



RANCANGAN APLIKASI KRIPTOGRAFI KLASIK DAN PLAYFAIR CIPHER BERBASIS JAVA

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 : BENRIKSON SIMALANGO

N.P.M : 1414370725

PROGRAM STUDI : SISTEM KOMPUTER

**FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
2019**

LEMBAR PENGESAHAN

RANCANGAN APLIKASI KRIPTOGRAFI KLASIK DAN PLAYFAIR CIPHER BERBASIS JAVA

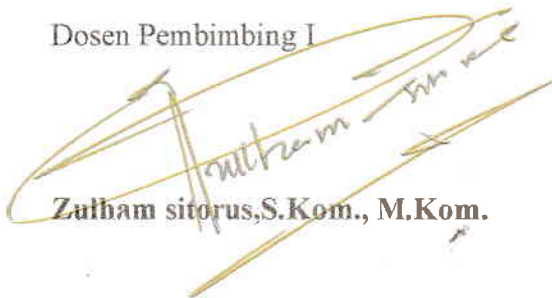
Disusun Oleh :

Nama : Benrikson Simalango
NPM : 1414370725
Program studi : Ilmu Komputer

Skripsi Telah Disetujui Oleh Dosen Pembimbing Skripsi

Pada tanggal : 28 Agustus 2019

Dosen Pembimbing I



Zulham sitorus, S.Kom., M.Kom.

Dosen Pembimbing II



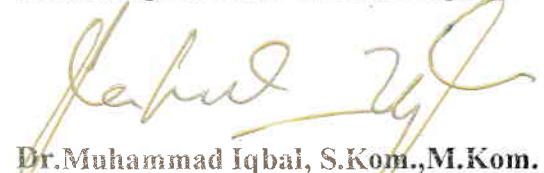
Akhyar Lubis, S.Kom., M.Kom

Mengetahui,

Dekan Fakultas Sains dan Teknologi



Ketua Program Studi sistem Komputer



Dr. Muhammad Iqbal, S.Kom., M.Kom.

PERNYATAAN ORISINALITAS

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



1414370725

SURAT PERNYATAAN

Saya yang bertanda tangan dibawah ini :

Nama : Bendriksan Simalungu
NPM : 1414370725
Prodi : Sistem Komputer
Konsentrasi : KJIK
Judul Skripsi : Rancangan Aplikasi Kriptografi Kunci dan Keypair Cipher Berbasis Java

Dengan ini saya menyatakan bahwa :

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

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

Medan, 28 agustus 2019

Yang membuat pernyataan

 Bendriksan

ANDA BEBAS PUSTAKA

No. 1910/Perp/EP/2019

Dinyatakan tidak ada sangkut paut dengan UPT Perpustakaan

UNIVERSITAS PEMBANGUNAN PASCA SARJANA (UNPAB) INDONESIA

08 MAR 2019

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau



Medan, 05 Maret 2019
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama : BENRIKSON BENDIKTUS SIMALANGO
Tempat/Tgl. Lahir : MEDAN / 09 Oktober 1987
Nama Orang Tua : JHONER SIMALANGO
N. P. M : 1414370725
Fakultas : SAINS & TEKNOLOGI
Program Studi : Sistem Komputer
No. HP : 085361038431
Alamat : JL.PASUNDAN no 3b

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul Rancangan aplikasi kriptografi klasik dan playfair cipher berbasis java, Selanjutnya saya menyatakan :

1. Melampirkan KKM yang telah disahkan oleh Ka. Prodi dan Dekan
2. Tidak akan menuntun 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 exemplar (1 untuk perpustakaan, 1 untuk mahasiswa) dan jilid kertas jeruk 5 exemplar untuk penguji (bentuk dan warna penjiilidan 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.	250,000
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

UK.T. 50%

Rp.

1.855.000
3.240.000
Rp. 5.095.000

12/03-19
M

Ukuran Toga :



Hormat saya

BENRIKSON BENDIKTUS SIMALANGO
1414370725

Catatan :

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

Telah di terima
berkas persyaratan
dapat di proses
Medan, 12 MAR 2019
Ka. BPAA

TEGUH WAHYONO, SE., MM.





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

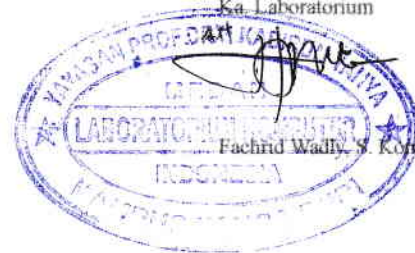
KARTU BEBAS PRAKTIKUM

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

Nama : BENRIKSON SIMALANGO
N.P.M. : 1414370725
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, 12 Maret 2019
Ka. Laboratorium



Plagiarism Detector v. 1079 - Originality Report:

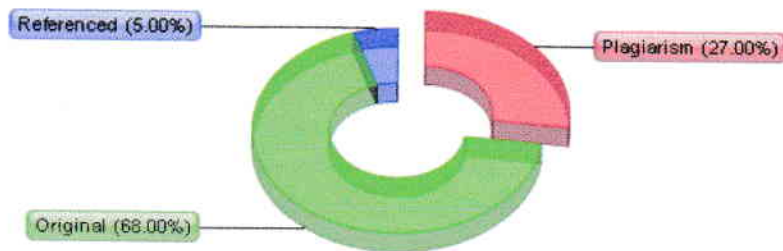
Analyzed document: 3/8/2019 11:43:28 AM

"BENRIKSON SIMALANGO_1414370752_SISTEM KOMPUTER.docx"

Licensed to: Universitas Pembangunan Panca Budi_License3



Relation chart:



Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

Top sources of plagiarism:

% 6	wrds: 411	http://semuasatu233.blogspot.com/2014/09/pengertian-dan-fungsi-uml_13.html
% 4	wrds: 293	https://tid3ustj.blogspot.com/2013/02/tahukah-kamu-tentang-kriptografi-sandi.html
% 4	wrds: 284	http://a11-4701-03695.blogspot.com/2010/10/sistem-cipher-substitusi-adalah-sebuah.html

[Show other Sources:]

Processed resources details:

186 - Ok / 36 - Failed

[Show other Sources:]

Important notes:

Wikipedia:

Google Books:

Ghostwriting services:

Anti-cheating:



UNIVERSITAS PEMBANGUNAN PANCA BUDI FAKULTAS SAINS & TEKNOLOGI

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

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

PERMOHONAN MENGAJUKAN JUDUL SKRIPSI

Yang bertanda tangan di bawah ini :

Nama Lengkap	: BENRIKSON BENDIKTUS SIMALANGO
Tempat/Tgl. Lahir	: MEDAN / 09 Oktober 1987
Nomor Pokok Mahasiswa	: 1414370725
Program Studi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer
Jumlah Kredit yang telah dicapai	: 125 SKS, IPK 3.36

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

No.	Judul Skripsi	Persetujuan
1.	Rancangan aplikasi pekerjaan harian lepas untuk pemberi kerja dan pencari kerja berbasis android	<input type="checkbox"/>
2.	rancangan aplikasi pengamanan data dengan menggunakan sistem kriptografi rsa berbasis java	<input type="checkbox"/>
3.	Rancangan aplikasi keamanan data menggunakan sistem kriptografi ElGamal berbasis java <i>Playfair cipher</i>	<input checked="" type="checkbox"/>

Judul yang disetujui oleh Kepala Program Studi diberikan tanda

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

Medan, 21 Mei 2018

Pemohon,

 (BENRIKSON BENDIKTUS SIMALANGO)

Nomor :
 Tanggal :
 Disahkan oleh :

 (Sri Sandi Andira, S.T., M.Sc.)

Tanggal : 29.0.2018
 Disetujui oleh :
 Dosen Pembimbing I:

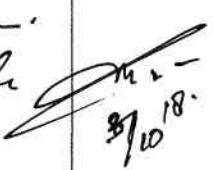
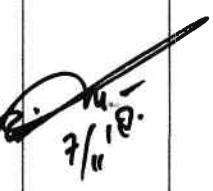


Tanggal :
 Disetujui oleh:
 Ka. Prodi Sistem Komputer

 (MULHAMMAD IOBAL, S.Kom., M.Kom.)

Tanggal : 30/05/2018
 Disetujui oleh:
 Dosen Pembimbing II:

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

Universitas : Universitas Pembangunan Panca Budi
 Fakultas : SAINS & TEKNOLOGI
 Dosen Pembimbing I : ZULHAM SITORUS
 Dosen Pembimbing II : AKHYAR LUBIS
 Nama Mahasiswa : BENRIKSON BENDIKTUS SIMALANGO
 Jurusan/Program Studi : Sistem Komputer
 Nomor Pokok Mahasiswa : 1414370725
 Jenjang Pendidikan : Si Ilmu komputer
 Judul Tugas Akhir/Skripsi : Rancangan Aplikasi Kriptografi klasik dan
 Playfair cipher Berbasis Java

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
3/10 18.	Revisi Judul, sesuai dengan permasalahan, dan sejarahnya. Terlibat magistat.	 3/10 18.	
7/11 18.	Revisi i, ii, iii, Analisa di pergilas, proses enkripsi dan dekripsi. Audio.	 7/11 18.	
8/1 19.	Ranang ulang bab iii dan iv. Untuk perancangan dan hasilnya di sesuaikan.		
28/1 19.	Au. Seminar.		

Medan, 14 September 2018

Diketahui/Disetujui oleh :
 Dekan



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



UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI

Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

Universitas : Universitas Pembangunan Panca Budi
 Fakultas : SAINS & TEKNOLOGI
 Dosen Pembimbing I : Zulhan Setiawan
 Dosen Pembimbing II : Murya Lubis
 Nama Mahasiswa : BENRIKSON BENDIKTUS SIMALANGO
 Jurusan/Program Studi : Sistem Komputer
 Nomor Pokok Mahasiswa : 1414370725
 Jenjang Pendidikan : Si Ilmu Komputer
 Judul Tugas Akhir/Skripsi : Rancangan Aplikasi Kriptografi Klasik dan
 Modern Cipher Berbasis Java

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
25/29 Feb	Acc. Sidang mjd hjn		
2/8/18	Acc. Sidang		

Medan, 11 Oktober 2018



*) Coret yang tidak perlu

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI

Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571
 website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
 Medan - Indonesia

Universitas : Universitas Pembangunan Panca Budi
 Fakultas : SAINS & TEKNOLOGI
 Dosen Pembimbing I : Zuhani Sitorus
 Dosen Pembimbing II : Akhyar Tubis
 Nama Mahasiswa : BENRIKSON BENDIKTUS SIMALANGO
 Jurusan/Program Studi : Sistem Komputer
 Nomor Pokok Mahasiswa : 1414370725
 Jenjang Pendidikan : SI Ilmu komputer
 Judul Tugas Akhir/Skripsi : Rancangan Kriptografi Klasik dan Playfair cypher berbasis Java

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
14/9/2018	- Perbaiki di latar belakang. rumusan masalah & batasan - tambahkan kesimpulan teori terkait		
27/9/2018	Ace Bab I, Perbaiki di penulisan Ace Bab I, II, III		
3/12/2018	Demo Aplikasi ? Bab I, & Definisi ? Ace Bab II		
24/09/2019	Conslusi Ace Summary		

Medan, 14 September 2018

Diketahui/Disetujui oleh :



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



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

Universitas : Universitas Pembangunan Panca Budi
 Fakultas : SAINS & TEKNOLOGI
 Dosen Pembimbing I : *DILHAM Situmorang*
 Dosen Pembimbing II : *Allyar Lubis*
 Nama Mahasiswa : BENRIKSON BENDIKTUS SIMALANGO
 Jurusan/Program Studi : Sistem Komputer
 Nomor Pokok Mahasiswa : 1414370725
 Jenjang Pendidikan : S.
 Judul Tugas Akhir/Skripsi : *Rancangan Kriptografi klasik dan Playfair*
untuk keabsahan Jawa

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
<i>22/2/2019</i>	<i>Aa Sidang</i>	<i>[Signature]</i>	
<i>30/08/2019</i>	<i>Ace Jolid</i>	<i>[Signature]</i>	

Medan, 11 Oktober 2018
 Disetujui oleh :
 Dekan,


 Indra, S.T., M.Sc.

*) Coret yang tidak perlu

ABSTRAK

Pengamanan setiap pesan memo atau file penting dari suatu pemimpin tertinggi dari suatu lembaga kepada masing masing anggotanya adalah suatu hal yang wajib dilakukan . Perintah atau pesan strategi penting dari pemimpin tidak boleh jatuh kepihak yang salah tidak bertanggung jawab . dalam pengiriman pesan saat ini melalui media komunikasi jaringan internet public sangat rentan untuk bias di curi ataupun di ubah oleh pihak tertentu yang memang berminat mencuri filetersebut. Kriptografi pada setiap pesan atau perintah dapat diterapkan untuk menjaga kerahasiaan apabila pendistribusian pesan melalui jaringan internet public di curi tapi tak dapat dipahami isinya. Dengan memberikan modifikasi pada aplikasi kriptografi playfair cipher sekarang bias digunakan untuk pengiriman file penting dalam kapasitas yang cukup dan aman kepada setiap bawahannya di daerah masing masing. Hal ini dapat membuat pendistribusian pesan menjadi aman untuk melalui media apapun seperti internet jaringan public.

