RANCANGAN KEAMANAN INFORMASI PESAN TEKS MENGGUNAKAN ALGORITMA *BEAUFORT CIPHER*

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

SKRIPSI

OLEH:

NAMA	:	**MUHAMMAD RIDHO UTOMO**
NPM	:	**1514370369**
PROGRAM STUDI	:	**SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2020

LEMBAR PENGESAHAN

RANCANGAN KEAMANAN INFORMASI PESAN TEKS MENGGUNAKAN ALGORITMA *BEAUFORT CIPHER*

Disusun Oleh:

NAMA	:	**MUHAMMAD RIDHO UTOMO**
NPM	:	**1514370369**
PROGRAM STUDI	:	**SISTEM KOMPUTER**

Skripsi Telah Disetujui oleh Dosen Pembimbing Skripsi
Pada Tanggal : 29 November 2020

Dosen Pembimbing I	Dosen Pembimbing II
A. P. U. Siahaan, S.Kom., M.Kom.	Heri Kurniawan., S.Kom., M.Kom.

Mengetahui:

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

SURAT PERNYATAAN

Yang Bertanda Tangan Dibawah Ini :

a	:	MUHAMMAD RIDHO UTOMO
M	:	1514370369
at/Tgl. Lahir	:	MEDAN / 14 Februari 1998
at	:	Jl.Puskesmas 1 Gg.Puskesmas Pembantu No.18 A
HP	:	082366948168
a Orang Tua	:	SULISTIONO/RENI HARNISA
tas	:	SAINS & TEKNOLOGI
ram Studi	:	Sistem Komputer
	:	Rancangan Keamanan Informasi Pesan Teks Menggunakan Algoritma Beaufort Cipher

ma dengan surat ini menyatakan dengan sebenar - benarnya bahwa data yang tertera diatas adalah sudah benar sesuai an ijazah pada pendidikan terakhir yang saya jalani. Maka dengan ini saya tidak akan melakukan penuntutan kepada 3. Apabila ada kesalahan data pada ijazah saya.

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

Medan, 13 September 2020

METERAI TEMPEL 6000

MUHAMMAD RIDHO UTOMO

1514370369

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI

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

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

PERMOHONAN JUDUL TESIS / SKRIPSI / TUGAS AKHIR*

Saya yang bertanda tangan di bawah ini :

Nama Lengkap	: MUHAMMAD RIDHO UTOMO
Tempat/Tgl. Lahir	: MEDAN / 14 Februari 1998
Nomor Pokok Mahasiswa	: 1514370369
Program Studi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer
Jumlah Kredit yang telah dicapai	: 141 SKS, IPK 3.30
Nomor Hp	: 082366948168
Dengan ini mengajukan judul sesuai bidang ilmu sebagai berikut	:

No.	Judul
1.	Rancangan Keamanan Informasi Pesan Teks Menggunakan Algoritma Beaufort Cipher0

Catatan : Diisi Oleh Dosen Jika Ada Perubahan Judul

Coret Yang Tidak Perlu

Medan, 14 Agustus 2020
Pemohon,

(Muhammad Ridho Utomo)

Rektor I,

Cahyo Pramono, SE., MM

Tanggal : .....
Disahkan oleh :
Dekan

(Hamdani, ST., MT)

Tanggal : 22 - 06 - 2021
Disetujui oleh :
Dosen Pembimbing I :

(Andysah Putera Utama Siahaan, S.Kom., M.Kom)

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

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

Tanggal : 22 - 06 - 2021
Disetujui oleh:
Dosen Pembimbing II:

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

SURAT KETERANGAN PLAGIAT CHECKER

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

emikian disampaikan.

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

Ka.LPMU

Cahyo Pramono, SE.,MM

originality report 7.9.2020 10-4 × originality report 7.9.2020 12 7 × +

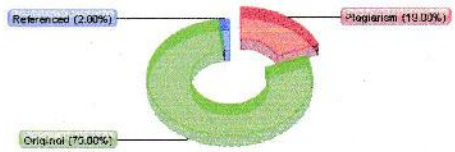
File | C:/Users/LPMU/Documents/Plagiarism%20Detector%20reports/originality%20report%207.9.2020%2012 7 3%20 %20MUHAMMAD%20RIDHO%20UTOMO 1514370369_SISTEM%20KO...

Plagiarism Detector v. 1460 - Originality Report 07-Sep-20 12:06:59

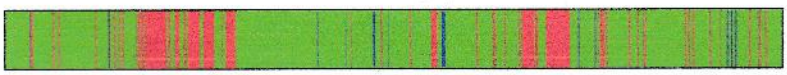
Analyzed document: MUHAMMAD RIDHO UTOMO_1514370369_SISTEM KOMPUTER.docx Licensed to: Universitas Pembangunan Panca Budi_License03

Comparison Preset: Rewrite. Detected language: Indonesian

Relation chart:



Distribution graph:



Top sources of plagiarism:

% 0 words: 774 https://analitik.com/pengolahan-data/

% 0 words: 774 https://analitik.com/pengolahan-data

% 0 words: 537 https://id.123dok.com/document/zx5jnn4q-rancang-aplikasi-multimedia-gagandegan

[Show other Sources:]

Processed resources details:

92 - Ok / 22 - Failed

[Show other Sources:]

Important notice:

2 new notificatio

IND 09:50 08-Sep-20

YAYASAN PROF. DR. H. KADIRUN YAHYA

UNIVERSITAS PEMBANGUNAN PANCA BUDI

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

LEMBAR BUKTI BIMBINGAN SKRIPSI

lama Mahasiswa	:	MUHAMMAD RIDHO UTOMO
PM	:	1514370369
rogram Studi	:	Sistem Komputer
enjang endidikan	:	Strata Satu
osen Pembimbing	:	Andysah Putera Utama Siahaan, S.Kom.,M.Kom
udul Skripsi	:	Rancangan Keamanan Informasi Pesan Teks Menggunakan Algoritma Beaufort Cipher

Tanggal	Pembahasan Materi	Status	Keterangan
7 Mei 2020	ACC BAB 2, lanjut ke BAB 3.	Revisi	
9 Mei 2020	ACC Bab 3, Lanjut ke Bab 4 dan 5	Revisi	
7 Juli 2020	ACC Seminar Hasil	Revisi	
01 September 2020	ACC Sidang	Disetujui	
29 November 2020	ACC Jllid	Disetujui	

Medan, 31 Mei 2021
Dosen Pembimbing,

Andysah Putera Utama Siahaan,
S.Kom.,M.Kom

YAYASAN PROF. DR. H. KADIRUN YAHYA

UNIVERSITAS PEMBANGUNAN PANCA BUDI

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

LEMBAR BUKTI BIMBINGAN SKRIPSI

Nama Mahasiswa	:	MUHAMMAD RIDHO UTOMO
NPM	:	1514370369
Program Studi	:	Sistem Komputer
Jenjang Pendidikan	:	Strata Satu
Dosen Pembimbing	:	Heri Kurniawan, S.Kom., M.Kom
Judul Skripsi	:	Rancangan Keamanan Informasi Pesan Teks Menggunakan Algoritma Beaufort Cipher

Tanggal	Pembahasan Materi	Status	Keterangan
19 Mei 2020	Periksa file yg saya kirim Lanjut	Revisi	
24 Juli 2020	Acc semhas	Revisi	
07 September 2020	Acc Sidang	Disetujui	
17 Desember 2020	Acc jilid	Disetujui	

Medan, 31 Mei 2021
Dosen Pembimbing,

Heri Kurniawan, S.Kom., M.Kom

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

SURAT BEBAS PUSTAKA
NOMOR: 3027/PERP/BP/2020

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

: MUHAMMAD RIDHO UTOMO
: 1514370369
t/Semester : Akhir
s : SAINS & TEKNOLOGI
n/Prodi : Sistem Komputer

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

Medan, 07 September 2020
Diketahui oleh,
Kepala Perpustakaan,

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

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

KARTU BEBAS PRAKTIKUM
Nomor. 1414/BL/LAKO/2020

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

	: MUHAMMAD RIDHO UTOMO
I.	: 1514370369
at/Semester	: Akhir
tas	: SAINS & TEKNOLOGI
an/Prodi	: Sistem Komputer

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

Medan, 13 September 2020
Ka. Laboratorium

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

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

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau

Medan, 13 September 2020
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	: MUHAMMAD RIDHO UTOMO
Tempat/Tgl. Lahir	: MEDAN / 14 Februari 1998
Nama Orang Tua	: SULISTIONO
N. P. M	: 1514370369
Fakultas	: SAINS & TEKNOLOGI
Program Studi	: Sistem Komputer
No. HP	: 082366948168
Alamat	: Jl.Puskesmas 1 Gg.Puskesmas Pembantu No.18 A

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **Rancangan Keamanan Informasi Pesan Teks Menggunakan Algoritma Beaufort Cipher**, Selanjutnya saya menyatakan :

1. Melampirkan KKM yang telah disahkan oleh Ka. Prodi dan Dekan
2. Tidak akan menuntut ujian perbaikan nilai mata kuliah untuk perbaikan indek prestasi (IP), dan mohon diterbitkan ijazahnya setelah lulus ujian meja hijau.
3. Telah tercap keterangan bebas pustaka
4. Terlampir surat keterangan bebas laboratorium
5. Terlampir pas photo untuk ijazah ukuran 4x6 = 5 lembar dan 3x4 = 5 lembar Hitam Putih
6. Terlampir foto copy STTB SLTA dilegalisir 1 (satu) lembar dan bagi mahasiswa yang lanjutan D3 ke S1 lampirkan ijazah dan 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.	0
2.	[170] Administrasi Wisuda	: Rp.	1,500,000
3.	[202] Bebas Pustaka	: Rp.	100,000
4.	[221] Bebas LAB	: Rp.	5,000
Total Biaya		**: Rp.**	**1,605,000**

Periode Wisuda Ke : 66

Ukuran Toga : XL

Diketahui/Disetujui oleh :

Hormat saya

Hamdani, ST., MT
Dekan Fakultas SAINS & TEKNOLOGI

MUHAMMAD RIDHO UTOMO
1514370369

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.

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

NAMA	: MUHAMMAD RIDHO UTOMO
NPM	: 1514370369
FAKULTAS / PROGRAM STUDI	: SAINS DAN TEKNOLOGI / SISTEM KOMPUTER
JUDUL SKRIPSI	: RANCANGAN KEAMANAN INFORMASI PESAN TEKS MENGGUNAKAN ALGORITMA *BEAUFORT CIPHER*

Dengan ini menyatakan bahwa :

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

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

Medan, 31 Juli 2021

(MUHAMMAD RIDHO UTOMO)

PERNYATAAN ORISINALITAS

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

Medan, 31 Juli 2021

(MUHAMMAD RIDHO UTOMO)

ABSTRAK

MUHAMMAD RIDHO UTOMO

Rancangan Keamanan Informasi Pesan Teks Menggunakan Algoritma *Beaufort Cipher*

2020

Dalam mengirimkan pesan, tidak boleh ada informasi yang bocor ke tangan yang tidak bertanggung jawab karena dapat menyebabkan kerugian material yang besar. Pengiriman pesan harus memiliki sistem keamanan yang baik agar terlindungi dari usaha dan percobaan peretasan pada pesan tersebut. Teknik kriptografi dapat digunakan dalam melindungi pesan. Algoritma *Beaufort Cipher* adalah salah satu dari algoritma kriptografi klasik yang mudah diaplikasikan pada pengiriman pesan teks. Algoritma ini bekerja dengan menggunakan sebuah kunci saja sehingga mudah untuk diingat dan diaplikasikan. Algoritma *Beaufort Cipher* merupakan algoritma kriptografi yang bekerja menggunakan karakter yang terdaftar pada tabel ASCII. Modulo yang digunakan adalah 256 untuk menghindari hasil enkripsi dan dekripsi berada di luar karakter ASCII yang telah ditentukan.

Kata Kunci: algoritma, keamanan, enkripsi, dekripsi, kriptografi, Beaufort

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Kuasa, karena dengan berkat dan rahmat-Nya penulis masih diberikan kesempatan untuk menyelesaikan skripsi ini sebagaimana mestinya. Skripsi ini berjudul "**RANCANGAN KEAMANAN INFORMASI PESAN TEKS MENGGUNAKAN ALGORITMA *BEAUFORT CIPHER***". Dalam kesempatan ini, penulis mengucapkan rasa terima kasih yang tak terhingga kepada pihak-pihak yang telah membantu dalam penyelesaian skripsi ini. Penulis ingin mengucapkan terima kasih kepada :

1. Orang tua saya yang selalu memberikan semangat, dukungan dan motivasi dalam penyusunan skripsi ini.
2. Bapak Dr. H. Muhammad Isa Indrawan, S.E., M.M., selaku Rektor Universitas Pembangunanan Panca Budi Medan.
3. Bapak Ir. Bhakti Alamsyah, M.T., Ph.D., selaku Rektor I, Universitas Pembangunanan Panca Budi Medan.
4. Bapak Hamdani, S.T., M.T., selaku Dekan Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
5. Bapak Eko Hariyanto, S.Kom., M.Kom., selaku Ketua Program Studi Sistem Komputer Universitas Pembangunan Panca Budi Medan.
6. Bapak Andysah Putera Utama Siahaan, S.Kom., M.Kom., selaku Dosen Pembimbing I yang telah memberikan arahan dan membimbing dalam penyelesaian skripsi ini.
7. Bapak Heri Kurniawan, S. Kom., M.Kom., selaku Dosen Pembimbing II yang telah memberikan ilmu pengetahuan, serta bimbingan dalam penyelesaian skripsi ini.
8. Dosen-dosen pada Program Studi Sistem Komputer Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
9. Staff dan karyawan pada Universitas Pembangunan Panca Budi Medan.
10. Seluruh teman-teman penulis dari program studi Sistem Komputer, Fakultas Sains dan Teknologi, Universitas Pembangunan Panca Budi, Medan

Penulis juga menyadari bahwa penyusunan skripsi ini belum mendapatkan kesempurnaan dalam segi penulisan ataupun isi. Hal ini disebabkan pengetahuan penulis yang sangat terbatas. Penulis sangat mengharapkan adanya kritik dan saran dari pembaca untuk dapat memperbaiki isi skripsi.

Medan, 29 November 2020
Penulis

Muhammad Ridho Utomo
1514370369

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Latar Belakang

Komunikasi pada zaman sekarang sudah dapat secara mudah dilakukan. Ini terlihat pesan-pesan yang disampaikan tidak perlu menggunakan surat atau kertas lagi. Pesan tersebut dapat dikirimkan melalui media elektronik. Tetapi dalam pengiriman pesan sering mendapat kendala keamanan. Pesan merupakan informasi yang bersifat pribadi yang akan dikirimkan ke orang lain dengan berisi berita tertentu. Pesan dikirimkan karena tidak berdekatannya antara penerima dan pengirim sehingga membutuhkan suatu media elektronik sebagai penghubung.

