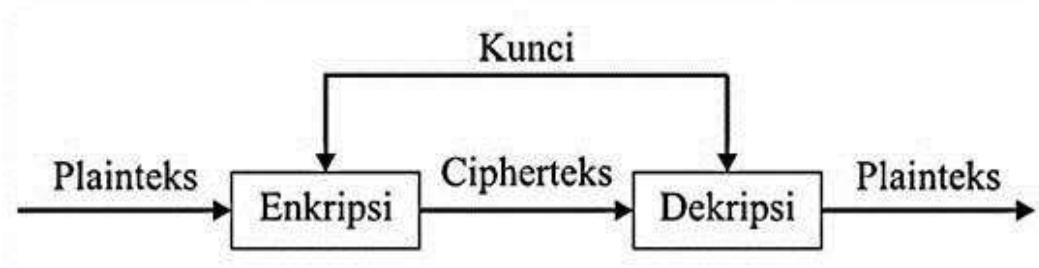
1. Algoritma Simetris

Dimana kunci yang digunakan pada proses enkripsi dan dekripsi adalah kunci yang sama. Dalam kriptografi kunci simetris dapat diasumsikan bahwa si penerima dan pengirim pesan telah terlebih dahulu berbagi kunci sebelum pesan dikirimkan.Keamanan dari sistem ini terletak pada kerahasiaan kuncinya.

Pada umumnya yang termasuk ke dalam kriptografi simetris ini beroperasi dalam mode blok (*block cipher*), yaitu setiap kali proses enkripsi atau dekripsi dilakukan terhadap satu blok data (yang berukuran tertentu), atau beroperasi dalam mode aliran (*stream cipher*), yaitu setiap kali enkripsi atau dekripsi dilakukan terhadap satu bit atau satu *byte* data.

Contoh algoritma simetris, yaitu : Trithemius, *Double Transposition Cipher,*DES (*Data Encryption Standard),* AES (*Advanced Encryption Standard)*

(Kamil, 2016). Proses dari skema kriptografi simetris dapat dilihat pada gambar 2.2.



Gambar 2.2. Skema Algoritma Simetris
Sumber :(Kamil, 2016)

Kelebihan kriptografi simetris adalah **(Kamil, 2016)** :

a. Proses enkripsi atau dekripsi kriptografi simetris membutuhkan waktu yang singkat.

b. Ukuran kunci simetris *relative* lebih pendek.

c. Otentikasi pengiriman pesan langsung dari *ciphertext* yang diterima, karena kunci hanya diketahui oleh penerima dan pengirim saja.

Kelemahan kriptografi simetris adalah **(Kamil, 2016)** :

a. Kunci simetris harus dikirim melalui saluran komunikasi yang aman, dan kedua entitas yang berkomunikasi harus menjaga kerahasiaan kunci.

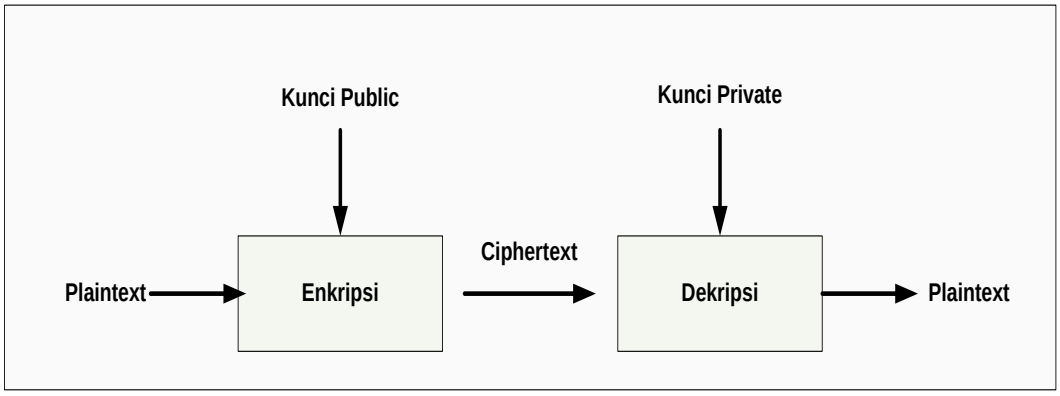
b. Kunci harus sering diubah, setiap kali melaksanakan komunikasi. Apabila kunci tersebut hilang atau lupa, maka pesan tersebut tidak dapat dibuka.

2. Algoritma Asimetris

Berbeda dengan kriptografi kunci simetris, kriptografi kunci public memiliki dua buah kunci yang berbeda pada proses enkripsi dan dekripsinya.

Dimana kunci yang digunakan untuk proses enkripsi atau sering disebut *public key* dan dekripsi atau sering disebut *private key* menggunakan kunci yang berbeda. Entitas pengirim akan mengenkripsi dengan menggunakan kunci *public*, sedangkan entitas penerima mendekripsi menggunakan kunci *private* **(Kamil, 2016)**.

Contoh algoritma asimetris, yaitu RSA (*Riverst Shamir Adleman)*, Knapsack, Rabin, ElGamal **(Munir, 2014)**.Skema dari kriptografi dapat dilihat pada gambar 2.3.



Gambar 2.3. Skema Algoritma Asimetris
Sumber : (Kamil, 2016)

Kelebihan kriptografi asimetris adalah **(Kamil,2016)** :

a. Hanya kunci *private* yang perlu dijaga kerahasiaannya oleh setiap entitas yang berkomunikasi. Tidak ada kebutuhan mengirim kunci *private* sebagaimana kunci simetri.
b. Pasangan kunci *private* dan kunci *public* tidak perlu diubah dalam jangka waktu yang sangat lama.
c. Dapat digunakan dalam pengaman pengiriman kunci simetris.

Kelemahan kriptografi asimetris adalah **(Kamil, 2016)** :

a. Proses enkripsi dan dekripsi umumnya lebih lambat dari algortima simetri, karena menggunakan bilangan yang besar dan operasi bilangan yang besar.

b. Ukuran *ciphertext* lebih besar dari *plaintext*.

c. Ukuran kunci relatif lebih besar daripada ukuran kunci simetris.

2.8. Algoritma *Symmetric Stream Cipher*

Algoritma yang dikembangkan pada metode *symmetric stream ciper* ini dapat menerima 2 jenis kunci yaitu kunci utama dan *PrivateCrypto Code* (kunci khusus yang hanya bisa dibuka yang memiliki kunci tersebut).

Stream cipher digunakan untuk mengenkripsi *plaintext* menjadi *ciphertext bit per bit* (1 bit setiap kali transformasi) atau *byte per byte* (1 karakter = 1 byte). *Stream cipher* pertama diperkenalkan oleh *Vernam* yang diadopsi dari *one-time pad cipher*, yaitu tiap karakter diganti dengan bit 0 atau 1 **(Putra,etal, 2017 : 263)**. *Ciphertext*atau proses enkripsi diperoleh dengan rumus:

ki = ci – pi

Sedangkan untuk proses dekripsi diperoleh rumus :

ki = pi – ci

Dimana

pi : bit *plainteks*

ci : bit *Cipherteks*

ki : bit kunci

2.9. Proses Pembentukan Kunci

Algoritma pembentukan kunci K1 adalah :

1. Variabel KEY1 diset dengan nilai dari kunci utama
2. Variabel KEYLen diset dengan panjang kunci utama
3. Matrix K1(0)..K1(462) direset dengan nilai menaik dari 0 sampai dengan 462
4. Mengacak K1(0)..K1(462) dengan rumus ”j=(j + K1(i) + KEY1(i Mod KEYLen)) Mod 463” sebanyak 463 kali.

Algoritma untuk pembentukan kunci K2 sebagai berikut:

a. KEY2(0..16) dibentuk dengan

```
For i = 0 To 463 - 1
KEY2(i Mod 17) = KEY2(i Mod 17) Xor (K1(i) And 255) Next
```

b. Mereset nilai dari K2(0..250)=0..250

c. Kemudian nilai K2 saling dipertukarkan dengan cara yang sama seperti K1 yaitu :

```
For i = 0 To 251 - 1
j = (j + K2(i) + KEY2(i Mod 17)) Mod 251
tmp = K2(i)
K2(i) = K2(j)
K2(j) = tmp
Next
```

2.10. Pembentukan *Dummy String*

Dummy String merupakan teks yang tambahan yang panjangnya random antara 16 sampai dengan 255 byte.

2.11. Unified Modelling Language (UML)

Menurut **Nugroho (2015 : 20)** "UML (*Unified Modeling Language*) adalah salah satu perkakas (tool) yang sangat bermanfaat untuk melakukan analisis dan perancangan sistem dalam konteks "pemrograman berorientasi objek" perangkat lunak yang berparadigma berorientasi objek. Pemodelan (*modeling*) sesungguhnya digunakan untuk penyederhanaan permasalahan-permasalahan yang kompleks sedemikian rupa sehingga lebih mudah dipelajari dan dipahami".

Penggunaan model ini bertujuan untuk mengidentifikasikan bagian-bagian yang termasuk dalam lingkup sistem yang dibahas dan bagaimana hubungan antara sistem dengan subsistem maupun sistem lain diluarnya.

1. Use Case Diagram

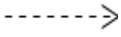
Use caseDiagram menggambarkan fungsi-fungsi sistem dari sudut pandang pengguna eksternal dan dalam sebuah cara yang mudah dipahami. *Use case* merupakan penyusunan kembali lingkup fungsional sistem yang disederhanakan lagi

Use case diagram merupakan suatu diagram yang berisi *use case*, *actor*, serta *relationship* diantaranya. *Use Case Diagram* dapat digunakan untuk kebutuhan apa saja yang diperlukan dalam suatu sistem, sehingga sistem dapat digambarkan dengan jelas bagaimana proses dari sistem tersebut, bagaimana cara

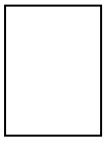
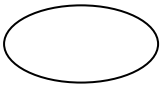
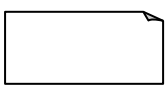
aktor menggunakan sistem, serta apa saja yang dapat dilakukan pada suatu sistem. **(Indrajani, 2015 : 30)**.

Menurut **Indrajani (2015 : 31)** adapun simbol dari *use case* adalah sebagai berikut :

Tabel 2.1. Simbol U*se CaseDiagram*

No	Simbol	Nama	Keterangan
1		*Actor*	Menspesifikasikan himpuan peran yang pengguna mainkan ketika berinteraksi dengan *use case*.
2		*Dependency*	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri *(independent)* akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri (*independent*).
3		*Generalization*	Hubungan dimana objek anak (*descendent*) berbagi perilaku dan struktur data dari objek yang ada di atasnya objek induk (*ancestor*).
4		*Include*	Menspesifikasikan bahwa *use case* sumber secara *eksplisit*.

Tabel 2.1 (Lanjutan)

No	Simbol	Nama	Keterangan
5		*Extend*	Menspesifikasikan bahwa *use case* target memperluas perilaku dari *use case* sumber pada suatu titik yang diberikan.
6		*Association*	Apa yang menghubungkan antara objek satu dengan objek lainnya.
7		*System*	Menspesifikasikan paket yang menampilkan sistem secara terbatas.
8		*Use Case*	Dekripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu *actor*.
9		*Collaboration*	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk menyediakan perilaku yang lebih besar dari jumlah dan elemen-elemennya (sinergi).
10		*Note*	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi.

Sumber : Indrajani (2015 : 31).

2. *Activity Diagram*

Activity diagram menurut **Indrajani (2015 : 37)** adalah salah satu cara untuk memodelkan *event-event*yang terjadi dalam suatu *use case*. Diagram ini juga dapat digantikandengan sejumlah teks.

Tabel 2.2. Simbol *Activity*Diagram

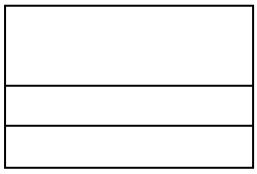
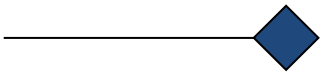
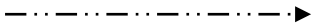
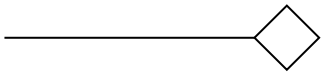
No	Gambar	Nama	Keterangan
1		*Actifity*	Memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain
2		*Action*	State dari sistem yang mencerminkan eksekusi dari suatu aksi
3		*Initial Node*	Bagaimana objek dibentuk atau diawali.
4		*Actifity Final Node*	Bagaimana objek dibentuk dan dihancurkan
5		*Fork Node*	Satu aliran yang pada tahap tertentu berubah menjadi beberapa aliran

Sumber : Indrajani (2015 : 38).

3. Class Diagram

Menurut **Indrajani (2015 : 35)**, *Class diagram* digunakan untuk menggambarkan perbedaan yang mendasar antara *clas*, hubungan antara *class*, dan di mana *sub-sistem class* tersebut. Simbol yang digunakan dalam *class diagram* adalah sebagai berikut :

Tabel 2.3.Simbol yang digunakan dalam *Class* Diagram.