Kata kunci : Kriptografi, Memo, Rahasia, Playfair Cipher

DAFTAR ISI

	Halaman
KATA PENGANTAR	i
DAFTAR ISI	iii
DAFTAR GAMBAR	vi
DAFTAR TABEL	viii
DAFTAR LAMPIRAN	ix
BAB 1 PENDAHULUAN	
1.1 Latar Belakang Masalah	1
1.2 Perumusan Masalah	2
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Metode Penelitian	4
BAB 2 LANDASAN TEORI	
2.1 Pengertian Aplikasi	5
2.2 Kriptografi	6
2.2.1 Tujuan Kriptografi	7
2.2.2 Penyandian Kriptografi	8
2.2.3 Terminologi Kriptografi	10
2.3 Definisi Kriptografi	11
2.3.1 Caesar Cipher	11
2.3.2 Monoalphabetic Cipher	13

2.3.3 Playfair Cipher	13
2.4 Bahasa Pemrograman Java	15
2.5 Provider Java Kriptografi	18
2.6 Struktur Data	18
2.7 UML (Unified Modeling Language)	20
2.7.1 Pengertian Umum	20
2.7.2 Penggunaan Unified Modeling Language (UML)	20
2.7.3 Tabel Diagram Main Concept UML	21
2.7.4 Activity Diagram	23
2.7.5 <i>UseCase</i> Diagram	25
2.7.6 Class Diagram	26
2.8 Pengertian Flowchart	27
2.8.3 Jenis Jenis Flowchart	29
2.8.4 Pedoman Dalam Membuat Flowchart	29
2.9 Netbeans	30
2.9.1 Definisi Netbeans	30
2.9.2 Komponen Tolls Pallet Netbeans IDE	31
2.9.3 Fitur pada Netbeans	34

BAB 3 ANALISA DAN PERANCANGAN SISTEM

3.1 Analisa Playfair Cipher	35
3.2 Persamaan Proses Enkripsi	36
3.3 Perancangan Arsitektur Aplikasi	39
3.4 Diagram Usecase	40
3.5 Perancangan Antarmuka	42

3.6 Diagram Alur	48
------------------------	----

BAB 4 IMPLEMENTASI DAN PENGUJIAN APLIKASI

4.1 Rancangan Aplikasi	51
4.2 Tahap Implementasi kelas	52
4.3 Perancangan Struktur Data	53
4.4 Tampilan Antarmuka	58
4.5 Proses Pengujian Aplikasi	62
4.5.1 Pengujian Enkripsi	63
4.5.2 Pengujian Dekripsi Cipher Text	66

BAB 5 PENUTUP

5.1 Kesimpulan	69
5.2 Saran	69

DAFTAR PUSTAKA

DAFTAR RIWAYAT HIDUP

LAMPIRAN

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Skema penyandian kunci simetrik	9
Gambar 2.2 Skema kriptografi asimetris	10
Gambar 2.3 Fase pemrograman java	15
Gambar 2.4 Contoh activity diagram	23
Gambar 2.5 Contoh usecase Diagram	25
Gambar 2.6 Contoh class diagram	26
Gambar 2.7 Tampilan menu utama netbeans IDE	30
Gambar 2.8 Toolpallet netbeans IDE	31
Gambar 2.9 Navigator window pada netbeans	32
Gambar 2.10 Tampilan jendela pallet pada netbeans	33
Gambar 3.1 Perancangan arsitektur aplikasi	39
Gambar 3.2 Diagram usecase perangkat lunak	40
Gambar 3.3 Perancangan Tampilan jendela masuk	42
Gambar 3.4 Perancangan tampilan jendela pertama	43
Gambar 3.5 Rancangan Tampilan monoalphabetic	45
Gambar 3.6 Rancangan tampilan antarmuka playfair cipher	49
Gambar 3.7 Flowchart proses enkripsi aplikasi kriptografi	50
Gambar 3.8 Flowchart proses dekripsi aplikasi kriptografi	53
Gambar 4.1 Screenshot code pembentukan string key	54
Gambar 4.2 Source code kelas tampilan antarmuka aplikasi.....	56
Gambar 4.3 Sourcecode action button monoalphabetic	57
Gambar 4.4 action button playfaircipher enkripsi	58
Gambar 4.5 Tampilan frame masuk aplikasi	58

Gambar 4.6 Tampilan antar muka caesar cipher	59
Gambar 4.7 Tampilan antarmuka monoalphabetic cipher	60
Gambar 4.8 Tampilan antarmuka playfair cipher	61
Gambar 4.9 Proses enkripsi pesan dengan playfair cipher.....	63
Gambar 4.10 Proses enkripsi pesan dengan monoalphabetic	64
Gambar 4.11 Proses enkripsi pesan dengan playfair cipher	65
Gambar 4.12 Proses enkripsi pesan dengan caesar cipher.....	66
Gambar 4.13 Proses dekripsi pesan monoalphabetic cipher	67
Gambar 4.14 Proses dekripsi pesan playfair cipher	68

DAFTAR TABEL

	Halaman
Tabel 2.1 Contoh tabel kunci playfair cipher	14
Tabel 2.2 Diagram main konsep	22
Tabel 2.3 Symbol activity diagram	24
Tabel 2.4 Symbol flowchart dan fungsinya	26
Tabel 3.1 Contoh matriks kunci	37
Tabel 3.2 Usecase narative aplikasi	41
Tabel 4.1 Daftar implementasi kelas	52

KATA PENGANTAR

Puji dan syukur kepada Tuhan yang Maha Esa karena dengan berkat dan kasih anugrah nya penulis masih diberi kesehatan dan kesempatan untuk menyelesaikan tugas akhir saya yang berjudul : “ RANCANGAN APLIKASI KRIPTOGRAFI KLASIK DAN PLAYFAIR CIPHER BERBASIS JAVA”

Dalam kesempatan ini penulis ingin menyampaikan terima kasih sebesar-besarnya kepada pihak banyak pihak yang telah membantu dalam menyelesaikan penyusunan Tugas Akhir ini. Penulis ingin mengucapkan terima kasih sebesar-besarnya kepada :

1. Bapak Dr.H.Muhammad Isa Indrawan,S.E,M.M selaku Rektor Universitas Pembangunan Panca Budi.
2. Ibu Sri Shindi Indira, S.T .,M.SC selaku Dekan Fakultas Sains dan Teknologi Universitas Pembangunan Panca BuDI
3. Bapak Muhammad Iqbal, S.Kom, M.Kom selaku Ketua Program Studi Sistem Komputer Universitas Panca Budi
4. Bapak Zulham Sitorus,S.Kom, M.Kom selaku Dosen Pembimbing I Universitas Pembangunan Panca Budi Medan
5. Bapak Akhyar Lubis , S.Kom, M.Kom selaku Dosen Pembimbing II selaku Universitas Pembangunan Panca Budi Medan

6. Bapak dan Ibu Dosen dan staff Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi yang telah banyak memberikan bimbingan akeademis selama perkuliahan ini
7. Orang tua yang sangat saya sayangi yang telah banyak memberikan dukungan moril, material dan doa kepada saya sehingga dapat menyelesaikan kuliah ini untuk dapat mencapai gelar S.Kom pada Universitas Panca Budi
8. Teman-teman semasa kuliah yang sudah saling membantu dan menemani selama kita kuliah bersama di Universitas Pembangunan Panca Budi

Penulis juga menyadari bahwa penyusunan Tugas Akhir ini belum begitu sempurna baik dalam penulisan maupun isinya yang disebabkan keterbatasan kemampuan penulis. Oleh karena itu penulis mengharapkan adanya kritik dan saran yang sifatnya membangun dari pembaca untuk penyempurnaan Tugas Akhir Ini.

Medan 28 Agustus 2019

Penulis

BENRIKSON SIMALANGO
NPM. 1414370725

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Salah satu permasalahan dalam sistem pertukaran informasi transaksi data atau file, adalah pencurian data file. Setiap transaksi pengiriman data yang melintas pada jaringan publik seperti internet dapat diasumsikan mudah diakses oleh siapapun termasuk oleh pihak tertentu yang memang berniat untuk mencuri atau mengubah data. Suatu data penting yang dikirim melalui jaringan internet publik rentan dengan adanya kemungkinan untuk diambil ataupun di ubah data aslinya. Sudah banyak kasus yang terjadi akibat data yang dicuri seseorang atau sebuah lembaga mengalami kerugian yang besar.

Salah satu teknik untuk menjaga kerahasiaan pesan yang paling banyak digunakan dan dikenal saat ini adalah teknik enkripsi data menggunakan sebuah aplikasi khusus enkripsi dan deskripsi data yang menggunakan kriptografi. Teknik kriptografi telah banyak digunakan saat perang dunia untuk menyampaikan pesan rahasia dari pemimpin tertinggi di pusat kepada setiap komandan perang di tempat tertentu. Dalam perkembangan algoritma kriptografi, data yang akan dikirim terlebih dahulu dienkripsi sehingga tidak mudah di baca oleh pihak yang tidak berwenang/berhak (margoselo,2003). Dalam era digital saat ini suatu aplikasi komputer dapat dirancang dengan bahasa pemrograman tertentu menggunakan algoritma yang sudah ada.

Kelengkapan perpustakaan kumpulan program program yang disertakan dalam pemrograman java yang sangat memudahkan penulis dalam penggunaan

untuk membangun aplikasinya kriptografi berbasis java. Berdasarkan uraian tersebut penulis tertarik untuk mengkaji lebih lanjut teknik kriptografi playfair cipher dan merancang aplikasinya dengan bahasa pemrograman berbasis java. Dengan membuat sebuah pemrograman java dan dikompilasi hasilnya dapat dijalankan diatas beberapa platform tanpa perubahan seperti pada komputer sistem operasi komputer windows dan sistem operasi komputer lainnya. Oleh karena itu, penulis tertarik mengembangkan dan mengambil judul skripsi **“Rancangan Aplikasi Kriptografi Klasik Dan Playfair Cipher Berbasis Java”**.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan penulis ingin memberikan suatu perancangan atau implementasi sistem rumusan masalah dalam penelitian yaitu sebagai berikut:

1. Bagaimana membuat aplikasi enkripsi dan deskripsi file atau pesan yang terjamin keamanannya .
2. Bagaimana merancang dan mengimplementasikan suatu sistem aplikasi kriptografi pengamanan file berbasis java.
3. Bagaimana mengetahui tingkat keamanan aplikasi kriptografi pada proses enkripsi dan deskripsi file data text.

1.3 Batasan Masalah

Program aplikasi komputer yang dibuat akan menerapkan bahasa pemrograman java. Proses yang dilakukan oleh pemrograman aplikasi ini memiliki batasan masalah sebagai berikut:

1. Dukungan hardware komputer dan sistem operasi khusus komputer windows
2. Hanya dapat mengamankan data dengan ukuran yang terbatas
3. Batasan suatu aplikasi dalam proses kecepatan enkripsi dan deskripsi file

1.4 Tujuan penelitian

Tujuan dari penelitian yang di bahas dalam pembuatan aplikasi kriptografi playfair cipher berbasis java adalah sebagai berikut ini :

1. Menyelesaikan design program aplikasi yang telah di setuju sebelumnya.
2. Menguji apakah aplikasi berjalan sesuai dengan struktur aliran program aplikasi yang telah di rancang.
3. Menguji bahwa pemakai program aplikasi (*user*) dapat menjalankan program aplikasi tersebut.
4. Menguji fungsi utama dari aplikasi kriptografi berbasis java.

1.5 Manfaat Penelitian

Berikut ini beberapa manfaat penelitian yang akan dibahas dalam penelitian.

Ada pun manfaat dari penelitian membuat aplikasi ini adalah sebagai berikut:

1. Mengembangkan sistem aplikasi keamanan data kriptografi yang efisien dan berbeda dari yang sudah ada.
2. Menerapkan apa yang telah dipelajari selama perkuliahaan untuk pengembangan yang lebih lanjut dalam membuat suatu aplikasi

1.6 Metode penelitian

Berikut ini adalah metode penelitian yang akan dibahas dalam penelitian ini adalah sebagai berikut :

1. Membaca dan mempelajari karya tulis yang pernah dibuat atau diterbitkan melalui media cetak seperti buku, jurnal dan skripsi yang telah terbukti dan teruji hasilnya.
2. Melakukan penelitian dengan mempelajari setiap detail aplikasi sejenis yang pernah ada sebelumnya.
3. Melakukan best practise yang terdapat dalam industri perangkat lunak sejenis dengan penggunaa metode unified model languange. Keuntungan dari penggunaan metode ini adalah akses yang mudah terhadap pengetahuan dasar sehingga memungkinkan untuk secara sistemis dan teratur mengontrol perubahan yang terjadi pada perangkat lunak.

BAB II

LANDASAN TEORI

2.1 Pengertian Aplikasi

Menurut Jogiyanto (1992:12) Aplikasi adalah penggunaan dalam suatu komputer, instruksi (instruction) atau pernyataan yang disusun sedemikian rupa sehingga komputer dapat memproses input menjadi output. Aplikasi komputer merupakan sebuah program perangkat lunak dari komputer untuk mempermudah setiap pengguna komputer melakukan tugas-tugas nya sesuai kebutuhan kerja. Hengky W.Pramana (2012:2) mengungkapkan: aplikasi adalah suatu perangkat lunak komputer yang dibuat untuk melayani kebutuhan akan beberapa aktifitas yang memakai komputer seperti sistem perniagaan, game, pelayanan masyarakat, periklanan atau sebagian proses yang banyak dilakukan oleh manusia.

Aplikasi komputer dapat dirancang dari berbagai jenis bahasa pemrograman komputer sesuai kebutuhan dan fungsi aplikasi tersebut. Jadi dapat diambil kesimpulan perangkat aplikasi adalah suatu sub kelas perangkat lunak komputer yang memanfaatkan langsung komputer mengerjakan suatu perintah tugas yang diinginkan pengguna komputernya. Contoh aplikasi yang paling sering dipakai adalah pemutar media, pengolah gambar dan pengolah karakter kata. Beberapa dari aplikasi hanya dapat digunakan untuk satu sistem operasi komputer seperti misalnya aplikasi Microsoft word hanya dapat dijalankan pada sistem operasi. Beberapa aplikasi yang saling terkait dan saling terhubung digabung bersama menjadi satu paket disebut

juga sebagai *application suite*. Seperti yang diimplimentasikan dalam *Microsoft office*. Aplikasi dalam suatu paket Microsoft office ini biasanya memiliki antar muka (*interface*) yang memiliki kesamaan dan penggunaan yang saling terkait sehingga memudahkan pengguna untuk mempelajari dan menggunakan setiap aplikasi tersebut.

2.2 Kriptografi

Kriptografi (*cryptography*) merupakan ilmu dan seni penyandian untuk menjaga pesan agar menjaga keamanan dan kerahasiaan pesan. Kriptografi berasal dari dua kata Yunani, yaitu *Crypto* berarti “*secret*” (rahasia) dan *grapho* berarti “*writing*” (tulisan). Merupakan metode untuk mengamankan data teks, metode ini dilakukan dengan penyandian atau pengacakan data asli sehingga pihak lain yang tidak mempunyai hak akses atas data tersebut tidak dapat memperoleh informasi yang ada didalamnya (Ariyus,2006:77).

