KOMBINASI ALGORITMA BEAUFORT DENGAN ROT13 DALAM PENGAMANAN INFORMASI

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	:	**SUGANDA RANDIKA**
NPM	:	**1514370106**
PROGRAM STUDI	:	**SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

LEMBAR PENGESAHAN

KOMBINASI ALGORITMA BEAUFORT DENGAN ROT13 DALAM PENGAMANAN INFORMASI

Disusun Oleh:

NAMA	:	**SUGANDA RANDIKA**
NPM	:	**1514370106**
PROGRAM STUDI	:	**SISTEM KOMPUTER**

Skripsi Telah Disetujui oleh Dosen Pembimbing Skripsi
Pada Tanggal :

Dosen Pembimbing I	Dosen Pembimbing II
A. P. U. Siahaan, S.Kom., M.Kom.	Nadya Andhika Putri, S.Kom., M.Kom.

Mengetahui:

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

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama	: Suganda Randika
Npm	: 1514370106
Prodi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer
Judul/Skripsi	: Kombinasi Algoritma Beaufort dengan Rot13 dalam Pengamanan Informasi

Dengan ini menyatakan bahwa :

1. Tugas akhir /Skripsi saya bukan hasil plagiat.
2. Saya tidak akan menuntut perbaikan nilai indeks prestasi kumulatif (IPK) setelah meja hijau.
3. Skripsi saya dapat dipublikasikan oleh pihak lembaga, dan saya tidak akan menuntut akibat publikasi tersebut.

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

Medan, 21 Januari 2020

Yang membuat penyataan

Suganda Randika
1514370106

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

KARTU BEBAS PRAKTIKUM

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

Nama	:	SUGANDA RANDIKA
N.P.M.	:	1514370106
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, 11 Desember 2019
Ka. Laboratorium

Fachrid Wadly, S. Kom

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

iversitas : Universitas Pembangunan Panca Budi
kultas : SAINS & TEKNOLOGI
sen Pembimbing I : Andysah putera utama siahaan, S.kom, M.kom
sen Pembimbing II : Nadya Anshika putri, S.kom, M.kom
ma Mahasiswa : SUGANDA RANDIKA
usan/Program Studi : Sistem Komputer
mor Pokok Mahasiswa : 1514370106
jang Pendidikan : .....
dul Tugas Akhir/Skripsi : Kombinasi algoritma beaufort dengan ROT13 dalam pengamanan informasi

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
6-8-19	Acc Sempro.		
6-10-19	perbaiki Bab I dan II, Lanjut Bab III		
1-10-19	Acc Bab I. Acc Bab II, Perbaiki Bab III, Lanjut Bab IV		
8-10-19	Acc Bab III, Acc Bab IV Perbaiki Kesimpulan !		
10-19	Program perbaiki enkripsi simbol dan tanda baca.		
14-19	Acc Bab I-V, lengkapi lampiran.		
11-19	Acc Seminar Hasil		
11-19	Acc Sidang		
01-20	Acc Jilid		

Medan, 05 Agustus 2019
Diketahui/Disetujui oleh :
Dekan,

Hamdani, S.T., M.T

oret 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

niversitas : Universitas Pembangunan Panca Budi
akultas : SAINS & TEKNOLOGI
osen Pembimbing I : Andysah putera utama siahaan, S.kom, M.kom
osen Pembimbing II : Nadya Andhika putri, S.kom, M.kom
ama Mahasiswa : SUGANDA RANDIKA
rusan/Program Studi : Sistem Komputer
omor Pokok Mahasiswa : 1514370106
njang Pendidikan :
dul Tugas Akhir/Skripsi : Kombinasi algoritma beaufort dengan ROT13 dalam pengamanan informasi

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
5/8 2019	Acc Seminar Judul		
10/10	Revisi Bab I		
16/10	Revisi Bab II		
25/10	Revisi Bab III		
1/11	Revisi Bab III, IV		
9/11	Revisi Bab IV, V		
27/11	Acc Seminar Hasil		
3/1	Acc Sidang		
	Acc Jilid		

Medan, 05 Agustus 2019
Diketahui/Disetujui oleh :
Dekan,

Hamdani, S.T., M.T

et yang tidak perlu

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	: SUGANDA RANDIKA
Tempat/Tgl. Lahir	: medan / 10 Juni 1996
Nomor Pokok Mahasiswa	: 1514370106
Program Studi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer
Jumlah Kredit yang telah dicapai	: 143 SKS, IPK 3.48
Nomor Hp	: 082161093460
Dengan ini mengajukan judul sesuai bidang ilmu sebagai berikut	:

No.	Judul
1.	Kombinasi Algoritma Beaufort dengan ROT13 dalam Pengamanan Informasi

Catatan : Diisi Oleh Dosen Jika Ada Perubahan Judul

*Coret Yang Tidak Perlu

Rektor I,

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

Medan, 30 Juli 2019

Pemohon,

(Suganda Randika)

Tanggal : .....

Disahkan oleh :

Dekan

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

Tanggal : .....

Disetujui oleh :

Dosen Pembimbing I :

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

Tanggal : .....

Disetujui oleh:

Ka. Prodi Sistem Komputer

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

Tanggal : .....

Disetujui oleh:

Dosen Pembimbing II:

(Nadya Andhika Putri, S.Kom., M.Kom)

Plagiarism Detector v. 1456 - Originality Report

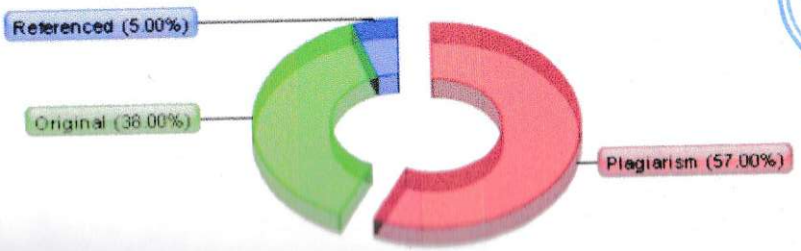
Analyzed document: 11/26/19 08:02:44

"SUGANDA RANDIKA_1514370106_SISTEM KOMPUTER.docx"

Check Type: Internet - via Google and Bing

Licensed to: **Universitas Pembangunan Panca Budi_License3**

Relation chart:



Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

Top sources of plagiarism:

% 35	wrds: 647	http://docplayer.info/31314300-Implementasi-kriptografi-pengamanan-data-pada-pes...
% 27	wrds: 534	http://informatika.stei.itb.ac.id/~rinaldi.munir/Buku/Kriptografi/Bab-1_Penganta...
% 26	wrds: 488	https://fmipa.unmul.ac.id/files/docs/20-31%20Jurnal%20Fresly.pdf

Telah Diperiksa oleh LPMU
dengan Plagiarisme 57 %
Medan, 17 Desember 2019
A/n Ka. LPMU
Husni M. Rifonga, BA, MSc
Cahyo Pramono, SE,MM

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau

Medan, 11 Desember 2019
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

Telah di terima
berkas persyaratan
dapat di proses
Medan, 11/12/19
An Ka. BPAA
TEGUH WAHYONO, SE., MM

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	: SUGANDA RANDIKA
Tempat/Tgl. Lahir	: Medan / 10 Juni 1996
Nama Orang Tua	: IMAM SUHADI
N. P. M	: 1514370106
Fakultas	: SAINS & TEKNOLOGI
Program Studi	: Sistem Komputer
No. HP	: 082161093460
Alamat	: Jl Perkutut

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **Kombinasi Algoritma Beaufort dengan ROT13 dalam Pengamanan Informasi**, 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.	~~600,000~~ 100.000,-	
2. [170] Administrasi Wisuda	: Rp.	1,500,000	
3. [202] Bebas Pustaka	: Rp.	100,000	
4. [221] Bebas LAB	: Rp.	5,000	
Total Biaya	: Rp.	~~2,205,000~~ 1.705.000,-	11/12-19

Periode Wisuda Ke : **64**

Ukuran Toga : **M**

Diketahui/Disetujui oleh :

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

Hormat saya

SUGANDA RANDIKA
1514370106

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.

Ka. UKM UNPAB
11/12-19
Roro Ajian Agustin, S.Sos., MSP

TANDA BEBAS PUSTAKA
No. 1312 / PERP / BP / 2019
Dinyatakan tidak ada sangkut
paut dengan UPT. Perpustakaan
Medan, 11 DEC 2019
Ka. UPT. Perpustakaan
Khairidah, S.I.P

ABSTRAK

SUGANDA RANDIKA
Kombinasi Algoritma Beaufort dengan ROT13 dalam pengamanan Informasi
2019

Keamanan informasi merupakan hal yang paling penting dilakukan dalam melindungi kebocoran dan pencurian data. Data merupakan hal yang paling vital untuk dilindungi agar tidak terjadi penyelewengan atau modifikasi bahkan pencurian yang akan merugikan pemiliknya. Untuk melindungi data tersebut, algoritma kriptografi sangat berperan penting dalam membantu proses pengamanan data. Hal ini melibatkan proses enkripsi dan dekripsi. Algoritma Beaufort adalah salah satu algoritma kriptografi klasik yang berguna untuk mengamankan informasi sehingga informasi tersebut tidak dapat terbaca secara umum. Untuk meningkatkan kekuatan algoritma Beaufort, algoritma ini dapat dikombinasikan dengan algoritma lain. Pada penelitian ini kombinasi algoritma Beaufort dan ROT13 merupakan pilihan yang baik. Algoritma Beaufort akan menggeser plaintext sebesar kunci yang digunakan. Peranan ROT13 akan menggeser kembali plaintext tersebut dengan 13. Hasil dari kombinasi kedua algoritma ini akan menghasilkan ciphertext. Kekuatan dari algoritma Beaufort akan bertambah dengan kehadiran algoritma ROT13.

Kata Kunci: Beaufort, dekripsi, enkripsi, kriptografi, ROT13.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di dalam suatu keamanan berupa pesan teks banyak terjadi kesalahan pada saat pengiriman pesan terkadang banyak juga yang memunculkan masalah saat ketika pengiriman, terkadang pesan yang telah dikirimkan tidak lagi berupa bentuk asli seperti yang sebelumnya pengirim kirimkan ke penerima. Sebab itu dikarenakan adanya pihak ketiga yang mencoba membobol atau mengubah pesan teks yang asli tersebut. Oleh karena itu muncul ilmu yang mempelajari tentang bagaimana cara untuk menjaga pesan atau data agar tetap aman saat dikirimkan ke penerima tanpa mengalami gangguan dari pihak ketiga yang biasa disebut dengan kriptografi.

Kriptografi berfungsi untuk menjaga keamanan informasi seperti data rahasia, integritas data, dan autentikasi sebuah data meskipun pihak ketiga dapat membaca dan melihat isi pesan tersebut akan tetapi ia akan sulit untuk dapat memahami isi pesan tersebut.

Pada dasarnya kriptografi pesan yang digunakan hanyalah bersifat umum, Kriptografi melingkupi proses transformasi informasi yang berlangsung dua arah yang terdiri dari proses enkripsi dan dekripsi yang dimana data asli hanya bisa diketahui oleh pengirim dan penerima dengan menggunakan kunci rahasia. Namun ada beberapa hal yang harus di tingkatkan dalam pengamanan ini yaitu pentingnya mendistribusikan kunci yang digunakan dalam keadaan aman. Sebuah cara pun

ditemukan untuk mengatasi sebuah keamanan yang dirancang oleh sebuah algoritma yang dikembangkan dari salah satu algoritma klasik yaitu algoritma *beaufort* yang akan dikombinasikan dengan ROT13, *beaufort* sendiri merupakan salah satu teknik enkripsi substitusi yang berfungsi untuk menyamarkan pesan teks tertentu dengan menggunakan tabel abjad dan keyword yang telah ditetapkan. Sedangkan ROT13 itu merupakan algoritma yang memiliki perubahan jumlah geseran dan arah geseran, dengan demikian dalam suatu proses kombinasi ini akan dibutuhkan sebuah computer atau laptop yang merupakan sebuah alat yang canggih sehingga penulis dapat membuat sebuah media keamanan pesan teks atau informasi menggunakan *software* pemrograman Visual Basic 2010.

Sehubungan dengan uraian diatas, maka diangkatlah judul skripsi sebagai berikut "**Kombinasi Algoritma Beaufort dengan ROT13 dalam pengamanan Informasi***".* Dimana akan dibuat sebuah media aplikasi yang bertujuan sebagai keamanan pada sebuah pesan teks atau informasi.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas maka rumusan masalah yang akan dibahas dalam skripsi ini adalah sebagai berikut:

1. Ada beberapa hal yang menghambat proses pengiriman data yang telah disepakati?.
2. Bagaimana membuat enkripsi dan dekripsi informasi dengan cara mengkombinasikan algoritma *beaufort* dengan ROT13?.

1.3 Batasan Masalah

Karena keterbatasan dan waktu maka penulis akan membatasi pokok permasalahan yang akan dibahas sebagai berikut:

1. Media aplikasi keamanan pesan teks ini dibuat dengan menggunakan *visual basic* versi 2010.
2. Algoritma yang digunakan pada keamanan pesan teks ini yaitu *beaufort* dan ROT13 untuk pengamanan informasi.
3. Modulo yang digunakan adalah 256.

1.4 Tujuan Penulisan

Adapun tujuan dari penulisan ini ialah sebagai berikut:

1. Untuk mengetahui enkripsi dan dekripsi pesan teks dengan menggunakan algoritma *beaufort* dengan ROT13.
2. Untuk mengetahui fungsi dari kriptografi dalam mengamankan pesan teks dari pihak yang tidak berkepentingan.

1.5 Manfaat Penulisan

Adapun manfaat dari penulisan ini ialah sebagai berikut:

1. Memberikan keamanan dan kenyamanan pada saat melakukan pengiriman informasi.
2. Menghasilkan kombinasi algoritma yang baru dalam melakukan proses kriptografi.

BAB II

LANDASAN TEORI

2.1 Algoritma

Ditinjau dari asal usul katanya, kata algoritma sendiri mempunyai sejarah yang aneh. Orang hanya menemukan kata algorism yang berarti proses menghitung dengan angka arab. Para ahli bahasa berusaha menemukan asal kata ini namun hasilnya kurang memuaskan. Akhirnya para ahli sejarah matematika menemukan asal kata tersebut yang berasal dari penulis buku arab yang terkenal yaitu Abu Ja'far Muhammad Ibnu Musa Al-Khuwarizmi, menulis buku yang berjudul Kitab Aljabar Walmuqabala yang artinya "buku pemugaran dan pengurangan" (The book off restoration and reduction). Dari judul buku itu juga diperoleh akar kata "Aljabar" (Algebro) perubahan dari kata algorism menjadi algorithm muncul karena kata algorism sering dikelirukan dengan arithmetic, sehingga akhiran -sm berubah menjadi -thm. Lambat laun kata algorithm berangsur-angsur dipakai sebagai metode perhitungan (komputasi) secara umum, sehingga kehilangan makna kata aslinya. Dalam bahasa Indonesia, kata algorithm diserap menjadi algoritma. Algoritma adalah urutan langkah-langkah logis penyelesaian masalah yang disusun secara sistematik dan logis (Skiena, 2008). Kata logis merupakan kata kunci dalam algoritma. Langkah-langkah dalam algoritma harus logis dan harus dapat ditentukan bernilai salah atau benar (Prayitno & Nurdin, 2017).