Pesan yang dikirim terkadang memiliki informasi yang tidak boleh tersebar secara umum. Pesan ini harus diterima oleh penerima pesan yang sebenarnya. Pengiriman pesan rahasia memerlukan teknik pengiriman yang baik dan aman agar pesan tersebut terhindar dari percobaan pembongkaran pesan secara paksa. Pengiriman pesan memerlukan teknik kriptografi untuk mengamankan pesan tersebut. Kebocoran informasi akan mengakibatkan kerugian yang sangat besar bagi pengirim dan penerima pesan terlebih-lebih kerugian dalam bidang keuangan dan material.

Ada beberapa cara yang dapat dilakukan dalam mengamankan pesan teks. Salah satunya adalah dengan menerapkan teknik kriptografi. Teknik kriptografi berfungsi untuk menyandikan pesan teks pesan yang dikirim merupakan pesan terenkripsi sehingga informasi yang terkandung di dalam pesan tersebut aman dari

gangguan dan ancaman pihak yang tidak bertanggung jawab. Ada banyak algoritma juga yang dapat digunakan dalam melakukan pengamanan terhadap dokumen yang akan dirahasiakan. Penulis mencoba mengangkat algoritma *Beaufort Cipher* dalam mengamankan pesan berbasis teks.

Algoritma *Beaufort Cipher* bekerja dengan cara menyandikan *plaintext* menjadi *Ciphertext* dengan menggunakan kunci angka. Cara kerja *Beaufort Cipher* ini adalah dengan cara menggeser posisi karakter *plaintext* dengan kunci angka yang sudah ditentukan. Pesan yang sudah terenkripsi diharapkan sudah tidak dapat difahami oleh orang-orang yang ingin membongkar paksa pesan tersebut.

Algoritma *Beaufort Cipher* ini akan diprogram dengan menggunakan bahasa pemrograman visual berbasis desktop yaitu Microsoft Visual Basic.Net 2010. Hasil program aplikasi diharapkan dapat melaksanakan proses pengaman informasi menggunakan algoritma *Beaufort Cipher*. Berdasarkan latar belakang tersebut, maka penulis mengambil judul "**RANCANGAN KEAMANAN INFORMASI PESAN TEKS MENGGUNAKAN ALGORITMA *BEAUFORT CIPHER***".

1.2 Rumusan Masalah

Adapun rumusan masalah yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut:

1. Bagaimana cara kerja algoritma *Beaufort Cipher*?
2. Bagaimana mengamankan pesan teks dengan algoritma *Beaufort Cipher*?

3. Bagaimana menentukan kunci yang digunakan pada algoritma *Beaufort Cipher*?
4. Bagaimana mengembalikan *Ciphertext* ke *plaintext* dengan kunci yang sudah ditentukan sebelumnya?

1.3 Batasan Masalah

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

1. Pesan yang dikirim adalah berbasis teks yang dimasukkan langsung pada textbox.
2. Kunci yang digunakan adalah hanya berbentuk angka pada setiap proses enkripsi dan dekripsi.
3. Bahasa pemrograman yang digunakan adalah Microsoft Visual Basic.NET 2010.
4. Program aplikasi berbasis *desktop* dan tidak *online*.
5. Panjang maksimal karakter adalah 1000 karakter.

1.4 Tujuan Penelitian

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

1. Untuk mengetahui cara kerja algoritma *Beaufort Cipher*.
2. Untuk mengamankan pesan berbasis teks.
3. Untuk menentukan kunci yang digunakan pada algoritma *Beaufort Cipher*.

4. Untuk mengembalikan *Ciphertext* ke *plaintext* dengan kunci yang sudah ditentukan sebelumnya.

1.5 Manfaat Penelitian

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

1. Pesan teks akan aman pada saat dikirimkan dan terhindar dari penyalahgunaan informasi.
2. Menghindari pencurian informasi.
3. Menambah pengetahuan tentang algoritma *Beaufort Cipher*.

BAB II

LANDASAN TEORI

2.1 Data Processing

Tanpa pemrosesan data, perusahaan membatasi akses mereka ke data yang dapat mengasah daya saing mereka dan memberikan wawasan bisnis yang kritis. Itulah mengapa sangat penting bagi semua perusahaan untuk memahami perlunya memproses semua data mereka, dan bagaimana cara mengatasinya. Pemrosesan data terjadi ketika data dikumpulkan dan diterjemahkan menjadi informasi yang dapat digunakan. Biasanya dilakukan oleh ilmuwan data atau tim ilmuwan data, penting untuk pemrosesan data dilakukan dengan benar agar tidak berdampak negatif pada produk akhir, atau output data. Pemrosesan data dimulai dengan data dalam bentuk mentah dan mengubahnya menjadi format yang lebih mudah dibaca (grafik, dokumen, dll.), Memberikannya bentuk dan konteks yang diperlukan untuk ditafsirkan oleh komputer dan digunakan oleh karyawan di seluruh organisasi (Sun et al., 2014).

Pemrosesan data adalah konversi data menjadi bentuk yang dapat digunakan dan diinginkan. Konversi atau "pemrosesan" ini dilakukan menggunakan urutan operasi yang telah ditentukan baik secara manual atau otomatis. Sebagian besar pemrosesan dilakukan dengan menggunakan komputer dan dengan demikian dilakukan secara otomatis. Data output atau "diproses" dapat diperoleh dalam berbagai bentuk. Contoh bentuk-bentuk ini termasuk gambar, grafik, tabel, file vektor, audio, grafik atau format lain yang diinginkan.

Bentuk yang diperoleh tergantung pada perangkat lunak atau metode pemrosesan data yang digunakan. Ketika dilakukan sendiri itu disebut sebagai pemrosesan data otomatis.

Pemrosesan data pada dasarnya menyinkronkan semua data yang dimasukkan ke dalam perangkat lunak untuk menyaring informasi yang paling berguna darinya. Ini adalah tugas yang sangat penting bagi perusahaan mana pun karena membantu mereka mengekstraksi konten yang paling relevan untuk digunakan nanti. Setiap sektor penting, baik bank, sekolah, perguruan tinggi atau perusahaan besar, hampir semua membutuhkan pemrosesan data ini. Pemrosesan ini dilakukan untuk menyimpan informasi yang paling halus dalam sistem mereka untuk digunakan nanti. Pemrosesan manual sangat memakan waktu dan mengharuskan Anda melibatkan terlalu banyak orang untuk melakukannya. Ini benar-benar bukan tugas yang layak ketika Anda memiliki data dalam jumlah besar. Saat ini orang-orang industri bergantung pada perangkat lunak yang kuat dan efisien untuk membantu dalam memproses semua data itu. Ini membantu mereka dalam mencapai akurasi yang lebih besar dan meningkatkan efisiensi mereka. Dengan pemrosesan data yang tepat, semakin banyak informasi yang dapat disortir. Ini membantu dalam mendapatkan pandangan yang lebih jelas tentang materi dan memiliki pemahaman yang lebih baik tentang hal itu. Ini dapat mengarah pada produktivitas yang lebih baik dan lebih banyak keuntungan untuk berbagai bidang bisnis.

2.1.1 Aplikasi Pengolahan Data Dunia Nyata

Dengan penerapan algoritma dan protokol keamanan yang tepat, dapat dipastikan bahwa input dan informasi yang diproses aman dan disimpan dengan aman tanpa akses atau perubahan yang tidak sah. Dengan data yang diproses dengan benar, para peneliti dapat menulis materi ilmiah dan menggunakannya untuk tujuan pendidikan. Hal yang sama dapat diterapkan untuk evaluasi bidang dan faktor ekonomi dan tersebut. Dalam industri perawatan kesehatan, data yang diproses dapat digunakan untuk pengambilan informasi yang lebih cepat dan bahkan menyelamatkan nyawa. Selain itu, rincian penyakit dan catatan teknik perawatan dapat mengurangi waktu untuk mencari solusi dan membantu mengurangi penderitaan pasien.

Mengolah data berdasarkan jenis dan informasi dapat menghemat banyak ruang yang dihabiskan oleh data yang tidak terorganisir dan disimpan secara sembarangan. Data yang diproses juga dapat membantu memastikan bahwa semua staf dan pekerja dapat memahaminya dengan mudah. Mereka dapat mengimplementasikannya dalam pekerjaan, yang jika tidak dapat mengambil lebih banyak waktu dan berakhir dalam memberikan output yang menurun. Ini dapat membahayakan kepentingan bisnis atau organisasi.

2.1.2 Fokus Pengolahan Data

Sebagian besar bisnis dan bidang memerlukan data untuk memberikan kualitas layanan yang baik. Memiliki kumpulan wawasan tentang data yang dikumpulkan dan implikasinya adalah aspek yang sangat penting dalam

mengelolanya dan memastikan keaslian statistik. Ini sangat penting untuk layanan yang berkaitan dengan teknologi keuangan. Ini karena data transaksi dan perincian pembayaran harus disimpan dengan benar agar mudah diakses oleh pelanggan dan juga pejabat perusahaan sesuai kebutuhan. Pemrosesan tidak terbatas pada komputer dan dapat dilakukan secara manual juga.

Sementara opsi manual menggunakan kekuatan otak dan kecerdasan, teknik pemrosesan data elektronik dapat menghemat banyak waktu dan memastikan alur kerja yang lancar dan memastikan kepatuhan terhadap tenggat waktu. Akurasi juga lebih tinggi dengan pemrosesan elektronik. Salah satu aspek penting dari ini adalah untuk memastikan bahwa wawasan yang terbentuk disimpan untuk masa depan dan digunakan bersama untuk menghemat daya dan waktu komputasi.

2.1.3 Dasar-dasar Pemrosesan Data

Pemrosesan data diperlukan oleh aktivitas apa pun yang membutuhkan pengumpulan data. Data yang dikumpulkan ini perlu disimpan, disortir, diproses, dianalisis, dan disajikan. Proses lengkap ini dapat dibagi menjadi 6 tahap primer sederhana yaitu:

1 Pengumpulan data

2 Penyimpanan data

3 Penyortiran data

4 Memproses data

5 Analisis data

6 Presentasi dan kesimpulan data

Setelah data dikumpulkan, kebutuhan untuk entri data muncul untuk penyimpanan data. Penyimpanan dapat dilakukan dalam bentuk fisik dengan menggunakan kertas, notebook atau dalam bentuk fisik lainnya. Dengan kemunculan dan semakin meningkatnya penekanan pada Sistem Komputer, Big Data & Data Mining pengumpulan data besar dan sejumlah operasi perlu dilakukan untuk analisis dan presentasi yang bermakna, data disimpan dalam bentuk digital. Memiliki data mentah dan data yang diolah menjadi bentuk digital memungkinkan pengguna untuk melakukan sejumlah besar operasi dalam waktu singkat dan memungkinkan konversi ke berbagai jenis. Dengan demikian pengguna dapat memilih output yang paling sesuai dengan kebutuhan.

Penggunaan dan pemrosesan data yang terus-menerus ini mengikuti siklus yang disebut sebagai siklus pemrosesan data dan siklus pemrosesan informasi. Siklus ini dapat memberikan hasil instan atau memakan waktu tergantung pada kebutuhan pemrosesan data. Kompleksitas dalam bidang ini meningkat yang menciptakan kebutuhan akan teknik-teknik canggih.

Penyimpanan data diikuti dengan menyortir dan memfilter. Tahap ini sangat dipengaruhi oleh format penyimpanan data. Ini lebih lanjut tergantung pada perangkat lunak yang digunakan. Data umum dan non-kompleks dapat disimpan sebagai file teks, tabel atau kombinasi keduanya dalam Microsoft Excel atau perangkat lunak serupa. Sebagai tugas menjadi kompleks yang memerlukan melakukan operasi khusus dan khusus. Mereka membutuhkan alat pengolah data

dan perangkat lunak yang berbeda yang dimaksudkan untuk memenuhi kebutuhan khusus.

Menyimpan, menyortir, memfilter, dan memproses data dapat dilakukan dengan perangkat lunak tunggal atau kombinasi perangkat lunak mana saja yang layak dan diperlukan. Pemrosesan demikian yang dilakukan oleh perangkat lunak dilakukan sesuai dengan rangkaian operasi yang telah ditentukan. Sebagian besar perangkat lunak modern memungkinkan pengguna untuk melakukan tindakan berbeda berdasarkan analisis atau studi yang akan dilakukan. Ini menyediakan file output dalam berbagai format (Barone et al., 2017).

2.2 Keamanan Data

Keamanan data adalah seperangkat standar dan teknologi yang melindungi data dari kehancuran, modifikasi, atau pengungkapan yang disengaja atau tidak disengaja. Keamanan data dapat diterapkan dengan menggunakan berbagai teknik dan teknologi, termasuk kontrol administratif, keamanan fisik, kontrol logis, standar organisasi, dan teknik perlindungan lainnya yang membatasi akses ke pengguna atau proses yang tidak sah atau berbahaya (Rao & Selvamani, 2015).

Keamanan data mengacu pada langkah-langkah privasi digital pelindung yang diterapkan untuk mencegah akses tidak sah ke komputer, database, dan situs web. Keamanan data juga melindungi data dari korupsi. Keamanan data adalah aspek penting dari TI untuk organisasi dari berbagai ukuran dan tipe. Keamanan data juga dikenal sebagai keamanan informasi atau keamanan komputer.

Contoh teknologi keamanan data termasuk backup, masking data dan penghapusan data. Ukuran teknologi keamanan data utama adalah enkripsi, di mana data digital, perangkat lunak / perangkat keras, dan hard drive dienkripsi dan karenanya tidak dapat dibaca oleh pengguna dan peretas yang tidak sah. Salah satu metode yang paling umum dijumpai dalam mempraktikkan keamanan data adalah penggunaan otentikasi. Dengan otentikasi, pengguna harus memberikan kata sandi, kode, data biometrik, atau bentuk data lainnya untuk memverifikasi identitas sebelum akses ke sistem atau data diberikan. Keamanan data juga sangat penting untuk catatan perawatan kesehatan, sehingga pendukung kesehatan dan praktisi medis di AS dan negara-negara lain berupaya menerapkan privasi rekam medis elektronik dengan menciptakan kesadaran tentang hak-hak pasien terkait dengan pelepasan data ke laboratorium, dokter, rumah sakit dan fasilitas medis lainnya.