Simbol	Nama	Fungsi
	*Class*	Menggambarkan *Class* baru pada diagram.
	Association	Menggambarkan relasi antar asosiasi
	*Composition*	Jika sebuah *class* tidak bisa berdiri sendiri dan harus merupakan bagian dari *class* yang lain, maka class tersebut memiliki relasi *Composition* terhadap *class* tempat dia bergantung tersebut.
	*Depedency*	Umumnya penggunaan *dependency* digunakan untuk menunjukkan operasi pada suatu *class* yang menggunakan *class* yang lain.
	*Aggregation*	*Aggregation* mengindikasikan keseluruhan bagian *relationship* dan biasanya disebut sebagai relasi.

Sumber : Indrajani (2015 : 35).

2.13 Perangkat Lunak Pengembang Sistem

Perangkat lunak yang digunakan untuk pengembangan sistem pakar ini adalah dengan menggunakan bahasa pemrograman *PHP* dan *web databaseMySQL*yang berbasis *web*.

1. MySQL

Menurut Fahmy Umar (2015) "*MySQL* adalah sebuah bentuk *database* yang berjalan sebagai *server*, tidak meletakkan *database* tersebut dalam satu mesin dengan aplikasi yang digunakan, sehingga dapat meletakkan sebuah database pada sebuah mesin khusus dan dapat diletakkan ditempat yang jauh komputer pengaksesannya. *MySQL* merupakan *database* yang sangat kuat dan cukup stabil digunakan sebagai media penyimpanan data.*MySQL* adalah salah satu *databasemanajementsystem*dari sekian banyak *DBMS* seperti *Oracle*, *MS SQL, Postgre SQL*, dan lainnya".

a. Standarisasi MySQL

Standarisasi *MySQL* dimulai pada tahun 1986, ditandai dengan dikeluarkannya standar *SQL* oleh *ANSI*. Standar ini sering disebut dengan *SQL86*. Standar tersebut kemudian diperbaiki pada tahun 1989 kemudian diperbaiki lagi pada tahun 1992. Versi terakhir dikenal dengan *SQL92*. Pada tahun 1999 dikeluarkan standarbaru yaitu *SQL99*, akan tetapi kebanyakan implementasi mereferensi pada *SQL92*.

b Perintah Dasar MySQL

Beberapa perintah dasar MySQL yang sering digunakan adalah sebagai berikut :

1) Membuat Database

Untuk membuat database digunakan sintaks :

```
CREATE DATABASE NAMA_DATABASE ;
```

Contoh :

```
mysql>CREATE DATABASE Mahasiswa ;
```

```
mysql>USE NAMA_DATABASE ;
```

2) Membuat Tabel

Untuk membuat tabel digunakan sintaks :

```
CREATE TABLE NAMA_TABEL(field spesifikasi_field,…);
```

Contoh :

```
mysql>CREATE TABLE biodata (nama VARCHAR(50), npm
VARCHAR(10),
->alamat VARCHAR(50),jnskelamin CHAR(1),tgllahir
date);
```

3) Menampilkan Tabel

```
mysql>SHOW TABLES;
+---------------------+
| Tables in menagerie |
+---------------------+
| biodata             |
+---------------------+
```

4) Menyimpan Data

Untuk menyimpan data dalam tabel digunakan sintaks :

INSERT INTO NAMA_TABEL **VALUES(‘data_kolom1’,’data_kolom2’,…) ;**

Contoh :

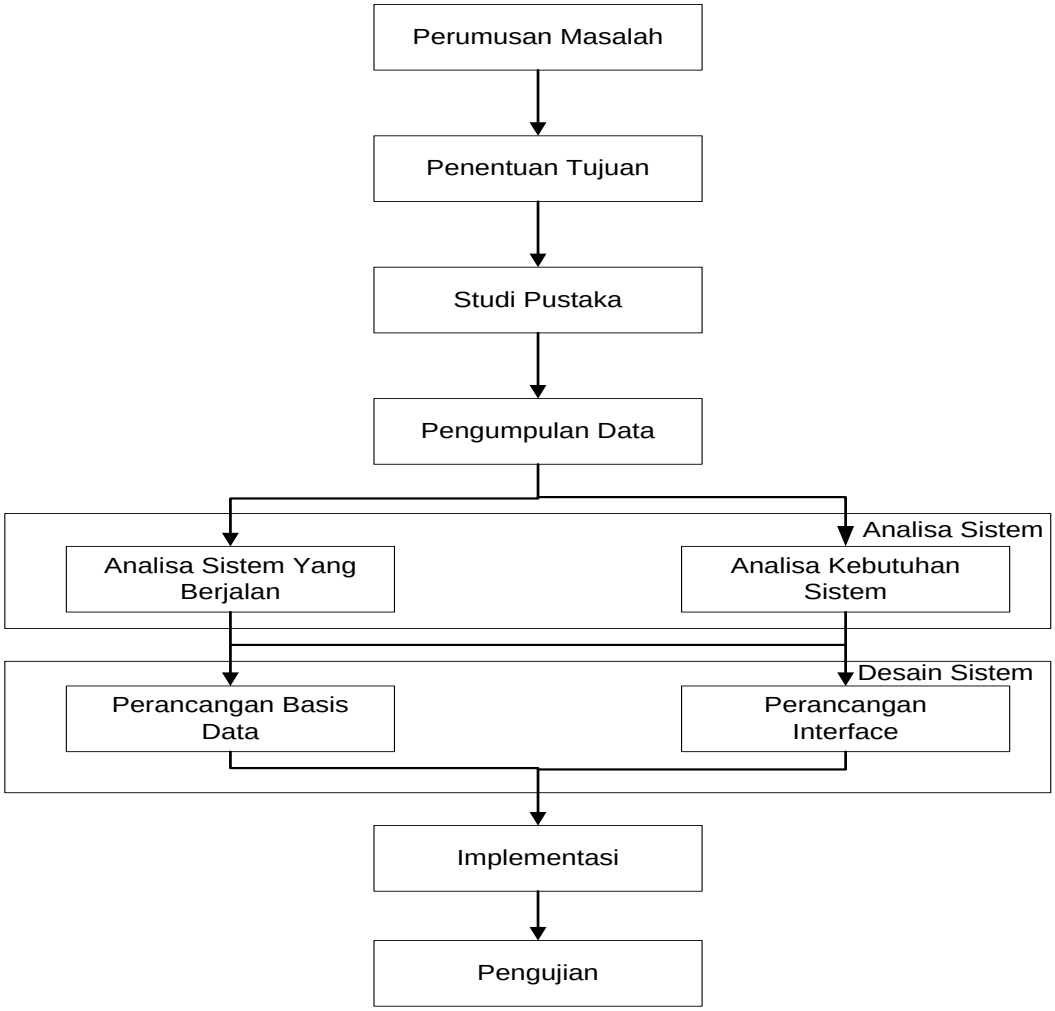
```
mysql>INSERT INTO biodata
->VALUES ('yudi','0514373062','Jl.Gatot
Subroto','L','13-12-1987’);
```

BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Adapun tahapan penelitian yang akan dilakukan dalam penulisan skripsi ini adalah sebagai berikut :



Gambar 3.1 Tahapan Penelitian

3.2 Metode Pengumpulan Data

Agar mendapat keterangan-keterangan data yangdiperlukanguna memperoleh suatu pembenaran ilmiah, maka penulis melakukan penelitian dengan metode penelitian sebagai berikut:

1. Studi Kepustakaan (*library search*)

   Untuk mendapatkan hasil teori yang valid untuk dijadikan sebuah landasan, penulis mencari beberapa buku referensi dari beberapa perpustakaan.

2. Pengumpulan data melalui*surfing* (*fieldresearch*) Pencarian atau penjelajahan melalui *internet*.

3. AnalisaSistem

   Menganalisis atau mendefinisikan solusi untuk sistem informasi dan proses organisasi.

4. Perancangansistem merancang*input*, *output*, struktur file, *program*, prosedur, perangkat keras dan perangkat lunak yang diperlukan untuk mendukung sisteminformasi.

5. Pengujian Sistem

   Membangun perangkat lunak yang diperlukan untuk mendukung sistem dan melakukan testing secara akurat.

6. ImplementasiSistem

   Beralih dari sistem lama ke sistem baru, melakukan pelatihan dan panduan seperlunya.

7. Penulisan LaporanPenelitian Ini adalah tahap akhir dari penelitian.

3.3 Analisis Sistem

Analisis sistem sejenis digunakan untuk membandingkan aplikasi pengamanan data menggunakan metode *symmetric stream chipher* yang sudah ada dengan skripsi yang akan dibuat. Tujuan membandingkan aplikasi pengamanan data menggunakan metode *symmetric stream chipher* ini adalah untuk menambah kebutuhan yang masih kurang dari aplikasi pengamanan data menggunakan metode *symmetric stream chipher* sejenis yang sudah ada. Berdasarkan deskripsi sistem lama yang telah dijelaskan pada analisis sistem saat ini dan analisis sistem sejenis, ada beberapa permasalahan dari sistem yang sudah ada, yaitu belum tersedianya aplikasi pengamanan data menggunakan metode *symmetric stream chipher* menggunakan *Visual Basic.net*

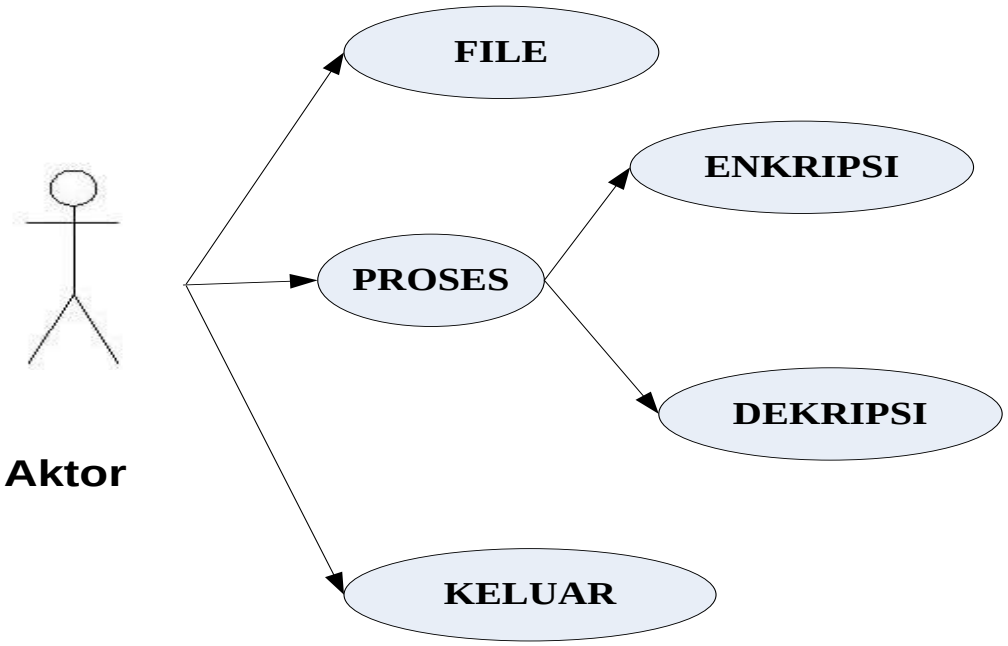
3.4 Sistem Yang Diusulkan

Perancangan sistem adalah suatu upaya untuk membuat suatu sistem yang baru atau memperbaiki sistem yang lama secara keseluruhan atau memperbaiki sistem yang telah ada. Tujuan dari perancangan sistem adalah untuk memenuhi kebutuhan*user* (pemakai) mengenai gambaran yang jelas tentang perancangan aplikasi pengamanan data menggunakan metode *symmetric stream chipher* yang akan dibuat serta diimplementasikan. Desain sistem secara umum mengidentifikasikan komponen-komponen sistem yang akan didesain secara terinci. Desain terinci dimaksudkan untuk pemrogram komputer dan ahli teknik lainnya yang akan mengimplementasikan sistem. Alat bantu perancangan yang digunakan adalah *UML (Unified Modeling Language)* Yaitu :.

1. *Use Case Diagram*

Use Case Diagram digunakan untuk mengetahui secara jelas tentang gambaran isi dari aplikasi perangkat lunak ini yang mana menu utama dijadikan sebagai tingkatan tertinggi dalam struktur.

Pada menu utama terdapat pilihan menu utama yang terdiri dari dua jenis menu yaitu menu file dan proses serta menu keluar.