2.1.1 Kriteria Algoritma

Kriteria Algoritma Donald E. Knuth mengemukakan, Algoritma yang baik memiliki Kriteria sebagai berikut:(Muhammad Khoiruddin Harahap & Khairina, 2017)

1. Input Dari sisi Input, minimal program harus memiliki nol atau lebih pengguna. Program pasti memiliki input, Yang dimaksud memiliki nol input berarti program tidak mendapatkan masukan data dari pengguna secara langsung, namun semua data yang akan digunakan oleh program sudah di deklarasikan di dalam kode program yang akan dieksekusi.
2. Output Dari sisi output, minimal program harus memiliki 1 output. Program pasti menghasilkan output karena program dibuat untuk tujuan tertentu.
3. Finite (terbatas) Program harus pasti dan berhenti, bukan tak terhingga, suatu program yang dieksekusi haruslah berhenti dan selesai, bukan berjalan terus menerus hingga hang up atau not responding, dan akhirnya harus di kill (dimatikan) dengan paksa.
4. Definite (pasti) Program harus jelas arah dan tujuannya. Suatu program harus jelas kapan mulai dan kapan berakhir, apa tujuannya, dan memiliki logika yang jelas agar dapat menghasilkan output yang sesuai dengan yang diharapkan.
5. Efisien Artinya, Program harus efisien, tidak memakan banyak memory, tidak melakukan hal – hal yang tidak perlu.

2.2 Kriptografi

Rinaldi Munir dalam bukunya Pengantar Kriptografi menjelaskan bahwa ”Kriptografi (*cryptography*) berasal dari Bahasa Yunani yaitu “*cryptós*” artinya “*secret*” (rahasia), sedangkan “gráphein” artinya “*writing*” (tulisan). Jadi, kriptografi berarti “*secret writing*” (tulisan rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Definisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih dari sekedar *privacy*, tetapi juga untuk tujuan data *integrity*, *authentication*, dan *non-repudiation*”.

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakukan enkripsi dan dekripsi. Pesan yang akan dienkripsi disebut sebagai *plaintext* (teks biasa). Disebut demikian karena infomasi ini dengan mudah dapat dibaca dan dipahami oleh siapa saja. Algoritma yang dipakai untuk mengenkripsi dan mendekripsi sebuah *plaintext* melibatkan pengguna suatu bentuk kunci. *Plaintext* yang telah dienkripsi (kodean) dikenal sebagai *ciphertext* (teks sandi). Pesan *plaintext* yang telah dienkripsi (atau dikodekan) dikenal sebagai *ciphertext* (teks sandi). Di dalam kriptografi kita akan

sering menemukan istilah atau terminology. Beberapa istilah yang harus diketahui yaitu :(Pabokory, Astuti, & Kridalaksana, 2015)

1. Pesan, *Plainteks,* dan *Cipherteks*

   Pesan *(message)* ialah data atau informasi yang dapat dibaca dan dimengerti arti dan maknanya. Biasa disebut untuk pesan adalah *(plaintext)* atau teks jelas *(cleartext).*

2. Pengirim dan Penerima

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

3. Enkripsi dan dekripsi

   Proses menyandikan *plaintext* menjadi *ciphertext* disebut enkripsi *(encryption)* atau *enciphering* (standard nama menurut ISO 7498-2). Sedangkan proses mengembalikan *ciphertext* menjadi *plaintext* semula disebut dekripsi *(decryption)* atau *deciphering* (standard nama menurut ISO 7498-2).

4. *Cipher* dan kunci

   Algoritma kriptografi disebut juga *cipher,* yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *cipher* membutuhkan algoritma yang beda untuk enkripsi dan dekripsi. Konsep matematisnya yang didasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen-elemen *plaintext* dan himpunan yang berisi *ciphertext*. Enkripsi dan dekripsi

merupakan fungsi yang memetakan elemen-elemen antara dua himpunan tersebut. Misalkan P menyatakan plainteks dan C menyatakan cipherteks, maka :

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

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

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

2.3 Aspek- aspek Keamanan Komputer

Keamanan komputer memiliki beberapa aspek penting antara lain:

1. a. Kerahasiaan *(confidentiality)* ialah fasilitas yang diarahkan untuk menjaga supaya pesan tidak mudah dibaca oleh pihak-pihak yang tidak berhak.
2. Integritas data *(data integrity)* ialah fasilitas yang mengamankan bahwa pesan masih asli atau belum pernah dipalsukan selama pengiriman.

3. Otentikasi *(authentication)* ialah fasilitas yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran bagian yang berkomunikasi *(user autehentication).*
4. *Non-repudiation* ialah fasilitas untuk menjaga entitas yang berkomunikasi melakukan penyangkalan *Advanced Encryption Standard (AES).*
5. *Authority* ialah informasi yang berbeda pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak untuk mengaksesnya.
6. *privacy* lebih kearah data-data yang bersifat pribadi.
7. *Access Control* ialah Aspek ini berhubungan dengan cara pengaturan akses ke informasi. Ha ini biasanya berhubungan dengan masalah otentikasi dan privasi. Kontrol akses seringkali dilakukan dengan menggunakan kombinasi user id dan password ataupun dengan mekanisme lain. (Dony Ariyus, 2008)

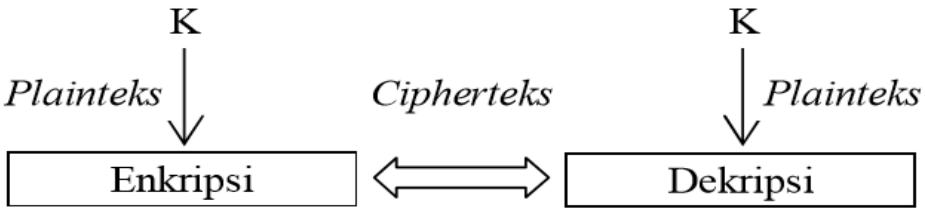
2.4 Macam-macam Algoritma Kriptografi

Berdasarkan kunci enkripsi dan dekripsi algoritma kriptografi dibagi menjadi tiga bagian.

2.4.1 Algoritma kriptografi Simetris

Konsep dasar kriptografi simetris adalah kunci enkripsi dan dekripsi yang sama. Nama lain kriptografi ini adalah kriptografi kunci privat, kriptografi kunci rahasia, atau kriptografi konvensional. Kriptografi ini mengasumsikan penerima

dan pengirim pesan telah berbagi kunci tertentu sebelum pesan dikirim sehingga keamanan terletak pada kerahasiaan kunci. Umumnya *cipher* yang termasuk dalam kriptografi ini beroperasi dalam mode blok, yaitu setiap kali enkripsi atau dekripsi dilakukan pada satu blok data (yang berukuran tertentu), atau beroperasi dalam mode aliran, yaitu setiap kali enkripsi atau dekripsi dilakukan terhadap satu bit atau satu byte data. Proses kriptografi ini dapat dilihat pada gambar berikut ini. (Prayitno & Nurdin, 2017)

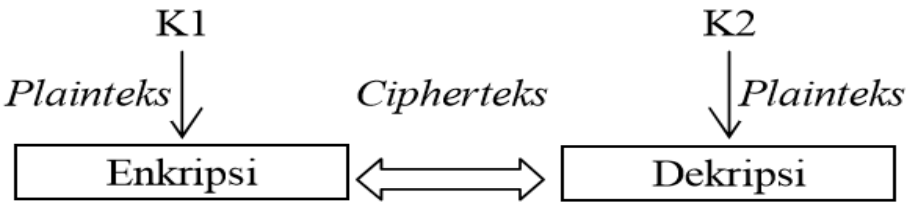


Gambar 2.1 Skema Kriptografi simetris
Sumber: (Ariyus, 2008)

2.4.2 Algoritma Kriptografi Asimetris

Algoritma Asimetris adalah algoritma kriptografi yang mempergunakan kunci yang berbeda pada enkripsi dan dekripsinya (Jensen et al., 2009). Pada kriptografi asimetris kunci untuk enkripsi tidak rahasia dan dapat diketahui siapapun (diumumkan ke publik), sementara kunci untuk dekripsi hanya diketahui oleh penerima pesan (karena itu rahasia). Pada kriptografi jenis ini, setiap orang yang berkomunikasi mempunyai sepasang kunci, yaitu kunci privat dan kunci publik. Pengirim mengenkripsi pesan dengan menggunakan kunci publik si penerima pesan (receiver). Hanya penerima pesan yang dapat mendekripsi pesan karena hanya ia yang mengetahui kunci privatnya sendiri (Munir, 2006). Algoritma

yang termasuk dalam algoritma asimetri adalah RSA, RSA-CRT, Elgamal, DSA, dsb. Skema kriptografi asimetri dapat dilihat pada gambar berikut ini. (JESFER ROBIN ARIOS, 2018)



Gambar 2.2 Skema Kriptografi asimetris
Sumber: (Ariyus, 2008)

2.4.3 Hash Function

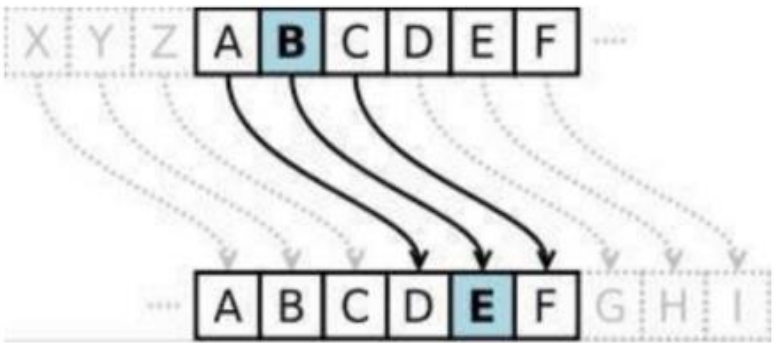
Fungsi *Hash* sering disebut dengan fungsi *Hash* satu arah (*one-way function*), *message disegt*, *fingerprint* fungsi kompresi dan message *authentication code* (MAC), merupakan suatu fungsi matematika yang mengambil masukkan panjang variabel dan mengubahnya ke dalam urutan biner dengan panjang yang tetap (Siahaan, 2016). Fungsi *Hash* biasanya diperlukan bila ingin membuat sidik jari dari suatu pesan. Sidik jari pada pesan merupakan suatu tanda bahwa pesan akan dibahas lebih lanjut pada bagian berikutnya. (Dony Ariyus, 2008)

2.5 Algoritma Kriptografi Klasik

Algoritma kriptografi klasik digunakan sejak sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris (Delfs & Knebl, 2015). Metode menyembunyikan pesannya adalah dengan teknik substitusi atau transposisi atau keduanya. Teknik substitusi adalah menggantikan karakter dalam *plaintext* menjadi karakter lain yang hasilnya adalah *ciphertext*. Sedangkan

transposisi adalah teknik mengubah *plaintext* menjadi *ciphertext* dengan cara permutasi karakter. Kombinasi keduanya secara kompleks adalah yang melatarbelakangi terbentuknya berbagai macam algoritma kriptografi modern. Contoh algoritma kriptografi klasik yaitu: *Caesar Cipher* (Sumandri, 2017)

Metode penyandian ini dinamakan *Caesar Chiper*, setelah digunakan Julius Caesar untuk berkomunikasi dengan para panglimanya . Dalam kriptografi Caesar Chiper dikenal dengan beberapa nama seperti: *shift cipher, Caesar's code* atau *Caesar shift*. *Caesar Chiper* merupakan teknik enkripsi yang paling sederhana dan banyak digunakan. Chiper ini berjenis chiper substitusi, dimana setiap huruf pada *plaintext*nya digantikan dengan huruf lain yang tetap pada posisi alfabet [4]. Misalnya diketahui bahwa pergeseran = 3, maka huruf A akan digantikan oleh huruf D, huruf B menjadi huruf E, dan seterusnya.



Gambar 2.3 Proses pergeseran tiga huruf
Sumber: (Sumandri, 2017)

Transformasi *Caesar Chiper* dapat direpsentasikan dengan menyelaraskan *plaintext* dengan chipertext ke kiri atau kanan sebanyak jumlah pergeseran yang diinginkan. Sebagai contoh dengan jumlah pergeseran sebanyak 3.

Plaintex : ABCDEFGHIJKLMNOPQRSTUVWXYZ

Ciphertext : DEFGHIJKLMNOPQRSTUVWXYZABC

Untuk membaca pesan yang dienkripsi penerima dapat menyelaraskan huruf chipertext yang diterima dengan plaintext yang tepat berada di atasnya. Sebagai contoh dekripsinya sebagai berikut.

Ciphertext : VHPLQDU QDVLRQDO PDWHPDWLND

Plaintext : SEMINAR NASIONAL MATEMATIKA

Proses enkripsi pada *Caesar Cipher* dapat direperesentasikan menggunakan operator aritmetika modulo 26 setelah sebelumnya setiap huruf di transformasi kedalam angka, yaitu: A = 0, B = 1,…, Z = 25. Maka Caesar Cipher dirumuskan sebagai berikut: Proses enkripsi suatu huruf x dengan pergeseran n dapat dinyatakan secara matematis sebagai berikut:

Enkripsi: $C = E(P) = (P + 5) \bmod 26$ (1)

Dekripsi: $P = D(C) = (C - 5) \bmod 26$ (2)

Jika pergeseran huruf sebanyak x, maka dapat dijadikan dalam persamaan (3) dan (4):

$C = E(P) = (P + x) \bmod 26$ (3)

$P = D(C) = (C - x) \bmod 26$ (4)

dengan C adalah ciphertext, P adalah plaintext, x adalah kunci rahasia, E(P) adalah enkripsi, dan D(C) adalah dekripsi. Untuk lebih menyulitkan kriptanalis dapat digunakan perkalian dengan n, n adalah bilangan ganjil pada *plaintext*. Ini dijelaskan pada persamaan (5) dan (6):

$$C = E(P) = ((n * P) + x) \bmod 26 \quad (5)$$

$$P = D(C) = ((C - x)/ n) \bmod 26 \quad (6)$$

dengan n = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23,25. Tidak berlaku dengan n adalah bilangan negatif, karena akan menghasilkan huruf yang sama dalam enkripsi. Kelemahan dari *Caesar Cipher* adalah dapat dipecahkan dengan cara brute force attack, suatu bentuk serangan yang dilakukan dengan mencoba-coba berbagai kemungkinan untuk menemukan kunci. Bisa juga menggunakan *exhaustive key search*, karena jumlah kunci sangat sedikit (hanya ada 26 kunci).