2.2.1 Pentingnya Keamanan Data

Semua bisnis saat ini menangani data hingga taraf tertentu. Dari raksasa perbankan yang menangani data pribadi dan keuangan dalam volume besar hingga bisnis satu orang yang menyimpan detail kontak pelanggannya di ponsel, data berperan di perusahaan baik besar maupun kecil.

Tujuan utama keamanan data adalah untuk melindungi data yang dikumpulkan, disimpan, diterima, atau ditransmisikan oleh suatu organisasi. Kepatuhan juga merupakan pertimbangan utama. Tidak masalah perangkat, teknologi, atau proses mana yang digunakan untuk mengelola, menyimpan, atau

mengumpulkan data, itu harus dilindungi. Pelanggaran data dapat menyebabkan kasus litigasi dan denda yang sangat besar, belum lagi kerusakan reputasi organisasi. Pentingnya melindungi data dari ancaman keamanan lebih penting saat ini daripada sebelumnya.

Keamanan data mengacu pada proses melindungi data dari akses yang tidak sah dan korupsi data sepanjang siklus hidupnya. Keamanan data termasuk enkripsi data, tokenization, dan praktik manajemen kunci yang melindungi data di semua aplikasi dan platform. Organisasi di seluruh dunia banyak berinvestasi dalam kemampuan pertahanan cyber teknologi informasi untuk melindungi aset penting mereka. Apakah suatu perusahaan perlu melindungi merek, modal intelektual, dan informasi pelanggan atau menyediakan kontrol untuk infrastruktur penting, sarana untuk mendeteksi insiden dan merespons melindungi kepentingan organisasi memiliki tiga elemen umum: orang, proses, dan teknologi.

2.2.2 Solusi Keamanan Data

Data membutuhkan enkripsi dalam mengamankan informasi yang ada dalam data tersebut. Dengan enkripsi data canggih, tokenization, dan manajemen utama untuk melindungi data di seluruh aplikasi, transaksi, penyimpanan, dan platform big data, Teknik ini menyederhanakan perlindungan data sensitif bahkan dalam kasus penggunaan yang paling kompleks sekalipun. Beberapa model keamanan data antara lain:

1. Keamanan akses cloud - Platform perlindungan yang memungkinkan Anda untuk pindah ke cloud dengan aman sambil melindungi data dalam aplikasi cloud.
2. Enkripsi data - Solusi keamanan data-sentris dan tokenisasi yang melindungi data di lingkungan perusahaan, cloud, seluler, dan data besar.
3. Modul keamanan perangkat keras - Modul keamanan perangkat keras yang menjaga data keuangan dan memenuhi persyaratan keamanan dan kepatuhan industri.
4. Manajemen kunci - Solusi yang melindungi data dan memungkinkan kepatuhan regulasi industri.
5. Enterprise Data Protection - Solusi yang menyediakan pendekatan data-centric end-to-end untuk perlindungan data perusahaan.
6. Keamanan Pembayaran - Solusi menyediakan enkripsi dan tokenisasi point-to-point lengkap untuk transaksi pembayaran ritel, memungkinkan pengurangan lingkup PCI.
7. Big Data, Hadoop, dan perlindungan data IofT - Solusi yang melindungi data sensitif di Danau Data - termasuk Hadoop, Teradata, Micro Focus Vertica, dan platform Big Data lainnya.
8. Keamanan Aplikasi Seluler - Melindungi data sensitif di aplikasi seluler asli sembari menjaga data dari ujung ke ujung.
9. Keamanan Peramban Web - Melindungi data sensitif yang diambil di peramban, dari titik pelanggan memasukkan pemegang kartu atau data

pribadi dan menjaganya agar tetap terlindungi melalui ekosistem ke tujuan tuan rumah tepercaya.

10. eMail Security - Solusi yang menyediakan enkripsi ujung ke ujung untuk email dan olahpesan seluler, menjaga informasi pribadi dan informasi kesehatan pribadi tetap aman dan pribadi.

2.2.3 Kerahasiaan

Kerahasiaan mengacu pada melindungi informasi agar tidak diakses oleh pihak yang tidak berwenang. Dengan kata lain, hanya orang yang diberi wewenang untuk melakukannya yang dapat memperoleh akses ke data sensitif. Bayangkan catatan bank harus dapat diakses, tentu saja, dan karyawan di bank yang membantu dalam menjalankan transaksi harus dapat mengaksesnya, tetapi tidak ada orang lain yang seharusnya. Kegagalan untuk menjaga kerahasiaan berarti bahwa seseorang yang seharusnya tidak memiliki akses telah berhasil mendapatkannya, melalui perilaku yang disengaja atau karena kecelakaan. Kegagalan kerahasiaan seperti itu, umumnya dikenal sebagai pelanggaran, biasanya tidak dapat diperbaiki. Setelah rahasia itu terungkap, tidak ada cara untuk mengetahuinya. Jika catatan bank diposting di situs web publik, semua orang dapat mengetahui nomor rekening bank, saldo, dll., Informasi itu tidak dapat dihapus dari pikiran, kertas, komputer, dan tempat lain mereka. Hampir semua insiden keamanan utama yang dilaporkan di media saat ini melibatkan kerugian besar kerahasiaan. Jadi, secara ringkas, pelanggaran kerahasiaan berarti

bahwa seseorang memperoleh akses ke informasi yang seharusnya tidak memiliki akses ke sana.

2.2.4 Integritas

Integritas mengacu pada memastikan keaslian informasi — bahwa informasi tidak diubah, dan bahwa sumber informasi itu asli. Bayangkan jika seseorang memiliki situs web dan Anda menjual produk di situs itu. Sekarang bayangkan penyerang dapat berbelanja di situs web dan dengan jahat mengubah harga produk Anda sehingga mereka dapat membeli apa pun dengan harga berapa pun yang mereka pilih. Itu akan menjadi kegagalan integritas karena informasi dalam hal ini, harga suatu produk telah diubah dan perubahan ini tidak dapat digagalkan. Contoh lain dari kegagalan integritas adalah ketika sesorang mencoba terhubung ke situs web dan penyerang jahat antara Anda dan situs web mengalihkan lalu lintas ke situs web yang berbeda. Dalam hal ini, situs yang dituju tidak asli.

2.2.5 Ketersediaan

Ketersediaan berarti informasi dapat diakses oleh pengguna yang berwenang. Jika penyerang tidak dapat mengkompromikan dua elemen pertama dari keamanan informasi (lihat di atas) mereka dapat mencoba melakukan serangan seperti penolakan layanan yang akan menurunkan server, membuat situs web tidak tersedia untuk pengguna yang sah karena kurangnya ketersediaan.

2.2.6 Kontrol Akses

Kesalahan terbesar yang bisa dilakukan oleh perancang aplikasi adalah mengabaikan kontrol akses sebagai bagian dari fungsionalitas yang diperlukan. Jarang bahwa setiap pengguna atau sistem yang berinteraksi dengan suatu aplikasi harus memiliki hak yang sama di seluruh aplikasi itu. Beberapa pengguna mungkin memerlukan akses ke data tertentu dan bukan yang lain; beberapa sistem harus atau tidak dapat mengakses aplikasi. Akses ke komponen, fungsi, atau modul tertentu dalam aplikasi juga harus dikontrol. Kontrol akses juga penting untuk kepatuhan audit dan peraturan. Beberapa cara umum mengelola kontrol akses adalah:

1. Baca, tulis, dan jalankan hak istimewa: File
2. Kontrol akses berbasis peran: administrator, pengguna
3. Alamat IP akses berbasis host, nama mesin
4. Objek kode kontrol akses tingkat objek, banyak pembaca / penulis tunggal

2.3 Algoritma

Untuk membuat komputer melakukan apa pun, sesorang harus menulis program komputer. Untuk menulis program komputer, sesorang harus memberi tahu komputer, langkah demi langkah, persis apa yang sesorang inginkan. Komputer kemudian "mengeksekusi" program, mengikuti setiap langkah secara mekanis, untuk mencapai tujuan akhir. Ketika sesorang memberi tahu komputer apa yang harus dilakukan, sesorang juga harus memilih bagaimana melakukannya. Di situlah algoritma komputer masuk. Algoritma adalah teknik dasar yang

digunakan untuk menyelesaikan pekerjaan (Gurevich, 2012). Mari kita ikuti contoh untuk membantu mendapatkan pemahaman tentang konsep algoritma. Katakanlah sesorang memiliki seorang teman yang tiba di bandara, dan teman sesorang perlu pergi dari bandara ke rumah. Berikut adalah empat algoritma berbeda yang mungkin akan diberikan kepada orang lain untuk sampai ke rumah:

1. Algoritma taksi:
    a. Pergi ke tempat taksi.
    b. Naik taksi.
    c. Berikan alamat saya pada pengemudi.

2. Algoritma panggilan-saya:
    a. Ketika pesawat Anda tiba, hubungi ponsel saya.
    b. Temui saya di luar klaim bagasi.

3. Algoritma rent-a-car:
    a. Naik shuttle ke tempat rental mobil.
    b. Menyewa mobil.
    c. Ikuti petunjuk untuk sampai ke rumah saya.

4. Algoritma bus:
    a. Di luar klaim bagasi, naik bus nomor 70.
    b. Transfer ke bus 14 di Main Street.

c. Turun di Elm street.

d. Berjalanlah dua blok ke utara ke rumah saya.

Keempat algoritma ini mencapai tujuan yang persis sama, tetapi masing-masing algoritma melakukannya dengan cara yang sama sekali berbeda. Setiap algoritma juga memiliki biaya dan waktu perjalanan yang berbeda. Naik taksi, misalnya, mungkin adalah cara tercepat, tetapi juga yang paling mahal. Naik bus jelas lebih murah, tetapi jauh lebih lambat. Anda memilih algoritma berdasarkan keadaan.

Dalam pemrograman komputer, seringkali ada banyak cara berbeda - algoritma - untuk menyelesaikan tugas yang diberikan. Setiap algoritma memiliki kelebihan dan kekurangan dalam situasi yang berbeda. Penyortiran adalah satu tempat di mana banyak penelitian telah dilakukan karena komputer menghabiskan banyak daftar penyortiran waktu. Berikut adalah lima algoritma berbeda yang digunakan dalam penyortiran:

1. Bin sort
2. Gabungkan semacam
3. Semacam gelembung
4. Semacam shell
5. Quicksort

Jika ada sejuta nilai integer antara 1 dan 10 dan perlu diurutkan, jenis bin sort adalah algoritma yang tepat untuk digunakan. Jika Anda memiliki sejuta judul

buku, quicksort mungkin merupakan algoritma terbaik. Dengan mengetahui kekuatan dan kelemahan dari berbagai algoritma, Anda memilih yang terbaik untuk tugas yang ada.

2.3.1 Desain Konseptual

Algoritma adalah serangkaian instruksi, sering disebut sebagai "proses," yang harus diikuti ketika memecahkan masalah tertentu. Meskipun secara teknis tidak dibatasi oleh definisi, kata itu hampir selalu terkait dengan komputer, karena algoritma yang diproses komputer dapat mengatasi masalah yang jauh lebih besar daripada manusia, jauh lebih cepat. Karena komputasi modern menggunakan algoritma jauh lebih sering daripada pada titik lain dalam sejarah manusia, bidang telah tumbuh di sekitar desain, analisis, dan penyempurnaan. Bidang desain algoritma membutuhkan latar belakang matematika yang kuat, dengan gelar ilmu komputer yang sangat dicari kualifikasi. Ini menawarkan semakin banyak pilihan karir yang sangat dikompensasi, karena kebutuhan akan lebih banyak (dan juga lebih canggih) algoritma terus meningkat.

Pada tingkat yang paling sederhana, algoritma pada dasarnya hanya seperangkat instruksi yang diperlukan untuk menyelesaikan tugas. Pengembangan algoritma, meskipun umumnya tidak disebut demikian, telah menjadi kebiasaan yang populer dan pengejaran profesional untuk semua catatan sejarah. Jauh sebelum fajar era komputer modern, orang menetapkan rutinitas yang telah ditentukan untuk bagaimana mereka akan melakukan tugas sehari-hari, sering menuliskan daftar langkah-langkah yang harus diambil untuk mencapai tujuan

penting, mengurangi risiko melupakan sesuatu yang penting. Ini, pada dasarnya, adalah apa itu algoritma. Desainer mengambil pendekatan yang mirip dengan pengembangan algoritma untuk tujuan komputasi: pertama, mereka melihat masalah. Kemudian, mereka menguraikan langkah-langkah yang akan diperlukan untuk menyelesaikannya. Akhirnya, mereka mengembangkan serangkaian operasi matematika untuk mencapai langkah-langkah tersebut.

2.3.2 Tugas Algoritma

Tugas sederhana dapat diselesaikan dengan algoritma yang dihasilkan dengan beberapa menit, atau paling banyak pekerjaan pagi. Tingkat kompleksitas menjalankan tantangan yang panjang, namun, sampai pada masalah yang sangat rumit sehingga mereka telah menghalangi matematikawan yang tak terhitung jumlahnya selama bertahun-tahun - atau bahkan berabad-abad. Komputer modern menghadapi masalah pada tingkat ini di bidang-bidang seperti keamanan dunia maya, serta penanganan data besar - penyortiran set data yang efisien dan menyeluruh sedemikian besar sehingga bahkan komputer standar tidak dapat memprosesnya secara tepat waktu. Contoh data besar mungkin termasuk "setiap artikel di Wikipedia," "setiap halaman web yang diindeks dan diarsipkan akan kembali ke tahun 1998," atau "enam bulan terakhir pembelian online yang dilakukan di Amerika."

2.3.3 Rekayasa Algoritma

Ketika desain algoritma baru diterapkan dalam istilah praktis, disiplin terkait dikenal sebagai rekayasa algoritma. Kedua fungsi tersebut sering dilakukan oleh orang yang sama, meskipun organisasi yang lebih besar (seperti Amazon dan Google) mempekerjakan desainer dan insinyur khusus, mengingat tingkat kebutuhan mereka akan algoritma baru dan khusus. Seperti proses desain, rekayasa algoritma sering kali melibatkan akreditasi sains komputer, dengan latar belakang yang kuat dalam matematika: di mana mereka ada sebagai profesi yang terpisah dan terspesialisasi, insinyur algoritma mengambil ide-ide konseptual dari desainer dan proses kreatif dari mereka yang akan dipahami oleh komputer. Dengan kemajuan teknologi digital yang mantap, para insinyur yang berdedikasi akan terus menjadi semakin umum.