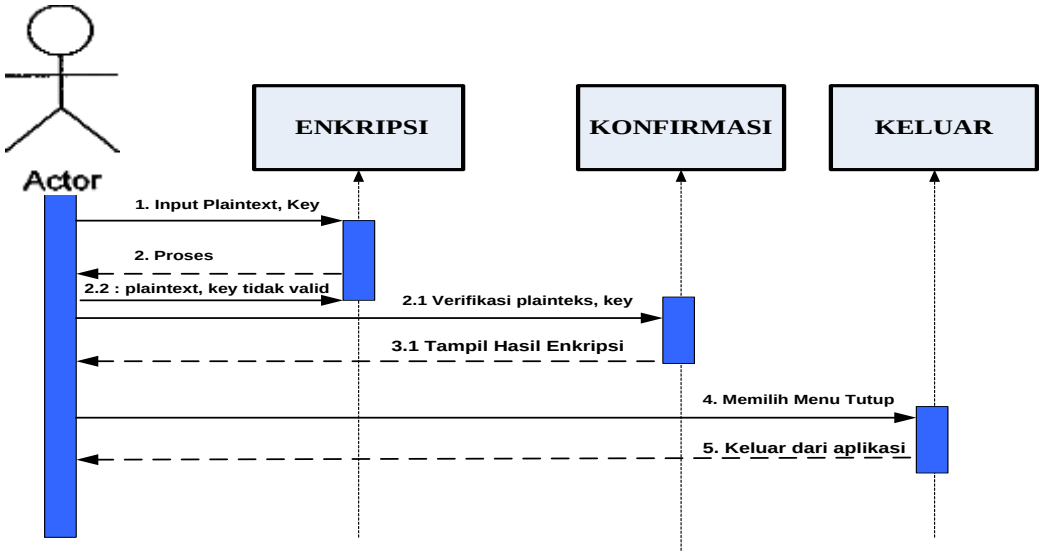


Gambar 3.2 : *Use Case* Diagram Aplikasi Kriptografi Metode Symmetric Cipher

Aktor dapat mengakses menu utama yang terdiri dari tiga menu file, menu proses dan menu keluar

2. *Sequence Diagram Enkripsi*

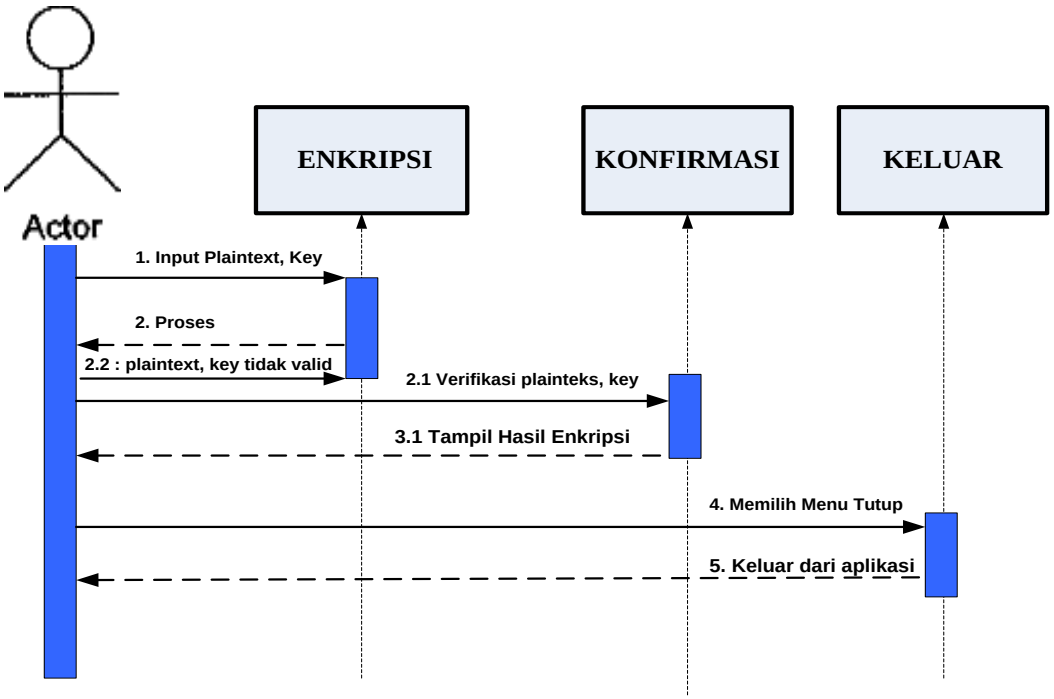
Perancangan *sequence diagram* enkripsi dibuat untuk menjelaskan yang terjadi didalam sistem ketika proses enkripsi seperti gambar dibawah ini.



Gambar 3.3 :*Sequence Diagram* Proses Enkripsi aplikasi aplikasi pengamanan data menggunakan metode *symmetric stream chipher*.

3. *Sequence Diagram* Dekripsi

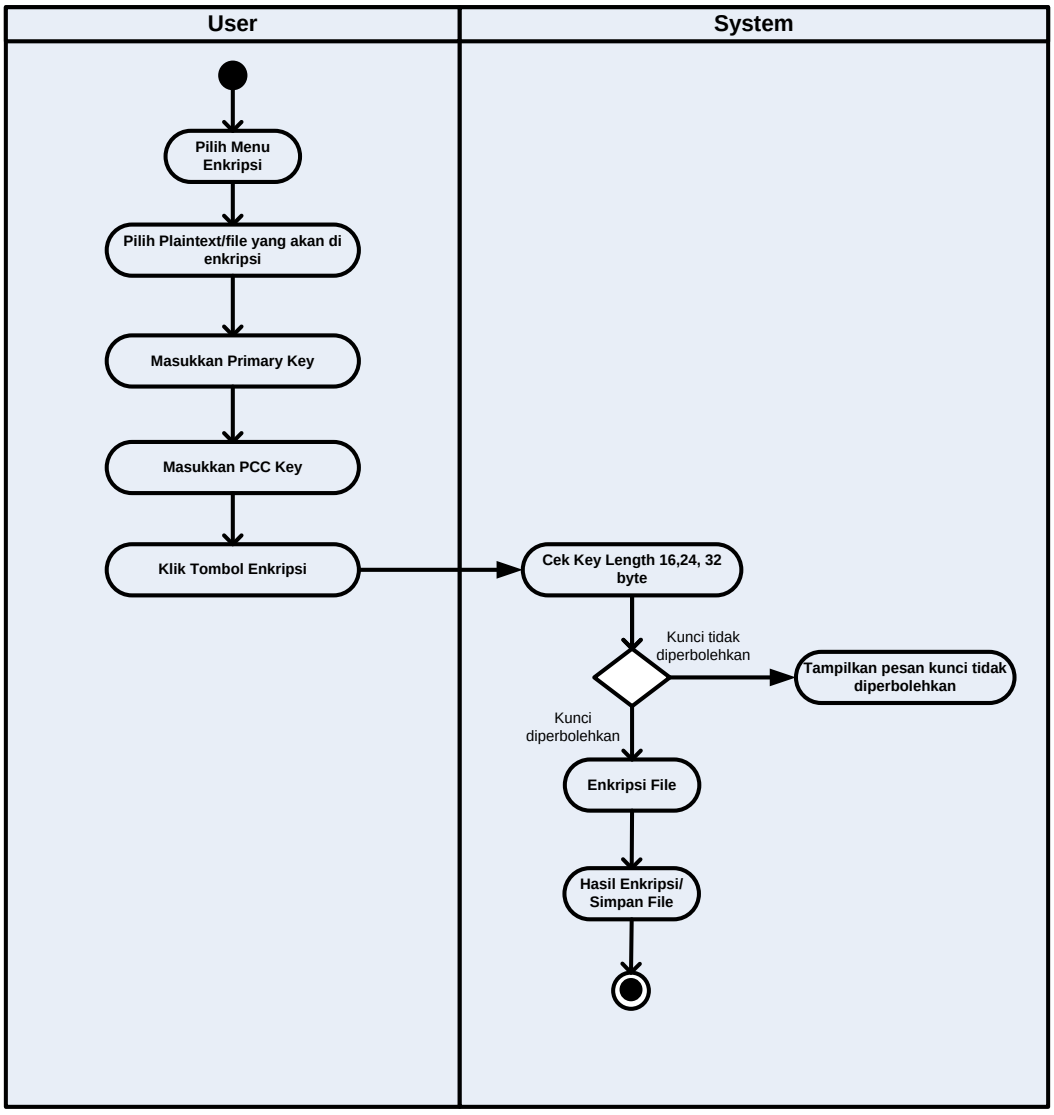
Perancangan *sequence diagram* dekripsi dibuat untuk menjelaskan yang terjadi didalam sistem ketika proses dekripsi seperti gambar dibawah ini.



Gambar 3.4 : *Sequence Diagram*Proses Dekripsi Aplikasi aplikasi pengamanan data menggunakan metode *symmetric stream chipher*.

4. Activity Diagram Enkripsi

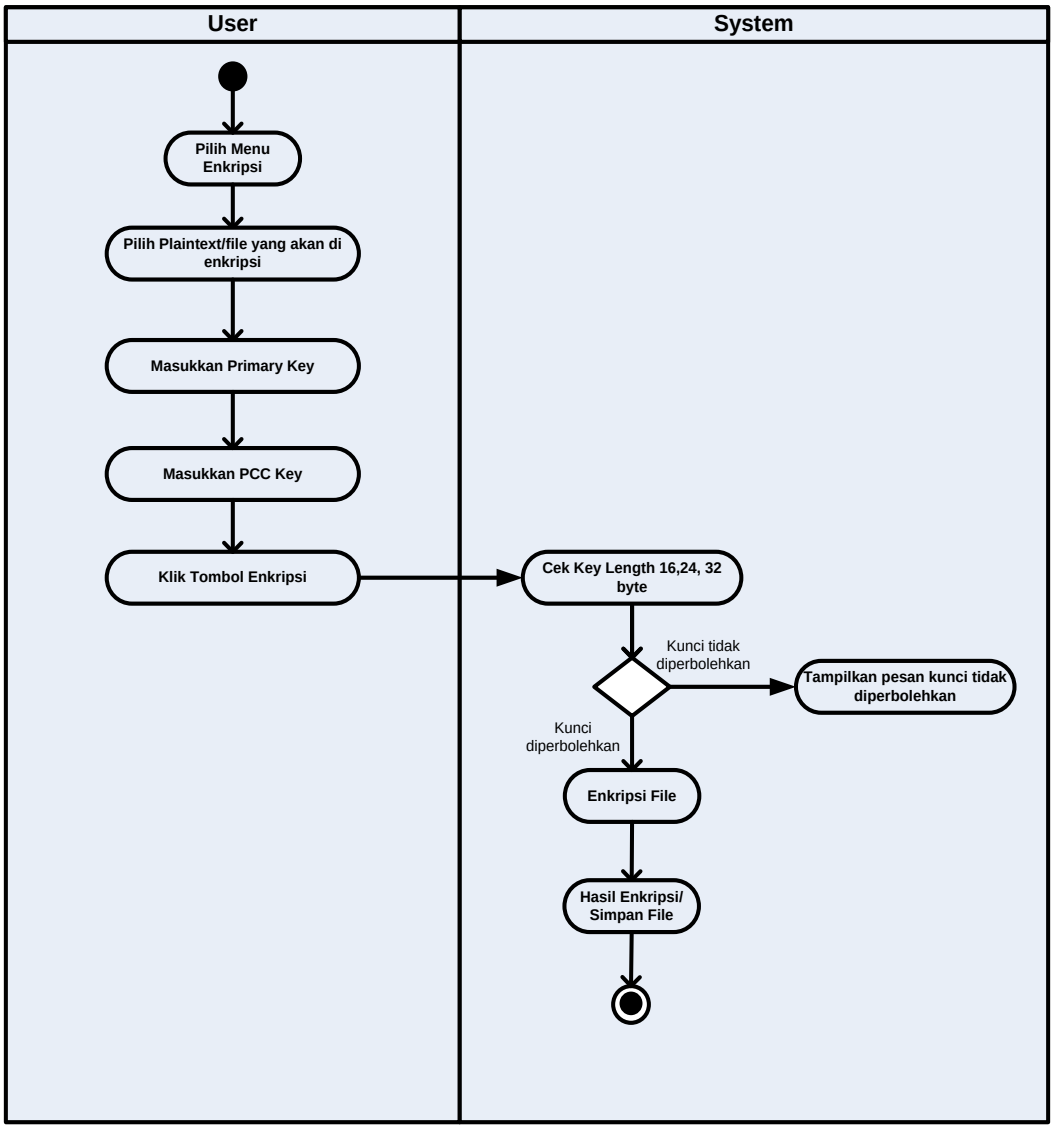
Dalam *activity diagram* enkripsi terdapat dua *partition* yaitu user dan *system*. User memilih menu *encrypt* dan memasukan plaintext dan kunci atau inputan file yang akan di enkripsi dan memilih tombol proses maka sistem akan melakukan verifikasi terhadap kunci yang digunakan apabila sesuai panjang kuncinya maka proses enkripsi akan dilakukan seperti ditunjukan pada gambar dibawah ini.