2.6 Algoritma Kriptografi Modern

Algoritma kriptografi modern umumnya beroperasi dalam mode bit ketimbang mode karakter (seperti yang dilakukan pada cipher substitusi atau cipher transposisi dari algoritma kriptografi klasik) (Oktaviana & Siahaan, 2016). Operasi dalam mode bit berarti semua data dan informasi (baik kunci, *plainteks*, maupun *ciphertext*) dinyatakan dalam rangkaian (*string*) *bit biner*, 0 dan 1. Algoritma enkripsi dan dekripsi memproses semua data dan informasi dalam bentuk rangkaian bit. Rangkaian bit yang menyatakan plaintext dienkripsi menjadi ciphertext dalam bentuk rangkaian bit, demikian sebaliknya. Enkripsi modern berbeda dengan enkripsi konvensional. Enkripsi modern sudah menggunakan komputer untuk

pengoperasiannya, berfungsi untuk mengamankan data baik yang ditransfer melalui jaringan komputer mauapun yang bukan. Hal ini sangat berguna untuk melindungi *privacy,* data *integrity*, *authentication* dan *non-repudiation*. Perkembangan algoritma kriptografi modern berbasis bit didorong oleh penggunaan komputer digital yang merepresentasikan data dalam bentuk biner (Firmansyah, 2012)

2.7 Beaufort

Beaufort cipher merupakan salah satu algoritma dalam teknik keamanan kriptografi klasik (Marwati & Yulianti, 2018). Kunci (K) pada beaufort cipher adalah urutan karakter-karakter K = k1 ... kd dimana k1 didapat dari banyaknya pergeseran dari alfabet ke-i sama seperti *viginere cipher*. Artinya bahwa jumlah kunci yang dibangkitkan harus sama dengan jumlah karakter *plaintext* yang diamankan. Algoritma ini melakukan proses enkripsi dan dekripsi secara stream (masing-masing karakter *plaintext* harus memiliki pasangan kunci). Hal ini yang menyebabkan algoritma ini sama hampir sama dengan algoritma *vigeneere cipher*. Adapun formulasi yang digunakan dalam proses enkripsi dan dekripsi adalah:

Formula proses enkripsi : Ci = Ek(Mi) = (Ki – Mi) Mod 26
Formula proses dekripsi : Mi = Dk(Ci) = (Ki – Ci) Mod 26

Keterangan :
Mi = Pesan yang akan dienkripsi (plain)
Ci = Sandi (cipher) Ki = Kunci
Ek = Fungsi Enkripsi Dk = Fungsi Dekripsi

Nilai mod 26 di atas tergantung dari jumlah kebutuhan karakter yang digunakan, pada awalnya beaufort cipher hanya menggunakan 26 karakter, namun seiring dengan perkembangan teknologi komputer saat ini, maka dapat menggunakan mod 256 (mengguakan seluruh tabel ASCII).

2.8 ROT13

ROT13 (*Rotate 13*) merupakan perkembangan atau modifikasi dari metode *Caesar Cipher* dalam segi perubahan jumlah geseran dan juga arah geseran. ROT13 adalah enkripsi substitution cipher yang umum digunakan di sistem operasi UNIX. Pada sistem enkripsi ROT13 sebuah huruf digantikan dengan huruf yang letaknya di atas 13 posisi darinya. Caesar Cipher ROT13 adalah fungsi yang menggunakan kode Kaisar dengan pergeseran k=13. ROT13 didesain untuk keamanan pada sistem operasi UNIX yang sering digunakan pada forum online, berfungsi untuk menyelubungi isi artikel sehingga hanya orang yang berhak yang dapat membacanya. Sistem enkripsi ROT13 kali ini dengan menggeser maju karakter sebanyak 13 kali, terhitung 1 adalah karakter didepannya, dan pergeseran karakter berdasarkan urutan karakter pada tabel ASCII. Sebagai dekripsinya, dengan menggeser mundur karakter sebanyak 13 kali.

Salah satu pengembangan dari *Caesar cipher* adalah ROT13. ROT13 (Rotate 13) adalah enkripsi cipher substitusi yang umum digunakan di sistem operasi UNIX. Pada sistem ini sebuah huruf digantikan dengan huruf yang letaknya 13 posisi darinya. Sebagai contoh, huruf “A” digantikan dengan huruf “N”, huruf

“B” digantikan dengan huruf “O”, dan seterusnya. Secara matematis, hal ini dapat dituliskan sebagai :

$$C = ROT13 (P)$$

Untuk mengembalikan kembali ke bentuk semulanya (dekripsi) dilakukan proses enkripsi ROT13 dua kali. P = ROT13 (ROT13 (P))

Tabel 2.1 Susunan alfabet ROT13

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

Sumber: (Sumandri, 2017)

Contoh operasi *Caesar cipher* ROT13 :

ROT13 ('HELLO') = 'URYYB'

ROT13 ('URYYB') = 'HELLO'

ROT13 (ROT13 ('HELLO')) = 'HELLO'

ROT13 memang tidak didesain untuk keamanan tingkat tinggi. ROT13, misalnya digunakan untuk menyelubungi isi dari artikel (*posting*) di *Usenet news* yang berbau ofensif. Sehingga hanya orang yang betul-betul ingin membaca dapat melihat isinya. Contoh penggunaan lain adalah untuk menutupi jawaban dari sebuah teka teki (*puzzle*).

Dasar keilmuan dari Caesar cipher sebagian besar adalah matematika yang antara lain mencakup teori bilangan, aljabar dan fungsi. Subbab matematika tersebut sudah diajarkan sejak pendidikan sekolah bahkan diperluas lagi di perguruan tinggi. Rumus *Caesar cipher* secara umum :

$$C = E (P) = (P + k) \bmod 26$$

Dan fungsi dekripsi adalah :

$$P = D (C) = (C - k) \bmod 26$$

Catatan:

1. Pergeseran 0 sama dengan pergeseran 26(susunan huruf tidak berubah).
2. Pergeseran lain untuk k > 25 dapat juga dilakukan namun hasilnya akan kongruen dengan bilangan bulat dalam modulo 26. Misalnya k=37 kongruen dengan 11 dalam modulus 26, atau $37 \equiv 11 \pmod{26}$.

Persamaan di atas menggunakan subbab matematika teori bilangan khususnya dengan modulus. Operasi modulus adalah sebuah operasi yang menghasilkan sisa pembagian dari suatu bilangan terhadap bilangan lainnya. Contoh modulus :

$$1 = 7 \bmod 2$$

$$2 = 5 \bmod 3$$

2.9 Visual Basic 2010

Visual Basic 2010 pada dasarnya adalah sebuah bahasa pemrograman komputer. Dimana pengertian dari bahasa pemrograman itu adalah perintah-perintah atau instruksi yang dimengerti oleh komputer untuk melakukan tugas-tugas tertentu (Robins, Rountree, & Rountree, 2003). Visual Studio 2010 (yang sering juga disebut dengan VB .Net 2010) selain disebut dengan bahasa pemrograman, juga sering disebut sebagai sarana (*tool*) untuk menghasilkan program-progam aplikasi berbasiskan windows. Visual basic adalah sebuah bahasa pemrograman yang berpusat pada object (*Object Oriented Programming*) digunakan dalam pembuatan aplikasi Windows yang berbasis *Graphical User Interface*, hal ini menjadikan Visual Basic menjadi bahasa pemrograman yang wajib diketahui dan dikuasai oleh setiap programmer. Beberapa karakteristik obyek tidak dapat dilakukan oleh Visual Basic misalnya seperti Inheritance tidak bisa module dan *Polymorphism* secara terbatas bisa dilakukan dengan deklarasi class module yang mempunyai Interface tertentu. Beberapa kemampuan atau manfaat dari Visual Studio 2010 diantaranya seperti :

1. Untuk membuat program aplikasi berbasiskan windows.
2. Untuk membuat objek-objek pembantu program seperti, misalnya : kontrol ActiveX, file Help, aplikasi Internet dan sebagainya.
3. Menguji program (debugging) dan menghasilkan program berakhiran EXE yang bersifat executable atau dapat langsung dijalankan.

Visual Studio 2010 adalah bahasa yang cukup mudah untuk dipelajari. Bagi programmer pemula yang baru ingin belajar program, lingkungan Visual Studio dapat membantu membuat program dalam sekejap mata. Sedang bagi programer tingkat lanjut, kemampuan yang besar dapat digunakan untuk membuat programprogram yang kompleks, misalnya lingkungan net-working atau client server.. Bahasa Visual Studio cukup sederhana dan menggunakan kata-kata bahasa Inggris yang umum digunakan. Kita tidak perlu lagi menghafalkan sintaks-sintaks maupun format-format bahasa yang bermacam-macam, di dalam Visual Basic semuanya sudah disediakan dalam pilihan-pilihan yang tinggal diambil sesuai dengan kebutuhan. Selain itu, sarana pengembangannya yang bersifat visual memudahkan kita untuk mengembangkan aplikasi berbasiskan Windows, bersifat mouse-driven (digerakkan dengan mouse) dan berdaya guna tinggi.

2.10 Mengenal UML

Unified Modelling Language (UML) adalah sebuah "bahasa" yang telah menjadi standar dalam industri untuk visualisasi . Pemodelan Visual dengan Menggunakan UML dan mendokumentasikan sistem piranti lunak. UML menawarkan sebuah standar untuk merancang model sebuah sistem. Dengan menggunakan UML dapat dibuat model untuk semua jenis aplikasi piranti lunak, dimana aplikasi tersebut dapat berjalan pada piranti keras, sistem operasi dan jaringan apapun, serta ditulis dalam bahasa pemrograman apapun. Tetapi karena UML juga menggunakan class dan operation dalam konsep dasarnya, maka lebih

cocok untuk penulisan piranti lunak dalam bahasa berorientasi objek seperti C++, Java, atau VB. NET.

2.10.1 Diagram UML

Setiap sistem yang kompleks seharusnya bisa dipandang dari sudut yang berbeda – beda sehingga bisa mendapatkan pemahaman secara menyeluruh . Untuk upaya tersebut UML menyediakan 9 jenis diagram yang dapat dikelompokkan berdasarkan sifatnya statis atau dinamis. Ke 9 diagram dalam UML itu adalah :

1. Diagram Kelas

   Diagram kelas bersifat statis. Diagram ini memperlihatkan himpunan kelas-kelas, antarmuka-antarmuka, kolaborasi-kolaborasi serta relasi.

2. Diagram Objek

   Diagram objek bersifat statis. Diagram ini memperlihatkan objek-objek serta relasi antar objek. Diagram objek memperlihatkan instansiasi statis dari segala sesuatu yang dijumpai pada diagram kelas.

3. Use case Diagram

   Diagram ini bersifat statis. Diagram ini memperlihatkan himpunan use case dan aktor-aktor (suatu jenis khusus dari kelas). Diagram ini terutama sangat penting untuk mengorganisasi dan memodelkan perilaku dari suatu sistem yang dibutuhkan serta diharapkan pengguna.

4. Sequence Diagram (Diagram urutan)

   Diagram ini bersifat dinamis. Diagram sequence merupakan diagram interaksi yang menekankan pada pengiriman pesan (message) dalam suatu waktu tertentu.

5. *Collaboration* Diagram

   Diagram ini bersifat dinamis. Diagram kolaborasi adalah diagram interaksi yang menekankan organisasi struktural dari objek – objek yang menerima serta mengirim pesan (*message*).

6. *Statechart* Diagram

   Diagram ini bersifat dinamis. Diagram ini memperlihatkan state – state pada sistem, memuat state, transisi, event, serta aktifitas. Diagram ini terutama penting untuk memperlihatkan sifat dinamis dari antarmuka, kelas, kolaborasi dan terutama penting pada pemodelan sistem – sistem yang reaktif.

7. *Activity* Diagram

   Diagram ini bersifat dinamis. Diagram ini adalah tipe khusus dari diagram state yang memperlihatkan aliran dari suatu aktifitas ke aktifitas lainnya dari suatu sistem. Diagram ini terutama penting dalam pemodelan fungsi – fungsi dalam suatu sistem dan memberi tekanan pada aliran kendali antar objek.

8. *Component* Diagram

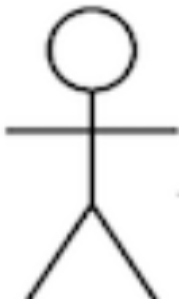
   Diagram ini bersifat statis. Diagram ini memperlihatkan organisasi serta kebergantungan pada komponen – komponen yang telah ada sebelumnya.

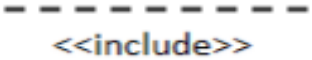
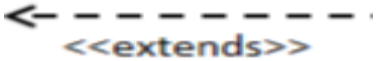
Diagram ini berhubungan dengan diagram kelas dimana komponen secara tipikal dipetakan ke dalam satu atau lebih kelaskelas, antarmuka – antarmuka serta kolaborasi – kolaborasi.

9. *Deployment* Diagram

   Diagram ini bersifat statis. Diagram ini memperlihatkan konfigurasi saat aplikasi dijalankan (saat *run time*). Dengan ini memuat simpul – simpul (node) beserta komponen – komponen yang ada di dalamnya. *Deployment* diagram berhubungan erat dengan diagram kompoen dimana *deployment* diagram memuat satu atau lebih komponen – komponen. Diagram ini sangat berguna saat aplikasi berlaku sebagai aplikasi yang dijalankan pada banyak mesin (*distributed computing*).

Tabel 2.2 Simbol-simbol Use case

Gambar	Keterangan
	Use case menggambarkan fungsionalita yang disediakan sistem sebagai unit-unit yang bertukar pesan antar unit dengan aktif, yang dinyatakan dengan menggunakan kata kerja.
	*Actor* atau Aktor adalah Abstraction dari orang atau sistem yang lain yang mengaktifkan fungsi dari target sistem. Untuk mengidentifika sikan aktir, harus ditentukan pembagian tenaga kerja dan tugas-tugas yang berkaitan dengan peran pada konteks target sistem. Orang atau sistem bisa muncul dalam beberapa peran. Perlu dicatat bahwa aktor berinteraksi dengan Use Case,

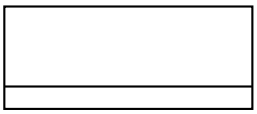
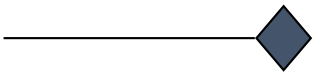
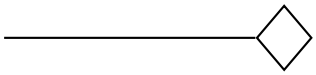
	tetapi tidak memiliki kontrol terhadap *use case.*
	Asosiasi antara aktor dan use case, digambarkan dengan garis tanpa panah yang mengindikasika n siapa atau apa yang meminta interaksi secara langsung dan bukannya mengindikasikan data.
	Asosiasi antara aktor dan use case yang menggunakan panah terbuka untuk mengindikasikan bila aktor berinteraksi secara pasif dengan sistem.
	Include, merupakan di dalam use case lain (required) atau pemanggilan use case oleh use case lain, contohnya adalah pemanggilan sebuah fungsi program.
	Extend, merupakan perluasan dari use case lain jika kondisi atau syarat.