2.4 Kriptografi

Kriptografi adalah teknik mengubah dan mentransmisikan data rahasia dengan cara disandikan sehingga hanya pengguna yang berwenang dan dimaksudkan dapat memperoleh atau bekerja di dalamnya. Ini adalah kata asal Yunani di mana "crypto" berarti tersembunyi dan "graphy" berarti menulis, jadi kriptografi berarti tulisan tersembunyi atau rahasia. Ini memperkenalkan triad seperti kerahasiaan, non-penolakan, integritas dan keaslian dalam komunikasi data yang sedang berlangsung.

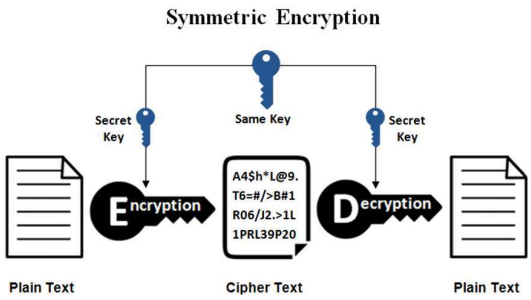
Kriptografi adalah disiplin atau teknik yang digunakan dalam melindungi integritas atau kerahasiaan pesan elektronik dengan mengubahnya menjadi bentuk

(*Ciphertext*) yang tidak dapat dibaca. Hanya penggunaan kunci rahasia yang dapat mengubah teks sandi menjadi bentuk yang dapat dibaca manusia (teks jelas). Perangkat lunak kriptografi dan / atau perangkat keras menggunakan rumus matematika (algoritma) untuk mengubah teks dari satu bentuk ke bentuk lainnya.

Komunikasi yang aman dapat disediakan menggunakan teknik, di hadapan konten pihak ketiga berbahaya yang disebut musuh. Teknik-teknik ini dapat disebut sebagai Kriptografi. Pesan pribadi apa pun dapat disembunyikan dari publik atau pihak ketiga, menggunakan seperangkat protokol. Protokol-protokol ini perlu dianalisis dan dibangun dengan cara yang efisien untuk menjaga kerahasiaan pesan yang dikirim. Kriptografi modern memiliki aspek tertentu yang merupakan pusatnya seperti integritas data, otentikasi, kerahasiaan dll. Di dunia modern, kriptografi sangat bergantung pada mata pelajaran seperti matematika dan ilmu komputer. Algoritma untuk Kriptografi dirancang sedemikian rupa sehingga sulit untuk dipecahkan dalam praktik oleh pihak ketiga jahat yang juga dikenal sebagai musuh. Pendekatan praktis terhadap pemecahan algoritma semacam itu akan gagal, namun, pendekatan teoritis mungkin memecahkan sistem tersebut. Dengan demikian, algoritma apa pun dapat disebut sebagai aman, jika sifat kuncinya tidak dapat disimpulkan, dengan *Ciphertext* yang diberikan. Kriptografi dapat dikategorikan menjadi dua cabang: Symmetric dan Asymmetric. Dengan pendekatan simetris, satu kunci digunakan untuk proses enkripsi dan dekripsi yaitu pengirim dan penerima harus memiliki kunci bersama. Namun, dengan pendekatan ini, distribusi kunci adalah tautan yang lemah, yang memunculkan pendekatan baru.

2.4.1 Kriptografi Simetris

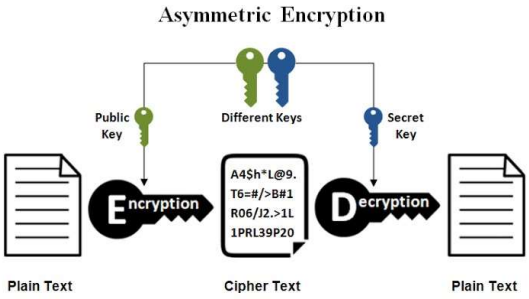
Kriptografi kunci simetris adalah setiap algoritma kriptografi yang didasarkan pada kunci bersama yang digunakan untuk mengenkripsi atau mendekripsi teks / cyphertext, dalam kontrak dengan kriptografi kunci asimetris, di mana kunci enkripsi dan dekripsi dihubungkan oleh berbeda. Enkripsi simetris umumnya lebih efisien daripada enkripsi asimetris dan karenanya lebih disukai ketika sejumlah besar data perlu dipertukarkan. Membuat kunci bersama sulit menggunakan hanya algoritma enkripsi simetris, sehingga dalam banyak kasus, enkripsi asimetris digunakan untuk membuat kunci bersama antara dua pihak. Contoh untuk kriptografi kunci simetris termasuk AES, DES, dan 3DES. Protokol pertukaran kunci yang digunakan untuk membangun kunci enkripsi bersama termasuk Diffie-Hellman (DH), Eliptic Curve (EC) dan RSA. Berikut ini skema dari kriptografi simetris (Ayushi, 2010).



Gambar 2.1 Skema kriptografi simetris
Sumber: (Ayushi, 2010)

2.4.2 Kriptografi Asimetris

Dalam versi kriptografi asimetris, pengirim dan penerima memiliki dua kunci, publik dan pribadi. Kunci pribadi dirahasiakan sedangkan kunci publik terbuka ke dunia luar. Set data apa pun, yang dienkripsi dengan kunci publik hanya dapat didekripsi menggunakan kunci pribadi yang sesuai. Ketika datang ke perbandingan, pendekatan simetris lebih cepat daripada yang asimetris. Contoh - tanda tangan digital menggunakan kriptografi asimetris untuk mengenkripsi pesan dalam hash alih-alih pesan lengkap. Berikut ini skema kriptografi asimetris (S. et al., 2012).



Gambar 2.2 Skema kriptografi asimetris
Sumber: (Ayushi, 2010)

2.5 *Beaufort Cipher*

Beaufort Cipher, dibuat oleh Sir Francis Beaufort, adalah *Cipher* pengganti yang mirip dengan *Cipher* Vigenère, dengan mekanisme penyandian dan tablo yang sedikit dimodifikasi. Aplikasi yang paling terkenal adalah di mesin sandi berbasis rotor, Hagelin M-209. *Cipher* Beaufort didasarkan pada kotak Beaufort yang pada dasarnya sama dengan kotak Vigenère tetapi dalam urutan

terbalik dimulai dengan huruf "Z" di baris pertama, di mana baris pertama dan kolom terakhir memiliki tujuan yang sama (Pratama & Tamatjita, 2015).

Untuk mengenkripsi, pertama pilih karakter *plaintext* dari baris atas tablo; sebut kolom ini P. Kedua, turunkan kolom P ke huruf kunci yang sesuai K. Akhirnya, pindah langsung ke kiri dari huruf kunci ke tepi kiri tablo, enkripsi *Ciphertext* dari *plaintext* P dengan kunci K akan ada di sana.

Misalnya jika mengenkripsi karakter teks biasa "d" dengan kunci "m" langkah-langkahnya adalah:

1. temukan kolom dengan "d" di atas,
2. melakukan perjalanan ke kolom itu untuk menemukan kunci "m",
3. perjalanan ke tepi kiri tablo untuk menemukan huruf *Ciphertext* ("J" dalam hal ini).

Untuk mendekripsi, prosesnya terbalik. *Beaufort Cipher* adalah *Cipher* timbal balik, yaitu, algoritma dekripsi dan enkripsi adalah sama.

2.6 Kriptanalis

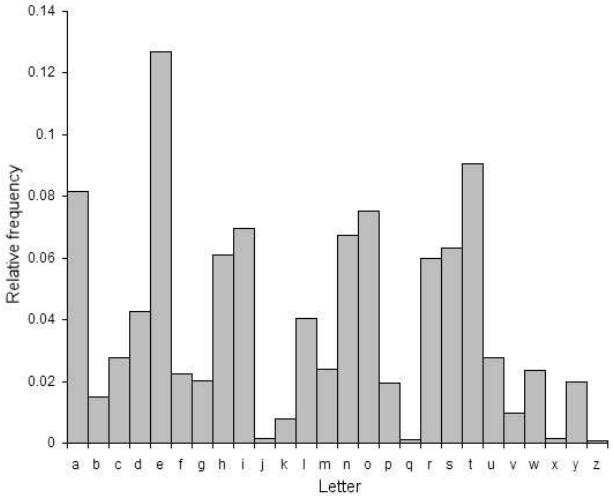
Kriptanalisis adalah seni memecahkan kode dan sandi. *Cipher* Caesar mungkin adalah yang paling mudah untuk dilanggar dari semua *Cipher*. Karena pergeseran harus berupa angka antara 1 dan 25, (0 atau 26 akan menghasilkan teks yang tidak berubah), kita cukup mencoba setiap kemungkinan dan melihat mana yang menghasilkan sepotong teks yang dapat dibaca. Jika Anda tahu apa sepotong

Ciphertext itu, atau Anda dapat menebaknya, maka ini akan memungkinkan Anda untuk segera menemukan kuncinya.

Jika ini tidak memungkinkan, pendekatan yang lebih sistematis adalah menghitung distribusi frekuensi huruf-huruf dalam teks sandi. Ini terdiri dari menghitung berapa kali setiap huruf muncul. Teks bahasa Inggris alami memiliki distribusi yang sangat berbeda yang dapat digunakan membantu memecahkan kode.

Ini berarti bahwa huruf e adalah yang paling umum, dan muncul hampir 13% dari waktu, sedangkan z muncul jauh lebih sedikit dari 1 persen waktu. Penerapan *Cipher* Caesar tidak mengubah frekuensi huruf ini, ia hanya menggesernya sedikit (untuk pergeseran 1, huruf *Ciphertext* yang paling sering menjadi f). Seorang cryptanalyst hanya harus menemukan pergeseran yang menyebabkan frekuensi *Ciphertext* cocok dengan frekuensi bahasa Inggris alami, kemudian mendekripsi teks menggunakan pergeseran itu. Metode ini dapat digunakan untuk dengan mudah memecahkan *Cipher* Caesar dengan tangan.

Semua strategi yang bekerja dengan substitusi *Cipher* juga akan bekerja dengan *Cipher* Caesar (tetapi metode yang bekerja pada *Cipher* Caesar tidak selalu bekerja pada *Cipher* substitusi umum) (Sinkov et al., 2009).



Gambar 2.3 Kemungkinan Kemunculan Karakter
Sumber: (Sinkov et al., 2009)

Untuk metode yang bekerja dengan baik pada komputer, kita perlu cara untuk mencari tahu dari mana dari 25 dekripsi yang mungkin terlihat paling mirip teks bahasa Inggris. Lihat Cryptanalysis of the Caesar *Cipher* untuk mengetahui cara memecahkannya menggunakan statistik quadgram. Kunci (atau pergeseran) yang menghasilkan dekripsi dengan kemungkinan tertinggi menjadi teks bahasa Inggris kemungkinan besar adalah kunci yang benar. Tentu saja, semakin banyak *Ciphertext* yang Anda miliki, semakin besar kemungkinan ini benar (ini adalah kasus untuk semua ukuran statistik, termasuk pendekatan frekuensi di atas). Jadi metode yang digunakan adalah mengambil *Ciphertext*, coba mendekripsi dengan masing-masing kunci, lalu lihat dekripsi mana yang terlihat terbaik. Metode kriptanalisis sederhana ini hanya bekerja pada *Cipher* yang sangat sederhana seperti *Cipher* Caesar dan *Cipher* rail rail, *Cipher* yang sedikit lebih kompleks dapat memiliki terlalu banyak kunci untuk memeriksa semuanya.

2.7 Unified Modeling Language (UML)

Unified Modeling Language (UML) adalah bahasa pemodelan standar yang memungkinkan pengembang menentukan, memvisualisasikan, membuat, dan mendokumentasikan artefak sistem perangkat lunak (Technopedia, 2019). Dengan demikian, *UML* membuat artefak ini dapat diskalakan, aman, dan kuat dalam eksekusi. *UML* adalah aspek penting yang terlibat dalam pengembangan perangkat lunak berorientasi objek. Ini menggunakan notasi grafis untuk membuat model visual dari sistem perangkat lunak. Arsitektur *UML* didasarkan pada fasilitas meta-objek, yang mendefinisikan dasar untuk membuat bahasa pemodelan. Mereka cukup tepat untuk menghasilkan seluruh aplikasi. *UML* yang sepenuhnya dapat dieksekusi dapat digunakan untuk berbagai platform menggunakan teknologi yang berbeda dan dapat digunakan dengan semua proses sepanjang siklus pengembangan perangkat lunak. *UML* dirancang untuk memungkinkan pengguna mengembangkan bahasa pemodelan visual yang ekspresif, siap pakai. Selain itu, mendukung konsep pengembangan tingkat tinggi seperti kerangka kerja, pola, dan kolaborasi (Wasserkrug et al., 2019).

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 (Sukmawati & Priyadi, 2019).

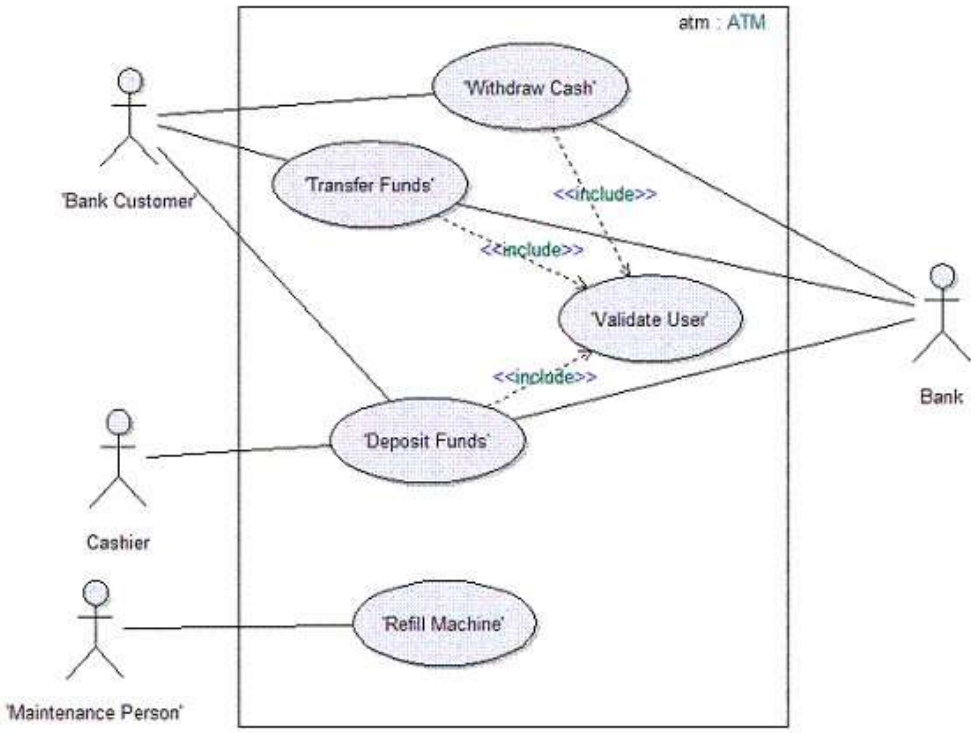
2.7.1 *Use Case Diagram*

Use Case Diagram adalah model tentang bagaimana berbagai jenis pengguna berinteraksi dengan sistem untuk memecahkan masalah. Dengan demikian, ini menggambarkan tujuan pengguna, interaksi antara pengguna dan sistem, dan perilaku sistem yang diperlukan dalam memenuhi tujuan-tujuan ini. Model use-case terdiri dari sejumlah elemen model. Elemen model yang paling penting adalah kasus penggunaan, aktor dan hubungan di antara mereka. Diagram use-case digunakan untuk menggambarkan secara grafis subset dari model untuk menyederhanakan komunikasi. Biasanya akan ada beberapa diagram kasus penggunaan yang terkait dengan model yang diberikan, masing-masing menunjukkan subset elemen model yang relevan untuk tujuan tertentu. Elemen model yang sama dapat ditampilkan pada beberapa diagram use-case, tetapi setiap instance harus konsisten. Jika alat digunakan untuk mempertahankan model use-case, kendala konsistensi ini otomatis sehingga setiap perubahan pada elemen model (mengubah nama misalnya) akan secara otomatis tercermin dalam setiap diagram use-case yang menunjukkan elemen itu (UTM, 2019).