Gambar 3.5. *Activity Diagram*Proses Enkripsi.

5. Activity Diagram Dekripsi

Dalam *activity diagram* dekripsi terdapat dua *partition* yaitu user dan *system*. User memilih menu dekripsidan memasukan enkripsi dan kunciatau memasukan inputan file yang akan di dekripsi dan memilih tombol proses maka sistem akan melakukan verifikasi terhadap kunci yang digunakan apabila sesuai panjang kuncinya maka proses dekripsi akan dilakukan seperti ditunjukan pada gambar dibawah ini.



Gambar 3.6. *Activity Diagram*Proses Enkripsi.

3.5 Penerapan Algoritma *Symmetric Stream Chipher Perhitungan Proses Pembentukan Kunci*

Adapun proses pembentukan kunci ini memerlukan *input* berupa kunci utama adalah sebagai berikut.

Misalkan Kunci Utama : ”REZTIA”, dan kunci PCC : UNPAB maka proses pembentukan kunci adalah sebagai berikut :

1. Kunci Utama : REZTIA
2. Inisialisasi KEY 1 (Key = Kunci Utama)

   KEY 1 : REZTIA

   KEY 1 : 82, 69, 90, 84, 73, 65

   KEY1Len : 6
3. Inisialisasi Nilai K1(), P1, S1

   K1(0 .. 462) diberi nilai terurut menaik 0 s/d 462

   P1 = 0

   S1 = 0

   Pertukarkan K1(j) dengan K1(i) sebanyak 463 Kali

   j = (j + K1(i) + KEY1(i Mod KEY1Len)) Mod 463

   Perulangan Ke - 0

   j = (0 + K1(0) + KEY1(0 Mod 8)) Mod 463

   j = (0 + 1 + KEY1(0)) Mod 463

   j = (0 + 1 + 68) Mod 463

   j = (69) Mod 463

   j = 69

Tukarkan K1(68) Dengan K1(0) = 0 Dengan 68

Perulangan Ke - 1

j = (68 + K1(1) + KEY1(1 Mod 8)) Mod 463

j = (68 + 1 + KEY1(1)) Mod 463

j = (68 + 1 + 69) Mod 463

j = (138) Mod 463

j = 138

Tukarkan K1(138) Dengan K1(1) = 1 Dengan 138

3.6 Perhitungan Proses Pembentukan Dummy String

Dummy String dibentuk secara *random*. Dalam proses pembentukannya *Dummy String* dapat menerima input *Seed String* sebagai nilai yang membantu untuk mengacak dan menjamin tingkat *random Dummy String*. Misalkan *Seed String* = 'REZTIA' maka proses pembentukan *Dummy String* adalah sebagai berikut :

1. *SeedString* : "REZTIA"

   SeedString : (82, 69, 90, 84, 73, 65)

   Panjang *string* 6

2. Inisialisasi *Random Size Dummy*

   SizeDummy = Int(224*rnd)+32

   SizeDummy = 34

3. Rubahnilai Variable *Size Dummy* dengan

   Size Dummy = *Size Dummy* Xor Asc(Mid(*SeedString*, k, 1)

   sebanyak Len*(seedstring)* kali

a. Size Dummy = 34 Xor 85 = 119

b. Size Dummy = 119 Xor 76 = 59

c. Size Dummy = 59 Xor 84 = 111

d. Size Dummy = 111 Xor 82 = 61

e. Size Dummy = 61 Xor 65 = 124

f. Size Dummy = 124 Xor 32 = 92

g. Size Dummy = 92 Xor 49 = 109

h. Size Dummy = 109 Xor 46 = 67

i. Size Dummy = 67 Xor 48 = 115

j. Size Dummy = 115 Xor 51 = 64

Size Dummy = 64

Jika Size Dummy > 255 maka Size Dummy = Size Dummy - X*224

Jika Size Dummy < 32 maka Size Dummy = Size Dummy + 224

Size Dummy = 64

3.7 Perhitungan Proses Enkripsi

Misalkan diambil hasil pembentukan kunci serta pembentukan *dummy* di atas dan *plaintext* = SKRIPSI, maka proses enkripsinya adalah sebagai berikut :

1. Plaintext = SKRIPSI

   KunciUtama = REZTIA

   Kunci PCC = UNPAB

2. Kompresidengan ASCII

   CompressedString :

DalamASCII : (83, 75, 82, 73, 80, 83, 73, 68, 69, 68, 69, 75, 83, 84, 77, 73, 75)

3. Membentuk*DummyString*

4. *SeedString* = REZTIA

DummyString =

DalamASCII :

(244, 4, 101, 141, 61, 88, 213, 222, 60, 12, 199, 170,131, 182, 31, 225, 181, 54, 96, 53, 65, 89, 136, 56, 64,213, 59, 10, 106, 93, 248, 123, 100, 130, 70, 37, 30,216, 29, 93, 117, 172, 249, 45, 128, 30, 188, 87, 230, 147, 255, 222, 64, 245, 232, 206, 136, 176, 244, 87, 14,201, 154, 179, 153, 234, 92, 247, 89, 15, 173, 6, 23,135, 189, 184, 46, 160, 12, 79, 116, 49, 109, 236, 159,240, 91, 239, 38, 159, 200, 49, 184, 169, 232, 71, 236,151, 208, 88, 99, 34, 157, 125, 58, 48, 26, 117, 208,38,191, 100, 11, 135, 251, 17, 180, 182, 5, 222, 249, 188,151, 127, 58, 229, 175, 108, 101, 142, 152, 242, 91, 88,
60, 190, 112, 21, 245, 149, 77, 173, 50, 44, 91, 253,113, 208, 133, 155, 19, 39, 122, 88, 13, 69, 213, 201,27, 56, 104, 22, 96, 143, 60, 84, 215, 235, 186, 20,234,29, 211, 233, 204, 206, 170, 238, 219, 226, 37, 51, 183,27, 251, 46, 105, 59, 103, 8, 53, 72, 93, 44, 168, 177,6, 250, 246, 103, 19, 99, 150, 253, 229, 150, 182, 19,221, 215, 90, 9,239, 141, 147, 137, 225, 0, 147, 30, 235, 13,67, 22, 158, 53, 66, 49, 99, 104, 43, 215, 25).

5. Menggabungkan *Dummy String* dengan *Compressed String*

New Plaintext = Dummy String & *Compressed String* & (2 byte terakhir *Dummy String*)

New Plaintext =

DalamASCII :

(244, 4, 101, 141, 61, 88, 213, 222, 60, 12, 199, 170,131, 182, 31, 225, 181, 54, 96, 53, 65, 89, 136, 56, 64,213, 59, 10, 106, 93, 248, 123, 100, 130, 70, 37, 30,216, 29, 93, 117, 172, 249, 45, 128, 30, 188, 87, 230,147, 255, 222, 64, 245, 232, 206, 136, 176, 244, 87, 14,201, 154, 179, 153, 234, 92, 247, 89, 15, 173, 6, 23,135, 189, 184, 46, 160, 12, 79, 116, 49, 109, 236, 159,240, 91, 239, 38, 159, 200, 49, 184, 169, 232, 71, 236,151, 208, 88, 99, 34, 157, 125, 58, 48, 26, 117, 208,38,191, 100, 11, 135, 251, 17, 180, 182, 5, 222, 249, 188,151, 127, 58, 229, 175, 108, 101, 142, 152, 242, 91, 88,

60, 190, 112, 21, 245, 149, 77, 173, 50, 44, 91, 253,113, 208, 133, 155, 19, 39, 122, 88, 13, 69, 213, 201,27, 56, 104, 22, 96, 143, 60, 84, 215, 235, 186, 20,234,29, 211, 233, 204, 206, 170, 238, 219, 226, 37, 51, 183,27, 251, 46, 105, 59, 103, 8, 53, 72, 93, 44, 168, 177,6, 250, 246, 103, 19, 99, 150, 253, 229, 150, 182, 19,221, 215, 90, 9,239, 80, 121, 79, 14, 14, 140, 73, 33,103, 218, 34, 141, 147, 137, 225, 0, 147, 30, 235, 13,

67, 22, 158, 53, 66, 49, 99, 104, 43, 215, 25, 72, 69,51, 13, 69, 21, 0, 0, 0, 13, 0, 32, 4, 40, 4, 41, 4, 65,4, 71, 4, 72, 4, 73, 3, 75, 4, 80, 4, 82, 3, 83, 3, 84,4, 85, 4, 135, 176, 162, 121, 99, 125, 0, 62, 178, 189,125, 13, 15, 251, 140, 53, 0, 215, 25).

Encrypted String =

Dalam ASCII :

(21, 216, 138, 57, 165, 148, 122, 89, 98, 124, 255, 40, 39, 94, 130, 75, 48, 169, 32, 58, 251, 164, 82, 234, 72, 149).

Karakter :

(!, Ï, ė, 9, Ṅ, ö, z, Y, b, |, nbsp, (, ‘, ^, é, K, 0, ®, space, : , 1, ṅ, R, Ű, H, Ỏ)

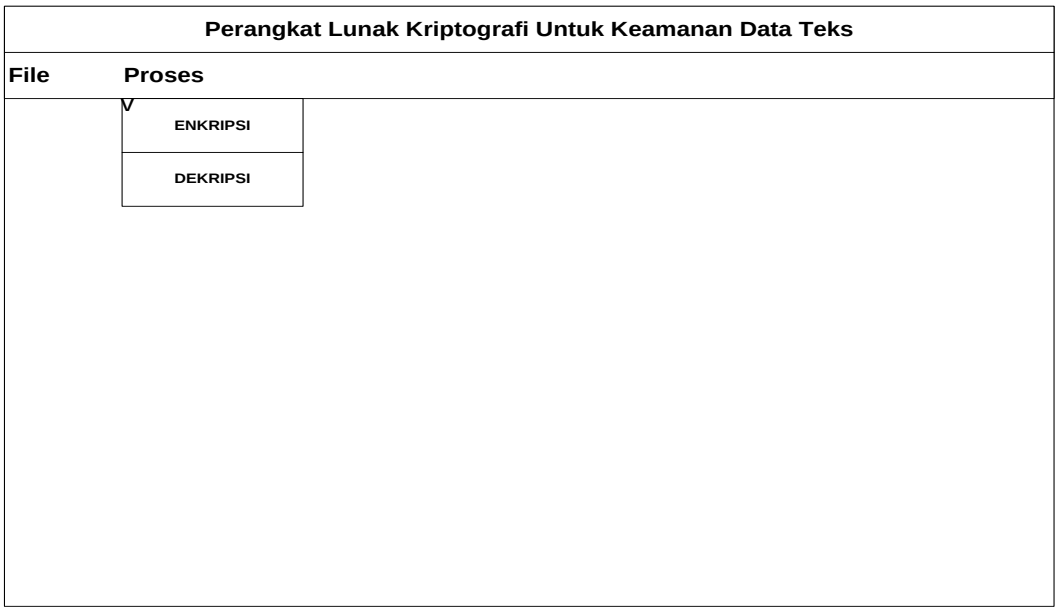
3.8 Perhitungan Proses Dekripsi

Proses dekripsi merupakan kebalikan dari proses enkripsi. Proses dekripsi dari metode *Symmetric Stream Chipher* menggunakan algoritma yang sama dengan proses enkripsi.