Sumber: (Kurniawan, 2018)

2.10.2 Class Diagram

Class diagram digunakan untuk menggambarkan perbedaan yang mendasar antara *class*, hubungan antara *class*, dan di mana *sub-sistem class* tersebut (Jogiyanto, 2006). Simbol yang digunakan dalam *class diagram* adalah sebagai berikut :

Tabel 2.3 Simbol-simbol Class Diagram

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

Sumber: (Kurniawan, 2018)

2.11 Flowchart

Flowchart adalah suatu metode untuk menggambarkan tahap-tahap pemecahan masalah dengan mempresentasikan simbol-simbol tertentu yang mudah dimengerti, mudah digunakan dan standar (Bhatia & Mitra, 2012).

1. System Flowchart

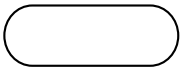
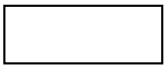
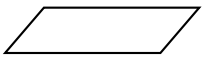
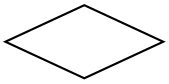
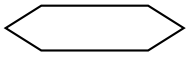
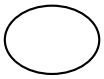
   System flowchart adalah urutan proses dalam system dengan menunjukkan alat. Media input, output, serta jenis media penyimpanan dalam proses pengolahan data. *System flowchart* ini tidak digunakan untuk menggambar

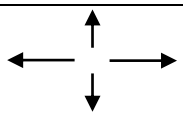
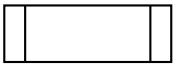
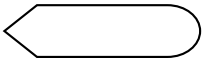
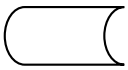
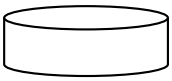
urutan langka untuk memecahkan masalah, tetapi hanya untuk menggambarkan prosedur dalam system yang di bentuk. Berikut ini adlah gambar dari simbol-simbol standar yang telah banyak digunakan pada penggunaan penggambaran *system flowchart*.

2. Program Flowchart

Program *flowchart* adalah diagram alir yang menggambarkan urutan logika dari suatu prosedur pemecahan masalah. Untuk menggambarkan program *flowchart* tersedia simbol-simbol standar, berikut ini adalah gambaran dari simbol-simbol standar yang digunakan program *flowchart*.

Tabel 2.4 Simbol-simbol Flowchart

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

Adapun tahapan penelitian yang dilakukan oleh penulis ini dengan judul "Kombinasi Algortima Beaufort dengan ROT13 dalam pengamanan Informasi" adalah sebagai berikut :

a. Studi Literatur *(Library Research)*

   Pada tahap ini dilakukan pengumpulan data-data yang diperlukan dengan mempelajari dan menyeleksi buku, jurnal, makalah dan beberapa situs yang berhubungan dengan penulisan skripsi ini.

b. Analisa

   Merupakan proses analisa terhadap permasalahan dan mendefenisikan model penyelesaian, termasuk dalam proses ini adalah melakukan analisis terhadap permasalahan yang akan diselesaikan.

c. Pembahasan

   Tahap ini dilakukan pembahasan perhitungan proses enkripsi dan dekripsi menggunakan algoritma Beaufort dan ROT13.

d. Implementasi dan pengujian

   Tahap ini melakukan implementasi sistem dari aplikasi enkripsi dan dekripsi menggunakan kombinasi dua buah menggunakan perangkat lunak bahasa pemrograman *Visual Basic 2010.*

3.2 Metode Pengumpulan Data

Pengumpulan data adalah pencarian terhadap susuatu kerena ada perhatian dan keinginan terhadap hasil suatu aktivitas. Metode pengumpulan data dalam penulisan ini dibagi menjadi tiga yaitu :

a. Studi Kepustakaan

   Pada tahap ini dilakukan dengan mengumpulkan data, mempelajari, dan membaca berbagai referensi baik itu buku, jurnal, makalah, internet, dan berbagai sumber lainnya untuk memperoleh informasi.

b. Observasi

   Observasi dilakukan untuk pengumpulan data, bahan yang dijadikan plaintext untuk kemudian diproses menjadi ciphertext dengan segala aspek kegiatan yang berhubungan dengan tujuan penelitian.

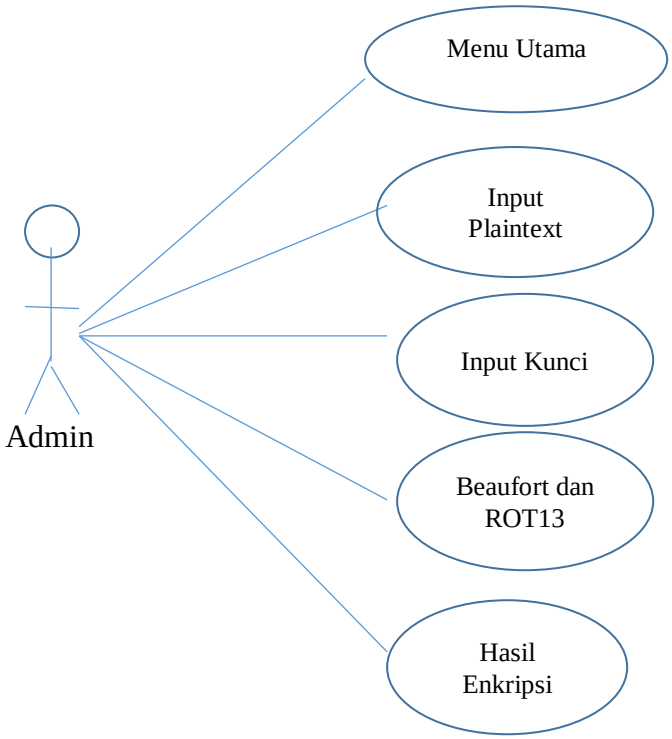
3.3 Rancangan Penelitian

Rancangan penelitian bertujuan untuk menggambarkan semua kondisi dan bagian-bagian yang berperan dalam sistem yang dirancang dan untuk memenuhi kebutuhan user (pemakai) mengenai gambaran yang jelas tentang perancangan sistem yang akan dibuat serta diimplementasikan.

3.3.1 Use Case Diagram

Use Case adalah deskripsi fungsi dari sebuah sistem dari perspektif pengguna. *Use Case* bekerja dengan cara mendeskripsikan tipikal interaksi antara *User* (pengguna) sebuah sistem dengan sistemnya sendiri melalui sebuah cerita

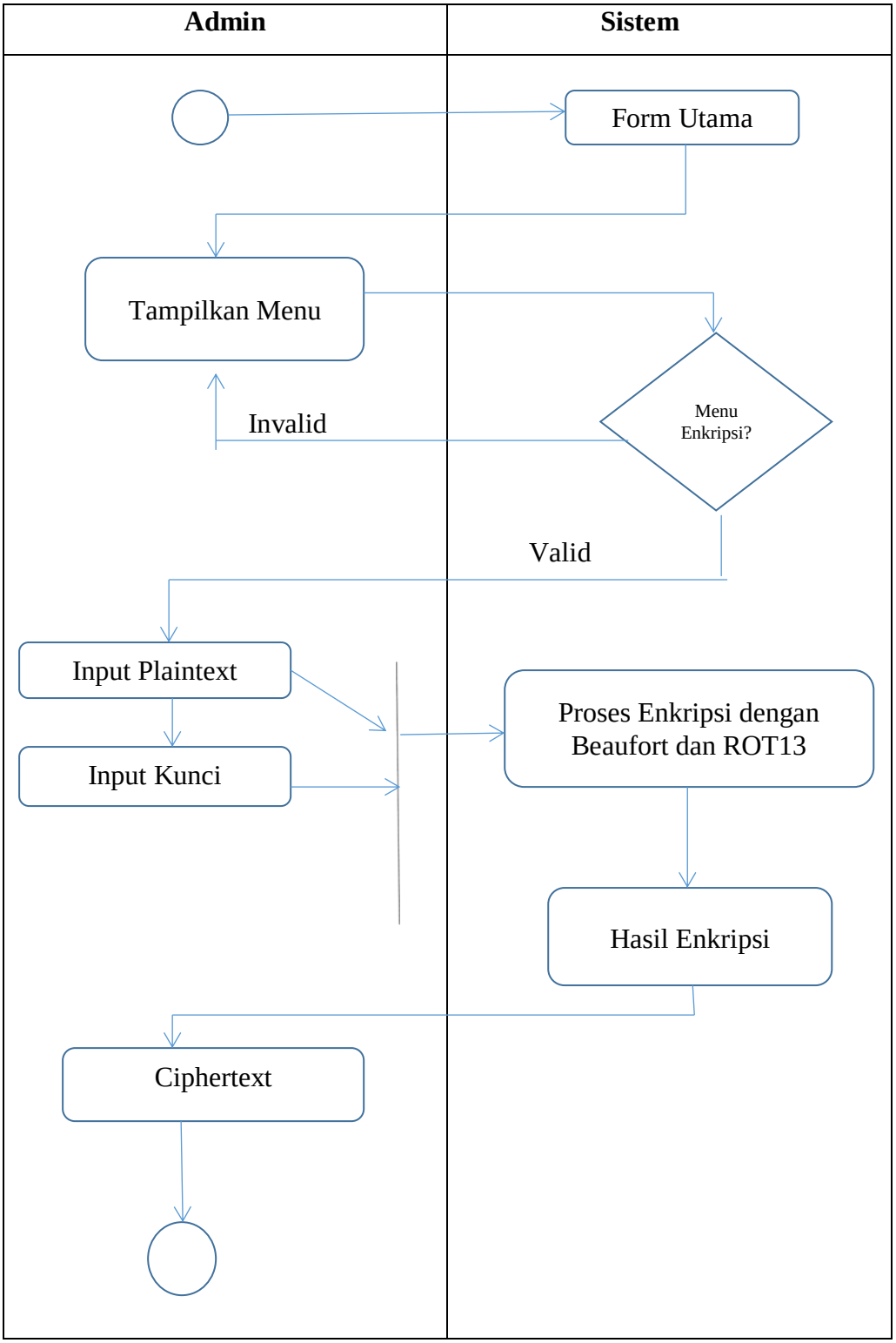
bagaimana sebuah sistem dipakai. Berikut ini adalah perancangan *Use Case* untuk admin dari sebuah sistem pendukung keputusan.



Gambar 3.1.Use Case Diagram

3.3.2 Activity Diagram

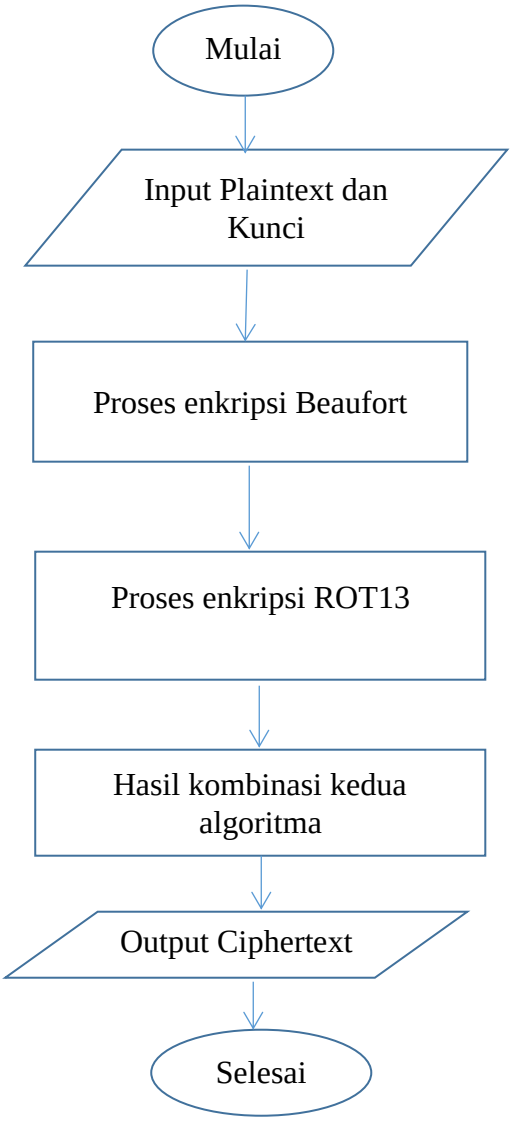
Activity diagram akan menggambarkan alur aktifitas dari sistem, untuk *Activity diagram* dari sistem pendukung keputusan dalam menentukan teh layak ekspor adalah sebagai berikut:



Gambar 3.2. Activity Diagram

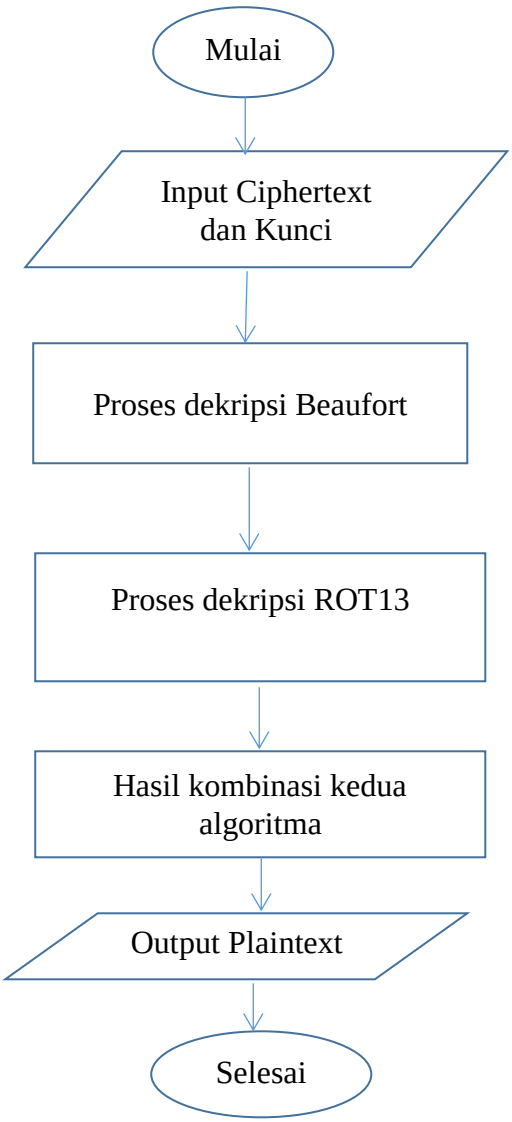
3.3.3 Flowchart

Flowchart akan menguraikan sistem kerja dari program yang akan dirancang, dimana rancangan *flowchart* proses enkripsi dapat dilihat pada gambar dibawah ini.