Model use-case dapat berisi paket yang digunakan untuk menyusun model untuk menyederhanakan analisis, komunikasi, navigasi, pengembangan, pemeliharaan, dan perencanaan. Faktanya, sebagian besar model use-case adalah tekstual, dengan teks yang ditangkap dalam Spesifikasi Use-Case yang terkait dengan setiap elemen model use-case. Spesifikasi ini menjelaskan alur peristiwa use case. Model use-case berfungsi sebagai utas pemersatu sepanjang pengembangan sistem. Ini digunakan sebagai spesifikasi utama dari persyaratan

fungsional untuk sistem, sebagai dasar untuk analisis dan desain, sebagai input untuk perencanaan iterasi, sebagai dasar mendefinisikan kasus uji dan sebagai dasar untuk dokumentasi pengguna. (Kurniawan, 2018).

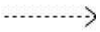
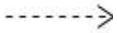
Use Case Diagram merupakan suatu diagram yang berisi *use case, actor*, serta *relationship* diantaranya. *Use Case Diagram* dapat digunakan untuk kebutuhan apa saja yang diperlukan dalam suatu sistem, sehingga sistem dapat digambarkan dengan jelas bagaimana proses dari sistem tersebut, bagaimana cara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

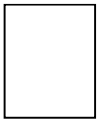


Gambar 2.4 *Use Case Diagram* ATM
Sumber: (Nurgoho, 2019)

Gambar di atas adalah contoh dari penggunaan *Use Case Diagram* pada mesin ATM. Use-case memiliki beberapa simbol untuk menyatakan kegiatan dari use-case tersebut. Adapun simbol dari *use case* adalah sebagai berikut:

Tabel 2.1 Simbol *Use Case Diagram*

No	Gambar	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.
3		*Generalization*	Hubungan dimana objek anak berbagi perilaku dan struktur data dari objek yang ada diatasnya .
4		*Include*	Menspesifikasikan bahwa *use case* sumber secara *eksplisit*.
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*	Deskripsi 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 prilaku 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: (Kurniawan, 2018)

2.7.2 *Activity Diagram*

Activity Diagram (Diagram Aktifitas) menggambarkan berbagai alir aktifitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, *decision* yang mungkin terjadi, dan bagaimana mereka berakhir (Ladjamudin, 2017).

Activity Diagram menurut adalah salah satu cara untuk memodelkan *event-event* yang terjadi dalam suatu *use case*. Diagram ini juga dapat digantikan dengan sejumlah teks.

Tabel 2.2 Simbol *Activity Diagram*

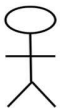
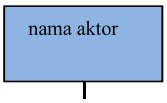
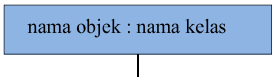
No	Gambar	Nama	Keterangan
1		*Actifity*	Memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain
2		*Action*	State dari sistem yang mencerminkan eksekusi dari suatu aksi
3		*Initial Node*	Bagaimana objek dibentuk /diawali.
4		*Actifity Final Node*	Bagaimana objek dibentuk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

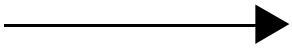
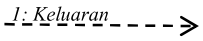
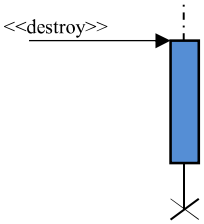
Sumber: (Kurniawan, 2018)

2.7.3 *Sequence Diagram*

Diagram sekuen menggambarkan kelakuan objek pada *use case* dengan mendeskripsikan waktu hidup objek dan *message* yang dikirimkan dan diterima antar objek. Untuk menggambarkan diagram sekuen maka harus diketahui objek-objek yang terlibat dalam sebuah *use case* beserta metode-metode yang dimiliki kelas yang diinstansiasi menjadi objek itu. Tabel berikut adalah simbol-simbol yang ada pada diagram sekuen.

Tabel 2.3 Simbol *Sequence Diagram*

Simbol-simbol	Deskripsi
Aktor  Atau 	Orang, proses atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat diluar sistem informasi itu sendiri, jadi walaupun simbol dari aktor adalah orang, tapi aktor belum tentu merupakan orang; biasanya dinyatakan menggunakan kata benda diawal *frase* nama aktor
Garis hidup / *Lifeline* 	Menyatakan kehidpan suatu objek
Objek 	Menyatakan objek yang berinteraksi

Waktu aktif 	Menyatakan objek dalam keadaan aktif dan berinteraksi, semua yang terhubung dengan waktu aktif ini adalah sebuah tahapan yang dilakukan didalamnya.
Pesan tipe *create*  <<create>>	Menyatakan suatu objek membuat objek yang lain, arah panah mengarah pada objek yang dibuat
Pesan tipe *call* 	Menyatakan suatu objek memanggil operasi / metode yang ada pada objek lain atau dirinya sendiri. Arah panah mengarah pada objek yang memiliki operasi / metode, karena ini memanggil operasi / metode maka operasi / metode yang dipanggil harus ada pada diagram kelas sesuai dengan kelas objek yang berinteraksi.
Pesan tipe *send* 	Menyatakan bahwa suatu objek mengirimkan data / masukan / informasi ke objek lainnya, arah panah mengarah pada objek yang dikirim
Pesan tipe *return* 	Menyatakan suatu objek yang telah menjalankan suatu operasi atau metode menghasilkan suatu kembalian ke objek tertentu, arah panah mengarah pada objek yang menerima kembalian
Pesan tipe *destroy* 	Menyatakan suatu objek mengakhiri hidup objek yang lain, arah panah mengarah pada objek yang diakhiri, sebaiknya jika ada create maka ada *destroy*

Sumber: (Kurniawan, 2018)

2.8 *Flowchart*

Flowchart digunakan dalam mendesain dan mendokumentasikan proses atau program sederhana. Seperti jenis diagram lainnya, diagram membantu memvisualisasikan apa yang sedang terjadi dan dengan demikian membantu memahami suatu proses, dan mungkin juga menemukan fitur-fitur yang kurang jelas dalam proses tersebut, seperti kekurangan dan hambatan. Ada berbagai jenis diagram alur: masing-masing jenis memiliki set kotak dan notasi sendiri. Dua jenis kotak yang paling umum dalam diagram alur adalah:

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

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

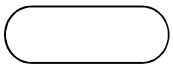
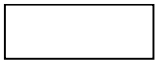
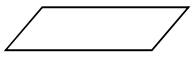
Diagram alir menggambarkan aspek-aspek tertentu dari proses dan biasanya dilengkapi dengan jenis diagram lainnya. Misalnya, Kaoru Ishikawa, mendefinisikan diagram alir sebagai salah satu dari tujuh alat dasar kendali mutu,

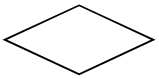
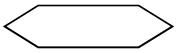
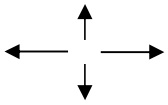
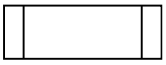
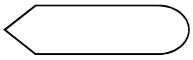
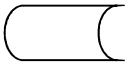
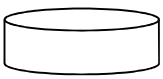
di sebelah histogram, diagram Pareto, lembar periksa, diagram kontrol, diagram sebab-akibat, dan diagram sebaran. Demikian pula, di *UML*, notasi pemodelan konsep standar yang digunakan dalam pengembangan perangkat lunak, diagram aktivitas, yang merupakan jenis diagram alur, hanyalah salah satu dari banyak jenis diagram yang berbeda.

Diagram Nassi-Shneiderman dan Drakon-chart adalah notasi alternatif untuk aliran proses. Nama alternatif umum termasuk diagram alir, diagram alur proses, diagram alur fungsional, peta proses, diagram proses, diagram proses fungsional, model proses bisnis, model proses, diagram alir proses, diagram alur kerja, diagram alir bisnis. Istilah "diagram alur" dan "diagram alir" digunakan secara bergantian (Nakatsu, 2019).

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

Tabel 2.4 Simbol *Flowchart*

NO	SIMBOL	FUNGSI
1.		**Terminal**, untuk memulai atau mengakhiri suatu program
2.		**Proses**, suatu simbol yang menunjukkan setiap pengolahan yang dilakukan.
3.		**Input-Output**, untuk memasukkan menunjukkan hasil dari suatu proses

4.		**Decision**, suatu kondisi yang akan menghasilkan beberapa kemungkinan jawaban atau pilihan
5.		**Preparation,** suatu symbol yang menyediakan tempat pengolahan
6.		**Connector**, suatu prosedur penghubung yang akan masuk atau keluar melalui symbol ini dalam lembar yang sama
7.		**Off-Page Connector**, merupakan symbol masuk atau keluarannya suatu prosedur pada lembaran kertas lainnya
8.		**Arus/Flow**, dari pada prosedur yang dapat dilakukan atas ke bawah dari bawah ke atas, ke atas dari kiri ke kanan ataupun dari kanan ke kiri
9.		**Predefined Process**, untuk menyatakan sekumpulan langkah proses yang ditulis sebagai prosedur
10.		Simbol untuk output, yang ditunjukkan ke suatu device, seperti printer, dan sebagainya
11		Penyimpanan file secara sementara
12		Menunjukkan input / Output Hardisk (media penyimpanan)

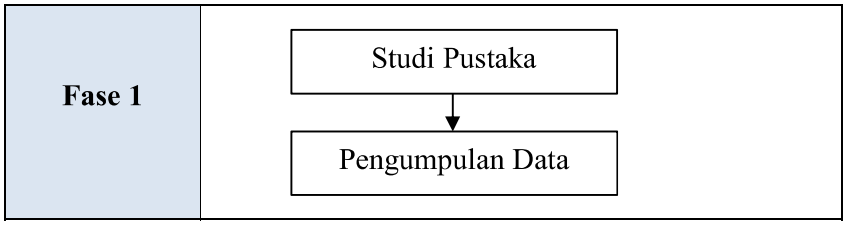
Sumber: (Kurniawan, 2018)

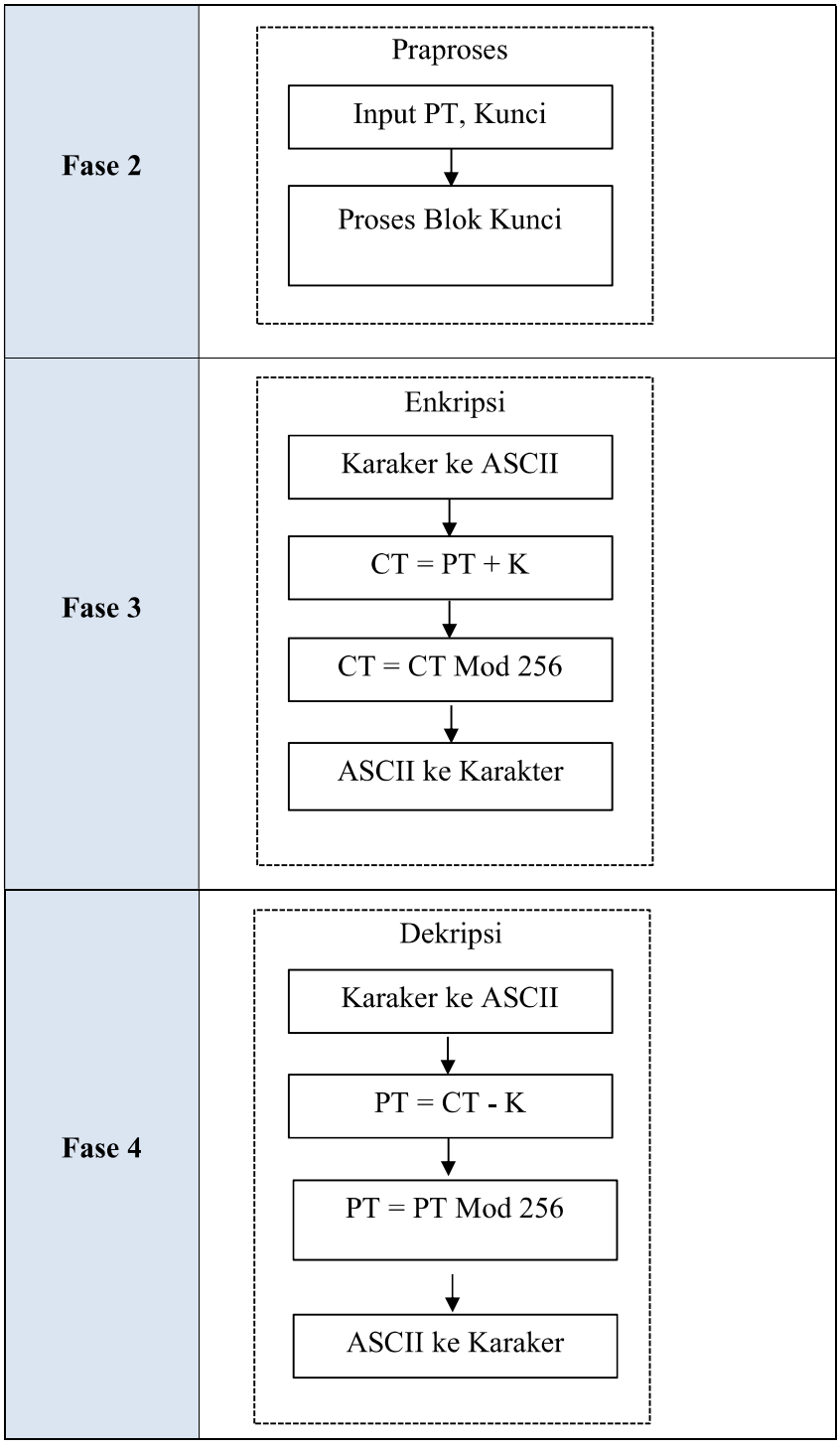
BAB III

METODE PENELITIAN

3.1 Tahapan Penelitian

Penelitian ilmiah melibatkan proses sistematis yang berfokus pada objektif dan mengumpulkan banyak informasi untuk dianalisis sehingga peneliti dapat sampai pada kesimpulan. Proses ini digunakan dalam semua proyek penelitian dan evaluasi, terlepas dari metode penelitian (metode ilmiah penyelidikan, penelitian evaluasi, atau penelitian tindakan). Proses ini berfokus pada pengujian firasat atau ide di taman dan pengaturan rekreasi melalui proses sistematis. Dalam proses ini, studi ini didokumentasikan sedemikian rupa sehingga individu lain dapat melakukan studi yang sama lagi. Ini disebut sebagai mereplikasi penelitian. Setiap penelitian yang dilakukan tanpa mendokumentasikan penelitian sehingga orang lain dapat meninjau proses dan hasilnya bukan investigasi menggunakan proses penelitian ilmiah. Gambar 3.1 mencantumkan langkah-langkah proses penelitian dan memberikan contoh setiap langkah untuk studi penelitian sampel.





