IMPLEMENTASI ALGORITMA VIGENERE CIPHER UNTUK KEAMANAN DATA

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	**: ARINI RAMADHAYANTY**
NPM	**: 1624371032**
PROGRAM STUDI	**: SISTEM KOMPUTER**

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

IMPLEMENTASI ALGORITMA VIGENERE CIPHER UNTUK KEAMANAN DATA

Disusun dan Diajukan Sebagai Salah Satu Syarat Untuk Menempuh Ujian Akhir
Memperoleh Gelar Sarjana Komputer Pada Fakultas Sains dan Teknologi
Universitas Pembangunan Panca Budi
Medan

SKRIPSI

OLEH

NAMA : ARINI RAMADHAYANTY
N.P.M : 1624371032
PROGRAM STUDI : SISTEM KOMPUTER

Skripsi Telah Disetujui oleh Dosen Pembimbing Skripsi
Pada Tanggal : 22 Agustus 2019

Dosen Pembimbing I	Dosen Pembimbing II
Andysah P. U. Siahaan, S.Kom, M.Kom., Ph.D.	Dr. Muhammad Iqbal, S.Kom., M.Kom.

Mengetahui,

Dekan Fakultas Sains dan Teknologi	Ketua Program Studi Sistem Komputer
Sri Shindi Indira, S.T., M.Sc.	Dr. Muhammad Iqbal, S.Kom., M.Kom.

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI

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

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

PERMOHONAN MENGAJUKAN JUDUL SKRIPSI

) yang bertanda tangan di bawah ini :

a Lengkap	: **ARINI RAMADHAYANTY**
pat/Tgl. Lahir	: **MEDAN / 09 Maret 1993**
or Pokok Mahasiswa	: **1624371032**
ram Studi	: **Sistem Komputer**
entrasi	: **Sistem Kendali Komputer**
lah Kredit yang telah dicapai	: **133 SKS, IPK 3.23**

an ini mengajukan judul skripsi sesuai dengan bidang ilmu, **dengan judul:**

Judul Skripsi	Persetujuan
Sistem Informasi Mutasi Pegawai pada kantor Pengadilan Agama Kota Binjai	☐
Rancangan Bangun Sistem Informasi Penggajian Pegawai pada kantor Pengadilan Agama Kota Binjai	☒
Implementasi Algoritma Vigener Cipher untuk keamanan data pada kantor Pengadilan Agama Kota Binjai	☑

ul yang disetujui oleh Kepala Program Studi diberikan tanda ☑

Rektor I,

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

Medan, 07 April 2018

Pemohon,

(ARINI RAMADHAYANTY)

Nomor : .....

Tanggal : .....

Disahkan oleh :

Dekan

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

Tanggal : 28 April 2018

Disetujui oleh:

Ka. Prodi Sistem Komputer

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

Tanggal : .....

Disetujui oleh :

Dosen Pembimbing I :

(.....)

Tanggal : .....

Disetujui oleh:

Dosen Pembimbing II:

(.....)

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

versitas : Universitas Pembangunan Panca Budi
ultas : SAINS & TEKNOLOGI
sen Pembimbing I : ANDYSAH PUTERA UTAMA SIAHAAN, S.Kom, M.Kom
sen Pembimbing II : DEBI YANDRA NISKA, S.Kom, M.Kom
na Mahasiswa : ARINI RAMADHAYANTY
usan/Program Studi : Sistem Komputer
nor Pokok Mahasiswa : 1624371032
jang Pendidikan :
ul Tugas Akhir/Skripsi : Implementasi Algoritma Vigenere Cipher untuk keamanan data

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
21/4 2018	Revisi Proposal		
4/5	Pembahasan Judul		
15/6	Revisi Bab I		
1/7	Revisi Bab II		
4/7	Revisi Bab II, III		
10/7	Revisi Bab III, IV		
13/7	Acc Seminar		
1/11 2018	Acc Sidang		
9/8 2019	Acc Judul		

Medan, 14 Juli 2018
Diketahui/Disetujui oleh :
Dekan,

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

FM-BPAA-2012-0

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 : DEBI YANDRA NISKA, S.Kom, M.Kom
ma Mahasiswa : ARINI RAMADHAYANTY
usan/Program Studi : Sistem Komputer
mor Pokok Mahasiswa : 1624371032
jang Pendidikan :
ul Tugas Akhir/Skripsi : Implementasi Algoritma Vigenere Cipher untuk keamanan data