Berdasarkan catatan sejarah diambil dari kata *Cryptography* sudah digunakan sejak bangsa Mesir 4000 tahun yang lalu oleh raja Mesir pada saat menghadapi perang untuk mengirimkan pesan rahasia kepada panglima perangnya melalui kurirnya. Teknik untuk mengacak pesan-pesan rahasia agar tidak dapat diketahui maknanya disebut enkripsi dan membentuk bidang keilmuan yang disebut kriptografi prinsipnya adalah menyembunyikan pesan informasi sedemikian rupa agar orang yang berhak saja yang dapat mengetahui informasi tersebut (Wibowo,2008).

Saat ini dalam kriptografi modern telah berkembang berbagai metode algoritma kriptografi. Pesan yang dirahasiakan dinamakan plainteks, sedangkan

pesan hasil penyandian disebut ciperteks. Proses penyandian plainteks menjadi ciperteks disebut enkripsi dan proses membalikan ciperteks menjadi plainteks asalnya disebut dengan deskripsi (Munir,2010).

1.2.1 Tujuan Kriptografi

Hal yang paling utama dari kriptografi adalah aspek keamanan. Menurut Santi (2010) ada empat tujuan mendasar dari kriptografi yang menerapkan aspek keamanan informasi. Aspek-aspek keamanan kriptografi adalah sebagai berikut:

1. Kerahasiaan (*confidentiality*)

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

2. Integritas Data (*data Integrity*)

Merupakan aspek layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman.

3. Otentikasi (*Authentication*)

Merupakan layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan /data (*original authentication*).

4. Penyangkalan (*non-repudiation*)

Merupakan layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

2.2.2 Penyandian Kriptografi

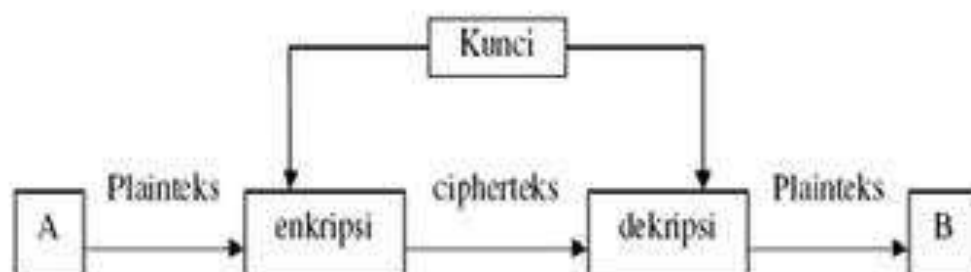
Sistem sistem kriptografi terus mengalami pengembangan Rangkuman beberapa mekanisme yang berkembang pada kriptografi modern adalah sebagai berikut ini:

1. Fungsi Hash.

Merupakan fungsi kriptografi modern yang melakukan pemetaan pada pesan dengan panjang sembarangan ke sebuah teks khusus yang disebut *message digest* dengan panjang tetap. Fungsi hash pada umumnya dipakai sebagai nilai uji (*check value*) pada mekanisme keutuhan data.

2. Penyandian Kunci Simetrik (*symmetric key encryption*)

Penyandian dengan kunci simetrik adalah penyandian yang kunci enkripsinya dan kunci deskripsinya bernilai sama. Kunci pada penyandian simetrik diasumsikan bersifat rahasia hanya pihak yang melakukan enkripsi dan deskripsi yang mengetahui nilainya. Oleh sebab itu penyandian dengan kunci simetrik disebut juga dengan penyandian menggunakan kunci rahasia (*secret key encryption*).

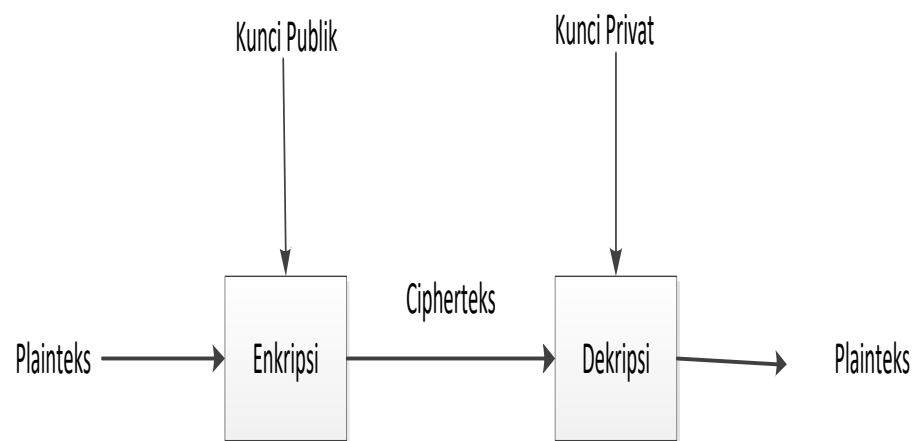


Gambar 2.1 Skema Penyandian kunci simetrik

Sumber :Kriptografi untuk Keamanan Jaringan;Rifki Sadikin(2012)

3. Penyandian Kunci Asimetrik (*Asymmetric key encryption*)

Sandi dengan kunci Asimetrik atau biasa disebut juga dengan penyandian kunci publik (*public key*). Merupakan penyandian dengan kunci enkripsi dan deskripsi berbeda nilai. Contoh algoritma diantaranya RSA, Elgemal, dan DSA. Gambar berikut ini menunjukkan bagaimana cara kerja kriptografi asimetris, *Plainteks* dienkripsi dengan kunci publik kemudian menghasilkan *cipherteks*. Kemudian untuk mendeskripsi *cipherteks* membutuhkan kunci *private* yang menghasilkan pesan asli atau *plainteks*.



Gambar 2.2 Skema Kriptografi Asimetris

Sumber: Kriptografi untuk Keamanan Jaringan; Rifki Sadikin (2012)

Berdasarkan gambar diatas, jika kunci 1 tidak sama dengan kunci 2, maka sistem kriptografinya dinamakan sistem kriptografi kunci asimetri. Kunci enkripsi yang juga disebut dengan kunci publik bersifat terbuka. Sedangkan, kunci deskripsi yang juga disebut kunci privat (*privat key*) bersifat tertutup/ rahasia.

2.2.3 Terminologi Kriptografi

Beberapa istilah terminology dalam kriptografi dapat dijelaskan sebagai berikut (Munir dalam Susilowati, 2016).

1. *Plaintext*: pesan, data ataupun suatu informasi yang dapat dibaca dan maknanya dapat dimengerti.
2. *Ciphertext*: suatu bentuk pesan yang tersandikan, sehingga maknanya tidak dapat dimengerti
3. pengirim: entitas yang mengirim pesan kepada entitas penerima
4. penerima: entitas yang menerima pesan dari entitas pengirim.
5. Media komunikasi data: media tempat lalu lintas data atas informasi pada proses pengiriman dan penerimaan data/ informasi
6. Enkripsi: proses untuk menyandikan *plaintext* menjadi *ciphertext*.
7. Deskripsi : proses pengurai sandi dari *ciphertext* menjadi *plaintext*
8. Kunci (key) : parameter yang digunakan untuk mentransformasi proses pengenkripsian dan pendeskripsian pesan.
9. Kunci simetri : kunci yang proses enkripsi dan deskripsi menggunakan kunci yang sama yang bersifat dan hanya boleh diketahui oleh pengirim dan penerima pesan . kunci simetri biasa disebut juga dengan kunci privat.
10. Kunci asimetri; kunci yang proses enkripsi dan deskripsinya menggunakan kunci yang berbeda yaitu kunci publik dan kunci privat.

2.3 Definisi Kriptografi

2.3.1 Caesar Cipher

Dalam kriptografi, sandi Caesar, atau sandi geser, kode Caesar atau Geseran Caesar adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (plaintext) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Misalnya, jika menggunakan geseran 3, W akan menjadi Z, I menjadi L, dan K menjadi N sehingga teks terang "wiki" akan menjadi "ZLNL" pada teks tersandi. Nama Caesar diambil dari Julius Caesar, jenderal, konsul, dan diktator Romawi yang menggunakan sandi ini untuk berkomunikasi dengan para panglimanya. Cara kerja sandi ini dapat diilustrasikan dengan membariskan dua set alfabet; alfabet sandi disusun dengan cara menggeser alfabet biasa ke kanan atau ke kiri dengan angka tertentu (angka ini disebut kunci). Misalnya sandi Caesar dengan kunci 3, adalah sebagai berikut:

Alfabet Biasa: ABCDEFGHIJKLMNOPQRSTUVWXYZ

Alfabet Sandi: DEFGHIJKLMNOPQRSTUVWXYZABC

Untuk menyandikan sebuah pesan, cukup mencari setiap huruf yang hendak disandikan di alfabet biasa, lalu tuliskan huruf yang sesuai pada alfabet sandi. Untuk memecahkan sandi tersebut gunakan cara sebaliknya. Contoh penyandian sebuah pesan adalah sebagai berikut:

teks terang: kirim pasukan ke sayap kiri

teks tersandi: NLULP SDVXNDQ NH VDBDS NLUL

Proses penyandian (enkripsi) dapat secara matematis menggunakan operasi modulus dengan mengubah huruf-huruf menjadi angka, $A = 0, B = 1, \dots, Z = 25$. Sandi dari "huruf" x dengan geseran n secara matematis dituliskan dengan,

$$E_n(x) = (x + n) \bmod 26.$$

Sedangkan pada proses pemecahan kode (dekripsi), hasil dekripsi (D_n) adalah $D_n(x) = (x - n) \bmod 26$. Setiap huruf yang sama digantikan oleh huruf yang sama di sepanjang pesan, sehingga sandi Caesar digolongkan kepada, substitusi monoalfabetik, yang berlawanan dengan substitusi polialfabetik.

2.3.2 Monoalphabetic Cipher

Monoalphabetic Cipher (Cipher abjad tunggal) adalah enkripsi metode substitusi yang memetakan tiap-tiap abjad dengan abjad lain secara random, bukan metode pergeseran seperti Caesar cipher. Misal $A \rightarrow D, B \rightarrow I, C \rightarrow Q$ dan seterusnya. Enkripsi ini adalah metode enkripsi kedua termudah setelah Caesar cipher. Hal ini dilakukan untuk mempersulit kriptaanalis dalam menganalisa pola susunan plain text-nya. Namun demikian enkripsi substitusi abjad tunggal ini mudah sekali untuk dipecahkan dengan analisis frekuensi. Kalau diamati dalam suatu bahasa apapun, pasti terdapat huruf yang sering muncul, dan pastinya adalah huruf vokal seperti A, I, U, E, O.

2.3.3 Playfair Cipher

1. Pengertian Playfair Cipher

Sandi playfair cipher pada awalnya Ditemukan oleh Baron Lyon Playfair dan sir Charles Wheatstone dipakai pada tentara inggris pada saat perang

boer kedua dan perang dunia pertama. Playfair merupakan digraphs cipher yang artinya setiap proses enkripsi dilakukan pada setiap dua huruf. Metode playfair menggunakan tabel 5 x 5 dan semua alphabet kecuali “J” diletakkan kedalam tabel. Sesuai kesepakatan huruf j sama dengan huruf I sebab huruf j mempunyai frekuensi kemunculan yang sangat jarang.

2. Proses Enkripsi Playfair Cipher

Metode playfair cipher adalah salah satu sandi klasik yang menggunakan teknik manual simetrik enkripsi dan merupakan salah satu sandi substitusi berpasangan. Playfair cipher sudah memiliki aturan yang mutlak diawali menentukan kata kunci yang diinginkan, setelah itu kata kunci yang diinginkan dibentuk menjadi bujur sangkar 5x5. Berikut ini adalah contoh tabel kunci bujur sangkar playfair cipher untuk mengenkripsi sebuah kata yaitu “INFORMATIKA”.

Tabel 2.1 Contoh tabel kunci playfair cipher

I	N	F	O	R
M	A	T	K	B
C	D	E	G	H
J	L	P	Q	S
U	V	W	X	Y

3. Aturan Proses Dekripsi

Aturan proses dekripsi dari algoritma playfair cipher adalah kebalikan dari proses enkripsinya ketentuannya jika terdapat 2 huruf dalam baris kunci yang sama maka masing masing huruf diganti dengan yang huruf dikirinya (pada kunci yang sudah diperluas).

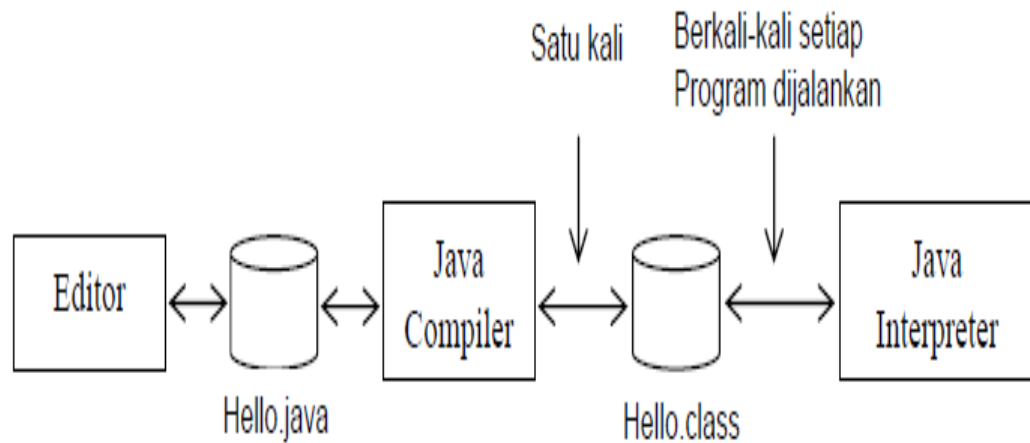
4. Apabila terdapat 2 huruf dalam kolom kunci yang sama

maka masing masing huruf diganti dengan huruf yang diatasnya (pada kunci yang sudah diperluas). Ketika dua huruf tidak terdapat pada baris atau kolom yang sama maka huruf pertama diganti pada huruf perpotongan baris huruf pertama dengan huruf kolom kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan.