Gambar 3.1 Kerangka Penelitian

Berikut adalah fase pada penelitian ini:

1. Studi Literatur

   Studi literatur dilakukan untuk mendapatkan referensi pengetahuan akan algoritma yang digunakan yaitu algoritma *Beaufort Cipher*. Pencarian materi dapat dilakukan secara langsung atau tidak langsung.

2. Analisa

   Analisa menjelaskan proses analisa permasalahan dan bagaimana permasalahan dapat diselesaikan dengan baik. Analisa akan memeriksa kebenaran dari rancangan yang akan dibuat.

3. Pembahasan

   Pembasahan menjelaskan tentang isi dari penelitian. Algoritma dan perhitungan manual akan dilakukan dalam melakukan proses enkripsi dan dekripsi terhadap *plaintext* dan *Ciphertext*.

4. Implementasi dan pengujian

   Implementasi mengacu kepada penggunaan program aplikasi sementara pengujian adalah untuk membuktikan kebenaran dari perhitungan manual yang dibandingkan dengan program aplikasi Microsoft Visual Basic.Net 2010.

3.2 Perancangan Penelitian

Perancangan penelitian adalah bagaimana suatu penelitian dimodelkan dalam suatu alur atau diagram. Banyak cara yang dapat dilakukan untuk merancang penelitian agar lebih terarah dan terstruktur. Perancangan ini

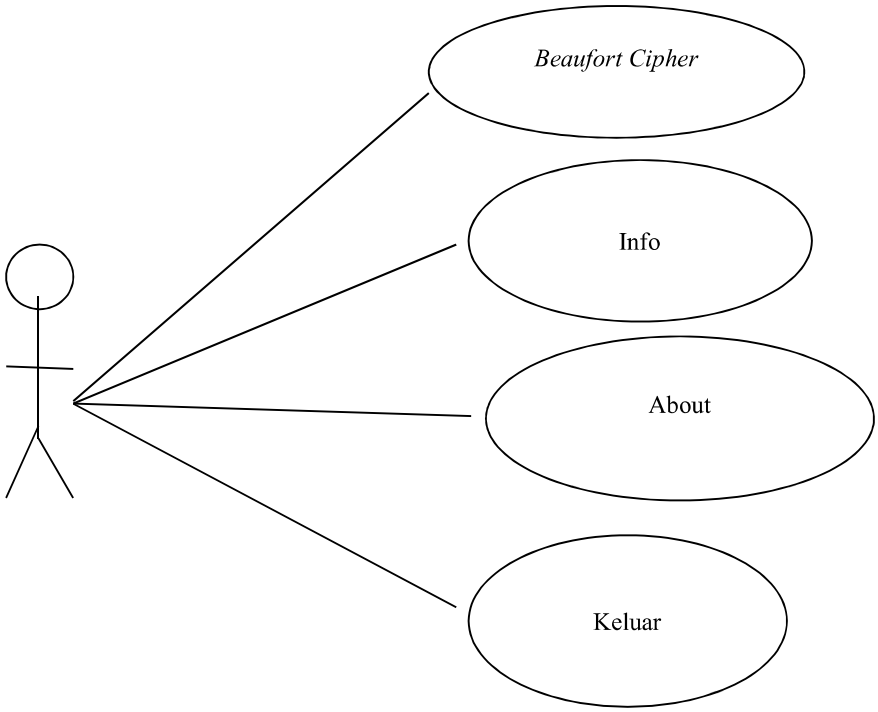
membutuhkan ketelitian yang tinggi agar tidak menyalahi aturan yang ada. Hal ini bertujuan agar program aplikasi yang telah dibuat dapat bekerja secara efisien dan efektif. Desain penelitian dapat digambarkan dengan bentuk Unified Modelling Language (*UML*). Pada *UML*, setiap arah penelitian tergambarkan dengan jelas dan terstruktur. Hal ini dapat memudahkan peneliti dalam menghasilkan output yang benar.

Perancangan penelitian yang menghasilkan batas kesalahan terkecil dalam penelitian disebut sebagai hasil perancangan yang terbaik. Perancangan penelitian berikut ini berfunsi untuk mendefinisikan setiap tahapan untuk melengkapi kegiatan kerja pengguna terhadap rancangan penelitian yang akan dilaksanakan. Metode yang digunakan dalam penelitian ini antara lain:

1. Observasi / Observasi Partisipan
2. Survei
3. Wawancara
4. Grup fokus
5. Eksperimen
6. Analisis Data Sekunder / Studi Arsip
7. Metode Campuran (kombinasi beberapa hal di atas)

3.2.1 *Use Case Diagram*

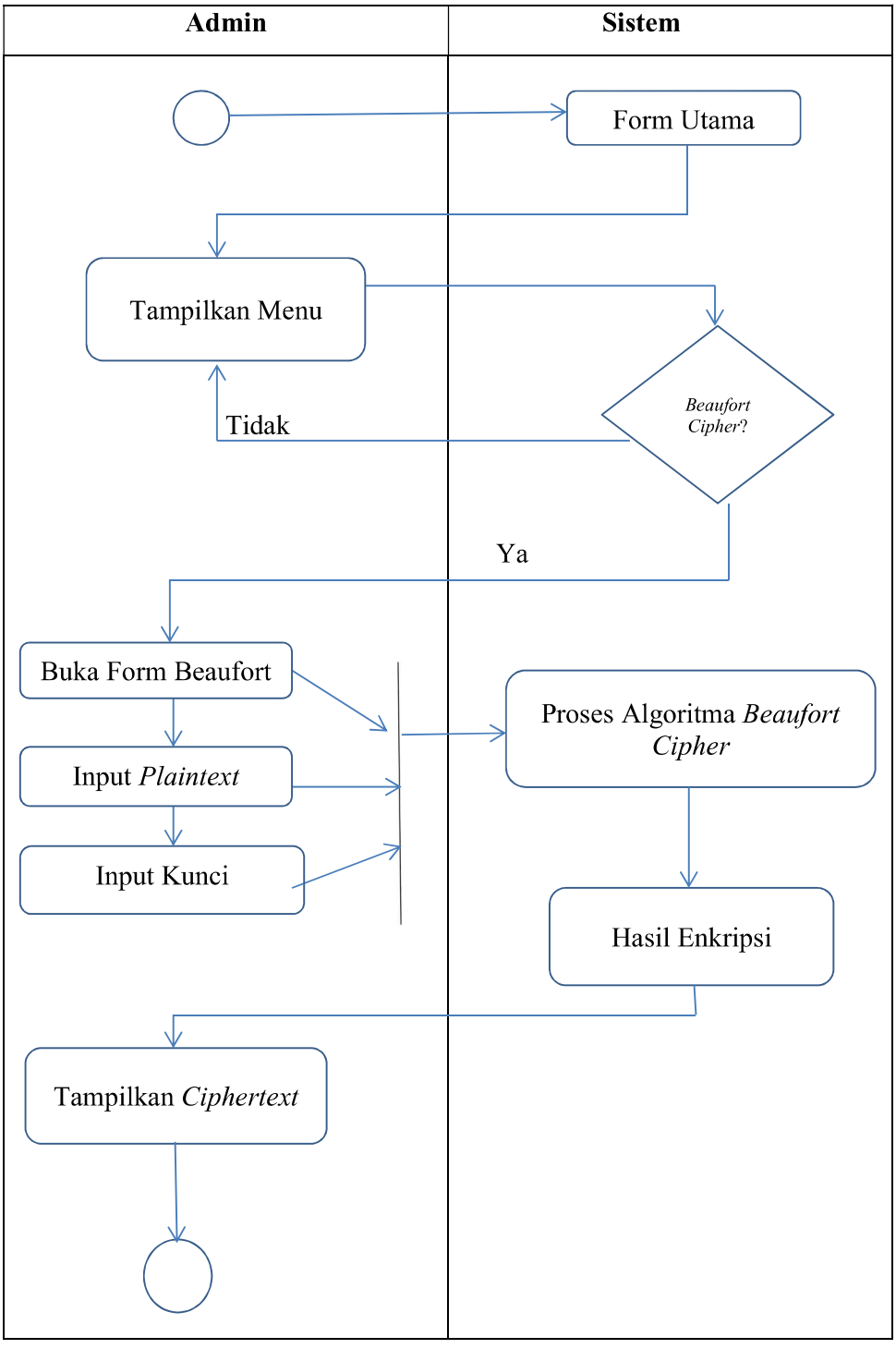
Use Case Diagram pada penelitian ini memiliki beberapa menu yang akan berfungsi untuk menjalankan bagiannya masing-masing. Gamabr 3.2 adalah perancangan *Use Case Diagram* dari algoritma *Beaufort Cipher*.



Gambar 3.2 *Use Case Diagram*

3.2.2 *Activity Diagram*

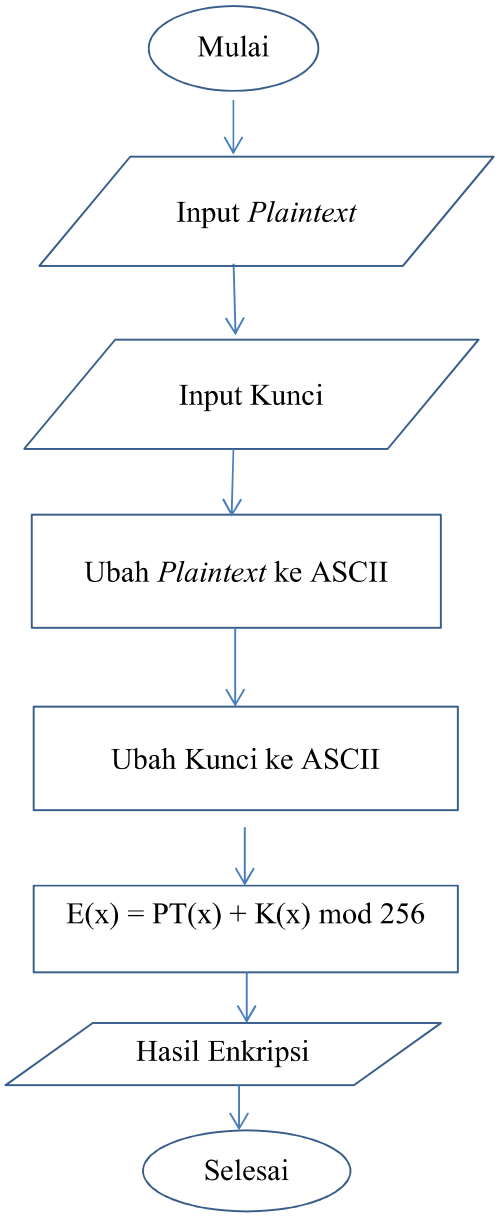
Activity Diagram menggambarkan perilaku alur kerja aktual suatu sistem dalam Teknologi Informasi. Diagram ini menggambarkan keadaan aktual dari suatu sistem dengan menunjukkan semua urutan kegiatan yang dilakukan. Juga, diagram ini dapat menunjukkan aktivitas yang kondisional atau paralel. Gambar 3.3 akan menjelaskan *Activity Diagram* tersebut.



Gambar 3.3 *Activity Diagram*

3.2.3 *Flowchart* Enkripsi

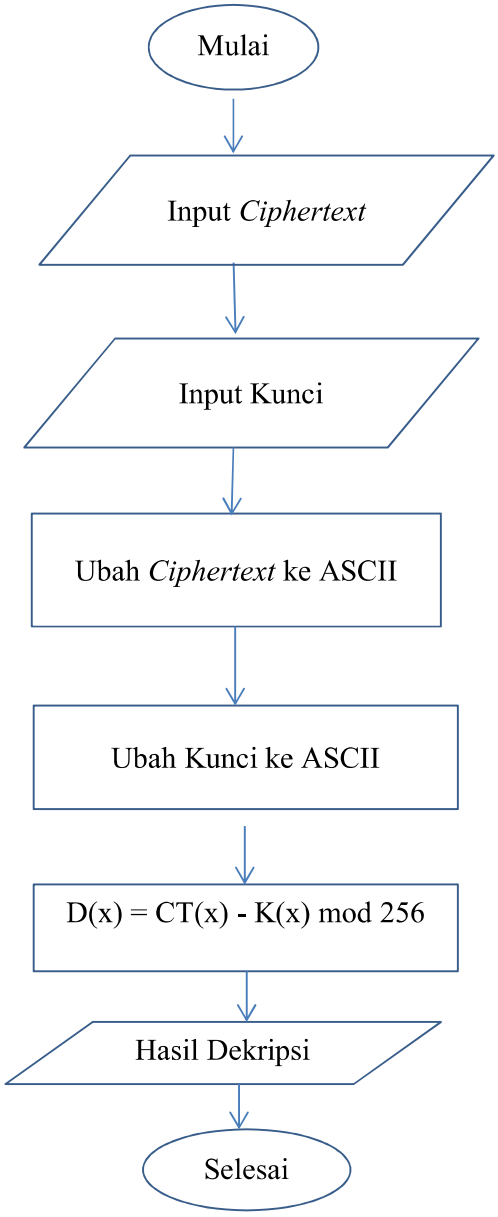
Flowchart enkripsi akan menerangkan cara kerja algoritma *Beaufort Cipher* dengan proses enkripsi. *Flowchart* enkripsi dapat dilihat pada gambar berikut ini.