3.9 Perancangan Aplikasi

1. Tampilan Halaman Utama

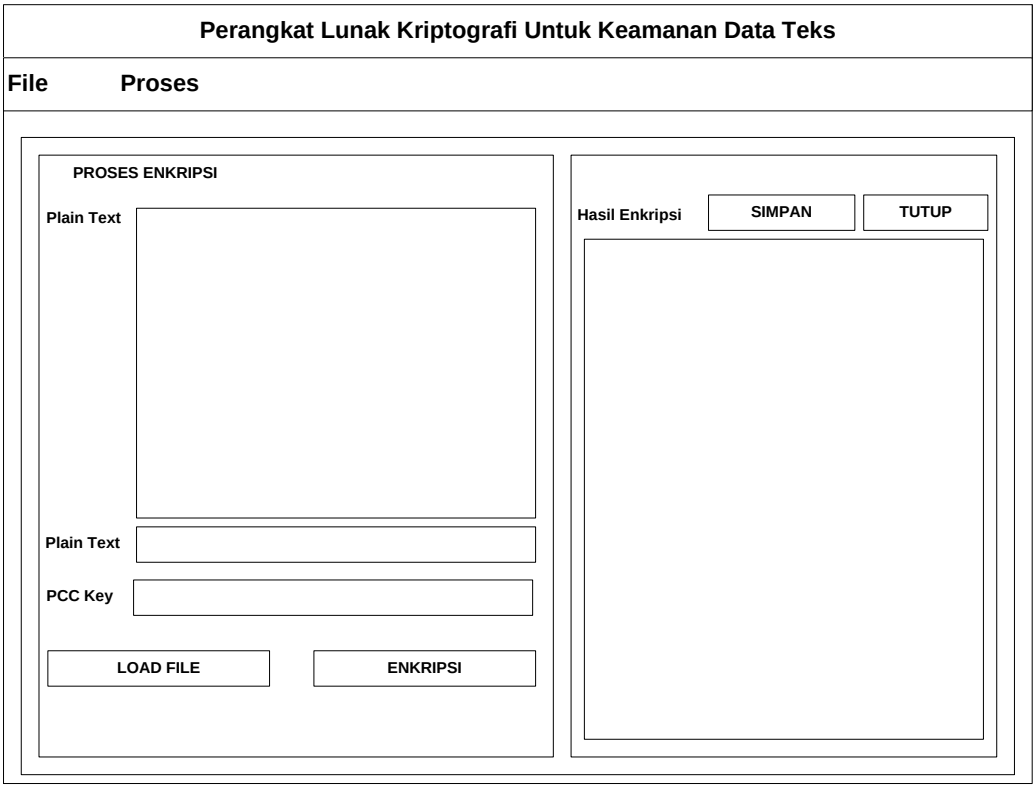
   Form pembuka hanya berfungsi sebagai *form* tampilan awal untuk memberikan informasi atau juga keterangan tentang penulis dan judul dari perancangan aplikasi ini. Belum ada terdapat fungsi khusus yang digunakan dalam proses pengamanan pada *form* tampilan ini. Untuk masuk ke form berikutnya bisa dilakukan dengan meng-klik tampilan ini.



Gambar 3.7 : Tampilan Halaman Utama

2. Tampilan Form Enkripsi

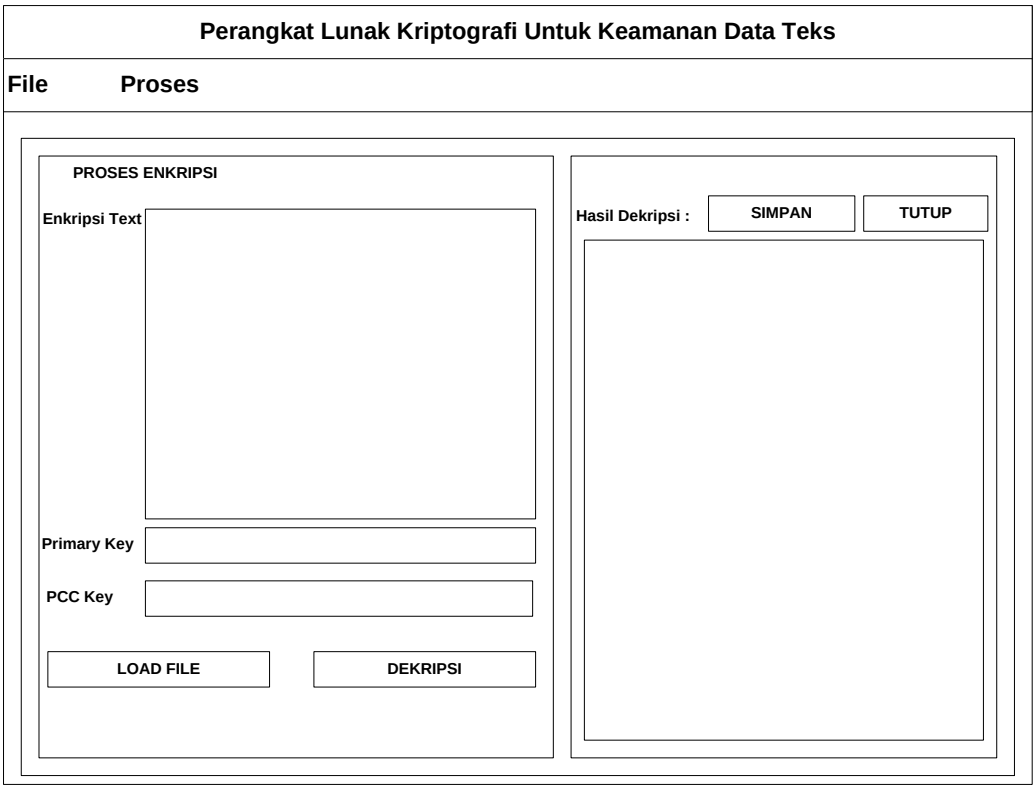
Pada kotak plainteks, pengguna dapat memasukkan kalimat yang diinginkan dan hasil chipherteksnya akan keluar pada kotak chipherteks setelah dilakukannya proses pada kotak proses. Dibawah ini merupakan tampilan dari *form file enkripsi* yang telah dirancang.



Gambar 3.8 Tampilan *Form File Enkripsi*

3. Tampilan Form Dekripsi

Pada Rancangan Proses dekripsi ini kotak cipherteks diletakkan diatas kotak plainteks, karena pada tampilan ini cipherteks telah ditentukan sebelumnya melalui proses enkripsi. Untuk tampilan *form file dekripsi* yang telah dirancang seperti gambar dibawah ini.



Gambar 3.9 Tampilan *Form File Dekripsi*

BAB IV
HASIL DAN PEMBAHASAN

4.1. Kebutuhan Spesifikasi Minimum Hardware dan Software

Agar sistem perancangan yang telah kita kerjakan dapat berjalan baik atau tidak, maka perlu kiranya dilakukan pengujian terhadap sistem yang telah kita kerjakan. Untuk itu dibutuhkan beberapa komponen utama mencakup perangkat keras (*hardware*), perangkat lunak (*software*).

1. Perangkat Keras (*Hardware*)

a. *Personal Computer dengan Processor minimal Intel Dual Core*

b. Resolusi *monitor* dengan kedalaman warna minimal 1024 x 768 *pixel.*

c. *Sound card* yang baik agar kualitas suara jadi lebih baik.

d. *Memory RAM* minimal *2 Gigabyte*

e. Ruang penyimpanan di *harddisk* minimal 50 *Gigabyte*

f. *Mouse* dan *Keyboard*

2. Perangkat Lunak (*Software*)

a. Sistem Operasi *Windows 7*

b. Bahasa Pemrograman *Visual Basic.net*

c. *Microsoft Visual Studio Versi 2010*

d. *Web Database MySQL* versi 5.0

4.2. Pengujian Aplikasi

Implementasi sistem adalah langkah-langkah atau prosedur-prosedur yang dilakukan dalam menyelesaikan desain sistem yang telah disetujui, untuk menguji, meng*install* dan memulai sistem baru atau sistem yang diperbaiki untuk menggantikan sistem yang lama.

Adapun tujuan dari implementasi sistem ini adalah sebagai berikut :

1. Menyelesaikan desain sistem yang telah disetujui sebelumnya
2. Memastikan bahwa pemakai *(user)* dapat mengoperasikan sistem baru
3. Menguji apakah sistem baru tersebut sesuai dengan pemakai. Memastikan bahwa konversi ke sistem baru berjalan yaitu dengan membuat rencana, mengontrol dan melakukan instalasi baru secara benar.

Adapun langkah-langkah menjalankan aplikasi pengamanan data dengan menerapkan metode *symmetric stream chipher* yaitu dengan membuka *program Visual Studio 2010, kemudian buka script program* kemudian tekan *enter* dan setelah dilakukan *Enter* maka akan terlihat tampilan sebagai berikut :

a. Buka *Software Microsoft Visual Studio 2010.*
b. Kemudian Pilih Nama *Project Kriptografi*, seperti pada gambar dibawah ini.

Gambar 4.1 : Tampilan Project Kriptografi.

c Untuk menjalankan *project*, kemudian klik tombol start pada *Project*, sehingga akan tampil halaman utama.

Gambar 4.2 : Tampilan Halaman Utama.

4.3. Tampilan Halaman Aplikasi

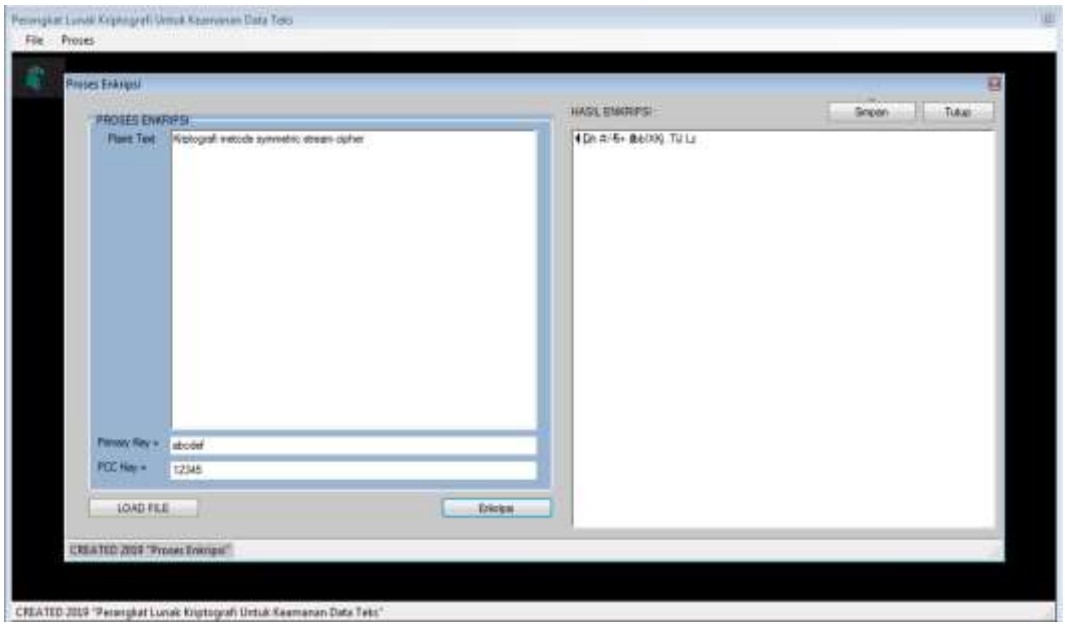
1. Tampilan Menu Utama

Merupakan halaman yang pertama diakses pada saat aplikasi dijalankan, halaman *Home* sebagai halaman utama aplikasi pengamanan data dengan menggunakan metode *symmetric stream chipher*. Menu utama menampilkan tombol menu *file* dan proses, menu proses terdiri dari proses enkripsi dan dekripsi. Tampilan menu utama dapat dilihat pada gambar 4.3.

Gambar 4.3 : Tampilan Menu Utama.

2. Tampilan Menu Proses Enkripsi

Merupakan halaman yang digunakan untuk menampilkan proses enkripsi. Pada tampilan enkripsi terdapat kotak *plain text*, *primary key* dan *PCC Key*, pengguna dapat memasukkan kalimat yang diinginkan atau melakukan *load file* yang akan dienkripsi dan hasil enkripsinya akan keluar pada kotak hasil enkripsi sebelah kanan setelah dilakukan proses pada tombol enkripsi. Apabila hasil enkripsi tersebut mau di simpan maka klik tombol simpan maka akan jadi sebuah file hasil enkripsi. Dibawah ini merupakan tampilan dari *form file* enkripsi yang telah dirancang. Tampilan menu proses enkripsi dapat dilihat pada gambar 4.4.



Gambar 4.4 : Tampilan Menu Proses Enkripsi.