Gambar 3.3. Flowchart Enkripsi

Kebalikan dari proses enkripsi adalah proses dekripsi. Uraian flowchart proses dekripsi dapat dilihat pada gambar berikut ini.



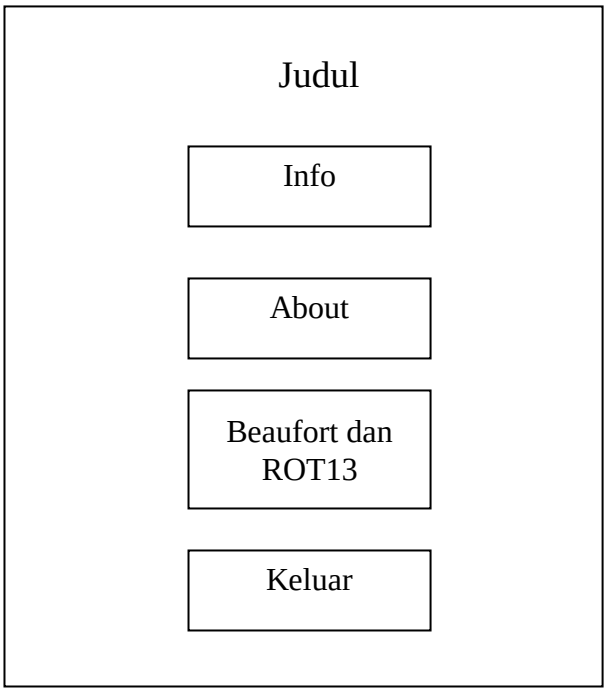
Gambar 3.4. Flowchart Dekripsi

3.3.4 Perancangan Antarmuka

Perancangan antarmuka *(User interface)* merupakan suatu bentuk tampilan dari program yang akan dibuat untuk kebutuhan *interface* dengan *User*.

Perancangan antar muka terdiri dari perancangan tampilan menu, tampilan *form*, tampilan pesan, dan keluaran. Berikut ini merupakan perancangan tampilan menu utama program aplikasi enkripsi dan dekripsi algoritma *Beaufort* dan ROT13.

Tampilan Halaman Menu Utama



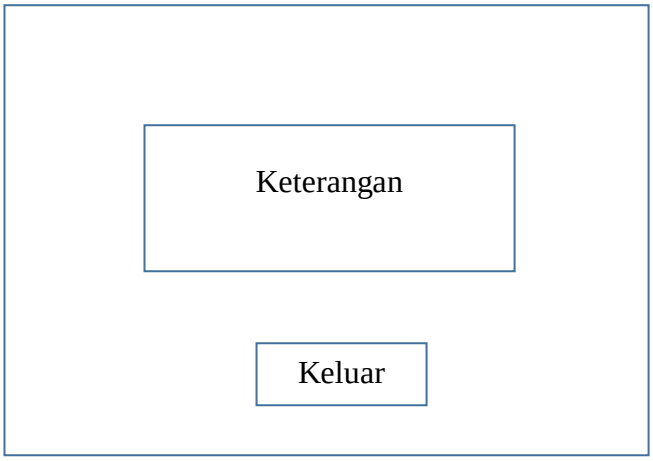
Gambar 3.5. Perancangan Menu Utama

Keterangan:

- Judul adalah menu yang berisi judul tentang Kombinasi Algortima Beaufort dengan ROT13 dalam pengamanan Informasi.
- Info adalah menu yang menjelaskan tentang deskripsi algoritma Beaufort dan ROT13.
- About adalah menu yang menampilkan informasi tentang penulis.
- Keluar adalah tombol untuk keluar dari aplikasi.

Tampilan Menu Info

Berikut ini adalah tampilan perancangan yang berisi tentang menu info.



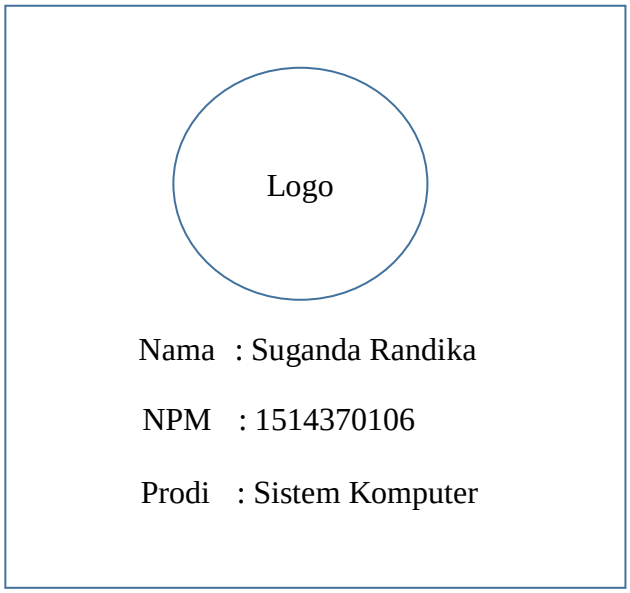
Gambar 3.6. Perancangan Menu Info

Keterangan:

- Keterangan adalah menu untuk menampilkan penjelasan algoritma Beaufort dan ROT13.
- Keluar adalah tombol untuk kembali ke menu utama.

Tampilan Menu About

Berikut ini adalah tampilan perancangan yang berisi tentang menu about.



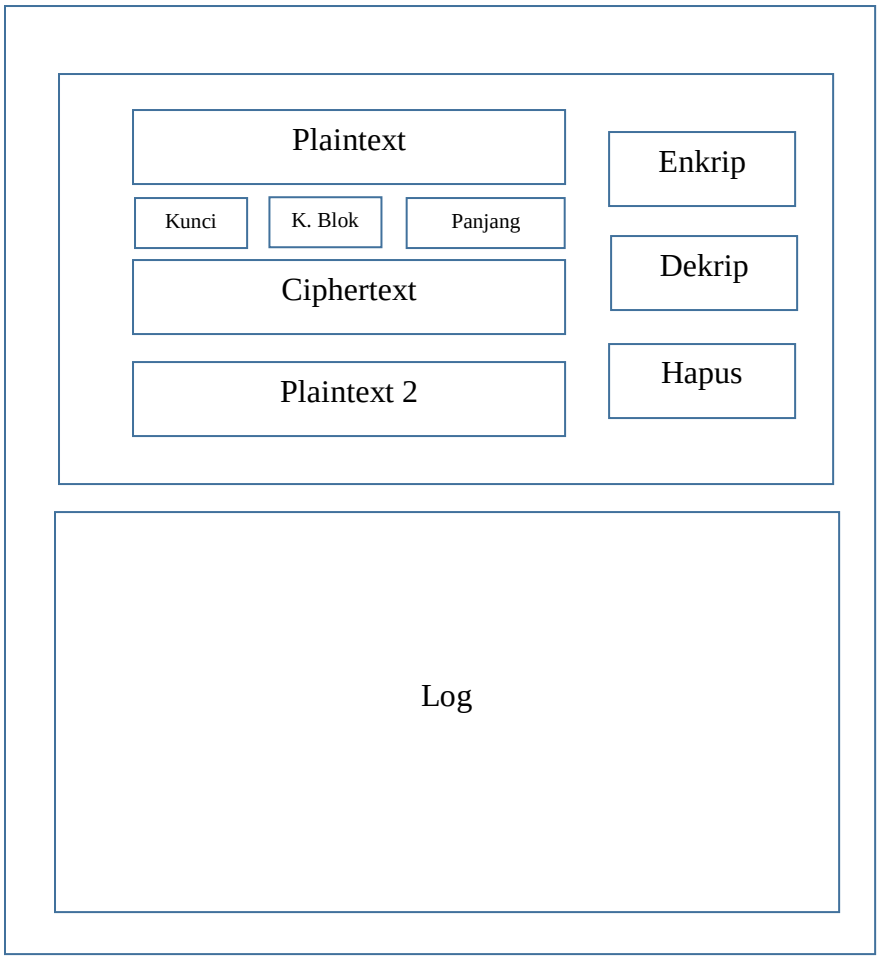
Gambar 3.7. Perancangan Menu About

Keterangan:

- Logo dimana pada bagian ini akan ditampilkan logo Universitas Pembangunan Panca Budi, Medan.
- Nama dimana pada bagian ini akan ditampilakan Nama dari penulis.
- NPM dimana pada bagian ini akan ditampilkan NPM dari penulis.
- Prodi dimana pada bagian ini akan ditampilkan Program Studi dari penulis.

Tampilan Beaufort dan ROT13

Berikut ini adalah perancangan tampilan menu enkripsi dan dekripsi kombinasi dari kedua algoritma.



Gambar 3.8. Perancangan Menu Beaufort ROT13

Keterangan:

- Plaintext adalah teks atau kata-kata yang digunakan sebagai sumber awal.
- Ciphertext adalah hasil proses enkripsi dari algoritma Beaufort dan ROT13.
- Plaintext 2 adalah hasil dekripsi dari algoritma Beaufort dan ROT13.
- Kunci adalah pergeseran karakter yang digunakan pada algoritma Beaufort.

- Kunci blok adalah pengulangan kunci sampai batas akhir karakter yang digunakan pada algoritma Beaufort .
- Panjang adalah seberapa banyak karakter yang digunakan.
- Enkrip adalah tombol yang digunakan untuk melakukan proses enkripsi.
- Dekrip adalah tombol yang digunakan untuk melakukan proses dekripsi.
- Hapus adalah tombol yang digunakan untuk mengkosongkan semua form isian.
- Log adalah riwayat dari proses enkripsi dan dekripsi kedua algoritma.

BAB IV

HASIL DAN PEMBAHASAN

4.1 Implementasi

Implementasi merupakan tahapan menerapkan hasil perancangan dan pembuatan aplikasi enkripsi dan dekripsi dari kombinasi algoritma *Beaufort* dan ROT13. Pada implementasi ini menjelaskan berbagai macam syarat dan persyaratan yang digunakan dalam menghasilkan program aplikasi ini. Ada beberapa bagian yang terlibat pada implementasi ini yaitu implementasi algortima dan implementasi antarmuka.

4.2 Spesifikasi Sistem

Penelitian ini merupakan penelitian yang berfokus pada pengembangan alur proses enkripsi dan dekripsi dari dua buah algoritma yang digunakan. Aplikasi membutuhkan sistem yang optimal agar hasil program aplikasi menjadi lebih baik. Perangkat utama sistem yang dibutuhkan dibagi menjadi dua yaitu perangkat keras dan perangkat lunak. Adapun spesifikasi perangkat keras dan perangkat lunak tersebut dapat dilihat pada bagian selanjutnya.

4.2.1 Spesifikasi Perangkat Keras

Proses kombinasi algoritma enkripsi dan dekripsi dengan menggunakan algoritma Beaufort dan ROT13 membutuhkan perangkat keras sebagai media fisik

sebagai sarana pendukung utama. Spesifikasi perangkat keras dapat dilihat pada Tabel 4.1.

Tabel 4.1 Spesifikasi Perangkat Keras

No.	Nama Komponen	Spesifikasi
1	Processor	Intel Core i3 2.4 GHz
2	RAM	4096 MB
3	Harddisk	500 GB
4	Monitor	14 inch

4.2.2 Spesifikasi Perangkat Lunak

Selain membutuhakn perangkat keras sebagai media fisik untuk mendukung implementasi enkripsi dan dekripsi ini, ada juga perangkat lunak sebagai sarana non-fisik yang harus mendukung perangkat keras tersebut untuk mengolah data dan perhitungan sehingga menghasilkan keputusan yang akurat. Spsesifikasi perangkat lunak dapat dilihat pada Tabel 4.2.

Tabel 4.2 Perangkat Lunak

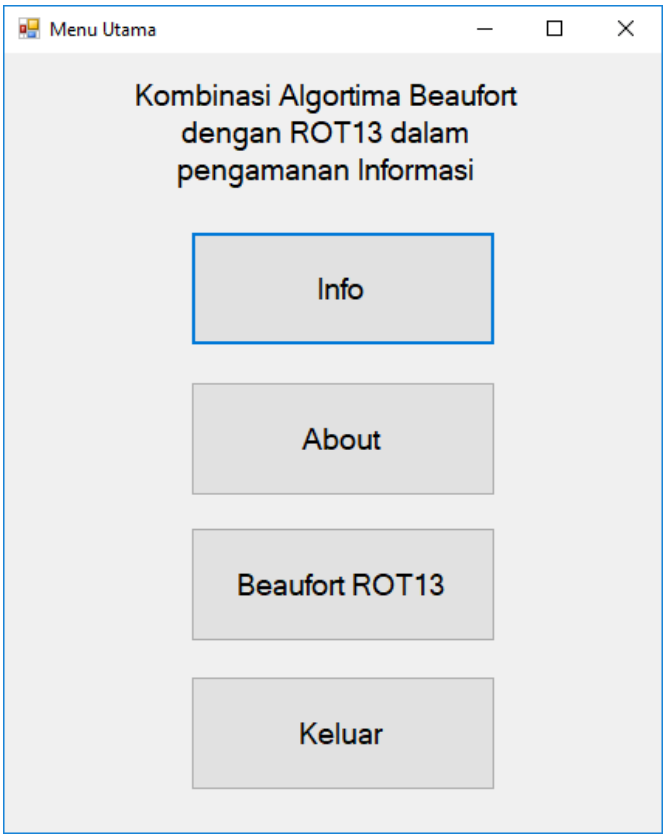
No.	Nama Komponen	Spesifikasi
1	Operating System	Windows 10 64 Bit
2	Programming Editor	Visual Studio 2010
3	Picture Editor	Snipping Tool
4	Data Editor	Microsoft Excel

4.3 Implementasi Antarmuka

Implementasi antarmuka program aplikasi enkripsi dan dekripsi dari kedua algoritma *Beaufort* dan ROT13 dibagi beberapa menu. Menu yang pertama muncul pada saat program aplikasi dijalankan adalah Menu Utama. Menu ini memiliki beberapa sub-menu yang apabila dijalankan akan membuka menu-menu lainnya yang berhubungan dengan program enkripsi dan dekripsi.

4.3.1 Menu Utama

Menu Utama adalah menu yang pertama sekali ditampilkan pada saat program aplikasi dijalankan. Berikut ini adalah tampilan bentuk dari menu utama.