Gambar 3.4 *Flowchart* enkripsi algoritma *Beaufort*

3.2.4 *Flowchart* Dekripsi

Flowchart dekripsi akan menjelaskan cara kerja algoritma *Beaufort Cipher* dengan proses dekripsi. *Flowchart* dekripsi dapat dilihat pada gambar berikut ini.



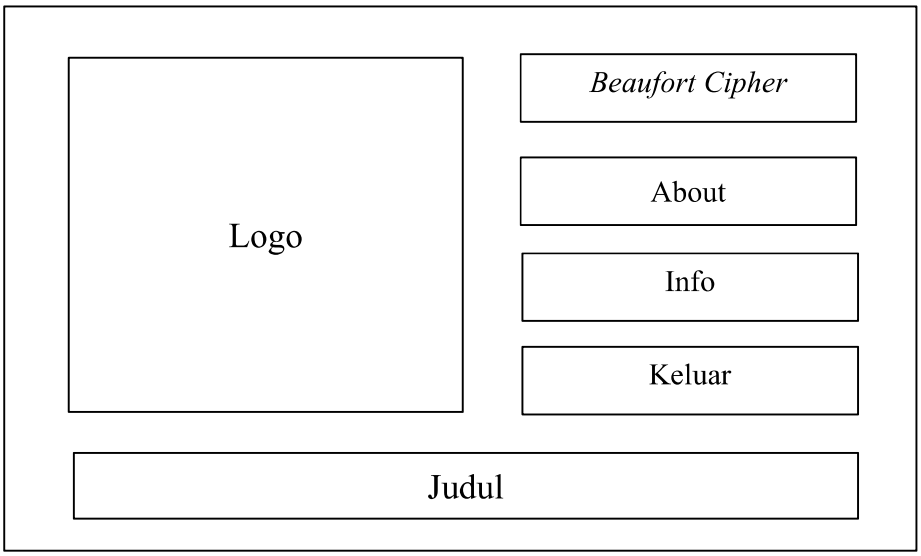
Gambar 3.5 *Flowchart* dekripsi algoritma *Beaufort*

3.3 *Interface Design*

Interface design atau desain antarmuka pengguna adalah proses membuat antarmuka dalam perangkat lunak atau perangkat yang terkomputerisasi dengan fokus pada penampilan atau gaya. Desain pada penelitian ini diciptakan agar menarik. Desain antar muka biasanya mengacu pada antarmuka pengguna grafis tetapi juga mencakup yang lain, seperti yang dikontrol suara. Berikut ini adalah bagian-bagian pada *interfece design* algoritma *Beaufort Cipher*.

3.3.1 Menu Utama

Menu utama adalah *interface* yang pertama sekali muncul pada saat progam aplikasi dijalankan. Gambar 3.6 adalah hasil perancangan menu utama yang memiliki beberapa komponen lainnya.



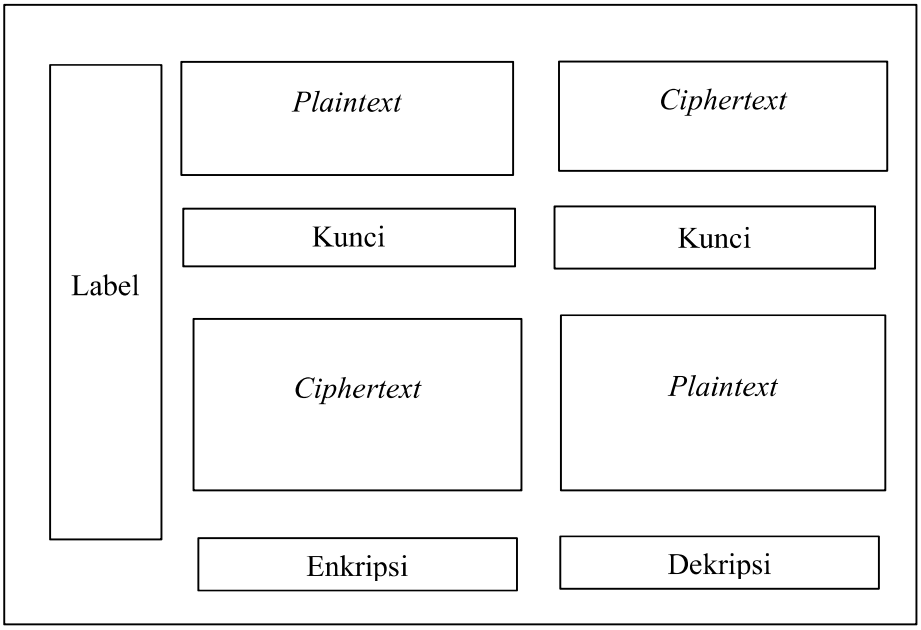
Gambar 3.6 Tampilan Menu Utama

Tampilan ini memiliki berapa sub-menu antara lain:

1. Logo
2. *Beaufort Cipher*
3. About
4. Info
5. Keluar
6. Judul

3.3.2 Menu *Beaufort Cipher*

Menu ini adalah *interface* utama yang berfungsi memproses enkripsi dan dekripsi algoritma *Beaufort Cipher*. *Inferface* ini adalah tempat untuk melakukan perhitungan kriptografi. Gambar 3.6 adalah tampilan menu ini.



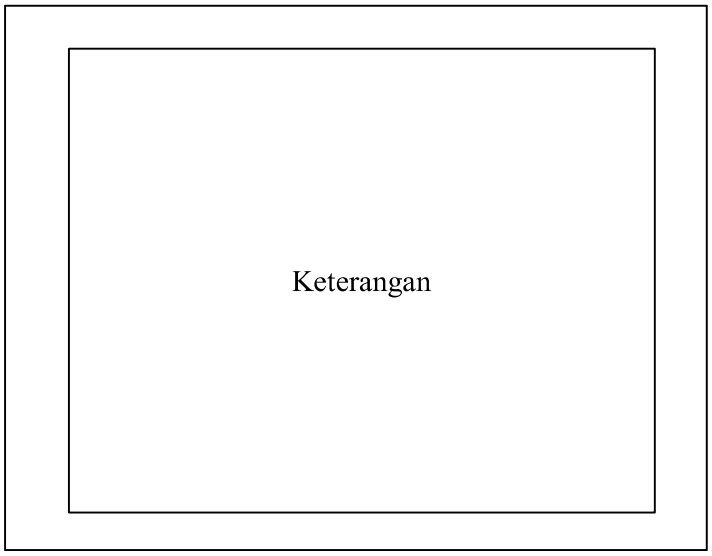
Gambar 3.7 Tampilan Menu *Beaufort Cipher*

Tampilan algoritma *Beaufort Cipher* memiliki beberapa bagian antara lain:

1. *Plaintext*
2. *Ciphertext*
3. Kunci
4. Tombol Enkripsi
5. Tombol Dekripsi

3.3.3 Menu Info

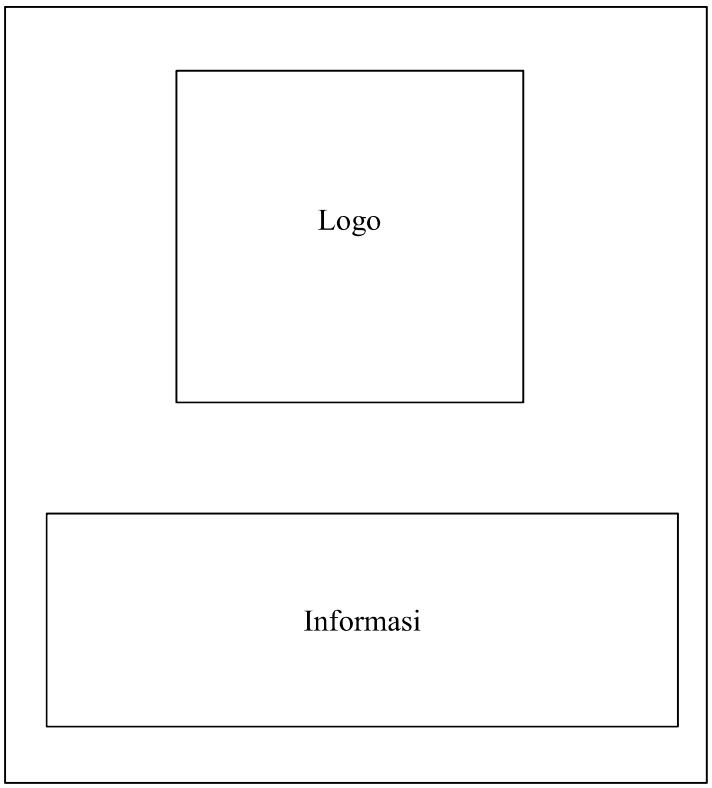
Menu ini menampilkan informasi tentang algoritma *Beaufort Cipher*. *Interface* memiliki beberapa objek. Gambar berikut ini adalah hasil perancangan menu Info.



Gambar 3.8 Tampilan Menu Info

3.3.4 Menu About

Interface pada menu about menjelaskan informasi penulis. *Interface* ini teridiri dari logo Universitas Pembangunan Panca Budi dan biodata. Gambar 3.9 adalah hasil tampilan dari menu About.



Gambar 3.9 Tampilan Menu About

BAB IV

HASIL DAN PEMBAHASAN

Bagian ini memberikan hasil perhitungan dan tampilan dari program aplikasi yang telah dibuat pada perancangan sebelumnya. Ada beberapa kebutuhan yang harus diselesaikan termasuk kebutuhan sistem dalam menjalankan program aplikasi tersebut.

4.1 Kebutuhan Sistem

Kebutuhan sistem merupakan hal yang paling penting dalam mendukung persiapan pelaksanaan program aplikasi. Kebutuhan ini meliputi kebutuah perangkat keras dan kebutuhan perangkat lunak.

4.1.1 Kebutuhan Perangkat Keras

Kebutuhan perangkat keras sangat diperlukan dalam memberikan tempat bagi program aplikasi untuk dijalankan. Perangkat keras merupakan perangkat utama yang penting. Tabel 4.1 menjelaskan spesifikasi perangkat keras.

Tabel 4.1 Spesifikasi perangkat keras

No.	Komponen	Spesifikasi
1	Processor	Intel Core i5 2.4 GHz
2	RAM	8192 MB
3	Storage	500 GB
4	Display	14 inch

4.1.2 Kebutuhan Perangkat Lunak

Kebutuhan perangkat lunak diperlukan untuk meneruskan sistem agar dapat dijalankan dengan baik. Tabel 4.2 adalah spsesifikasi perangkat lunak yang digunakan pada penelitian ini.

Tabel 4.2 Spesifikasi perangkat lunak

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

4.2 Hasil *Interface*

Hasil *interface* merupakan hasil keluaran dari kode program yang dihasilkan pada bahasa pemrograman. Hasil ini merupakan tampilan dari program aplikasi yang telah dirancang. Hasil ini berfungsi sebagai alat komunikasi antara pengguna dan sistem.

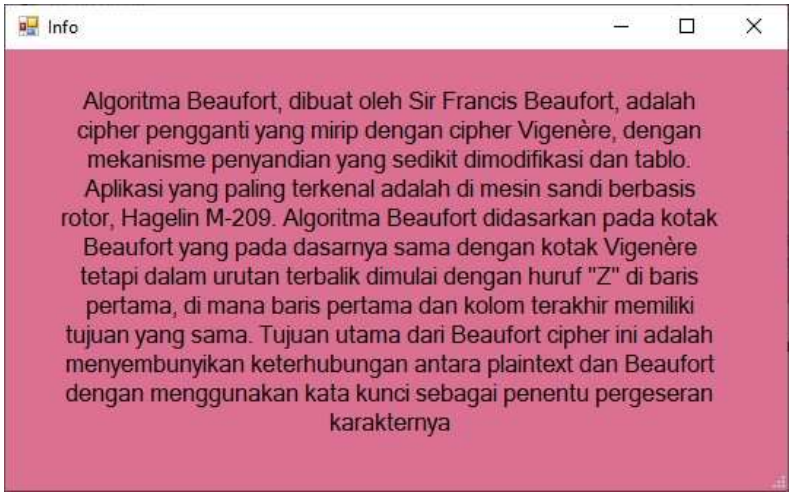
4.2.1 Halaman Menu Utama

Halaman menu utama adalah halaman pembuka program aplikasi yang akan berinteraksi langsung dengan pengguna program aplikasi. Halaman ini memiliki beberapa tombol untuk terhubung ke menu-menu lainnya. Halaman ini memiliki empat buah tombol navigasi yang mengarahkan ke bagian yang lain. Gambar 4.1 adalah hasil tampilan menu utama.

Gambar 4.1 Halaman Menu Utama

4.2.2 Halaman Info

Halaman info adalah menu yang menampilkan seputar informasi tentang algoritma *Beaufort Cipher*. Gambar 4.2 adalah hasil tampilan dari halaman info.



Gambar 4.2 Halaman Info

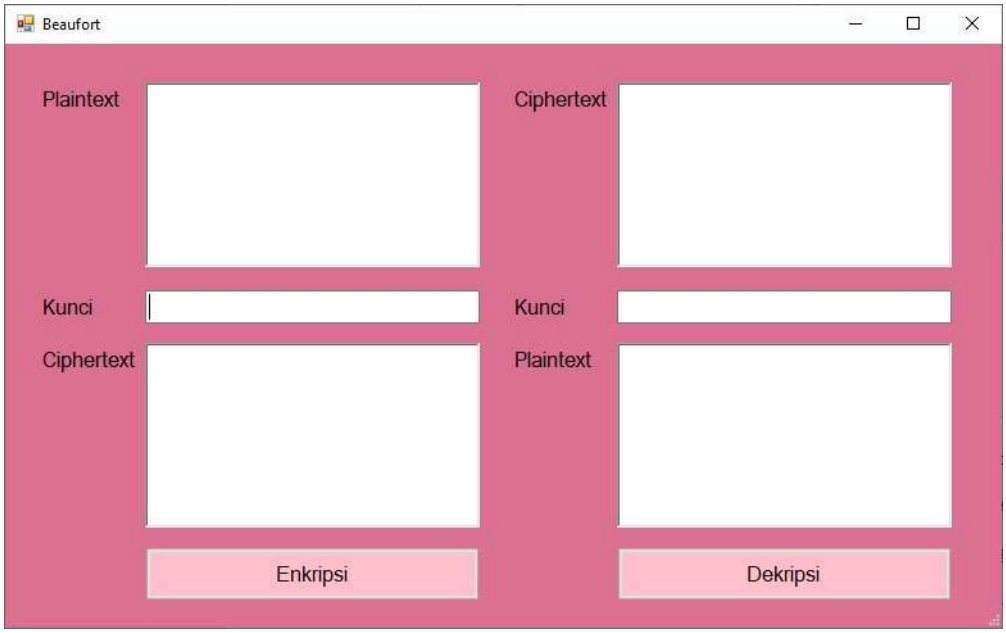
4.2.3 Halaman About

Halaman about menampilkan informasi penulis sebagai pemilik dari tugas akhir ini. Menu about memiliki sebuah objek label dan *picturebox*. Halaman about menunjukkan sebuah logo universitas yaitu logo Universitas Pembangunan Panca Budi dan keterangan lainnya. Gambar 4.3 adalah tampilan dari halaman about.