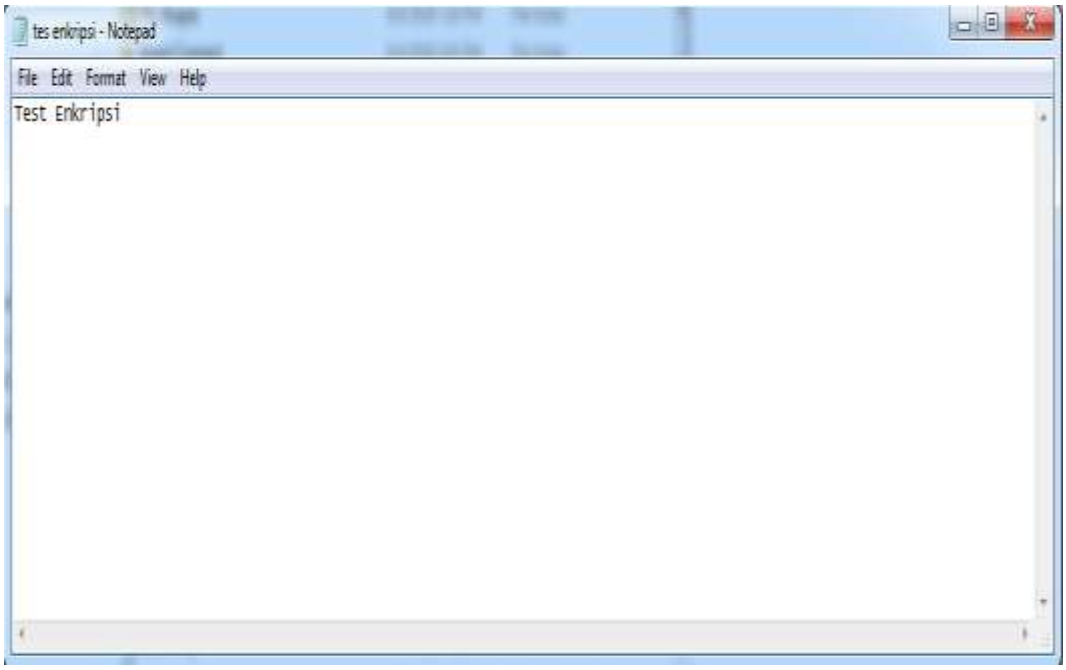
```
Imports System.IO
Public Class p_enkripsi
    Dim oReader As StreamReader
    Dim hsl_transpotion As String = ""
    Dim hsl_dummy As String = ""

    Private Sub btn_enkripsi_Click(ByVal sender As System.Object, ByVal e
As System.EventArgs) Handles btn_enkripsi.Click
```

```
    End Sub
    Private Sub btn_keluar_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles btn_keluar.Click
        Form1.Show()
        Me.Close()

    End Sub
    Sub dummy_key()

        Dim sdstring As String = "Enkripsi"
        Dim lenstring As Integer = Len(sdstring)
        Dim Dummy(Len(sdstring)) As String
        Dim sizedummy As Integer = Int(224 * Rnd()) + 32
        Dim i As Integer
        Dim asciiValue As Integer


        For i = 0 To lenstring - 1
            asciiValue = Convert.ToByte(CChar(Mid(sdstring, i + 1, 1)))
            Dummy(i) = asciiValue
        Next

        For i = 0 To lenstring - 1
            sizedummy = sizedummy Xor Dummy(i)
        Next

        Dim D1(sizedummy) As Integer

        For i = 0 To sizedummy - 1
            D1(i) = Int(224 * Rnd()) + 32
            hsl_dummy = hsl_dummy & Convert.ToChar(D1(i))
        Next

    End Sub
    Sub tranpotion_key()
        Dim asciiValue As Integer
        Dim ascci_primary As String = ""
        Dim KEY1Len As Integer = Len(Trim(Me.txt_kunci.Text))
        Dim KEY1(KEY1Len) As Integer


        Dim i As Integer
        Dim j As Integer = 0



        For i = 0 To KEY1Len - 1
            asciiValue = Convert.ToByte(CChar(Mid(Me.txt_kunci.Text, i + 1,
1)))
            KEY1(i) = asciiValue
        Next

        Dim K1(462) As Integer
        For i = 0 To 463 - 1
            K1(i) = i
        Next
```

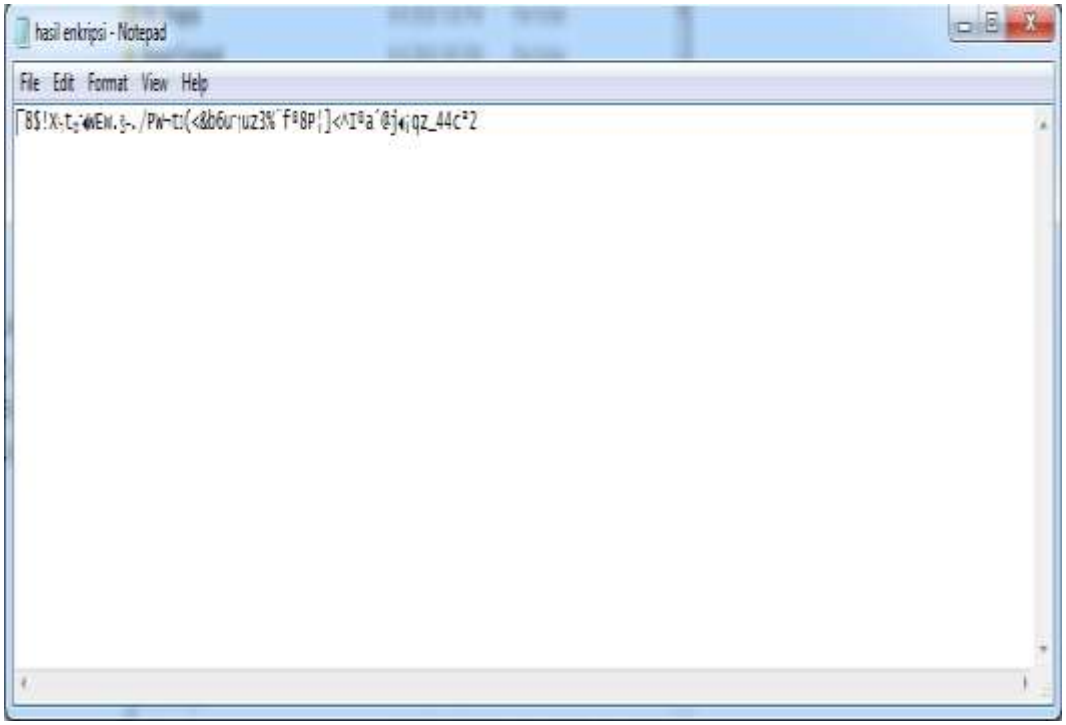
```
        For i = 0 To 463 - 1
            j = (j + K1(i) + KEY1(i Mod KEY1Len)) Mod 463

            'tukarkan
            K1(i) = j
            K1(j) = K1(i)
        Next

        Dim KEY2(16) As Integer
        For i = 0 To 463 - 1
            KEY2(i Mod 17) = KEY2(i Mod 17) Xor (K1(i) And 255)
        Next

        Dim K2(250) As Integer
        For i = 0 To 251 - 1
            K2(i) = i
        Next
        j = 0
        For i = 0 To 251 - 1
            j = (j + K2(i) + KEY2(i Mod 17)) Mod 251


            K2(i) = j
            K2(j) = K2(i)

        Next
        Dim KEY3(22) As Integer
        For i = 0 To 251 - 1
            KEY3(i Mod 23) = KEY3(i Mod 23) Xor (K2(i) And 255)
        Next

        Dim PCCLen As Integer = Len(Me.txt_keypcc.Text)
        Dim KEYPCC(PCCLen) As Integer

        For i = 0 To PCCLen - 1
            asciiValue = Convert.ToByte(CChar(Mid(Me.txt_keypcc.Text, i +
1, 1)))
            KEYPCC(i) = asciiValue
        Next

        If PCCLen > 0 Then
            For i = 0 To 22
                KEY3(i) = KEY3(i) Xor KEYPCC(i Mod PCCLen)
            Next
        End If

        Dim K3(180) As Integer
        For i = 0 To 181 - 1
            K3(i) = i
        Next

        j = 0
        For i = 0 To 181 - 1
            j = (j + K3(i) + KEY3(i Mod 23)) Mod 181


            K3(i) = j
```

```
            K3(j) = K3(i)

            hsl_transpotion = hsl_transpotion & Convert.ToChar(K3(i))
        Next

    End Sub
    Sub cek_hasil()
        On Error GoTo keluar
        tranpotion_key()

        Me.TextBox2.Text = Replace(Me.TextBox1.Text, hsl_transpotion, "")

        Dim dummysize As Integer = Len(Trim(Me.TextBox2.Text)) - 54
        Dim enkrip_string As String = Me.TextBox2.Text

        Me.TextBox2.Text = enkrip_string.Substring(0, dummysize)

        Me.TextBox2.Text = RijndaelSimple.Decrypt(Me.TextBox2.Text,
Me.txt_kunci.Text, Me.txt_keypcc.Text, "SHA1", 2, "@1B2c3D4e5F6g7H8", 192)

        hsl_transpotion = ""
        hsl_dummy = ""
        Me.TextBox2.Text = ""
        Exit Sub
keluar:
        MsgBox("Proses Enkripsi Gagal, Coba Ganti Primary Key atau PCC")
        Me.TextBox1.Text = ""
        Me.TextBox2.Text = ""
        hsl_transpotion = ""
        hsl_dummy = ""
    End Sub
    Private Sub Button3_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button3.Click


    End Sub

    Private Sub Button7_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button7.Click
        On Error GoTo keluar
        tranpotion_key()
        RichTextBox3.Text = hsl_transpotion
        Me.RichTextBox2.Text = Replace(Me.RichTextBox2.Text,
RichTextBox3.Text, "")


        Dim dummysize As Integer = Len(Trim(Me.RichTextBox2.Text)) - 54
        Dim enkrip_string As String = Me.RichTextBox2.Text

        Me.RichTextBox2.Text = enkrip_string.Substring(0, dummysize)
        Me.RichTextBox2.Text = RijndaelSimple.Decrypt(Me.RichTextBox2.Text,
Me.txt_kunci.Text, Me.txt_keypcc.Text, "SHA1", 2, "@1B2c3D4e5F6g7H8", 192)

        hsl_transpotion = ""
        hsl_dummy = ""

        Exit Sub
```

```
keluar:
        hsl_transpotion = ""
        hsl_dummy = ""
        MsgBox("Gagal Enkripsi, Coba cek kembali key yang diinput")
    End Sub

    Private Sub Button8_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button8.Click
        On Error GoTo keluar
        tranpotion_key()
        dummy_key()
        Me.RichTextBox2.Text = RijndaelSimple.Encrypt(Me.RichTextBox1.Text,
Me.txt_kunci.Text, Me.txt_keypcc.Text, "SHA1", 2, "@1B2c3D4e5F6g7H8", 192)
        Me.RichTextBox2.Text = hsl_transpotion & Me.RichTextBox2.Text &
hsl_dummy.Substring(1, 54)
        hsl_transpotion = ""
        hsl_dummy = ""
        Exit Sub

keluar:
        hsl_transpotion = ""
        hsl_dummy = ""
        MsgBox("Gagal Dekripsi, Coba cek kembali key yang diinput")
    End Sub

    Private Sub Button5_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs)

    End Sub

    Private Sub Button5_Click_1(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button5.Click

        OpenFileDialog1.FileName = ""
        OpenFileDialog1.Filter = "Text Files (*.txt*)|*.txt"
        If OpenFileDialog1.ShowDialog = Windows.Forms.DialogResult.OK Then
            oReader = New StreamReader(OpenFileDialog1.FileName, True)
            Me.RichTextBox1.Text = oReader.ReadToEnd
        End If
    End Sub

    Private Sub Button4_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button4.Click
        SaveFileDialog1.Filter = "Text Files (*.txt*)|*.txt"
        If SaveFileDialog1.ShowDialog = Windows.Forms.DialogResult.OK _
        Then
            My.Computer.FileSystem.WriteAllText _
            (SaveFileDialog1.FileName, RichTextBox2.Text, True)
            MsgBox("Berhasil Disimpan")
        End If
    End Sub
End Class
```



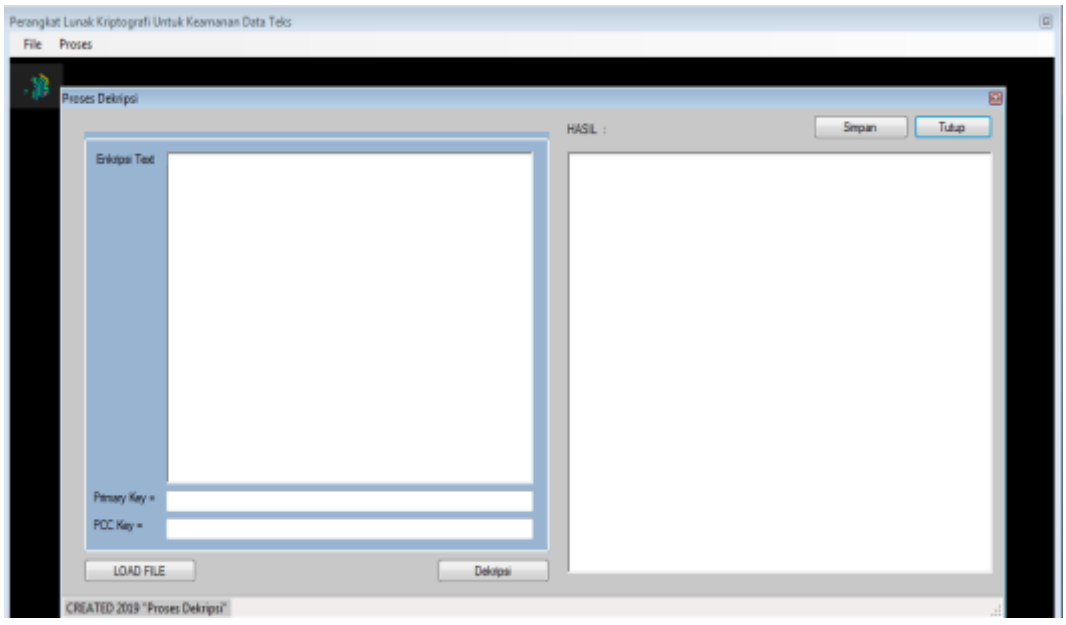
Gambar 4.5 : Tampilan File Text Sebelum Proses Enkripsi.