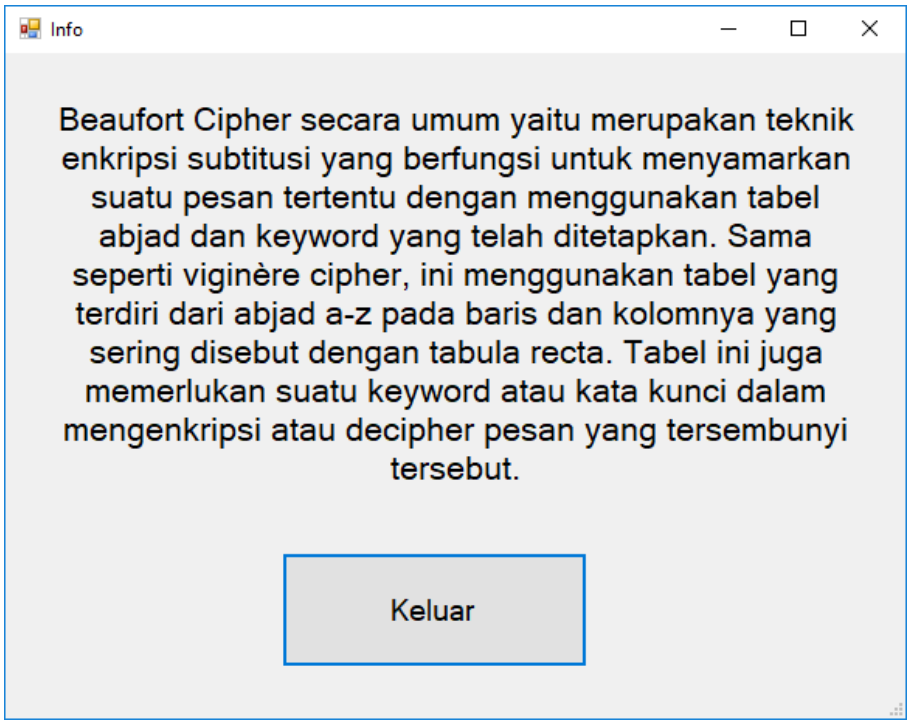
Gambar 4.1 Tampilan Menu Utama

Menu utama terdiri dari empat buah Button yaitu:

1. Info
2. About
3. Beaufort ROT13
4. Keluar

4.3.2 Menu Info

Menu Info adalah menu yang berisi informasi tentang materi Beaufort Cipher dan ROT13. Pada menu ini terdapat beberapa penjelasan dan deskripsi terhadap kedua algoritma tersebut. Berikut ini adalah tampilan Menu Info.



Gambar 4.2 Tampilan Menu Info

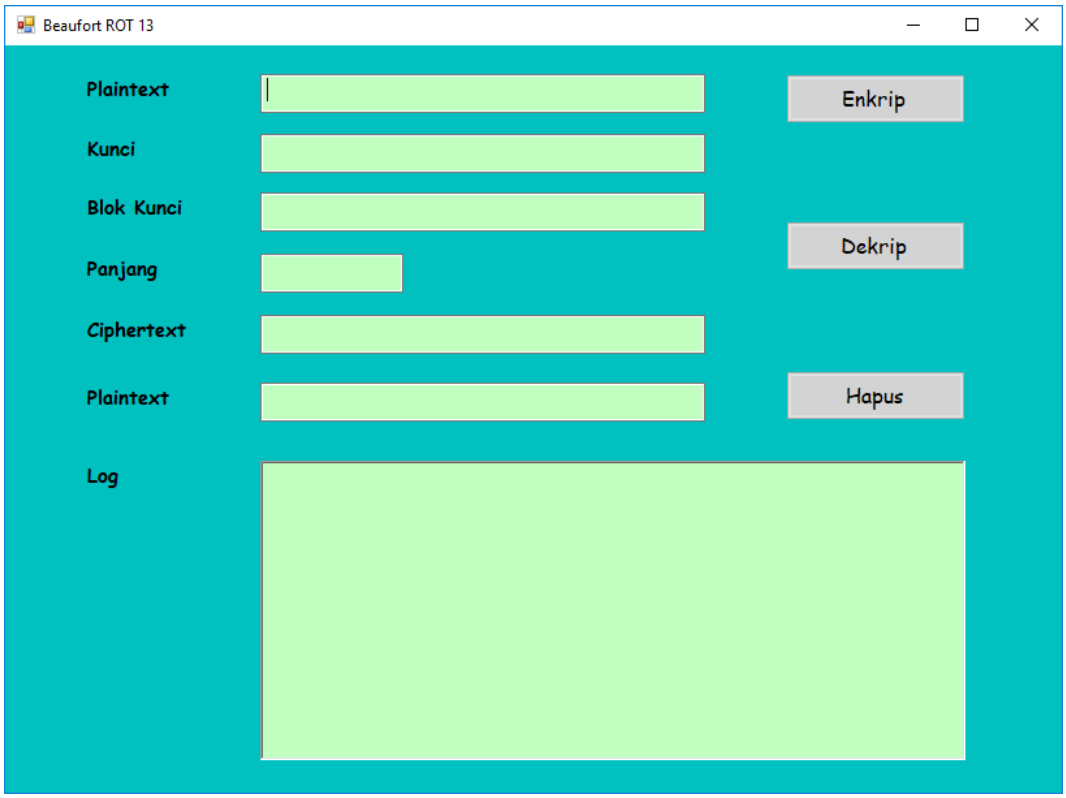
4.3.3 Menu About

Menu Info adalah menu yang berisi informasi tentang penulis, NPM, fakultas dan program studi Sistem Komputer. Berikut ini adalah tampilan menu About.

Gambar 4.3 Tampilan Menu About

4.3.4 Menu Beaufort ROT13

Menu Beaufort ROT13 adalah menu inti yang berisi program untuk melakukan proses enkripsi dan dekripsi. Menu ini memiliki beberapa textbox dan button untuk melakukan proses enkripsi dan dekripsi. Berikut ini adalah tampilan dari Menu Beaufort ROT13.



Gambar 4.4 Tampilan Menu Beaufort ROT13

4.4 Pengujian Sistem

Pengujian sistem adalah ujicoba proses enkripsi dan dekripsi yang dihitung secara manual. Hasil perhitungan manual harus sama dengan apa yang dilakukan

oleh perhitungan komputer. Berikut ini adalah contoh perhitungan enkripsi dan dekripsi yang dilakukan berdasarkan program aplikasi.

4.4.1 Enkripsi

Bagian ini akan dilakukan pengujian terhadap *plaintext* untuk mendapatkan hasil enkripsi dari kedua algoritma. Berikut adalah penjelasan dari perhitungan enkripsi tersebut.

Plaintext:

```
Kriptografi berfungsi untuk menjaga keamanan informasi
seperti data rahasia, integritas data, dan autentikasi sebuah
data meskipun pihak ketiga dapat membaca dan melihat isi pesan
tersebut akan tetapi ia akan sulit untuk dapat memahami isi
pesan tersebut.
```

Kunci:

```
Universitas
```

Hasil Perhitungan:

PT		**PT ASCII**		**KUNCI**		**ROT13**		**CT ASCII**		**CT**
K	=	75	+	85	+	13	=	173	=	
R	=	114	+	110	+	13	=	237	=	í
I	=	105	+	105	+	13	=	223	=	ß
P	=	112	+	118	+	13	=	243	=	ó
T	=	116	+	101	+	13	=	230	=	æ
O	=	111	+	114	+	13	=	238	=	î
G	=	103	+	115	+	13	=	231	=	ç
R	=	114	+	105	+	13	=	232	=	è
A	=	97	+	116	+	13	=	226	=	â
F	=	102	+	97	+	13	=	212	=	Ô

I	=	105	+	115	+	13	=	233	=	é
	=	32	+	85	+	13	=	130	=	,
B	=	98	+	110	+	13	=	221	=	Ý
E	=	101	+	105	+	13	=	219	=	Û
R	=	114	+	118	+	13	=	245	=	õ
F	=	102	+	101	+	13	=	216	=	Ø
U	=	117	+	114	+	13	=	244	=	ô
N	=	110	+	115	+	13	=	238	=	î
G	=	103	+	105	+	13	=	221	=	Ý
S	=	115	+	116	+	13	=	244	=	ô
I	=	105	+	97	+	13	=	215	=	×
	=	32	+	115	+	13	=	160	=	
U	=	117	+	85	+	13	=	215	=	×
N	=	110	+	110	+	13	=	233	=	é
T	=	116	+	105	+	13	=	234	=	ê
U	=	117	+	118	+	13	=	248	=	ø
K	=	107	+	101	+	13	=	221	=	Ý
	=	32	+	114	+	13	=	159	=	Ÿ
M	=	109	+	115	+	13	=	237	=	í
E	=	101	+	105	+	13	=	219	=	Û
N	=	110	+	116	+	13	=	239	=	ï
J	=	106	+	97	+	13	=	216	=	Ø
A	=	97	+	115	+	13	=	225	=	á
G	=	103	+	85	+	13	=	201	=	É
A	=	97	+	110	+	13	=	220	=	Ü
	=	32	+	105	+	13	=	150	=	–
K	=	107	+	118	+	13	=	238	=	î
E	=	101	+	101	+	13	=	215	=	×
A	=	97	+	114	+	13	=	224	=	à
M	=	109	+	115	+	13	=	237	=	í
A	=	97	+	105	+	13	=	215	=	×
N	=	110	+	116	+	13	=	239	=	ï
A	=	97	+	97	+	13	=	207	=	Ï
N	=	110	+	115	+	13	=	238	=	î
	=	32	+	85	+	13	=	130	=	,
I	=	105	+	110	+	13	=	228	=	ä
N	=	110	+	105	+	13	=	228	=	ä
F	=	102	+	118	+	13	=	233	=	é
O	=	111	+	101	+	13	=	225	=	á

R	=	114	+	114	+	13	=	241	=	ñ
M	=	109	+	115	+	13	=	237	=	í
A	=	97	+	105	+	13	=	215	=	×
S	=	115	+	116	+	13	=	244	=	ô
I	=	105	+	97	+	13	=	215	=	×
	=	32	+	115	+	13	=	160	=	
S	=	115	+	85	+	13	=	213	=	Õ
E	=	101	+	110	+	13	=	224	=	à
P	=	112	+	105	+	13	=	230	=	æ
E	=	101	+	118	+	13	=	232	=	è
R	=	114	+	101	+	13	=	228	=	ä
T	=	116	+	114	+	13	=	243	=	ó
I	=	105	+	115	+	13	=	233	=	é
	=	32	+	105	+	13	=	150	=	–
D	=	100	+	116	+	13	=	229	=	å
A	=	97	+	97	+	13	=	207	=	Ï
T	=	116	+	115	+	13	=	244	=	ô
A	=	97	+	85	+	13	=	195	=	Ã
	=	32	+	110	+	13	=	155	=	›
R	=	114	+	105	+	13	=	232	=	è
A	=	97	+	118	+	13	=	228	=	ä
H	=	104	+	101	+	13	=	218	=	Ú
A	=	97	+	114	+	13	=	224	=	à
S	=	115	+	115	+	13	=	243	=	ó
I	=	105	+	105	+	13	=	223	=	ß
A	=	97	+	116	+	13	=	226	=	â
,	=	44	+	97	+	13	=	154	=	š
	=	32	+	115	+	13	=	160	=	
I	=	105	+	85	+	13	=	203	=	Ë
N	=	110	+	110	+	13	=	233	=	é
T	=	116	+	105	+	13	=	234	=	ê
E	=	101	+	118	+	13	=	232	=	è
G	=	103	+	101	+	13	=	217	=	Ù
R	=	114	+	114	+	13	=	241	=	ñ
I	=	105	+	115	+	13	=	233	=	é
T	=	116	+	105	+	13	=	234	=	ê
A	=	97	+	116	+	13	=	226	=	â
S	=	115	+	97	+	13	=	225	=	á
	=	32	+	115	+	13	=	160	=	

D	=	100	+	85	+	13	=	198	=	Æ
A	=	97	+	110	+	13	=	220	=	Ü
T	=	116	+	105	+	13	=	234	=	ê
A	=	97	+	118	+	13	=	228	=	ä
,	=	44	+	101	+	13	=	158	=	ž
	=	32	+	114	+	13	=	159	=	Ÿ
D	=	100	+	115	+	13	=	228	=	ä
A	=	97	+	105	+	13	=	215	=	×
N	=	110	+	116	+	13	=	239	=	ï
	=	32	+	97	+	13	=	142	=	Ž
A	=	97	+	115	+	13	=	225	=	á
U	=	117	+	85	+	13	=	215	=	×
T	=	116	+	110	+	13	=	239	=	ï
E	=	101	+	105	+	13	=	219	=	Û
N	=	110	+	118	+	13	=	241	=	ñ
T	=	116	+	101	+	13	=	230	=	æ
I	=	105	+	114	+	13	=	232	=	è
K	=	107	+	115	+	13	=	235	=	ë
A	=	97	+	105	+	13	=	215	=	×
S	=	115	+	116	+	13	=	244	=	ô
I	=	105	+	97	+	13	=	215	=	×
	=	32	+	115	+	13	=	160	=	
S	=	115	+	85	+	13	=	213	=	Õ
E	=	101	+	110	+	13	=	224	=	à
B	=	98	+	105	+	13	=	216	=	Ø
U	=	117	+	118	+	13	=	248	=	ø
A	=	97	+	101	+	13	=	211	=	Ó
H	=	104	+	114	+	13	=	231	=	ç
	=	32	+	115	+	13	=	160	=	
D	=	100	+	105	+	13	=	218	=	Ú
A	=	97	+	116	+	13	=	226	=	â
T	=	116	+	97	+	13	=	226	=	â
A	=	97	+	115	+	13	=	225	=	á
	=	32	+	85	+	13	=	130	=	,
M	=	109	+	110	+	13	=	232	=	è
E	=	101	+	105	+	13	=	219	=	Û
S	=	115	+	118	+	13	=	246	=	ö
K	=	107	+	101	+	13	=	221	=	Ý
I	=	105	+	114	+	13	=	232	=	è