Gambar 4.3 Halaman About

4.2.4 Halaman *Beaufort Cipher*

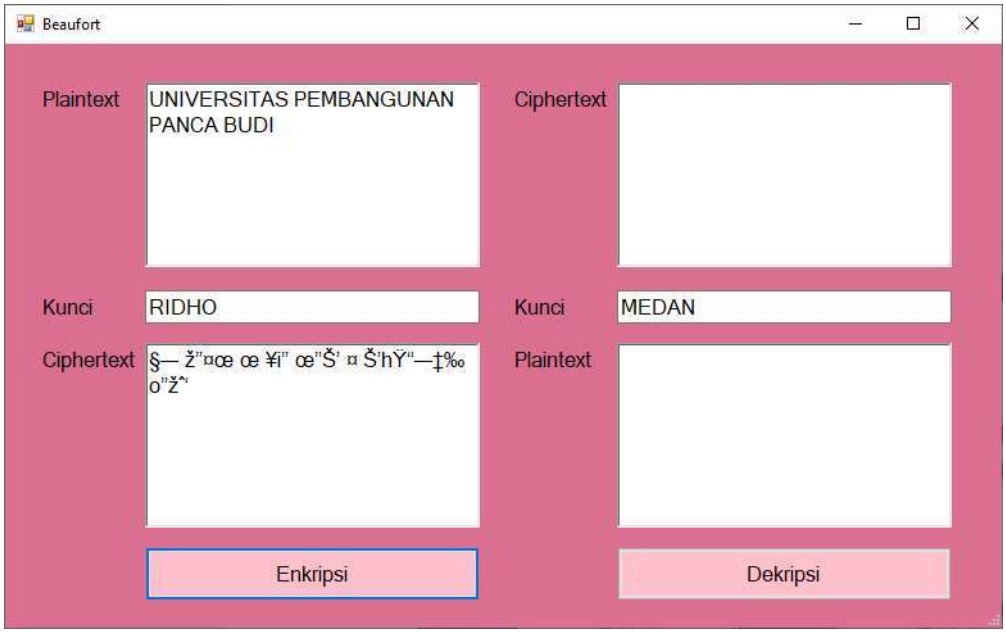
Halaman *Beufort Cipher* adalah halaman untuk melakukan proses enkripsi dan dekripsi dari algoritma ini. Gambar 4.4 adalah hasil tampilan dari halaman *Beaufort Cipher*.



Gambar 4.4 Halaman *Beaufort Cipher*

4.2.5 Proses Enkripsi

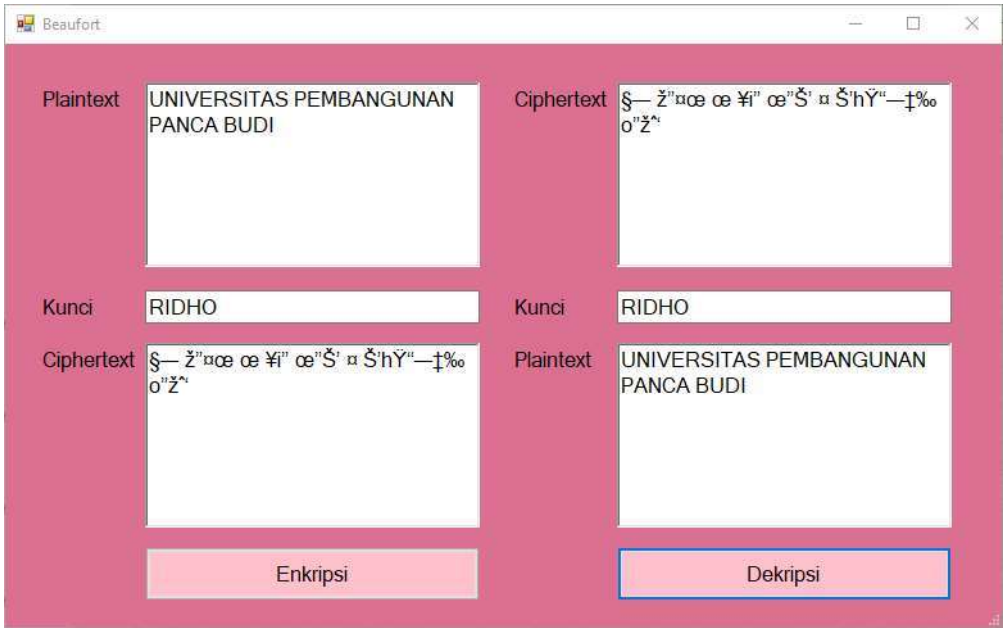
Proses enkripsi melakukan penyandian teks sehinga mengubah *plaintext* menjadi *ciphertext*. Proses ini memerlukan beberapa parameter input yang akan diproses ketika tombol Enkripsi ditekan. Gambar 4.5 adalah tampilan dari hasil perhitungan proses enkripsi algoritma *Beaufort Cipher*.



Gambar 4.5 Hasil Enkripsi *Beaufort Cipher*

4.2.6 Proses Dekripsi

Proses dekripsi melakukan pengembalian teks dari *ciphertext* menjadi *plaintext* kembali. Proses ini juga memerlukan beberapa parameter input yang akan diproses ketika tombol Dekripsi ditekan. Gambar 4.6 adalah tampilan dari hasil perhitungan proses dekripsi algoritma *Beaufort Cipher*.



Gambar 4.6 Hasil Dekripsi *Beaufort Cipher*

4.3 Pengujian Manual

Perhitungan berikut ini merupakan hasil proses enkripsi dan dekripsi dari algoritma *Beaufort Cipher* dengan beberapa parameter.

Parameter Input

Plaintext = UNIVERSITAS PEMBANGUNAN PANCA BUDI

Kunci = RIDHO

Hasil enkripsi dan dekripsi dapat dilihat pada perhitungan yang dijelaskan pada tabel 4.3 dan tabel 4.4.

Hasil Enkripsi

Tabel 4.3 Hasil enkripsi pengujian manual

PT	PT ASCII	KUNCI	KUNCI ASCII	CT ASCII	CT
U	85	R	82	167	§
N	78	I	73	151	—
I	73	D	68	141	
V	86	H	72	158	ž
E	69	O	79	148	”
R	82	R	82	164	¤
S	83	I	73	156	œ
I	73	D	68	141	
T	84	H	72	156	œ
A	65	O	79	144	
S	83	R	82	165	¥
	32	I	73	105	i
P	80	D	68	148	”
E	69	H	72	141	
M	77	O	79	156	œ
B	66	R	82	148	”
A	65	I	73	138	Š
N	78	D	68	146	’
G	71	H	72	143	
U	85	O	79	164	¤
N	78	R	82	160	
A	65	I	73	138	Š
N	78	D	68	146	’
	32	H	72	104	h
P	80	O	79	159	Ÿ
A	65	R	82	147	“
N	78	I	73	151	—
C	67	D	68	135	‡
A	65	H	72	137	‰
	32	O	79	111	o
B	66	R	82	148	”
U	85	I	73	158	ž

D	68	D	68	136	ˆ
I	73	H	72	145	‘

Hasil Dekripsi

Tabel 4.4 Hasil dekripsi pengujian manual

CT	CT ASCII	KUNCI	KUNCI ASCII	PT ASCII	PT
§	167	R	82	85	U
—	151	I	73	78	N
	141	D	68	73	I
ž	158	H	72	86	V
”	148	O	79	69	E
¤	164	R	82	82	R
œ	156	I	73	83	S
	141	D	68	73	I
œ	156	H	72	84	T
	144	O	79	65	A
¥	165	R	82	83	S
i	105	I	73	32	
”	148	D	68	80	P
	141	H	72	69	E
œ	156	O	79	77	M
”	148	R	82	66	B
Š	138	I	73	65	A
’	146	D	68	78	N
	143	H	72	71	G
¤	164	O	79	85	U
	160	R	82	78	N
Š	138	I	73	65	A
’	146	D	68	78	N
h	104	H	72	32	
Ÿ	159	O	79	80	P
“	147	R	82	65	A
—	151	I	73	78	N
‡	135	D	68	67	C

‰	137	H	72	65	A
o	111	O	79	32	
”	148	R	82	66	B
ž	158	I	73	85	U
ˆ	136	D	68	68	D
‘	145	H	72	73	I

BAB V

PENUTUP

5.1 Kesimpulan

Penulis dapat menarik beberapa kesimpulan berdasarkan hasil *running* program aplikasi. Adapun kesimpulan yang diperoleh adalah antara lain:

1. *Beaufort Cipher* bekerja dengan dengan cara melakukan pergeseran pada karakter.
2. *Beaufort Cipher* memiliki kunci yang dapat ditentukan sesuai dengan jumlah kunci yang diinginkan..
3. *M*odulo 256 digunakan untuk mejaga agar karakter hasil enkripsi dan dekripsi tidak berada diluar karakter pada tabel ASCII.

5.2 Saran

Penelitian juga meiliki kekurangan dalam melaksanakan penelitian ini. Ada beberapa saran yang dapat penulis kemukakan untuk meningkatkan kualitas penelitian ini. Adapun saran tersebut adalah antara lain:

1. Sebaiknya algoritma *Beaufort Cipher* dapat digunakan secara online.
2. *Beaufort Cipher* akan lebih jika dapat digunakan melalui jaringan internet atau berbasis *web.*
3. Hendaknya jumlah karakter yang dapat diproses lebih dari 100 karakter.

DAFTAR PUSTAKA

Ayushi, M. (2010). A Symmetric Key Cryptographic Algorithm. International Journal of Computer Applications, 1(15), 1–6. https://doi.org/10.5120/331-502

Barone, L., Williams, J., & Micklos, D. (2017). Unmet needs for analyzing biological big data: A survey of 704 NSF principal investigators. PLOS Computational Biology, 13(10), e1005755.https://doi.org/10.1371/journal.pcbi.1005755

Batubara, S., Hariyanto, E., Wahyuni, S., Sulistianingsih, I., & Mayasari, N. (2019, August). Application of Mamdani and Sugeno Fuzzy Toward Ready-Mix Concrete Quality Control. In Journal of Physics: Conference Series (Vol. 1255, No. 1, p. 012061). IOP Publishing.

Gurevich, Y. (2012). What Is an Algorithm? (pp. 31–42). https://doi.org/10.1007/978-3-642-27660-6_3

Indrawan, M. I., Alamsyah, B., Fatmawati, I., Indira, S. S., Nita, S., Siregar, M., ... & Tarigan, A. S. P. (2019, March). UNPAB Lecturer Assessment and Performance Model based on Indonesia Science and Technology Index. In Journal of Physics: Conference Series (Vol. 1175, No. 1, p. 012268). IOP Publishing.

Kurniawan, T. A. (2018). Pemodelan Use Case (UML): Evaluasi Terhadap beberapa Kesalahan dalam Praktik. Jurnal Teknologi Informasi Dan Ilmu Komputer, 5(1), 77. https://doi.org/10.25126/jtiik.201851610

Kurnia, D. (2020). Sistem Monitoring Login Failure Dengan Via Telegram Dari Serangan Brutus Pada Router Mikrotik. Majalah Ilmiah UPI YPTK, 97-101.

Ladjamudin, A.-B. bin. (2017). Analisis dan Desain Sistem Informasi. Graha Ilmu.

Nakatsu, R. T. (2019). Reasoning with Diagrams : Decision-Making and Problem-Solving with Diagrams. John Wiley & Sons.

Nurgoho, A. (2019). Rekayasa Perangkat Lunak Menggunakan UML dan JAVA. Andi Offset.

Pratama, G. M., & Tamatjita, E. N. (2015). Modifikasi Algoritma Vigenere Cipher Menggunakan Metode Catalan Number Dan Double Columnar TranspositioN. Compiler, 4(1), 31–40.

Rao, R. V., & Selvamani, K. (2015). Data Security Challenges and Its Solutions in Cloud Computing. Procedia Computer Science, 48, 204–209. https://doi.org/10.1016/j.procs.2015.04.171

Sari, R. M., & Tasril, V. (2020). Prediksi Jumlah APBD Kota Payakumbuh dengan metode K-Means. Jurnal Ipteks Terapan, 14(1), 45-50.

S., G., L. Ribeiro, A. R., & David, E. (2012). Asymmetric Encryption in Wireless Sensor Networks. In Wireless Sensor Networks - Technology and Protocols. InTech. https://doi.org/10.5772/48464

Sinkov, A., Feil, T., & Mathematical Association of America. (2009). Elementary cryptanalysis : a mathematical approach. Mathematical Association of America.

Sukmawati, R., & Priyadi, Y. (2019). Perancangan Proses Bisnis Menggunakan UML Berdasarkan Fit/Gap Analysis Pada Modul Inventory Odoo. INTENSIF: Jurnal Ilmiah Penelitian Dan Penerapan Teknologi Sistem Informasi, 3(2), 104. https://doi.org/10.29407/intensif.v3i2.12697 Sun, Y., Zhang, J., Xiong, Y., & Zhu, G. (2014). Data Security and Privacy in Cloud Computing. International Journal of Distributed Sensor Networks, 10(7), 190903. https://doi.org/10.1155/2014/190903

Technopedia. (2019). Unified Modeling Language (UML). Technopedia. https://www.techopedia.com/definition/3243/unified-modeling-language uml UTM. (2019). Concept: Use-Case Model. Univesidad Technologica de La Mixteca.http://www.utm.mx/~caff/doc/OpenUPWeb/ openup/guidances/concepts/use_ case_model_CD178AF9.html

Wasserkrug, S., Dalvi, N., Munson, E. V., Gogolla, M., Sirangelo, C., Fischer-Hübner, S., Ives, Z., Velegrakis, Y., Bevan, N., Jensen, C. S., & Snodgrass, R. T. (2019). Unified Modeling Language. In Encyclopedia of Database Systems (pp. 3232–3239). Springer US. https://doi.org/10.1007/978-0-387-39940-9_440