Gambar 4.6 : Tampilan File Text Setelah Proses Enkripsi.

3. Tampilan Menu Proses Dekripsi

Merupakan halaman yang digunakan untuk menampilkan proses dekripsi. Pada tampilan dekripsi terdapat kotak enkripsi *text*, *primary key* dan *PCC Key*, pengguna dapat memasukkan kalimat yang diinginkan atau melakukan *load file* yang akan dienkripsi dan hasil dekripsinya akan keluar pada kotak hasil dekripsi sebelah kanan setelah dilakukan proses pada tombol dekripsi. Apabila hasil dekripsi tersebut mau di simpan maka klik tombol simpan maka akan jadi sebuah file hasil dekripsi. Dibawah ini merupakan tampilan dari *form file* dekripsi yang telah dirancang. Tampilan menu proses dekripsi dapat dilihat pada gambar 4.7.



Gambar 4.7 : Tampilan Menu Proses Dekripsi.

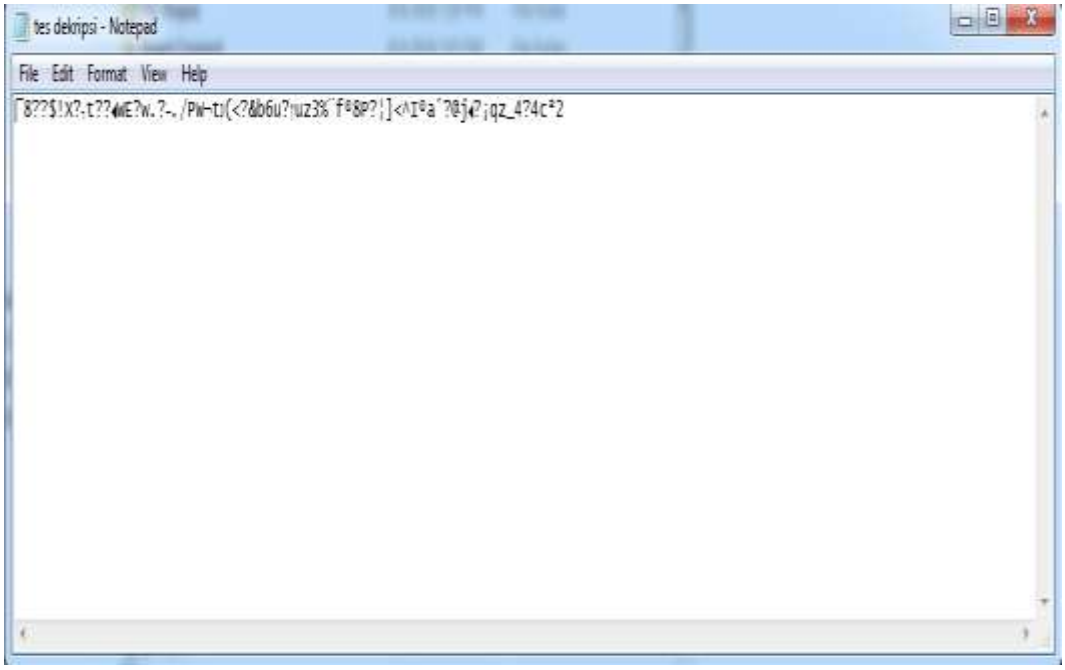
```
Imports System.IO
Public Class p_dekripsi
    Dim oReader As StreamReader
    Dim hsl_transpotion As String = ""
    Dim hsl_dummy As String = ""

    Private Sub btn_enkripsi_Click(ByVal sender As System.Object, ByVal e
As System.EventArgs)
```

```
    End Sub

    Private Sub btn_keluar_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs)
        Me.Close()
        Form1.Show()
    End Sub
    Sub dummy_key()

        Dim sdstring As String = "Enkripsi"
        Dim lenstring As Integer = Len(sdstring)
        Dim Dummy(Len(sdstring)) As String
        Dim sizedummy As Integer = Int(224 * Rnd()) + 32
        Dim i As Integer
        Dim asciiValue As Integer


        For i = 0 To lenstring - 1
            asciiValue = Convert.ToByte(CChar(Mid(sdstring, i + 1, 1)))
            Dummy(i) = asciiValue
        Next

        For i = 0 To lenstring - 1
            sizedummy = sizedummy Xor Dummy(i)
        Next

        Dim D1(sizedummy) As Integer

        For i = 0 To sizedummy - 1
            D1(i) = Int(224 * Rnd()) + 32
            hsl_dummy = hsl_dummy & Convert.ToChar(D1(i))
        Next

    End Sub
    Sub tranpotion_key()
        Dim asciiValue As Integer
        Dim ascci_primary As String = ""
        Dim KEY1Len As Integer = Len(Trim(Me.txt_kunci.Text))
        Dim KEY1(KEY1Len) As Integer


        Dim i As Integer
        Dim j As Integer = 0


        For i = 0 To KEY1Len - 1
            asciiValue = Convert.ToByte(CChar(Mid(Me.txt_kunci.Text, i + 1,
1)))
            KEY1(i) = asciiValue
        Next

        Dim K1(462) As Integer
        For i = 0 To 463 - 1
            K1(i) = i
        Next

        For i = 0 To 463 - 1
```

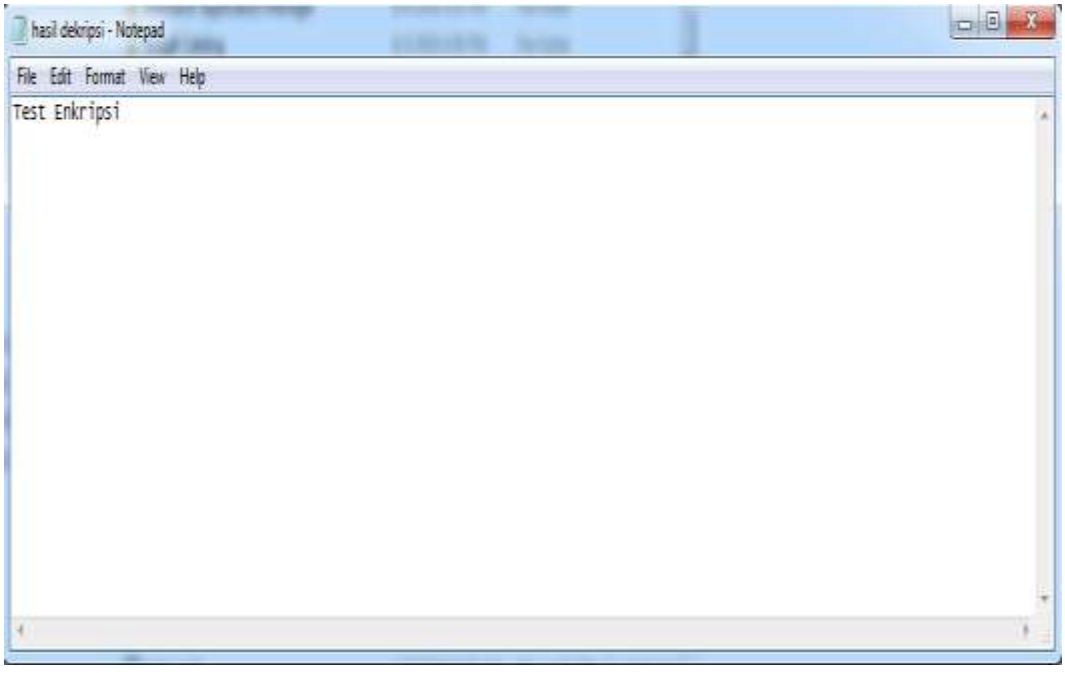
```
            j = (j + K1(i) + KEY1(i Mod KEY1Len)) Mod 463

            K1(i) = j
            K1(j) = K1(i)
        Next
        Dim KEY2(16) As Integer
        For i = 0 To 463 - 1
            KEY2(i Mod 17) = KEY2(i Mod 17) Xor (K1(i) And 255)
        Next

        Dim K2(250) As Integer
        For i = 0 To 251 - 1
            K2(i) = i
        Next

        j = 0
        For i = 0 To 251 - 1
            j = (j + K2(i) + KEY2(i Mod 17)) Mod 251


            K2(i) = j
            K2(j) = K2(i)

        Next
        Dim KEY3(22) As Integer
        For i = 0 To 251 - 1
            KEY3(i Mod 23) = KEY3(i Mod 23) Xor (K2(i) And 255)
        Next

        Dim PCCLen As Integer = Len(Me.txt_keypcc.Text)
        Dim KEYPCC(PCCLen) As Integer

        For i = 0 To PCCLen - 1
            asciiValue = Convert.ToByte(CChar(Mid(Me.txt_keypcc.Text, i +
1, 1)))
            KEYPCC(i) = asciiValue
        Next

        If PCCLen > 0 Then
            For i = 0 To 22
                KEY3(i) = KEY3(i) Xor KEYPCC(i Mod PCCLen)
            Next
        End If

        Dim K3(180) As Integer
        For i = 0 To 181 - 1
            K3(i) = i
        Next

        j = 0
        For i = 0 To 181 - 1
            j = (j + K3(i) + KEY3(i Mod 23)) Mod 181


            K3(i) = j
            K3(j) = K3(i)
```

```
            hsl_transpotion = hsl_transpotion & Convert.ToChar(K3(i))
        Next

    End Sub
    Sub cek_hasil()
        On Error GoTo keluar
        tranpotion_key()

        Me.TextBox2.Text = Replace(Me.TextBox1.Text, hsl_transpotion, "")

        Dim dummysize As Integer = Len(Trim(Me.TextBox2.Text)) - 54
        Dim enkrip_string As String = Me.TextBox2.Text

        Me.TextBox2.Text = enkrip_string.Substring(0, dummysize)

        Me.TextBox2.Text = RijndaelSimple.Decrypt(Me.TextBox2.Text,
Me.txt_kunci.Text, Me.txt_keypcc.Text, "SHA1", 2, "@1B2c3D4e5F6g7H8", 192)

        hsl_transpotion = ""
        hsl_dummy = ""

        Me.TextBox2.Text = ""
        Exit Sub
keluar:
        MsgBox("Proses Enkripsi Gagal, Coba Ganti Primary Key atau PCC")
        Me.TextBox1.Text = ""
        Me.TextBox2.Text = ""
        hsl_transpotion = ""
        hsl_dummy = ""
    End Sub
    Private Sub Button3_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs)

    End Sub

    Private Sub Button7_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button7.Click
        On Error GoTo keluar
        tranpotion_key()
        RichTextBox3.Text = hsl_transpotion
        Me.RichTextBox1.Text = Replace(Me.RichTextBox2.Text,
RichTextBox3.Text, "")


        Dim dummysize As Integer = Len(Trim(Me.RichTextBox1.Text)) - 54
        Dim enkrip_string As String = Me.RichTextBox1.Text

        Me.RichTextBox1.Text = enkrip_string.Substring(0, dummysize)
        Me.RichTextBox1.Text = RijndaelSimple.Decrypt(Me.RichTextBox1.Text,
Me.txt_kunci.Text, Me.txt_keypcc.Text, "SHA1", 2, "@1B2c3D4e5F6g7H8", 192)

        hsl_transpotion = ""
        hsl_dummy = ""
        Exit Sub


keluar:
```

```
        hsl_transpotion = ""
        hsl_dummy = ""
        MsgBox("Gagal Dekripsi, Coba cek kembali key yang diinput")
    End Sub

    Private Sub Button8_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button8.Click
        On Error GoTo keluar
        tranpotion_key()
        dummy_key()

        Me.RichTextBox2.Text = RijndaelSimple.Encrypt(Me.RichTextBox1.Text,
Me.txt_kunci.Text, Me.txt_keypcc.Text, "SHA1", 2, "@1B2c3D4e5F6g7H8", 192)
        Me.RichTextBox2.Text = hsl_transpotion & Me.RichTextBox2.Text &
hsl_dummy.Substring(1, 54)
        hsl_transpotion = ""
        hsl_dummy = ""
        Exit Sub


keluar:
        hsl_transpotion = ""
        hsl_dummy = ""
        MsgBox("Gagal Dekripsi, Coba cek kembali PCC key yang diinput")
    End Sub

    Private Sub Button5_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button5.Click
        OpenFileDialog1.FileName = ""
        OpenFileDialog1.Filter = "Text Files (*.txt*)|*.txt"
        If OpenFileDialog1.ShowDialog = Windows.Forms.DialogResult.OK Then
            oReader = New StreamReader(OpenFileDialog1.FileName, True)
            Me.RichTextBox2.Text = oReader.ReadToEnd
        End If
    End Sub

    Private Sub Button4_Click(ByVal sender As System.Object, ByVal e As
System.EventArgs) Handles Button4.Click
        SaveFileDialog1.Filter = "Text Files (*.txt*)|*.txt"
        If SaveFileDialog1.ShowDialog = Windows.Forms.DialogResult.OK _
        Then
            My.Computer.FileSystem.WriteAllText _
            (SaveFileDialog1.FileName, RichTextBox1.Text, True)
            MsgBox("Berhasil Disimpan")
        End If
    End Sub

    Private Sub btn_keluar_Click_1(ByVal sender As System.Object, ByVal e
As System.EventArgs) Handles btn_keluar.Click
        Form1.Show()
        Me.Close()

    End Sub
End Class
```



Gambar 4.8 : Tampilan File Text Sebelum Proses Dekripsi.