P	=	112	+	115	+	13	=	240	=	ð
U	=	117	+	105	+	13	=	235	=	ë
N	=	110	+	116	+	13	=	239	=	ï
	=	32	+	97	+	13	=	142	=	Ž
P	=	112	+	115	+	13	=	240	=	ð
I	=	105	+	85	+	13	=	203	=	Ë
H	=	104	+	110	+	13	=	227	=	ã
A	=	97	+	105	+	13	=	215	=	×
K	=	107	+	118	+	13	=	238	=	î
	=	32	+	101	+	13	=	146	=	’
K	=	107	+	114	+	13	=	234	=	ê
E	=	101	+	115	+	13	=	229	=	å
T	=	116	+	105	+	13	=	234	=	ê
I	=	105	+	116	+	13	=	234	=	ê
G	=	103	+	97	+	13	=	213	=	Õ
A	=	97	+	115	+	13	=	225	=	á
	=	32	+	85	+	13	=	130	=	‚
D	=	100	+	110	+	13	=	223	=	ß
A	=	97	+	105	+	13	=	215	=	×
P	=	112	+	118	+	13	=	243	=	ó
A	=	97	+	101	+	13	=	211	=	Ó
T	=	116	+	114	+	13	=	243	=	ó
	=	32	+	115	+	13	=	160	=	
M	=	109	+	105	+	13	=	227	=	ã
E	=	101	+	116	+	13	=	230	=	æ
M	=	109	+	97	+	13	=	219	=	Û
B	=	98	+	115	+	13	=	226	=	â
A	=	97	+	85	+	13	=	195	=	Ã
C	=	99	+	110	+	13	=	222	=	Þ
A	=	97	+	105	+	13	=	215	=	×
	=	32	+	118	+	13	=	163	=	£
D	=	100	+	101	+	13	=	214	=	Ö
A	=	97	+	114	+	13	=	224	=	à
N	=	110	+	115	+	13	=	238	=	î
	=	32	+	105	+	13	=	150	=	–
M	=	109	+	116	+	13	=	238	=	î
E	=	101	+	97	+	13	=	211	=	Ó
L	=	108	+	115	+	13	=	236	=	ì
I	=	105	+	85	+	13	=	203	=	Ë

H	=	104	+	110	+	13	=	227	=	ã
A	=	97	+	105	+	13	=	215	=	×
T	=	116	+	118	+	13	=	247	=	÷
	=	32	+	101	+	13	=	146	=	’
I	=	105	+	114	+	13	=	232	=	è
S	=	115	+	115	+	13	=	243	=	ó
I	=	105	+	105	+	13	=	223	=	ß
	=	32	+	116	+	13	=	161	=	¡
P	=	112	+	97	+	13	=	222	=	Þ
E	=	101	+	115	+	13	=	229	=	å
S	=	115	+	85	+	13	=	213	=	Õ
A	=	97	+	110	+	13	=	220	=	Ü
N	=	110	+	105	+	13	=	228	=	ä
	=	32	+	118	+	13	=	163	=	£
T	=	116	+	101	+	13	=	230	=	æ
E	=	101	+	114	+	13	=	228	=	ä
R	=	114	+	115	+	13	=	242	=	ò
S	=	115	+	105	+	13	=	233	=	é
E	=	101	+	116	+	13	=	230	=	æ
B	=	98	+	97	+	13	=	208	=	Ð
U	=	117	+	115	+	13	=	245	=	õ
T	=	116	+	85	+	13	=	214	=	Ö
	=	32	+	110	+	13	=	155	=	›
A	=	97	+	105	+	13	=	215	=	×
K	=	107	+	118	+	13	=	238	=	î
A	=	97	+	101	+	13	=	211	=	Ó
N	=	110	+	114	+	13	=	237	=	í
	=	32	+	115	+	13	=	160	=	
T	=	116	+	105	+	13	=	234	=	ê
E	=	101	+	116	+	13	=	230	=	æ
T	=	116	+	97	+	13	=	226	=	â
A	=	97	+	115	+	13	=	225	=	á
P	=	112	+	85	+	13	=	210	=	Ò
I	=	105	+	110	+	13	=	228	=	ä
	=	32	+	105	+	13	=	150	=	–
I	=	105	+	118	+	13	=	236	=	ì
A	=	97	+	101	+	13	=	211	=	Ó
	=	32	+	114	+	13	=	159	=	Ÿ
A	=	97	+	115	+	13	=	225	=	á

K	=	107	+	105	+	13	=	225	=	á
A	=	97	+	116	+	13	=	226	=	â
N	=	110	+	97	+	13	=	220	=	Ü
	=	32	+	115	+	13	=	160	=	
S	=	115	+	85	+	13	=	213	=	Õ
U	=	117	+	110	+	13	=	240	=	ð
L	=	108	+	105	+	13	=	226	=	â
I	=	105	+	118	+	13	=	236	=	ì
T	=	116	+	101	+	13	=	230	=	æ
	=	32	+	114	+	13	=	159	=	Ÿ
U	=	117	+	115	+	13	=	245	=	õ
N	=	110	+	105	+	13	=	228	=	ä
T	=	116	+	116	+	13	=	245	=	õ
U	=	117	+	97	+	13	=	227	=	ã
K	=	107	+	115	+	13	=	235	=	ë
	=	32	+	85	+	13	=	130	=	‚
D	=	100	+	110	+	13	=	223	=	ß
A	=	97	+	105	+	13	=	215	=	×
P	=	112	+	118	+	13	=	243	=	ó
A	=	97	+	101	+	13	=	211	=	Ó
T	=	116	+	114	+	13	=	243	=	ó
	=	32	+	115	+	13	=	160	=	
M	=	109	+	105	+	13	=	227	=	ã
E	=	101	+	116	+	13	=	230	=	æ
M	=	109	+	97	+	13	=	219	=	Û
A	=	97	+	115	+	13	=	225	=	á
H	=	104	+	85	+	13	=	202	=	Ê
A	=	97	+	110	+	13	=	220	=	Ü
M	=	109	+	105	+	13	=	227	=	ã
I	=	105	+	118	+	13	=	236	=	ì
	=	32	+	101	+	13	=	146	=	’
I	=	105	+	114	+	13	=	232	=	è
S	=	115	+	115	+	13	=	243	=	ó
I	=	105	+	105	+	13	=	223	=	ß
	=	32	+	116	+	13	=	161	=	¡
P	=	112	+	97	+	13	=	222	=	Þ
E	=	101	+	115	+	13	=	229	=	å
S	=	115	+	85	+	13	=	213	=	Õ
A	=	97	+	110	+	13	=	220	=	Ü

N	=	110	+	105	+	13	=	228	=	ä
	=	32	+	118	+	13	=	163	=	£
T	=	116	+	101	+	13	=	230	=	æ
E	=	101	+	114	+	13	=	228	=	ä
R	=	114	+	115	+	13	=	242	=	ò
S	=	115	+	105	+	13	=	233	=	é
E	=	101	+	116	+	13	=	230	=	æ
B	=	98	+	97	+	13	=	208	=	Ð
U	=	117	+	115	+	13	=	245	=	õ
T	=	116	+	85	+	13	=	214	=	Ö
.	=	46	+	110	+	13	=	169	=	©

4.4.2 Dekripsi

Bagian ini akan dilakukan pengujian terhadap ciphertext untuk mendapatkan hasil dekripsi dari kedua algoritma. Berikut adalah penjelasan dari perhitungan dekripsi tersebut.

Ciphertext:

```
-íßóæîçèâÔé,ÝÛõØôîÝô×                                    ×éêøÝŸíÛïØáÉÜ–
î×àí×ïÏî,ääéáñí×ô×                                        Õàæèäóé–
åÏôÃ›èäÚàóßâš Ëéêè Ùñéêâá ÆÜêäžŸä×ïŽá×ïÛñæèë×ô× ÕàØøÓç Úââá,è
ÛöÝèðëïŽðËã×î'êåêêÕá,ß×óÓó                               ãæÛâÃÞ×£Öàî–
îÓìËã×÷'èóß¡ÞåÕÜä£æäòéæÐõÖ›×îÓí                          êæâáÒä–
ìÓŸááâÜ Õðâìæ Ÿõäõãë,ß×óÓó ãæÛáÊÜãì'èóß¡ÞåÕÜä£æäòéæÐõÖ©
```

Kunci:

```
Universitas
```

Hasil Perhitungan:

CT		CT ASCII		KUNCI		ROT13		PT ASCII		PT
	=	173	-	85	-	13	=	75	=	K
Í	=	237	-	110	-	13	=	114	=	r

ß	=	223	-	105	-	13	=	105	=	i
Ó	=	243	-	118	-	13	=	112	=	p
Æ	=	230	-	101	-	13	=	116	=	t
Î	=	238	-	114	-	13	=	111	=	o
Ç	=	231	-	115	-	13	=	103	=	g
È	=	232	-	105	-	13	=	114	=	r
Â	=	226	-	116	-	13	=	97	=	a
Ô	=	212	-	97	-	13	=	102	=	f
É	=	233	-	115	-	13	=	105	=	i
‚	=	130	-	85	-	13	=	32	=	
Ý	=	221	-	110	-	13	=	98	=	b
Û	=	219	-	105	-	13	=	101	=	e
Õ	=	245	-	118	-	13	=	114	=	r
Ø	=	216	-	101	-	13	=	102	=	f
Ô	=	244	-	114	-	13	=	117	=	u
Î	=	238	-	115	-	13	=	110	=	n
Ý	=	221	-	105	-	13	=	103	=	g
Ô	=	244	-	116	-	13	=	115	=	s
×	=	215	-	97	-	13	=	105	=	i
	=	160	-	115	-	13	=	32	=	
×	=	215	-	85	-	13	=	117	=	u
É	=	233	-	110	-	13	=	110	=	n
Ê	=	234	-	105	-	13	=	116	=	t
Ø	=	248	-	118	-	13	=	117	=	u
Ý	=	221	-	101	-	13	=	107	=	k
Ÿ	=	159	-	114	-	13	=	32	=	
Í	=	237	-	115	-	13	=	109	=	m
Û	=	219	-	105	-	13	=	101	=	e
Ï	=	239	-	116	-	13	=	110	=	n
Ø	=	216	-	97	-	13	=	106	=	j
Á	=	225	-	115	-	13	=	97	=	a
É	=	201	-	85	-	13	=	103	=	g
Ü	=	220	-	110	-	13	=	97	=	a
–	=	150	-	105	-	13	=	32	=	
Î	=	238	-	118	-	13	=	107	=	k
×	=	215	-	101	-	13	=	101	=	e
À	=	224	-	114	-	13	=	97	=	a
Í	=	237	-	115	-	13	=	109	=	m
×	=	215	-	105	-	13	=	97	=	a

Ï	=	239	-	116	-	13	=	110	=	n
Ï	=	207	-	97	-	13	=	97	=	a
Î	=	238	-	115	-	13	=	110	=	n
,	=	130	-	85	-	13	=	32	=	
Ä	=	228	-	110	-	13	=	105	=	i
Ä	=	228	-	105	-	13	=	110	=	n
É	=	233	-	118	-	13	=	102	=	f
Á	=	225	-	101	-	13	=	111	=	o
Ñ	=	241	-	114	-	13	=	114	=	r
Í	=	237	-	115	-	13	=	109	=	m
×	=	215	-	105	-	13	=	97	=	a
Ô	=	244	-	116	-	13	=	115	=	s
×	=	215	-	97	-	13	=	105	=	i
	=	160	-	115	-	13	=	32	=	
Õ	=	213	-	85	-	13	=	115	=	s
À	=	224	-	110	-	13	=	101	=	e
Æ	=	230	-	105	-	13	=	112	=	p
È	=	232	-	118	-	13	=	101	=	e
Ä	=	228	-	101	-	13	=	114	=	r
Ó	=	243	-	114	-	13	=	116	=	t
É	=	233	-	115	-	13	=	105	=	i
–	=	150	-	105	-	13	=	32	=	
Å	=	229	-	116	-	13	=	100	=	d
Ï	=	207	-	97	-	13	=	97	=	a
Ô	=	244	-	115	-	13	=	116	=	t
Ã	=	195	-	85	-	13	=	97	=	a
›	=	155	-	110	-	13	=	32	=	
È	=	232	-	105	-	13	=	114	=	r
Ä	=	228	-	118	-	13	=	97	=	a
Ú	=	218	-	101	-	13	=	104	=	h
À	=	224	-	114	-	13	=	97	=	a
Ó	=	243	-	115	-	13	=	115	=	s
ß	=	223	-	105	-	13	=	105	=	i
Â	=	226	-	116	-	13	=	97	=	a
Š	=	154	-	97	-	13	=	44	=	,
	=	160	-	115	-	13	=	32	=	
Ë	=	203	-	85	-	13	=	105	=	i
É	=	233	-	110	-	13	=	110	=	n
Ê	=	234	-	105	-	13	=	116	=	t

È	=	232	-	118	-	13	=	101	=	e
Ù	=	217	-	101	-	13	=	103	=	g
Ñ	=	241	-	114	-	13	=	114	=	r
É	=	233	-	115	-	13	=	105	=	i
Ê	=	234	-	105	-	13	=	116	=	t
Â	=	226	-	116	-	13	=	97	=	a
Á	=	225	-	97	-	13	=	115	=	s
	=	160	-	115	-	13	=	32	=	
Æ	=	198	-	85	-	13	=	100	=	d
Ü	=	220	-	110	-	13	=	97	=	a
Ê	=	234	-	105	-	13	=	116	=	t
Ä	=	228	-	118	-	13	=	97	=	a
Ž	=	158	-	101	-	13	=	44	=	,
Ÿ	=	159	-	114	-	13	=	32	=	
Ä	=	228	-	115	-	13	=	100	=	d
×	=	215	-	105	-	13	=	97	=	a
Ï	=	239	-	116	-	13	=	110	=	n
Ž	=	142	-	97	-	13	=	32	=	
Á	=	225	-	115	-	13	=	97	=	a
×	=	215	-	85	-	13	=	117	=	u
Ï	=	239	-	110	-	13	=	116	=	t
Û	=	219	-	105	-	13	=	101	=	e
Ñ	=	241	-	118	-	13	=	110	=	n
Æ	=	230	-	101	-	13	=	116	=	t
È	=	232	-	114	-	13	=	105	=	i
Ë	=	235	-	115	-	13	=	107	=	k
×	=	215	-	105	-	13	=	97	=	a
Ô	=	244	-	116	-	13	=	115	=	s
×	=	215	-	97	-	13	=	105	=	i
	=	160	-	115	-	13	=	32	=	
Õ	=	213	-	85	-	13	=	115	=	s
À	=	224	-	110	-	13	=	101	=	e
Ø	=	216	-	105	-	13	=	98	=	b
Ø	=	248	-	118	-	13	=	117	=	u
Ó	=	211	-	101	-	13	=	97	=	a
Ç	=	231	-	114	-	13	=	104	=	h
	=	160	-	115	-	13	=	32	=	
Ú	=	218	-	105	-	13	=	100	=	d
Â	=	226	-	116	-	13	=	97	=	a