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
13/7 18	Perbaiki BAB I	[signature]	
/9 18	Perbaiki BAB I, Lanjut BAB II	[signature]	
/9 18	Perbaiki BAB I & II, Lanjut BAB III	[signature]	
/10 18	Perbaiki BAB III, Lihat Program	[signature]	
/8 18	Cetak Keseluruhan	[signature]	
/8 18	ACC Seminar	[signature]	
/1 18	ACC Sidang	[signature]	
/9	Revisi [illegible] [illegible]	[signature]	
/9	Acc Jilid	[signature]	

Medan, 14 Juli 2018
Diketahui/Disetujui oleh :
Dekan,

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

TANDA BEBAS PUSTAKA
No. 1/perp/BP/2018
Dinyatakan tidak ada sangkut paut dengan UPT. Perpustakaan
Medan, 08 DEC 2018
Ka. UPT. Perpustakaan

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau

Medan, 13 November 2018
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

Telah Diperiksa oleh LPMU
dengan Plagiarisme 55 %
Medan, 5 Januari 2018
Ka. LPMU
Cahyo Pramono, SE,MM

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	: ARINI RAMADHAYANTY
Tempat/Tgl. Lahir	: MEDAN / 09 Maret 1993
Nama Orang Tua	: DRS.M.HARLIM AFRIANTO
N. P. M	: 1624371032
Fakultas	: SAINS & TEKNOLOGI
Program Studi	: Sistem Komputer
No. HP	: 085361000532
Alamat	: JL. KELAMBIR 5

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **Implementasi Algoritma Vigener Cipher untuk keamanan data**, 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
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~~
	s. Uk. Termin bersalan	Rp	2.205.000
			4.200.000
			6.405.000

08/11-18

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

Hormat saya
ARINI RAMADHAYANTY
1624371032

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.

Telah di terima berkas persyaratan dapat di proses
Medan, 27 APR 2019
an. Ka. BPAA
TEGUH WAHYONO, SE.

yang tidak perlu

Plagiarism Detector v. 1092 - Originality Report:

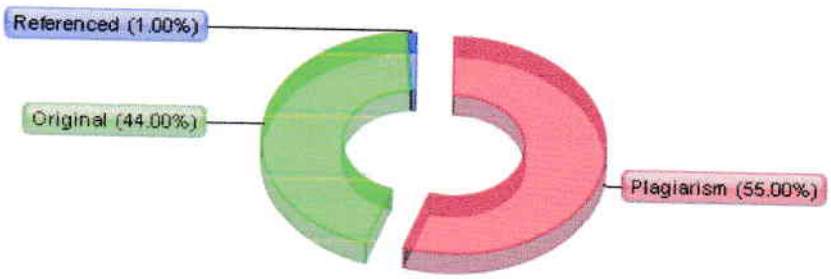
Analyzed document: 26-12-18 7:51:00 AM

"ARINI RAMADHAYANTY_1624371032_SISTEM KOMPUTER.docx"

Licensed to: **Universitas Pembangunan Panca Budi_License2**

UNIVERSITAS PEMBANGUNAN PANCA BUDI
Berimtan, Berilmu, Berkarya

Relation chart:



Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

Top sources of plagiarism:

% 143	wrds: 14204	http://gilangokto.blogspot.com/
% 108	wrds: 11063	http://www.vbforums.com/showthread.php?502451-What-does-(ByVal-sender-As-System-Object-ByV...
% 96	wrds: 9706	http://argaonthespot.blogspot.com/

ow other Sources:]

Processed resources details:

304 - Ok / 61 - Failed

ow other Sources:]

Important notes:

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	:	ARINI RAMADHAYANTY
N.P.M.	:	1624371032
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, 13 Desember 2018
Ka. Laboratorium

YAYASAN PROF. DR. H. KADIRUN YAHYA MEDAN LABORATORIUM KOMPUTER INDONESIA KAMPUS PANCA BUDI

Fachrid Wadly, S. Kom

SURAT PERNYATAAN

aya yang bertanda tangan di bawah ini :

lama	:	ARINI RAMADHAYANTY
IPM	:	162437P032
rodi	:	SISTEM KOMPUTER
onsentrasi	:	SISTEM KENDALI KOMPUTER
udul Skripsi	:	IMPLEMENTASI ALGORITMA VIGENERE CHIPHERE UNTUK KEAMANAN DATA