2.4 Bahasa Pemerograman Java

Bahasa pemrograman dibuat oleh James Gosling dirilis tahun 1995 oleh perusahaan sun Microsystem. Kelebihan utama dari bahasa pemrograman berbasis java adalah dapat dijalankan di beberapa platform/ sistem operasi komputer. Dengan membuat sebuah pemrograman java dan dikompilasi hasilnya dapat dijalankan diatas beberapa platform tanpa perubahan.

Gambar dibawah ini menjelaskan aliran proses kompilasi dan eksekusi sebuah program java:



Gambar 2.3 Fase sebuah pemrograman java

Sumber : Yuni Sugiarti S.T.,M.Kom (2018)

Bahasa pemrograman Java memiliki beberapa kelebihan dibandingkan bahasa pemrograman lainnya adapun kelebihan tersebut diantaranya :

2.4.1 Sederhana

Bahasa pemrograman Java dirancang untuk mudah dipelajari, terutama bagi programmer yang telah mengenal bahasa pemrograman C/C++ akan mudah sekali menguasai bahasa pemrograman java. programmer juga belajar java secara cepat jika telah memahami konsep dasar pemrograman berorientasi objek.

2.4.2 Aman

Bahasa pemrograman java handal dan aman karena kasus dalam pemrograman seperti buffer overflow yang umumnya menjadi lubang keamanan Aplikasi-aplikasi berbasis C/C++ tidak terjadi di java, karena pengaturan keamanannya yang baik.

2.4.3 Berorientasi Objek

Java merupakan bahasa pemrograman yang berorientasi objek dan bukan turunan dari bahasa pemrograman manapun dan tidak kompetibel dengan semuanya. Java memiliki keseimbangan menyediakan peng-class-an sederhana, dengan model antar muka dinamik dan intuitif hanya jika diperlukan.

2.4.4 Kokoh

Kesalahan sering terjadi saat kompilasi karena java merupakan bahasa pemrograman yang sensitive dalam hal deklarasi dan tipe data. Oleh karena hal tersebut, Java memiliki batasan agar dapat menemukan kesalahan lebih cepat saat mengembangkan program yaitu dengan langsung memeriksa program tersebut saat ditulis, dan sekali lagi ketika dijalankan.

2.4.5 Interaktif

Jalinan program-program java yang mudah digunakan memungkinkan programmer untuk memikirkan pembuatan perilaku khusus, tanpa harus mengintegrasikan perilaku tersebut dengan model pemrograman global yang mengatur perulangan kejadian.

2.4.6 Terinterpretasi dan berkinerja tinggi

Java dapat dirancang dengan baik dan bekerja dengan baik pada komputer spesifikasi rendah pada prosesor dan memory RAM nya. Walaupun java merupakan bahasa terinterpretasi, kode kode java telah dirancang mudah diterjemahkan kedalam bahasa asli mesin menghasilkan kinerja yang tinggi dan baik pada aplikasinya.

2.4.7 Multiplatform

Kelebihan utama dari java dapat dijalankan di beberapa platform/ sistem operasi komputer. beberapa platform yang mendukung java adalah Microsoft Windows, Linux, Mac OS dan Sun Solaris.

2.4.8 Pengumpulan sampah otomatis

Melakukan pengumpulan sampah otomatis artinya memiliki Fasilitas pengaturan penggunaan memori sehingga para pemrograman tidak perlu melakukan pengaturan memori secara langsung. Java mengalokasikan operator baru untuk mengalokasikan memori pada heap untuk objek baru.

2.4.9 Perpustakaan kelas yang lengkap

Java memiliki kelengkapan perpustakaan kumpulan program program yang disertakan dalam pemrograman java yang sangat memudahkan dalam penggunaan oleh para programmer untuk membangun aplikasinya.

2.5 *Provider Java cryptography.*

2.5.1 Fungsionalitas

Fungsionalitas dasar untuk menggunakan teknik-teknik Kriptografi disediakan oleh JCA (*Java Cryptography Architecture*) dan JCE (*Java Cryptography extension*). Pada *java development kit* sudah memuat sejumlah file policy yang memberikan beberapa batasan tertentu pada ukuran-ukuran kunci yang dapat digunakan. Ukuran kunci umumnya sebesar 128 bit. (kecuali untuk *cipher simetris Triple DES*) dan pembangkitan kunci diatasi 2048 bit.

2.5.2 Cara Kerja Provider

Provider memberikan kapabilitasnya untuk dipakai JCA (Java Cryptography Architecture) dan JCE (Java Cryptograph Extension). Melihat bagaimana provider digunakan ketika anda menginstansiasi sebuah obyek JCA atau JCE yang diciptakan menggunakan pola faktori “getinstance()”.

2.6 Struktur data

Dalam teknik pemrograman struktur data komputer berarti tata letak data yang berisi kolom data, setiap baris dari kumpulan tersebut dinamakan *record*. Struktur data terdiri dari beberapa jenis adalah sebagai berikut :

2.6.1 Array

Array adalah struktur data klasik yang menyimpan sekumpulan elemen bertipe sama, dan setiap elemen diakses langsung melalui indeksinya.

2.6.2 Linier

Linier merupakan bagian dari struktur data majemuk yang terdiri dari beberapa daftar yaitu sebagai berikut.

1. Stack (tumpukan)
2. Queue (antrian)
3. List (daftar)

2.6.3 Non Linier

1. Binary Tree

Binary tree atau pohon binary adalah himpunan terbatas yang mungkin kosong atau terdiri dari sebuah simpul yang disebut sebagai akar dan dua buah himpunan lain yang disjoint. Karakteristik dari *binary tree* adalah

setiap simpul yang paling banyak hanya memiliki dua buah anak dan mungkin juga tidak punya anak.

2. *Graph*

Graph merupakan struktur data paling umum yang memungkinkan pendefinisian keterhubungan tak terbatas antara entitas data.

2.6.4 *Record*

Record adalah kumpulan data yang terdiri dari beberapa *field* (halaman isian) dengan berbagai macam tipe data.

2.7 UML (*Unified Modeling Language*)

2.7.1 Pengertian Umum

Menurut Sugiarti (2013), UML (Unified Modeling Language) adalah bahasa grafis yang kompleks dan kaya dengan fitur. Unified Modeling Language merupakan sesuatu yang telah menjadi dasar standar industri untuk merancang, dan mendokumentasikan sistem piranti lunak. Model peranti lunak dapat dianalogikan pengkodean seperti pembuatan *blue print* pada pembangunan gedung.

2.7.2 Penggunaan Unified Modeling Language (UML)

Unified Modeling Language adalah salah satu bentuk notasi atau bahasa yang digunakan oleh profesional dibidang software alat bantu yang handal dalam pengembangan sistem berorientasi objek, biasa digunakan untuk:

1. Menggambarkan batasan sistem dan fungsi-fungsi sistem secara umum, dibuat dengan *usecase* dan *actor*

2. Menggambarkan kegiatan atau proses bisnis yang dilaksanakan secara umum, dibuat dengan *interaction diagram*
3. Representasi struktur statis sebuah sistem dalam bentuk *class diagram*
4. Membuat model behavior yang menggambarkan kebiasaan atau sifat sebuah sistem dengan *state transition diagram*
5. Menyatakan arsitektur implementasi fisik menggunakan *component and development diagram*
6. menyampaikan atau memperluas *functionality* atau *stereotypes*

2.7.3 Tabel Diagram Main Concept UML

1. Abstraksi konsep dasar UML yang terdiri dari *structural*, *classification*, *dynamic behavior*, dan *model management*.
2. *Main concept* bisa dipandang sebagai *term* yang akan muncul pada saat kita membuat diagram.
3. *View* adalah kategori dari diagram tersebut.

Konsep dasar tersebut dirangkum dalam diagram berikut ini:

Tabel 2. 2 Tabel *Diagram Main Concept UML*

<i>Major Area</i>	<i>View</i>	<i>Diagrams</i>	<i>Main concept</i>
<i>Structural</i>	<i>Static View</i>	<i>Class diagram</i>	<i>Class, association, generalization, dependency, realization, interface</i>
	<i>Usecase View</i>	<i>Usecase diagram</i>	<i>Usecase, actor, association, extend, include, usecase generalization</i>
	<i>Implementation View</i>	<i>Component diagram</i>	<i>Component, interface, dependency, location</i>
	<i>Deployment View</i>	<i>Deployment diagram</i>	<i>State, activity, completion transition, fork, join</i>
<i>Dynamic</i>	<i>State machine view</i>	<i>State chart diagram</i>	<i>State, activity, completion, transition, fork, join</i>
	<i>Interaction view</i>	<i>Sequence diagram</i>	<i>Interaction object, message, activation</i>

		<i>Collaboration diagram</i>	<i>Collaboration, interaction, collaboration, message</i>
<i>Model management</i>	<i>Model management view</i>	<i>Class diagram</i>	<i>Package subsystem, model</i>
<i>extesibility</i>	<i>all</i>	<i>all</i>	<i>stereotype, tagged values</i>

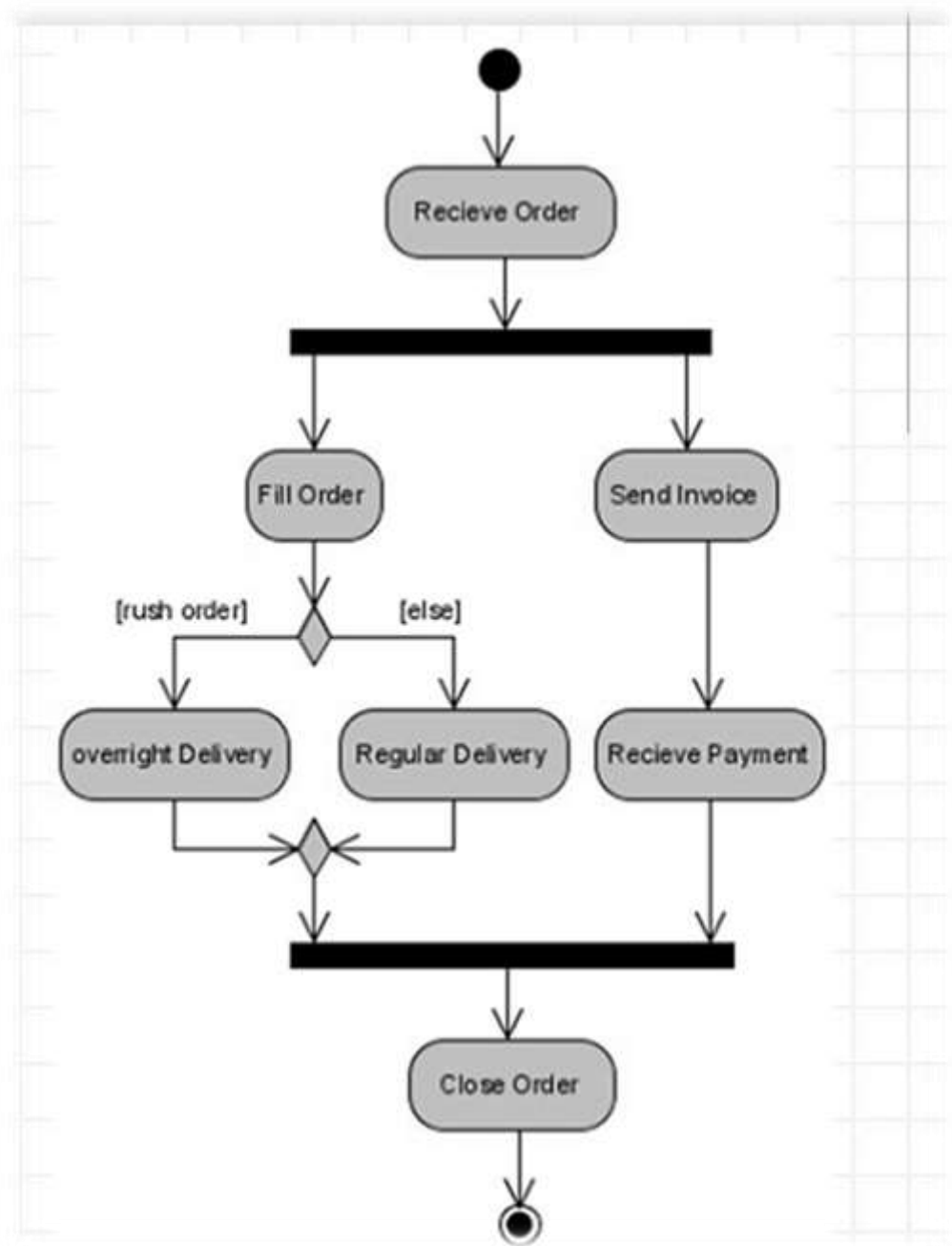
(Sumber:www.uml.org)

2.7.4 Activity Diagram

UML merupakan skema representasi grafis yang banyak digunakan secara luas untuk pemodelan sistem berorientasi objek. Salah satu model diagram nya adalah *activity diagram*.

1. Contoh Activity Diagram

Memodelkan aliran kerja objek selama eksekusi program . Activity diagram adalah flowchart yang memodelkan aksi yang akan dikerjakan oleh objek besertadengan ordenya




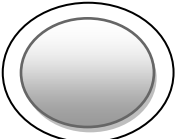
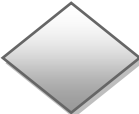
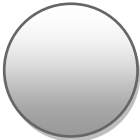


Gambar 2.4 Contoh Activity Diagram

Sumber : Yuni Sugiarti,S.T,M.Kom.(2018)

2. Keterangan Simbol *Activity* Diagram

Berikut ini adalah tabel keterangan dari simbol-simbol *activity* diagram tersebut.