Gambar 4.9 : Tampilan File Text Setelah Proses Dekripsi.

4.4. Pembahasan

Pengujian sistem dilakukan bertujuan untuk menemukan kesalahan atau kekurangan pada perangkat lunak yang diuji. Pengujian bermaksud untuk mengetahui perangkat lunak yang dibuat sudah memenuhi kriteria yang sesuai dengan tujuan perancangan perangkat lunak tersebut. Pengujian yang dilakukan yaitu pengujian *alpha*. Pengujian *alpha* yang digunakan adalah metode *black-box*.

Pengujian *fungsional* yang digunakan untuk menguji sistem yang baru adalah metode pengujian *alpha*. Pengujian *alpha* dilakukan dengan menggunakan metode *black box*. Pengujian *black box* berfokus pada persyaratan fungsional perangkat lunak.

4.4.1. Hasil Penelitian Enkripsi Pesan dengan Algoritma *Stream Chipher*

Dari beberapa percobaan pada proses enkripsi pesan dengan algoritma stream cipher, yang dapat dilihat di table 4.1, maka diperoleh suatu kesimpulan bahwa panjang *plaintext* akan mempengaruhi waktu enkripsi dan dekripsi pesan. Semakin panjang *plaintext* maka waktu yang dibutuhkan untuk enkripsi dan dekripsi akan lebih lama. Dari hasil implementasi yang dilakukan diperoleh kesimpulan bahwa *chiphertext* pada algoritma *stream chipher* memiliki tingkat keamanan yang rendah karena adanya kemungkinan *plaintext* dan *chiphertext* berkoresponden sehingga akan mudah bagi *kriptanalis* menemukan aliran-kunci dengan meng-XOR-kan bit-bit *plaintext* dan *chiphertext*. Sehingga hal ini dapat dikatakan adalah merupakan salah satu kelemahan dari algoritma *stream chipher*.

4.4.2. Hasil Penelitian Dekripsi Pesan dengan Algoritma *Stream Chipher*

Dari beberapa percobaan pada proses enkripsi pesan dengan algoritma *stream chipher*, yang dapat dilihat di table 4.2, maka diperoleh suatu kesimpulan bahwa waktu dekripsi lebih cepat dibandingkan dengan proses enkripsi karena pada proses enkripsi kunci *stream chipher* dalam bentuk desimal harus dikonversi terlebih dahulu ke bilangan *biner*. Besar file untuk *plaintext* dan *chiphertext* dalam proses enkripsi dan dekripsi adalah sama. Karena panjang kunci yang digunakan adalah sama.

Dari hasil implementasi disimpulkan bahwa Waktu yang dibutuhkan untuk dekripsi pada algoritma *stream chipher* lebih cepat dibandingkan dengan waktu yang dibutuhkan untuk proses enkripsi. Hal ini terjadi karena pada proses enkripsi, kunci yang dihasilkan bernilai desimal, sehingga harus dikonversi terlebih dahulu ke bilangan biner. Berbeda halnya dengan proses dekripsi yang hanya mengambil kunci dari *function* enkripsi.

BAB V
PENUTUP

5.1. Kesimpulan

Berdasarkan pembahasan dan evaluasi dari bab-bab sebelumnya, maka dapat diambil beberapa kesimpulan sebagai berikut :

1. Proses enkripsi dan dekripsi *symmetric stream chipher* diawali dengan pembentukan kunci dimana dalam pembentukan kunci ini menggunakan bantuan *primary key* dan PCC *key (Private Crypto Code)*.
2. Penerapan metode *symmetric stream chipher* dilakukan dengan cara mengenkripsi data teks rahasia. Metode ini merupakan metode yang memiliki tingkat keamanan yang tinggi karena diadaptasi dari *one time pad chipher* yang dikenal sebagai metode yang sukar untuk dipecahkan.
3. Perancangan aplikasi keamanan data teks menggunakan Microsoft Visual Studio 2010 serta menerapkan metode *symmetric stream chipher* dalam proses enkripsi dan dekripsinya. Aplikasi ini berguna untuk merubah pesan teks asli menjadi teks sandi atau sebaliknya dengan tujuan agar pesan tersebut tidak dapat dibaca oleh pihak yang tidak bertanggung jawab, selain itu aplikasi ini juga mempercepat proses enkripsi dan dekripsi dibandingkan dengan menggunakan cara manual.

5.2. Saran

Berikut adalah saran-saran untuk pengembangan lebih lanjut terhadap aplikasi proses penyandian data text dengan menerapkan metode *symmetric stream chipher*:

1. Sistem yang dibangun pada intinya hanya sebatas system enkripsi dan deskripsi data menggunakan metode *symmetric stream chipher* dengan menggunakan bahasa pemrograman *Visual Basic.Net*. Sehingga kedepannya diharapkan adanya pengembangan lagi untuk sistem yang lebih luas cakupannya seperti pengujian sistem secara *online* dan lain sebagainya.
2. Diperlukan *maintenace* terhadap sistem yang telah dibuat, supaya dapat digunakan secara berkelanjutan selama kebutuhan terhadap informasi yang dibutuhkan.
3. Untuk pengembangan selanjutnya diharapkan tidak hanya sistem enkripsi dan dekripsi file text saja, tapi lebih kompleks dengan file berbasis *Microsoft Office* dan lain-lain.

DAFTAR PUSTAKA

Aryza, S., Irwanto, M., Lubis, Z., Siahaan, A. P. U., Rahim, R., & Furqan, M. (2018). A Novelty Design Of Minimization Of Electrical Losses In A Vector Controlled Induction Machine Drive. In IOP Conference Series: Materials Science and Engineering (Vol. 300, No. 1, p. 012067). IOP Publishing.

Barus, S., Sitorus, V. M., Napitupulu, D., Mesran, M., & Supiyandi, S. (2018). Sistem Pendukung Keputusan Pengangkatan Guru Tetap Menerapkan Metode Weight Aggregated Sum Product Assesment (WASPAS). Jurnal Media Informatika Budidarma, 2(2).

Based Instruction". Jurnal Riset Komputer Mahasiswa Teknik Informatika STMIK Budi Darma Medan.

Batubara, Supina. "Analisis perbandingan metode fuzzy mamdani dan fuzzy sugeno untuk penentuan kualitas cor beton instan." IT Journal Research and Development 2.1 (2017): 1-11

Fachri, B. (2018, September). Aplikasi Perbaikan Citra Efek Noise Salt & Papper Menggunakan Metode Contraharmonic Mean Filter. In Seminar Nasional Royal (Senar) (Vol. 1, No. 1, Pp. 87-92).

Fachri, Barany. "Aplikasi Perbaikan Citra Efek Noise Salt & Papper Menggunakan Metode Contraharmonic Mean Filter." Seminar Nasional Royal (Senar). Vol. 1. No. 1. 2018.

Fachri, Barany. Aplikasi Perbaikan Citra Efek Noise Salt & Papper Menggunakan Metode Contraharmonic Mean Filter. In: Seminar Nasional Royal (Senar). 2018. P. 87-92.

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

Ginting, G., Fadlina, M., Siahaan, A. P. U., & Rahim, R. (2017). Technical approach of TOPSIS in decision making. Int. J. Recent Trends Eng. Res, 3(8), 58-64.

Hermansyah, Sembriring. 2012. "Sistem Informasi Jumlah Angkatan Kerja Menggunakan Visual Basic Pada Badan Pusat Statistik (Bps) Kabupaten Langkat". Jurnal Mahasiswa Teknik Informatika STMIK Kaputama.

Herry, Raditya 2014. “Buku Pintar VB.Net”. Jakarta : Elex Media Komputindo.

Indrajani, 2015. “Perencanaan Basis Data dalam All in 1”. Jakarta : Elex Media Komputindo.

Jogiyanto, Hartono. 2013. “Analisis & desain sistem informasi : pendekatan terstruktur teori dan praktek aplikasi bisnis”. Yogyakarta : Penerbit Andi.

Juansyah, Andi, 2015. “Pembangunan Aplikasi Child Tracker Berbasis Assisted – Global Positioning System (A-Gps) Dengan Platform Android”. Jurnal Ilmiah Komputer dan Informatika Universitas Komputer Indonesia.

Kamil, Ferdian, 2016. Implementasi Kriptografi Dengan Menggunakan Algoritma Advanced Encryption Standard (AES 256) Dan Lempel Ziv Welch(LZW) Sebagai Pengaman Data Pada PT .Lea Sanent. Jurnal Mahasiswa Program Studi Teknik Informatika STMIK Raharja

Khairul, K., IlhamiArsyah, U., Wijaya, R. F., & Utomo, R. B. (2018, September). Implementasi Augmented Reality Sebagai Media Promosi Penjualan Rumah. In Seminar Nasional Royal (Senar) (Vol. 1, No. 1, pp. 429-434).

Kurniawan, H. (2018). Pengenalan Struktur Baru untuk Web Mining dan Personalisasi Halaman Web. Jurnal Teknik dan Informatika, 5(2), 13-19

Mayasari, Nova. "Comparison of Support Vector Machine and Decision Tree in Predicting On-Time Graduation (Case Study: Universitas Pembangunan Panca Budi)." Int. J. Recent Trends Eng. Res 2.12 (2016): 140-151.

Nugroho, Bunafit. 2015. ”Aplikasi Pemrograman Web Dinamis Dengan PHP dan MySQL”. Yogyakarta : Penerbit Gava Media.

Pabokory, Fresly Nandar, 2015. Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. Jurnal Mahasiswa Program Studi Ilmu Komputer Universitas Mulawarman.

Putera, A., Siahaan, U., & Rahim, R. (2016). Dynamic key matrix of hill cipher using genetic algorithm. Int. J. Secur. Its Appl, 10(8), 173-180.

Putra, Dedek Irwansyah Dkk, 2017. “Perancangan Aplikasi Penyandian Data Text Menggunakan Metode Symmetric Stream Cipher”. Jurnal Mahasiswa Program Studi Teknik Informatika STMIK Budidarma Medan.

Putra, Randi Rian, and Cendra Wadisman. "Implementasi Data Mining Pemilihan Pelanggan Potensial Menggunakan Algoritma K Means." INTECOMS: Journal of Information Technology and Computer Science 1.1 (2018): 72-77.

Rahim, R., Supiyandi, S., Siahaan, A. P. U., Listyorini, T., Utomo, A. P., Triyanto, W. A., ... & Khairunnisa, K. (2018, June). TOPSIS Method Application for Decision Support System in Internal Control for Selecting Best Employees. In Journal of Physics: Conference Series (Vol. 1028, No. 1, p. 012052). IOP Publishing.

Sari, R. D., Supiyandi, A. P. U., Siahaan, M. M., & Ginting, R. B. (2017). A Review of IP and MAC Address Filtering in Wireless Network Security. Int. J. Sci. Res. Sci. Technol, 3(6), 470-473.

Siahaan, A. P. U., Aryza, S., Nasution, M. D. T. P., Napitupulu, D., Wijaya, R. F., & Arisandi, D. (2018). Effect of matrix size in affecting noise reduction level of filtering.

Siahaan, MD Lesmana, Melva Sari Panjaitan, and Andysah Putera Utama Siahaan. "MikroTik bandwidth management to gain the users prosperity prevalent." Int. J. Eng. Trends Technol 42.5 (2016): 218-222.

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

Tasril, V. (2018). Sistem Pendukung Keputusan Pemilihan Penerimaan Beasiswa Berprestasi Menggunakan Metode Elimination Et Choix Traduisant La Realite. INTECOMS: Journal of Information Technology and Computer Science, 1(1), 100-109.

Tumpal, Halomoan Manurung. 2016. “Perancangan Aplikasi Pembelajaran Logika Dan Algoritma Dengan Menggunakan Metode Computer