Dengan ini menyatakan bahwa :

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

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

Medan, 29 AGUSTUS 2019

Yang membuat pernyataan

ARINI RAMADHAYANTY

ABSTRAK

ARINI RAMADHAYANTY

IMPLEMENTASI ALGORITMA VIGENERE CIPHERE UNTUK

KEAMANAN DATA

2019

Kriptografi merupakan salah satu metode mengamankan data yang dapat digunakan untuk menjaga kerahasiaan data, keaslian data sera keaslian pengirim. Metode ini bertujuan agar informasi yang bersifat rahasia yang dikirm melalui telekomunikasi umum seperti LAN atau Internet. Kriptografi biasanya dalam bentuk enkripsi dan Deskripsi. Untuk menyembunyikan tulisan, biasanya mengguakan algoritma. Algoritma yang dipakai dalam aplikasi ini adalah Algoritma Vigenere Cipher. Dalam hal ini, penulis berkeinginan mengangkat topik enkripsi dan deskripsi menjadi sebuah penulisan ilmiah skripsi dengan menggunakan visual studio yang berkembang saat ini. Diharapkan dengan adanya aplikasi ini, mahasiswa serta dosen dapat melakukan uji coba enkripsi menggunakan algoritma Vigenere Cipher.

Kata Kunci: Kriptografi, Vigenere Cipher.

DAFTAR ISI

Halaman

DAFTAR GAMBAR

No Judul **Hal**

DAFTAR TABEL

BAB I

PENDAHULUAN

1. Latar Belakang

Keamanan data dan informasi merupakan hal yang sangat penting di era informasi saat ini. Umumnya, setiap institusi memiliki dokumen-dokumen penting dan bersifat rahasia yang hanya boleh diakses oleh orang tertentu. Sistem informasi yang dikembangkan harus menjamin keamanan dan kerahasian dokumen-dokumen tersebut. Namun kendalanya bahwa media-media yang digunakan sering kali dapat disadap oleh pihak lain. Oleh karena itu, diperlukan metode untuk mengamankannya, salah satunya dengan menggunakan metode *kriptografi*.

Dalam *kriptografi*, penulis ini membuat keamanan pesan menggunakan metode algoritma *vigenere cipher*. Proses pengamanan pesan tersebut hanya berupa text yang dikirim, dan penerima harus memiliki kunci untuk membuka pesan asli. Dengan adanya vigenere ini pesan teks yang muncul berupa hasil dari algoritma tersebut. Saat ini, ilmu kriptografi semakin banyak digunakan dan mulai berubah menjadi kebutuhan. Dengan maraknya perkembangan ilmu dan teknologi, informasi-informasi penting pun tidak lagi hanya berada pada media tulis saja.

Penulis akan membuat suatu aplikasi penerapan algoritma *vigenere* dengan menggunakan sistem yang berbasiskan desktop. Aplikasi yang akan penulis rancang adalah sebagai penerapan *algoritma vigenere* agar dapat memahami cara teknik

enkripsi dan dekripsi data teks yang digunakan kepada pengguna yang masih awam dalam teknik manipulasi data tersebut. Berdasarkan latar belakang diatas maka penulis tertarik untuk memilih judul "**Implementasi Algoritma *Vigenere Cipher* untuk Keamanan Data**".

2. Rumusan Masalah

Berdasarkan latar belakang masalah di atas maka rumusan masalah adalah sebagai berikut :

a. Bagaimana merancang sebuah aplikasi *enkripsi* dan *deskripsi* teks menggunakan algoritma *vigenere* sebagai pengaman informasi teks?
b. Bagaimana membuat aplikasi *enkripsi* dan *deskripsi* berbasis destop?

3. Batasan Masalah

Dalam perancangan aplikasi pengamanan informasi ini penulis membatasi masalah sebagai berikut :

a. Aplikasi yang dibangun hanya melakukan *enkripsi* dan *deskripsi* informasi *text*.
b. Perancangan aplikasi merupakan simulasi
c. Program yang digunakan dalam perancangan aplikasi ini adalah *visual basic .net 2010* menggunakan algoritma vigenere cipher dalam proses enkripsi dan dekripsi.

4. Tujuan Penelitian

Tujuan yang ingin dicapai penulis dalam perancangan aplikasi penerapan algoritma *vigenere* ini adalah :

a. Merancang aplikasi keamanan informasi text dengan menggunakan algoritma *vigenere cipher*.
b. Merancang sistem pengamanan informasi text dengan proses enkripsi dan dekripsi menggunakan metode algoritma *vigenere cipher*.