Tabel 2.3 *Symbol activity diagram*

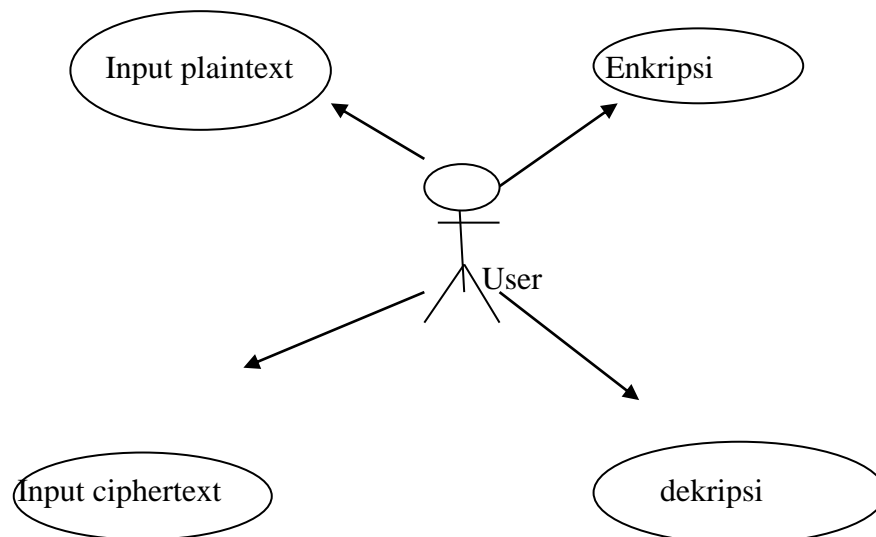
no	Gambar	Nama	Keterangan
		<i>Action</i>	State dari sistem yang mencerminkan sistem dari suatu aksi
		<i>Activity final node</i>	Bagaimana objek dibentuk dan diakhiri
		<i>Decision</i>	Digunakan untuk menggambarkan suatu keputusan
		<i>Initial node</i>	Bagaimana awal objek dibentuk
		<i>Line connector</i>	Menghubungkan suatu simbol dengan yang lain
		<i>Activity</i>	Bagaimana masing masing kelas saling berinteraksi

2.7.5 Use Case Diagram

Terdapat beberapa simbol dalam menggambarkan *usecase* diagram yaitu *usecase*, *actor*, dan relasi. Setiap *usecase* harus dijelaskan alur prosesnya melalui sebuah deskripsi *usecase* atau *scenario use case* sebagai berikut ini:

1. Penamaan use case yang menggunakan kata kerja.
2. Deskripsi yaitu penjelasan mengenai tujuan usecase

Berikut ini adalah salah satu contoh activity diagram mengirim enkripsi dan menerima pesan yang terenkripsi untuk kemudian di deskripsi.



Gambar 2.5 Contoh *usecase* mengirim dan menerima pesan

Sumber : Kumpulan Jurnal Ilmu Komputer (2017)

2.7.6 Class Diagram

Kelas/ *Class* adalah sebuah spesifikasi yang jika diinstansikan akan menghasilkan sebuah objek dan merupakan inti dari pengembangan dan desain berorientasi objek. Susunan struktur class yang baik pada diagram *class* memiliki jenis-jenis *class* berikut.

1. Class main
2. Class yang menangani tampilan sistem
3. Class yang memiliki fungsi awal dieksekusi ketika sistem dijalankan
4. Class yang diambil dari pendefinisian usecase
5. Class yang menangani fungsi mendefinisian usecase
6. Class yang diambil dari pendefinisian data
7. Class yang digunakan untuk membungkus data menjadi sebuah kesatuan yang akan disimpan ke basis data.



Gambar 2.6 Contoh class diagram

(Sumber : Sis.binus.ac.id)

2.7 Pengertian Flowchart

2.8.1 Definisi Flowchart



Flowchart atau bagan alir adalah sebuah jenis diagram yang mewakili algoritma atau proses yang menampilkan langkah-langkah dalam bentuk simbol grafis, dan urutannya dihubungkan dengan suatu tanda panah. Diagram alur digunakan untuk mendesain dan mendokumentasikan proses atau program logika.

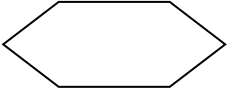



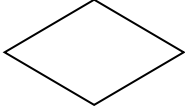
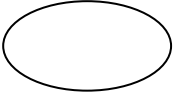

Flow chart atau diagram alir adalah sekumpulan simbol-simbol atau skema yang menunjukkan atau menggambarkan rangkaian kegiatan program dari awal hingga akhir. Diagram alir data adalah suatu diagram yang menggunakan notasi-notasi untuk menggambarkan arus dari data sistem, yang penggunaannya sangat membantu untuk memahami sistem secara logika, terstruktur dan jelas (Said, 2010).

2.8.2 Simbol Simbol Flowchart

Berikut ini adalah merupakan simbol-simbol flowchart yang umum digunakan dalam pemerograman :

Tabel 2.4 Tabel Simbol Flowchart dan Fungsinya

simbol	Nama	Fungsi
	Terminator	Permulaan atau akhir program
	Garis Alir	Arah aliran algoritma

	preparation	Proses inisialisasi / persiapan awal
	Proses	Proses pengolahan data
	Input data / Output data	Proses input/ output data, parameter, informasi
	Predefined process/ Sub program	Proses menjalankan sub program
	Decision	pilihan data selanjutnya, penyeleksian data
	onpage	Penghubung Flowchat yang berada satu halaman
	Offpage conector	Penghubung flowchart pada halaman berbeda

(Sumber: Buku Ajar Logika Algoritma; Maranatha pasaribu)

2.8.3 Jenis Jenis Flowchart

flowchart terbagi atas lima jenis yaitu :

1. Flowchart Sistem
2. Flowchart Paperwork / flowchart dokumen (*Document Flowchart*)
3. Flowchart Skematik (*Schematic Flowchart*)
4. Flowchart Program (*Program Flowchart*)
5. Flowchart proses (*Process Flowchart*)

2.8.4 Pedoman Dalam Membuat Flowchart

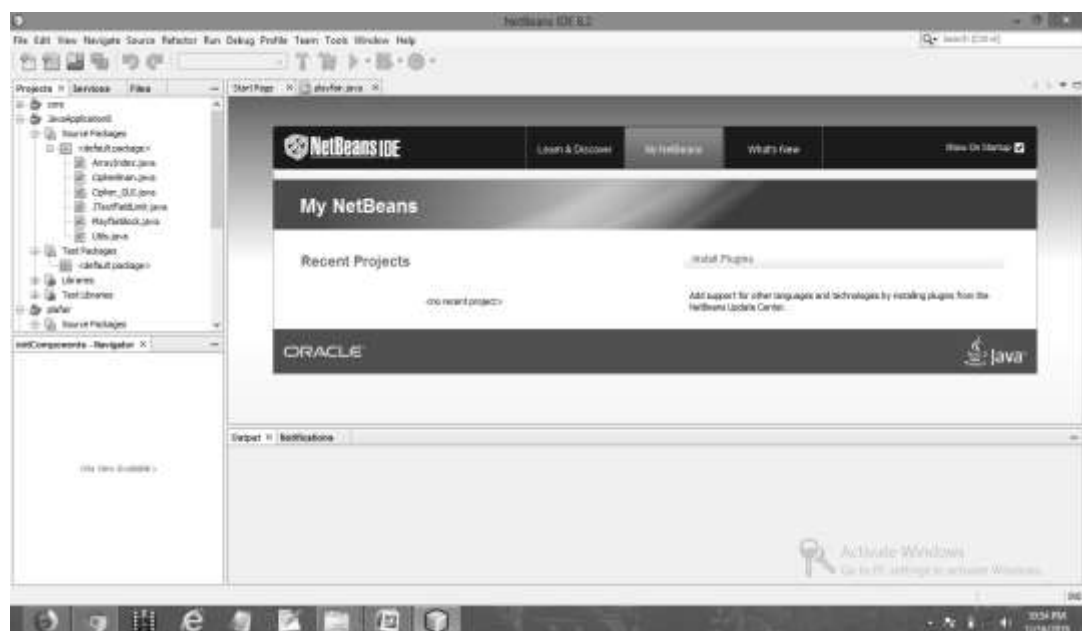
Bila seseorang analisis akan membuat sebuah Flowchart program ada beberapa hal yang perlu diperhatikan diantaranya yaitu:

1. Flowchart digambarkan dari halaman atas kebawah dan dari kiri ke kanan .
2. Aktifitas yang digambarkan harus didefinisikan dengan hati hati dan definisi harus mudah dipahami oleh pembacanya.
3. kapan aktifitas itu akan dimulai dan akan diakhiri harus dipahami dengan jelas
4. Setiap langkah aktifitas harus diuraikan menggunakan deskripsi kata kerja
5. Setiap langkah dari aktifitas harus berada pada urutan yang benar
6. Lingkup dan range aktifitas yang sedang digambarkan harus ditelusuri dengan hati- hati, percabangan yang memotong aktifitas yang sedang digambarkan tidak perlu digambarkan pada flowchart yang sama
7. Gunakan simbol flowchart yang standar

2.8 NetBeans

2.9.1 Definisi Netbeans

Netbeans merupakan modul pengembangan perangkat lunak komputer mengacu pada kedua platform kerangka untuk aplikasi desktop Java, dan sebuah lingkungan pengembangan terpadu (IDE) untuk pengembangan dengan Java , JavaScript , PHP , Python , Ruby , Groovy , C , C + + , Scala, Clojure, dan lain-lain. NetBeans IDE ditulis dalam Java dan berjalan di mana-mana JVM diinstal, termasuk Windows, Mac OS, Linux, dan Solaris. Sebuah JDK diperlukan untuk pengembangan fungsionalitas Java, tetapi tidak diperlukan untuk pembangunan di bahasa pemrograman lain. Berikut ini adalah tampilan menu utama netbean 8.2 :

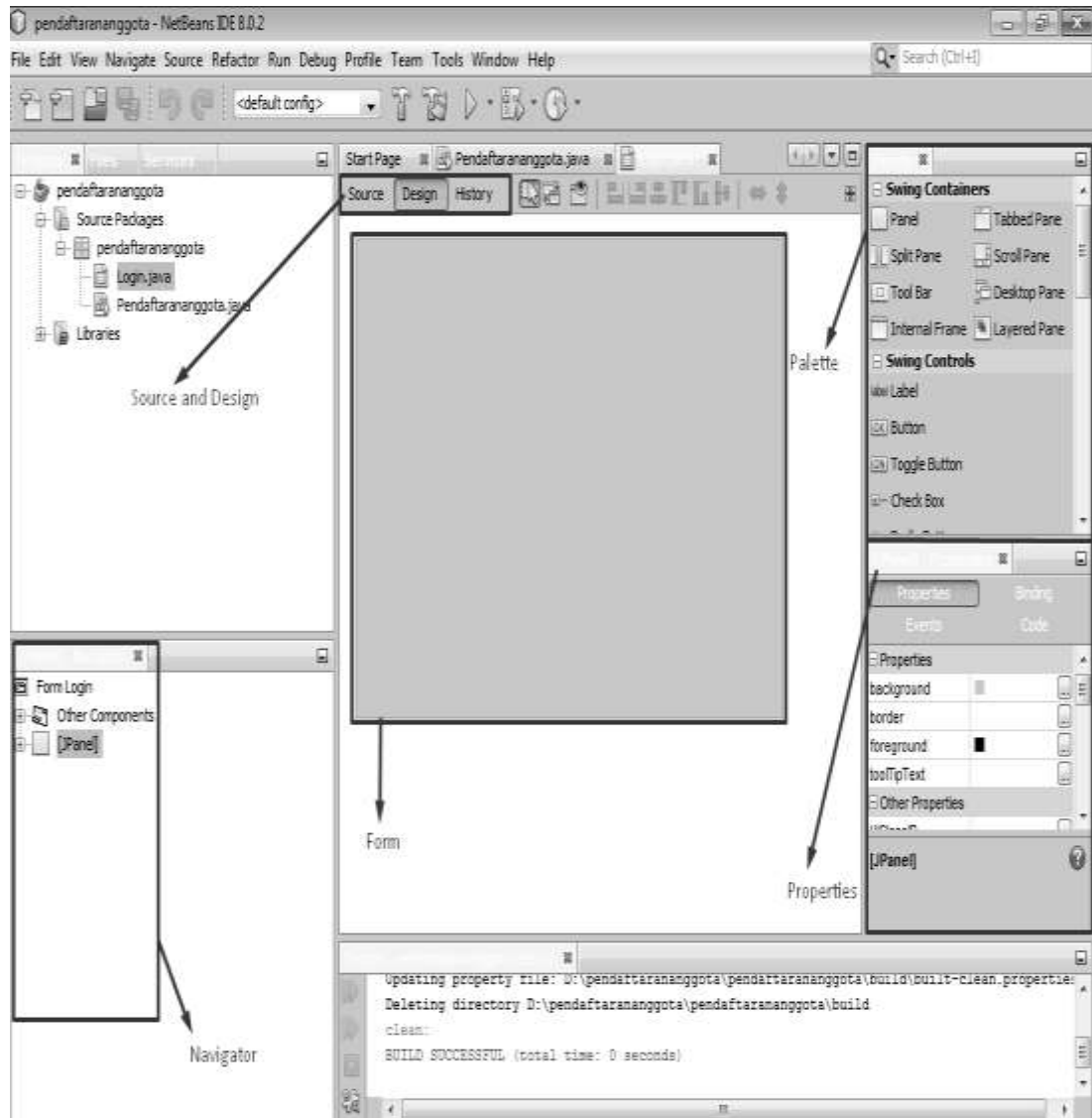


Gambar 2.7 Tampilan menu utama netbeans IDE

(Sumber : netbeans.org)