Â	=	226	-	97	-	13	=	116	=	t
Á	=	225	-	115	-	13	=	97	=	a
‚	=	130	-	85	-	13	=	32	=	
È	=	232	-	110	-	13	=	109	=	m
Û	=	219	-	105	-	13	=	101	=	e
Ö	=	246	-	118	-	13	=	115	=	s
Ý	=	221	-	101	-	13	=	107	=	k
È	=	232	-	114	-	13	=	105	=	i
Ð	=	240	-	115	-	13	=	112	=	p
Ë	=	235	-	105	-	13	=	117	=	u
Ï	=	239	-	116	-	13	=	110	=	n
Ž	=	142	-	97	-	13	=	32	=	
Ð	=	240	-	115	-	13	=	112	=	p
Ë	=	203	-	85	-	13	=	105	=	i
Ã	=	227	-	110	-	13	=	104	=	h
×	=	215	-	105	-	13	=	97	=	a
Î	=	238	-	118	-	13	=	107	=	k
’	=	146	-	101	-	13	=	32	=	
Ê	=	234	-	114	-	13	=	107	=	k
Å	=	229	-	115	-	13	=	101	=	e
Ê	=	234	-	105	-	13	=	116	=	t
Ê	=	234	-	116	-	13	=	105	=	i
Õ	=	213	-	97	-	13	=	103	=	g
Á	=	225	-	115	-	13	=	97	=	a
‚	=	130	-	85	-	13	=	32	=	
ß	=	223	-	110	-	13	=	100	=	d
×	=	215	-	105	-	13	=	97	=	a
Ó	=	243	-	118	-	13	=	112	=	p
Ó	=	211	-	101	-	13	=	97	=	a
Ó	=	243	-	114	-	13	=	116	=	t
	=	160	-	115	-	13	=	32	=	
Ã	=	227	-	105	-	13	=	109	=	m
Æ	=	230	-	116	-	13	=	101	=	e
Û	=	219	-	97	-	13	=	109	=	m
Â	=	226	-	115	-	13	=	98	=	b
Ã	=	195	-	85	-	13	=	97	=	a
Þ	=	222	-	110	-	13	=	99	=	c
×	=	215	-	105	-	13	=	97	=	a
£	=	163	-	118	-	13	=	32	=	

Ö	=	214	-	101	-	13	=	100	=	d
À	=	224	-	114	-	13	=	97	=	a
Î	=	238	-	115	-	13	=	110	=	n
–	=	150	-	105	-	13	=	32	=	
Î	=	238	-	116	-	13	=	109	=	m
Ó	=	211	-	97	-	13	=	101	=	e
Ì	=	236	-	115	-	13	=	108	=	l
Ë	=	203	-	85	-	13	=	105	=	i
Ã	=	227	-	110	-	13	=	104	=	h
×	=	215	-	105	-	13	=	97	=	a
÷	=	247	-	118	-	13	=	116	=	t
’	=	146	-	101	-	13	=	32	=	
È	=	232	-	114	-	13	=	105	=	i
Ó	=	243	-	115	-	13	=	115	=	s
ß	=	223	-	105	-	13	=	105	=	i
¡	=	161	-	116	-	13	=	32	=	
Þ	=	222	-	97	-	13	=	112	=	p
Å	=	229	-	115	-	13	=	101	=	e
Õ	=	213	-	85	-	13	=	115	=	s
Ü	=	220	-	110	-	13	=	97	=	a
Ä	=	228	-	105	-	13	=	110	=	n
£	=	163	-	118	-	13	=	32	=	
Æ	=	230	-	101	-	13	=	116	=	t
Ä	=	228	-	114	-	13	=	101	=	e
Ò	=	242	-	115	-	13	=	114	=	r
É	=	233	-	105	-	13	=	115	=	s
Æ	=	230	-	116	-	13	=	101	=	e
Ð	=	208	-	97	-	13	=	98	=	b
Õ	=	245	-	115	-	13	=	117	=	u
Ö	=	214	-	85	-	13	=	116	=	t
›	=	155	-	110	-	13	=	32	=	
×	=	215	-	105	-	13	=	97	=	a
Î	=	238	-	118	-	13	=	107	=	k
Ó	=	211	-	101	-	13	=	97	=	a
Í	=	237	-	114	-	13	=	110	=	n
	=	160	-	115	-	13	=	32	=	
Ê	=	234	-	105	-	13	=	116	=	t
Æ	=	230	-	116	-	13	=	101	=	e
Â	=	226	-	97	-	13	=	116	=	t

Á	=	225	-	115	-	13	=	97	=	a
Ò	=	210	-	85	-	13	=	112	=	p
Ä	=	228	-	110	-	13	=	105	=	i
–	=	150	-	105	-	13	=	32	=	
Ì	=	236	-	118	-	13	=	105	=	i
Ó	=	211	-	101	-	13	=	97	=	a
Ÿ	=	159	-	114	-	13	=	32	=	
Á	=	225	-	115	-	13	=	97	=	a
Á	=	225	-	105	-	13	=	107	=	k
Â	=	226	-	116	-	13	=	97	=	a
Ü	=	220	-	97	-	13	=	110	=	n
	=	160	-	115	-	13	=	32	=	
Õ	=	213	-	85	-	13	=	115	=	s
Ð	=	240	-	110	-	13	=	117	=	u
Â	=	226	-	105	-	13	=	108	=	l
Ì	=	236	-	118	-	13	=	105	=	i
Æ	=	230	-	101	-	13	=	116	=	t
Ÿ	=	159	-	114	-	13	=	32	=	
Õ	=	245	-	115	-	13	=	117	=	u
Ä	=	228	-	105	-	13	=	110	=	n
Õ	=	245	-	116	-	13	=	116	=	t
Ã	=	227	-	97	-	13	=	117	=	u
Ë	=	235	-	115	-	13	=	107	=	k
‚	=	130	-	85	-	13	=	32	=	
ß	=	223	-	110	-	13	=	100	=	d
×	=	215	-	105	-	13	=	97	=	a
Ó	=	243	-	118	-	13	=	112	=	p
Ó	=	211	-	101	-	13	=	97	=	a
Ó	=	243	-	114	-	13	=	116	=	t
	=	160	-	115	-	13	=	32	=	
Ã	=	227	-	105	-	13	=	109	=	m
Æ	=	230	-	116	-	13	=	101	=	e
Û	=	219	-	97	-	13	=	109	=	m
Á	=	225	-	115	-	13	=	97	=	a
Ê	=	202	-	85	-	13	=	104	=	h
Ü	=	220	-	110	-	13	=	97	=	a
Ã	=	227	-	105	-	13	=	109	=	m
Ì	=	236	-	118	-	13	=	105	=	i
’	=	146	-	101	-	13	=	32	=	

È	=	232	-	114	-	13	=	105	=	i
Ó	=	243	-	115	-	13	=	115	=	s
ß	=	223	-	105	-	13	=	105	=	i
¡	=	161	-	116	-	13	=	32	=	
Þ	=	222	-	97	-	13	=	112	=	p
Å	=	229	-	115	-	13	=	101	=	e
Õ	=	213	-	85	-	13	=	115	=	s
Ü	=	220	-	110	-	13	=	97	=	a
Ä	=	228	-	105	-	13	=	110	=	n
£	=	163	-	118	-	13	=	32	=	
Æ	=	230	-	101	-	13	=	116	=	t
Ä	=	228	-	114	-	13	=	101	=	e
Ò	=	242	-	115	-	13	=	114	=	r
É	=	233	-	105	-	13	=	115	=	s
Æ	=	230	-	116	-	13	=	101	=	e
Ð	=	208	-	97	-	13	=	98	=	b
Õ	=	245	-	115	-	13	=	117	=	u
Ö	=	214	-	85	-	13	=	116	=	t
©	=	169	-	110	-	13	=	46	=	.

BAB V

PENUTUP

5.1 Kesimpulan

Dari pembahasan yang dilakukan pada bab-bab sebelumnya, dapat ditarik beberapa kesimpulan, antara lain:

1. Algoritma Beaufort bekerja dengan cara menggeser ASCII dari plaintext sebesar kunci yang digunakan.
2. Kunci akan dikembangkan sesuai dengan panjang plaintext dengan menciptakan karakter tambahan yang diambil dari perulangan kunci tersebut.
3. ROT13 akan menambah pergeseran sebesar 13 pada saat proses enkripsi dan mengurangi pergeseran sebesar 13 juga pada proses dekripsi.
4. Nilai cipher yang lebih besar dari 255 akan di modulo dengan 256 sesuai dengan batasan karakter pada tabel ASCII.

5.2 Saran

Dari hasil pengujian terdapat beberapa saran untuk mengembangkan penelitian ini agar lebih baik dan terarah. Adapun saran tersebut antara lain:

1. Algoritma Beaufort dapat dilakukan skema Three-pass Protocol agar menghindari pertukaran kunci.
2. Algoritma Beaufort hendaknya dikombinasikan dengan algoritma lain agar meningkatkan keamanan data.

DAFTAR PUSTAKA

Andrian, Yudhi, and Purwa Hasan Putra. "Analisis Penambahan Momentum Pada Proses Prediksi Curah Hujan Kota Medan Menggunakan Metode Backpropagation Neural Network." Seminar Nasional Informatika (SNIf). Vol. 1. No. 1. 2017.

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi*.

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

Azmi, Fadhillah, And Winda Erika. "Analisis Keamanan Data Pada Block Cipher Algoritma Kriptografi Rsa." Cess (Journal Of Computer Engineering, System And Science) 2.1: 27-29.

Bhatia, S., & Mitra, P. (2012). Summarizing figures, tables, and algorithms in scientific publications to augment search results. *ACM Transactions on Information Systems*, *30*(1), 1–24. https://doi.org/10.1145/2094072.2094075

Delfs, H., & Knebl, H. (2015). Symmetric-Key Cryptography (pp. 11–48). https://doi.org/10.1007/978-3-662-47974-2_2

Dony Ariyus. (2008). *Pengantar Ilmu Kriptografi*. (FI sigit suyantoro, Ed.).

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

Firmansyah, E. R. (2012). Algoritma Kriptografi & Contohnya. *Universitas Islam Negeri Syarif Hidayatullah Jakarta*.

… Frieder, O. (2009). Asymmetric Encryption. In *Encyclopedia of Database*

Hafni, Layla, And Rismawati Rismawati. "Analisis Faktor-Faktor Internal Yang Mempengaruhi Nilai Perusahaan Pada Perusahaan Manufaktur Yang Terdaftar Di Bei 2011-2015." Bilancia: Jurnal Ilmiah Akuntansi 1.3 (2017): 371-382.

Hamdi, Muhammad Nurul, Evi Nurjanah, And Latifah Safitri Handayani. "Community Development Based Onibnu Khaldun Thought, Sebuah Interpretasi Program

Pemberdayaan Umkm Di Bank Zakat El-Zawa." El Muhasaba: Jurnal Akuntansi (E-Journal) 5.2 (2014): 158-180.

Indra Permana, Aminuddin "Sistem Pakar Mendeteksi Hama Dan Penyakit Tanaman Kelapa Sawit Pada Pt. Moeis Kebun Sipare-Pare Kabupaten Batubara." (2013).

Jensen, C. S., Snodgrass, R. T., Chomicki, J., Toman, D., Thalheim, B., Ferrari, E.,

JESFER ROBIN ARIOS. (2018). Implementasi Algoritma Kriptografi Beaufort Cipher dan Algoritma Kompresi Reverse Unary Code Pada File Citra. *Universitas Sumatera Utara Repositori Institusi USU*, 8.

Jogiyanto, H. M. (2006). *Analisis Dan Desain Sistem Informasi, Pendekatan Terstruktur Teori Dan Praktek Aplikasi Bisnis*. Yogyakarta: Andi Offset.

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

Marwati, R., & Yulianti, K. (2018). Cryptanalysis on classical cipher based on Indonesian language. *Journal of Physics: Conference Series*, *1013*, 012147. https://doi.org/10.1088/1742-6596/1013/1/012147

Muhammad Khoiruddin Harahap, & Khairina, N. (2017). Analisis Algoritma One Time Pad Dengan Algoritma Cipher Transposisi Sebagai Pengamanan Pesan Teks. *Jurnal & Penelitian Teknik Informatika*, *1*, 59.

Muttaqin, Muhammad. "Portal Academic Portal Innovation Based On Website In The Era Of Digital 4.0 Technology Now."

Oktaviana, B., & Siahaan, A. P. U. (2016). Three-Pass Protocol Implementation on Caesar Cipher in Classic Cryptography. *IOSR Journal of Computer Engineering*, *18*(4), 26–29.

Pabokory, F. N., Astuti, I. F., & Kridalaksana, A. H. (2015). Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Informatika Mulawarman : Jurnal Ilmiah Ilmu Komputer*, *10*, 22. https://doi.org/10.30872/jim.v10i1.23

Permana, A. I., and Z. Tulus. "Combination of One Time Pad Cryptography Algorithm with Generate Random Keys and Vigenere Cipher with EM2B KEY." (2020).

Permana, Aminuddin Indra. "Kombinasi Algoritma Kriptografi One Time Pad dengan Generate Random Keys dan Vigenere Cipher dengan Kunci EM2B." (2019).

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

Prayitno, A., & Nurdin, N. (2017). Analisa dan implementasi Kriptografi pada Pesan Rahasia menggunakan Algoritma Cipher Transposition. *Jurnal Eletronik Sistem & Komputer*, *3*, 2–5.

Puspita, Khairani, and Purwa Hasan Putra. "Penerapan Metode Simple Additive Weighting (SAW) Dalam Menentukan Pendirian Lokasi Gramedia Di Sumatera Utara." Seminar Nasional Teknologi Informasi Dan Multimedia, ISSN. 2015.

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

Robins, A., Rountree, J., & Rountree, N. (2003). Learning and Teaching Programming: A Review and Discussion. *Computer Science Education*, *13*(2), 137–172. https://doi.org/10.1076/csed.13.2.137.14200

SEMINAR MATEMATIKA DAN PENDIDIKAN MATEMATIKA.

Siahaan, A. P. U. (2016). A Three-Layer Visual Hash Function Using Adler-32. *International Journal of Computer Science and Software Engineering*, *5*(7), 142–147.

Skiena, S. S. (2008). *The Algorithm Design Manual*. London: Springer London. https://doi.org/10.1007/978-1-84800-070-4

Sumandri. (2017). Studi Model Algoritma Kriptografi Klasik dan Modern.

Syahputra, Rizki, And Hafni Hafni. "Analisis Kinerja Jaringan Switching Clos Tanpa Buffer." Journal Of Science And Social Research 1.2 (2018): 109-115.

Systems (pp. 142–142). Boston, MA: Springer US. https://doi.org/10.1007/978-0-387-39940-9_1485

Wahyuni, Sri. "Implementasi Rapidminer Dalam Menganalisa Data Mahasiswa Drop Out." Jurnal Abdi Ilmu 10.2 (2018): 1899-1902.

Yogyakarta: Andi Offset.

Yogyakarta: Andi Offset.