2.9.2. Komponen *Tools Palette NetBeans IDE*

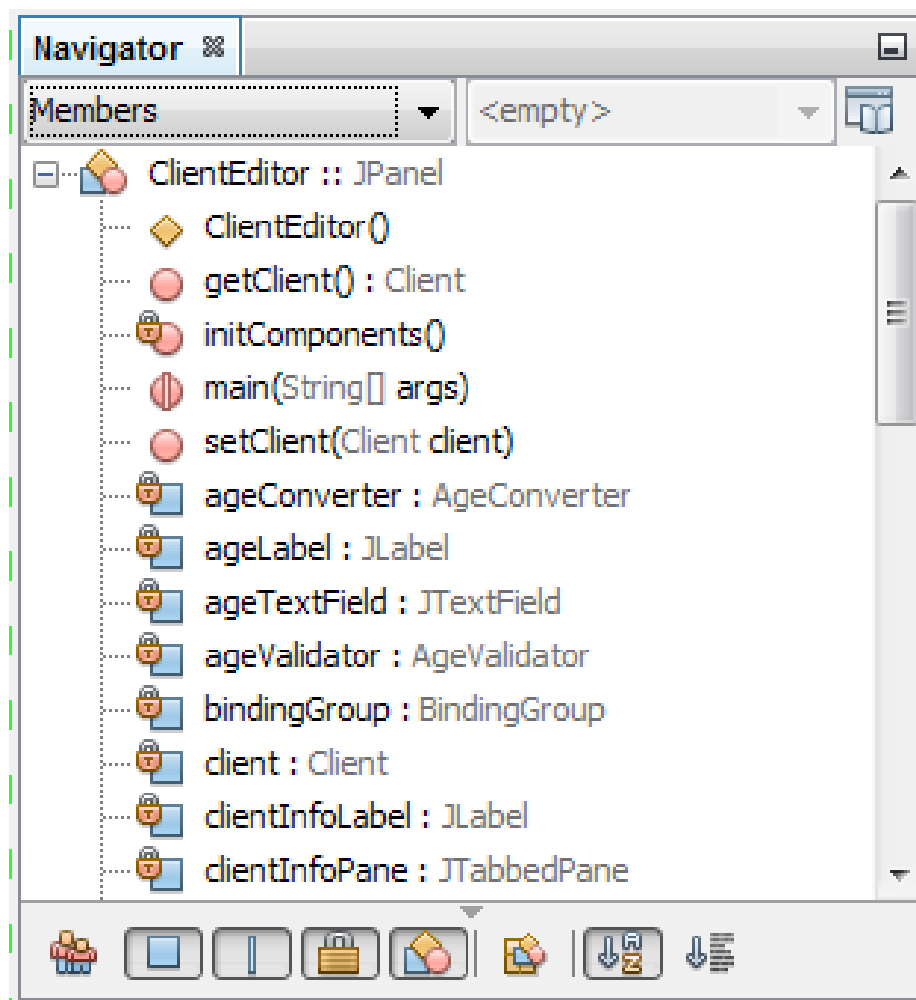
Berikut ini adalah gambar bagian komponen-komponen tool palette pada netbeans :



Gambar 2.8 Tool Pallet NetBeans IDE

(Sumber :netbeans.org)

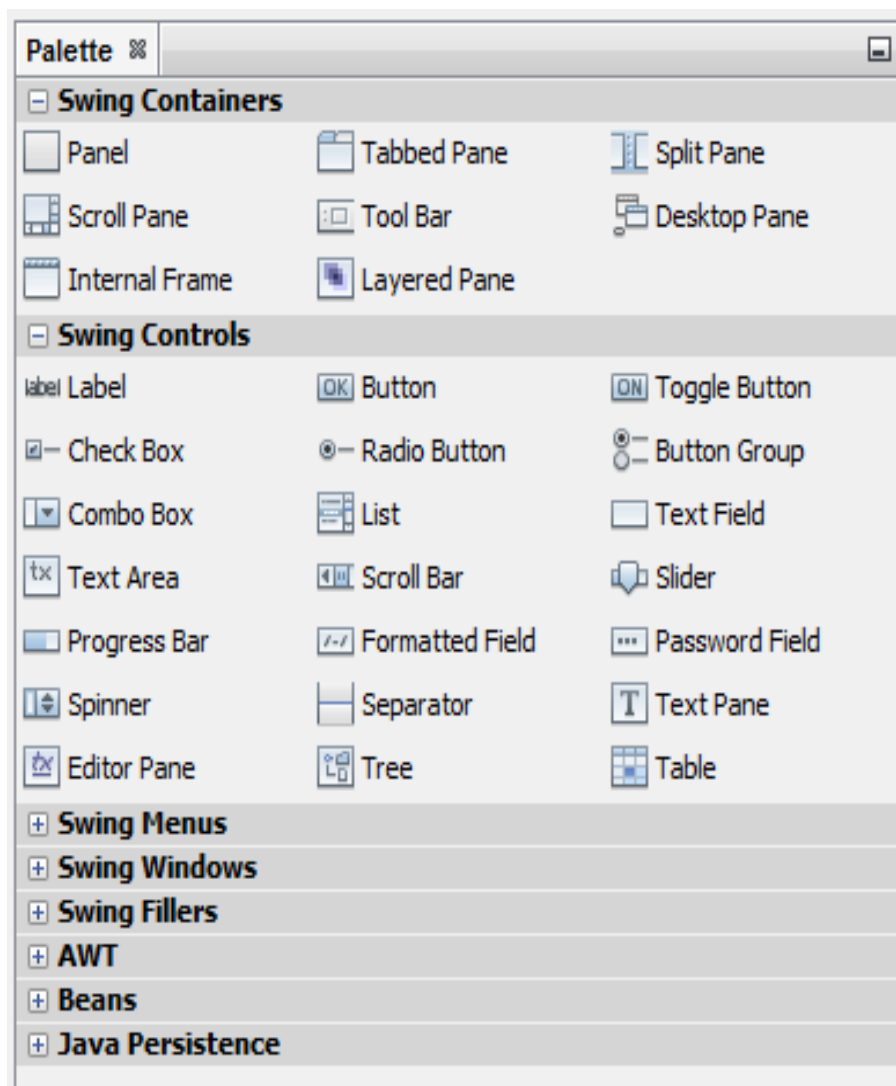
1. *Tab source* and design merupakan tempat untuk melihat hasil design antar muka suatu aplikasi java dan source codenya
2. *Navigator* merupakan petunjuk setiap bagian yang sudah diinput pada interface aplikasinya. Berikut ini adalah salah satu contoh navigator netbeans dengan proyek kerjanya :



Gambar 2.9 Navigator window pada netbeans

Sumber : ui.netbeans.org

3. *Form* merupakan *design* dari *interface* aplikasi java yang sedang dirancang
4. *Swing container* merupakan tempat pilihan bagian bagian yang dapat ditambahkan dalam interface aplikasinya seperti *text field*, *table*, *scroll bar* dan *button*. Berikut adalah tampilannya detailnya:



Gambar 2.10 Tampilan jendela *palette* pada netbeans

Sumber : netbeans.org

5. *Properti* merupakan setingan dari bagian yang telah ditambahkan pada interface seperti button dan textfield dapat dirubah ukuran dan nama variabelnya melalui property

2.9.3 Fitur pada NetBeans

Fitur fitur yang terdapat dalam netbeans antara lain:

1. Smart Code Completion: untuk mengusulkan nama variabel dari suatu tipe, melengkapi keyword dan mengusulkan tipe parameter dari sebuah method.
2. Bookmarking: fitur yang digunakan untuk menandai baris yang suatu saat hendak kita modifikasi.
3. Go to commands: fitur yang digunakan untuk jump ke deklarasi variabel, source code atau file yang ada pada project yang sama.
4. Code generator: jika kita menggunakan fitur ini kita dapat meng-generate constructor, setter and getter method dan yang lainnya.
5. Error stripe: fitur yang menandai baris yang eror dan memberi highlight merah.

BAB 3

ANALISA DAN PERANCANGAN SISTEM

3.1 Analisa Playfair Cipher

Playfair cipher merupakan digraph cipher setiap proses enkripsi maupun dekripsi dilakukan setiap dua huruf secara berpasangan (Setyaningsih, 2009). Playfair cipher menggunakan matriks 5 X 5 dimana setiap alphabet kecuali J dianggap sama dengan huruf I .karena dianggap frekuensi kemunculannya paling kecil. kunci yang digunakan berupa` kata dan bukan huruf yang berulang untuk itu perlu di analisa persamaan proses enkripsi dan dekripsi dari playfair cipher.

3.2 Persamaan Proses Enkripsi

Kunci dimasukkan dalam tabel matrik 5x5 dan kata yang pertama merupakan kunci, dilanjutkan dengan huruf huruf berikutnya sevar berturut mulai dari Baris pertama (Santi, 2010). berikut ini adalah contoh kasus matriks kunci persamaannya :

Misalkan A : matriks berukuran $m \times n$

p : entri pada matriks E

m,x : baris

y,n : kolom

Maka diperoleh :
$$A(Pmn, Pxn) = \begin{cases} (Pmy, Pxn) & ; m \neq x, n \neq y \\ (Pm(n+1), Px(y+1)) & ; m = x, n \neq y \\ (Pm(n+1), P(x+1) y); & m \neq x, n = y \end{cases}$$

1.2.1 Persamaan Proses Dekripsi

Secara matematis proses dekripsi pesan menggunakan playfair cipher yaitu sebagaimana pada persamaan berikut ini:

Misalkan B : matriks berukuran $m \times n$
 C : entri pada matriks D
 m, x : baris
 y, n : kolom

Maka diperoleh :

$$B(C_{mn}, C_{xy}) = \begin{cases} (C_{my}, C_{xn}) & ; m \neq x, n \neq y \\ (P_{m(n-1)}, C_{x(y-1)}) & ; m \neq x, n \neq y \\ (C_{(m-1)n}, C_{(x-1)y}) & ; m \neq x, n \neq y \end{cases}$$

1.2.2 Langkah Enkripsi Playfair Cipher

Kita dapat menentukan kata terlebih dahulu, misalnya adalah kata “MONARCHY” dan plaintext nya adalah “SEBAR ISU KOMUNIS” adapun proses langkah adalah sebagai berikut:

1. Langkah pertama

Membuat matriks kunci dengan cara kunci dimasukkan dalam matriks 5×5 seperti pada contoh tabel berikut ini:

Tabel 3.1 Contoh matriks kunci

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

2. Langkah kedua

Jika terdapat huruf J pada plaintext maka dapat diganti dengan huruf I

3. Langkah ketiga

Jika dua huruf yang sama berdampingan maka di sisipkan huruf X

4. Langkah keempat

Menambahkan huruf X diakhir kalimat karena plaintext nya ganjil

5. Langkah kelima

Menghilangkan spasi pada plaintext dan mengubah susunan plaintext menjadi pasangan huruf. "SE BA RI SU AG MA"

6. Langkah keenam

enkripsi pesan sesuai aturan, sehingga diperoleh:

SE : IL
 BA : IB
 RI : KA
 SU : XL
 AG : LI
 MA :NR

Jadi cipher teks dari kalimat “SEBAR ISU AGAMA” adalah “ILIBKAXLINR”

3.2.3 Langkah Proses Dekripsi

Setelah memperoleh *ciphertext* dan ingin mengembalikan ke plaintext dapat menggunakan langkah sebagai berikut:

1. Langkah pertama

Menghilangkan spasi pada ciphertext dan mengubah susunan ciphertext menjadi pasangan huruf. IL IB KA XL IN RO “

2. Langkah kedua

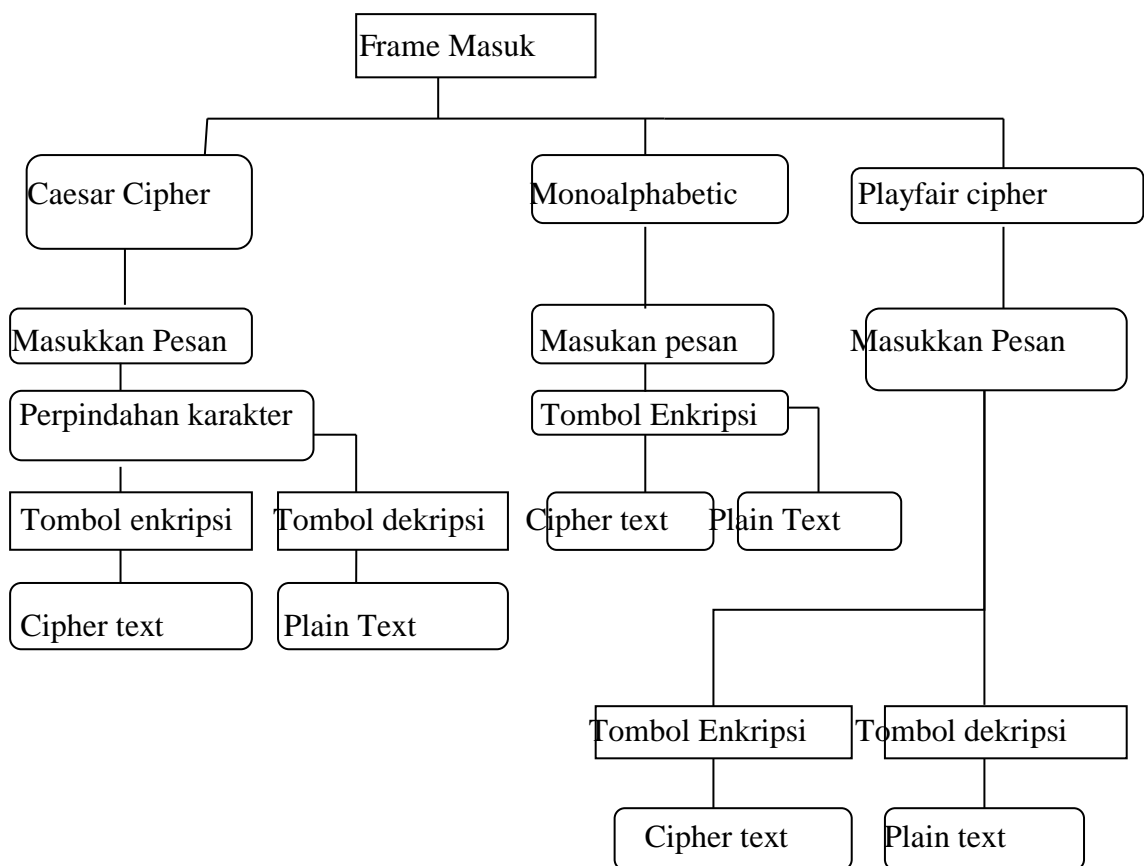
Dekripsi pesan sesuai aturan sehingga diperoleh

IL : SE
 IB : BA
 KA : RI
 XL : SU
 IN : AG
 RO : MA

Jadi dapat di pastikan cipher teks dari ” IL IB KA XL IN RO” adalah “SEBAR ISU AGAMA”

3.3 Perancangan Arsitektur Aplikasi

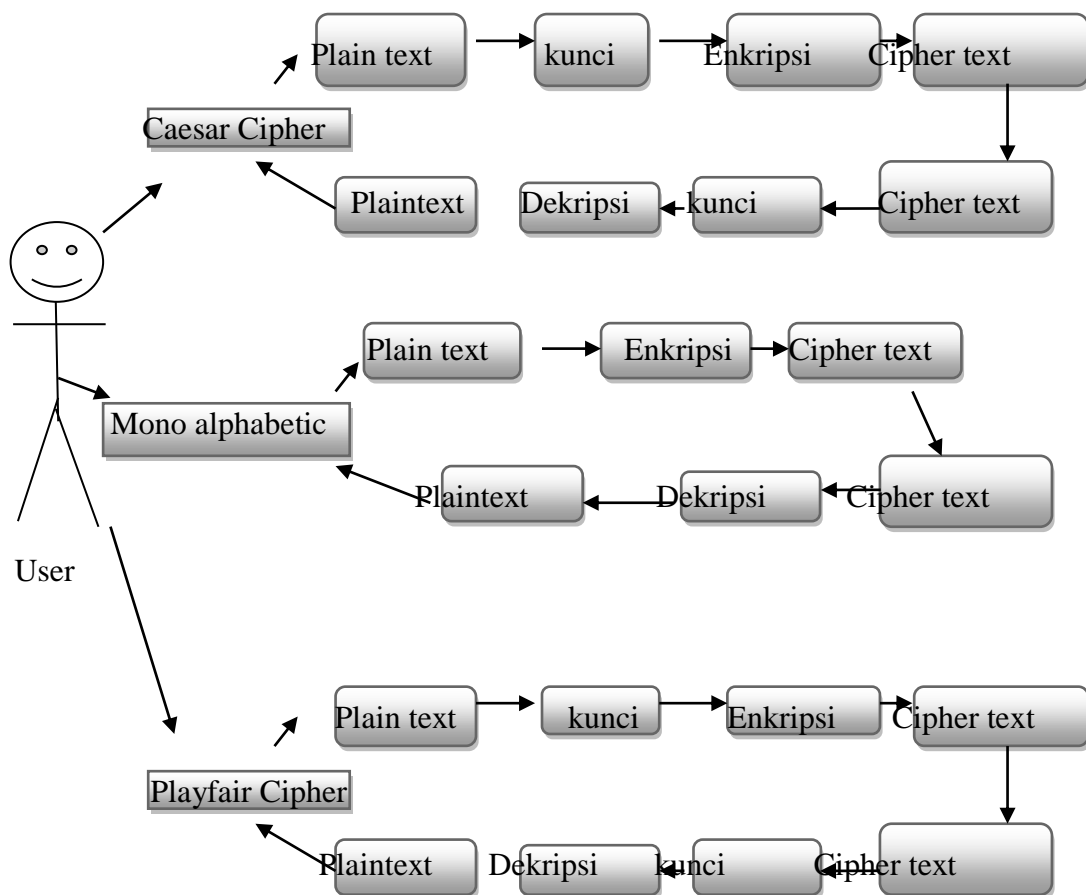
Perancangan aplikasi memiliki satu menu utama, dan pilihan button sehingga pihak pengirim dan penerima pesan dapat melakukan proses enkripsi dan deskripsi pesan.



Gambar 3.1 Perancangan Arsitektur Aplikasi Kriptografi

3.4 Diagram *Usecase*

Diagram *usecase* digunakan untuk menggambarkan fungsionalitas dari perangkat lunak kriptografi yang dirancang. Tampilan diagram use case dapat dilihat pada gambar berikut ini:



Gambar 3.2 Diagram use case perangkat lunak

Pada *diagram use case* diatas dapat kita buat skenario keterangan sebagai berikut ini:

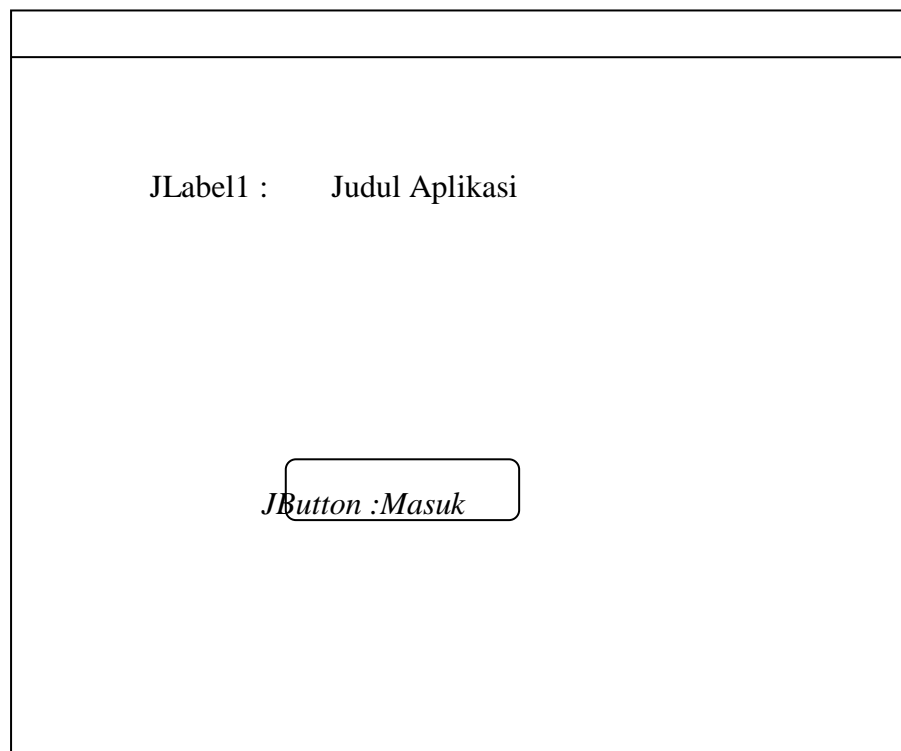
Tabel 3.2 *Use Case Narrative* Aplikasi

Aktor	Reaksi Sistem
1.User membuka aplikasi	1. Menampilkan form selamat datang
2,User tekan button masuk	2. Sistem menampilkan form aplikasi Caesar cipher dengan tambahan pilihan untuk monoalpabetic cipherdan playfair cipher dan user dapat melakukan proses kriptografi Caesar cipher
3. User tekan pilihan monoalphabetic	3. Sistem menampilkan form kerja monoalphabetic cipher dan user dapat melakukan proses kriptografi monoalphabetic
4. User tekan pilihan playfair cipher	4. Sistem menampilkan form kerja playfair cipher dan user dapat melakukan proses kriptografi playfair cipher.
5. User menekan tombol warna merah	
	6. Aplikasi kriptografi tertutup

3.5 Perancangan Antarmuka

Perancangan antarmuka perangkat lunak terdiri dari form tentang judul aplikasi dan jendela form menu utama yang berisi button untuk pilihan aplikasi kriptografi . Berikut ini adalah rancangan tampilan antarmuka tiap form:

1.5.1 Rancangan Antarmuka Tampilan Utama Aplikasi



Gambar 3.3 Rancangan Tampilan Antarmuka Aplikasi Jendela Masuk

Keterangan :

1. JLabel : Digunakan untuk member keterangan aplikasi
2. JButton : Digunakan untuk masuk ke jendela berikutnya

1.5.2 Rancangan Tampilan Pada *Interface Caesar Cipher*

Setelah menekan tombol masuk pada tampilan pertama , selanjutnya akan keluar tampilan *form caesar cipher* dengan bagian seperti berikut ini:

The diagram illustrates the layout of the Caesar Cipher application window. It features a header bar with three buttons: 'Button 1', 'Button 2', and 'Button 3'. The main content area includes a label 'Label1' centered at the top. Below it, there are two text areas: 'Text area 1' and 'Text area 2', each preceded by a label 'Label 2' and 'Label 3' respectively. At the bottom, there are two buttons: 'Button 4' and 'Button 5', and a large text area labeled 'Text area 3'.

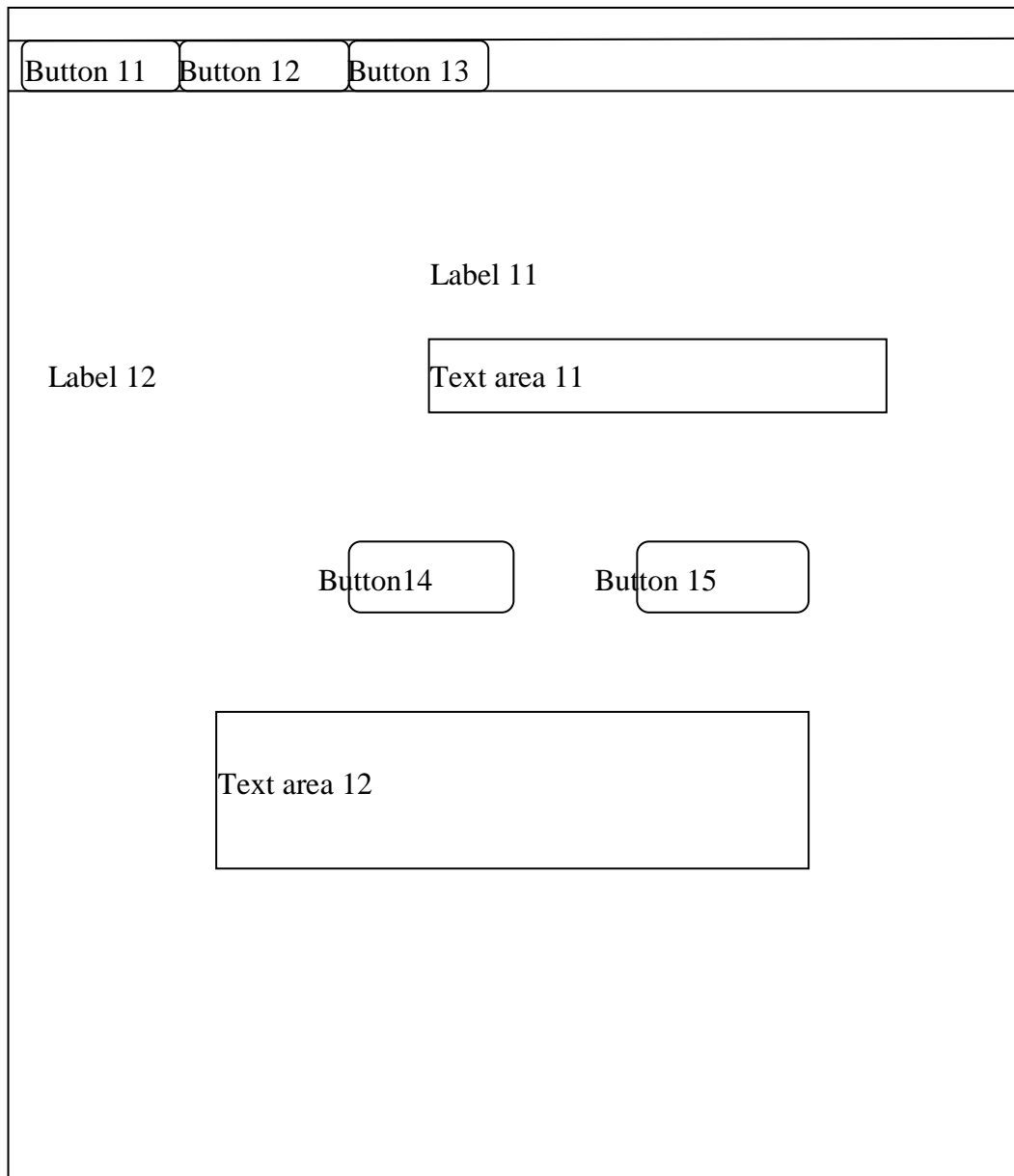
Gambar 3.4 Rancangan Tampilan Antarmuka Aplikasi Jendela Pertama

Keterangan

1. Button 1 : Tombol tab pilihan untuk masuk ke jendela aplikasi berikutnya
2. Button 2 : Tombol tab pilihan untuk masuk ke jendela aplikasi berikutnya
3. Button 3 : Tombol tab pilihan untuk masuk ke jendela aplikasi berikutnya
4. Button 4 : Tombol pilihan untuk melakukan perintah kerja Enkripsi
5. Button 5 : Tombol pilihan untuk melakukan perintah dekripsi
6. Label 1 : Label untuk judul form aplikasi
7. Label 2 : Label untuk keterangan text area 1
8. Label 3 : Label untuk keterangan text area 2
9. Text area 1 : Merupakan tempat memasukkan plain text
10. Text area 2 : Merupakan tempat memasukkan kunci
11. Text area 3 : Merupakan tempat hasil cipher text

3.5.3 Rancangan Tampilan Pada *Interface Monoalphabetic*

Setelah menekan button 2 yaitu button monoalphabetic pada tampilan pertama, selanjutnya akan keluar tampilan *form monoalphabetic* dengan bagian seperti berikut ini:



Gambar 3.5 Rancangan Tampilan Aplikasi Jendela Monoalphabetic

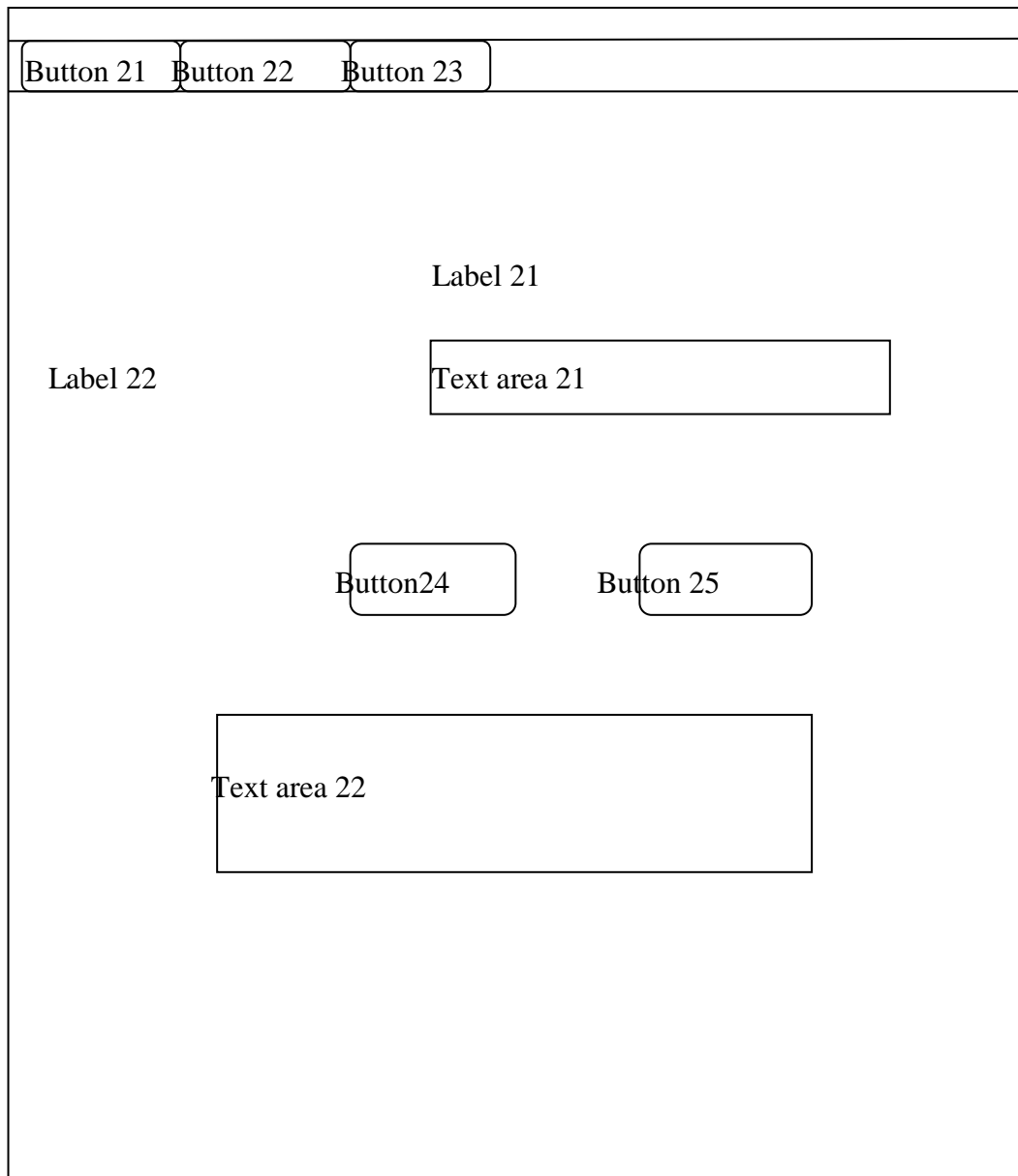
Keterangan

1. Button 11 : Tombol tab pilihan untuk masuk ke jendela aplikasi berikutnya
2. Button 12 : Tombol tab pilihan masuk ke jendela aplikasi berikutnya

3. Button 13 : Tombol tab pilihan masuk ke jendela aplikasi berikutnya
4. Button 14 : Tombol pilihan untuk melakukan perintah kerja Enkripsi
5. Button 15 : Tombol pilihan untuk melakukan perintah dekripsi
6. Label 11 : Label untuk judul form aplikasi
7. Label 12 : Label untuk keterangan text area 11
8. Text area 11 : Merupakan tempat memasukkan plain text
9. Text area 12 : Merupakan tempat hasil cipher text

3.5.4 Rancangan Tampilan Pada *Interface Playfair Cipher*

Saat menekan button 3 yaitu button playfair cipher pada tampilan pertama maka selanjutnya akan keluar tampilan pada layar monitor *form playfair cipher dengan bagian seperti berikut ini:*



Gambar 3.6 Rancangan Tampilan Antarmuka Aplikasi Jendela Playfair

Keterangan

1. Button 21 : Tombol tab pilihan untuk masuk ke jendela aplikasi berikutnya
2. Button 22 : Tombol tab pilihan masuk ke jendela aplikasi berikutnya

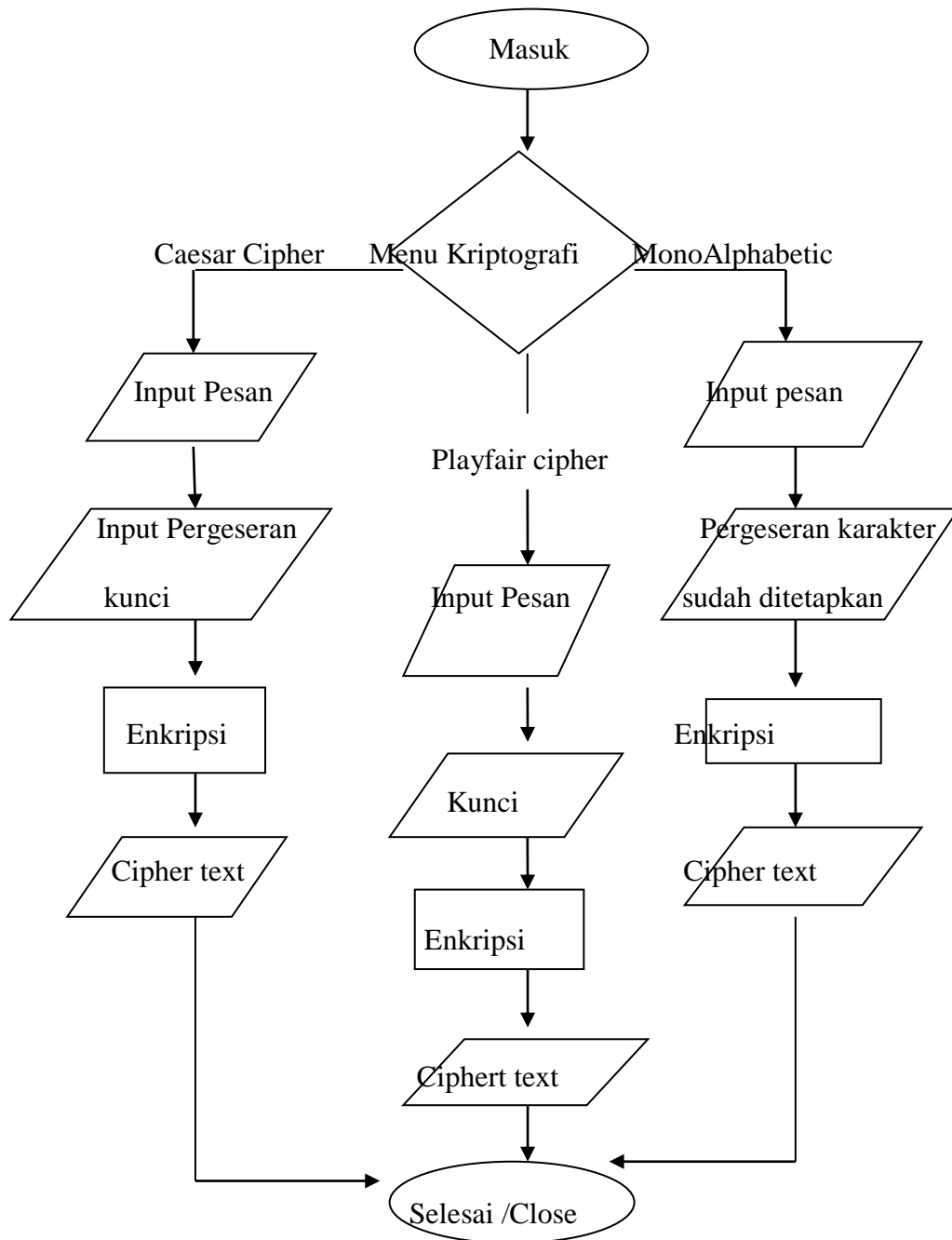
3. Button 23 : Tombol tab pilihan masuk ke jendela aplikasi berikutnya
4. Button 24 : Tombol pilihan untuk melakukan perintah kerja Enkripsi
5. Button 25 : Tombol pilihan untuk melakukan perintah dekripsi
6. Label 21 : Label untuk judul form aplikasi
7. Label 22 : Label untuk keterangan text area 11
8. Text area 21 : Merupakan tempat memasukkan plain text
9. Text area 22 : Merupakan tempat hasil cipher text

3.6 Diagram Alur

Flowchart dari aplikasi ini merupakan sebuah diagram simbol-simbol grafis yang menyatakan aliran algoritma atau proses yang menampilkan langkah-langkah yang disimbolkan beserta urutannya, dan dengan menghubungkan masing masing langkah tersebut menggunakan tanda panah.

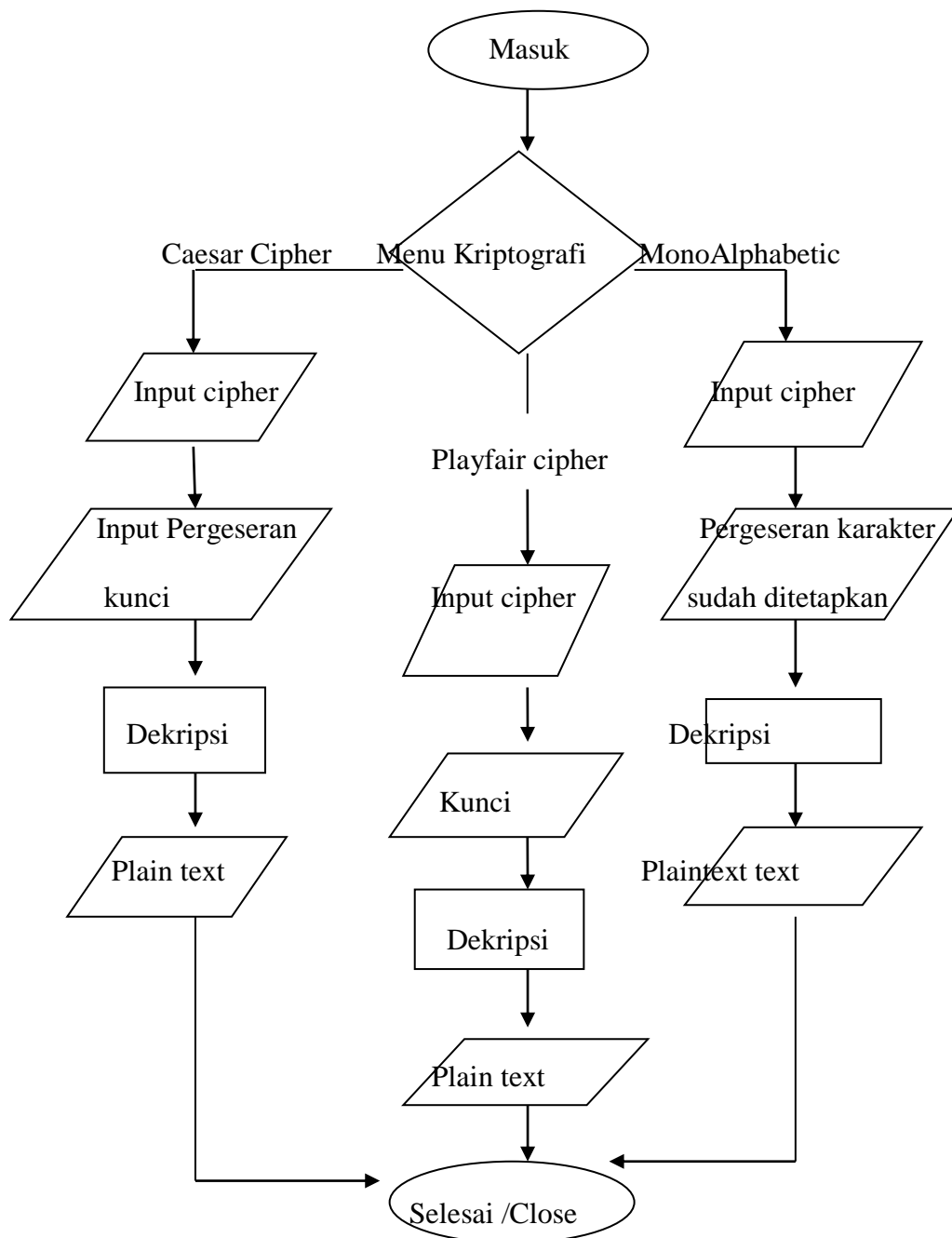
Diagram alur pada perancangan aplikasi bertujuan untuk mengetahui alur jalannya sistem enkripsi dan dekripsi pesan

3.6.1 Diagram Alur Proses Enkripsi



Gambar 3.7 Flowchart proses enkripsi aplikasi kriptografi

3.6.2 Diagram Alur Proses Dekripsi



Gambar 3.8 Flowchart proses dekripsi aplikasi kriptografi

DAFTAR PUSTAKA

- Agus Kurniawan. 2014. *Pemrograman Java Tingkat Lanjut*, Yogyakarta : CV.ANDI Offset.
- Dr. Eng. RH. Sianipar. 2017. *Java Untuk Kriptografi*, Yogyakarta : CV Andi Offset.
- 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.
- 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.
- Rinaldi Munir. *Algoritma Dan Pemrograman Dalam Bahasa Pascal Dan C*, Bandung: CV Informatika.
- Rifki Sadikin. 2012. *Kriptografi Untuk Keamanan Jaringan Dan Implementasinya Dalam Bahasa Java*, Yogyakarta: CV Andi Offset.
- 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.
- Sidik, A. P. (2018). Algoritma RSA dan Elgamal sebagai Algoritma Tambahan untuk Mengatasi Kelemahan Algoritma One Time Pad pada Skema Three Pass Protocol.
- 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.
- 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), 100-10
- Wijaya, Rian Farta, et al. "Aplikasi Petani Pintar Dalam Monitoring Dan Pembelajaran Budidaya Padi Berbasis Android." *Rang Teknik Journal* 2.1 (2019).
- Yuni Sugiarti, S.T.,M.Kom., 2018. *Dasar-Dasar Pemrograman Java Netbeans Database UML Dan Interface*, Bandung: PT Remaja Rosdakaryya.

Batubara, Supina, Sri Wahyuni, and Eko Hariyanto. "Penerapan Metode Certainty Factor Pada Sistem Pakar Diagnosa Penyakit Dalam." Seminar Nasional Royal (SENAR). Vol. 1. No. 1. 2018.