5. Manfaat Penelitian

Perancangan aplikasi penerapan *algoritma vigenere* ini bermanfaat bagi masyarakat luas antara lain :

a. Dengan menggunakan aplikasi ini seseorang dapat mengamankan suatu informasi tanpa perlu mengkhawatirkan dilihat oleh orang lain.
b. Dapat digunakan dalam proses keamanan data.
c. Proses pertukaran data atau informasi menjadi aman.

6. Metodologi Penelitian

Metode Pengumpulan Data yang digunakan dalam penelitian ini adalah metode deskriptif. Adapun teknik pengumpulan data dilakukan dengan cara sebagai berikut:

a) Studi literature

Pengumpulan data dengan cara mengumpulkan *literature*, jurnal, *paper* dan

bacaan-bacaan yang ada kaitannya dengan judul penelitian.

b) Studi Pustaka

Pengumpulan data dengan menggunakan atau mengumpulkan sumber-sumber tertulis, dengan cara membaca, mempelajari dan mencatat hal-hal penting yang berhubungan dengan masalah yang sedang dibahas guna memperoleh gambaran secara teoritis.

7. Sistematika Penulisan

Adapun struktur penulisan pada masing-masing bab dalam laporan tugas akhir ini adalah sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini memaparkan mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini mengaji teori-teori yang didapat dari sumber-sumber yang relevan untuk digunakan sebagai panduan dalam penelitian serta alat perancangan yang digunakan dalam penyusunan skripsi.

BAB III PERANCANGAN SISTEM

BAB IV Bab ini membahas perancangan tentang gambaran sistem serta deskripsi dari hasil analisis sistem yang akan dijadikan sebagai petunjuk untuk perancangan sistem selanjutnya.

IMPLEMENTASI SISTEM

BAB V Bab ini menguraikan langkah-langkah dalam implementasi sistem, disertai dengan komponen-komponen kebutuhan sistem.

PENUTUP

Merupakan bab yang memaparkan kesimpulan beserta saran-saran atas penelitian yang dibuat.

BAB II

LANDASAN TEORI

1. Aplikasi

Aplikasi adalah alat bantu untuk mempermudah dan mempercepat proses pekerjaan dan bukan merupakan beban bagi para penggunanya, atau aplikasi adalah satu unit perangkat lunak yang dibuat untuk melayani kebutuhan akan beberapa aktivitas seperti sistem perniagaan, *game*, pelayanan masyarakat, periklanan, atau semua proses yang hampir dilakukan manusia. Aplikasi berguna untuk melakukan pengolahan data maupun kegiatan-kegiatan seperti pembuatan dokumen atau pengolahan data Aplikasi adalah bagian PC yang berinteraksi langsung dengan *user*. Aplikasi berjalan di atas sistem operasi, sehingga agar aplikasi bisa diaktifkan perlu melakukan instalasi sistem operasi terlebih dahulu.

2. Kriptografi

a. Pengertian kriptografi

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti secret (rahasia) dan *graphia* berarti writing (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Dalam perkembangannya, *kriptografi* juga digunakan untuk mengidentifikasi

pengiriman pesan dan tanda tangan digital dan keaslian pesan dengan sidik jari digital. (*Dony Ariyus, 2005*)

Di dalam kriptografi kita akan sering menemukan berbagai istilah atau terminology. Beberapa istilah yang harus diketahui yaitu :

1. Pesan, plaintext, dan cipherteks

   Pesan (*message*) adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah (*plaintext*) atau teks jelas (*cleartext*). Agar pesan tidak dapat dimengerti maknanya oleh pihak lain yang tidak berkepentingan, maka pesan perlu disandikan kebentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut cipherteks atau kriptogram. Cipherteks harus dapat ditransformasikan kembali menjadi plaintext semula agar dapat diterima dan bisa dibaca.

2. Pengirim dan penerima

   Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sender*) adalah entitas yang mengirim pesan kepada entitas lainnya. Penerima (*receiver*) adalah entitas yang menerima pesan. Pengirim tentu menginginkan pesan dapat dikirm secara aman, yaitu pengirim yakin bahwa pihak lain tidak dapat membaca isi pesan yang dikirim. Solusinya adalah dengan cara menyandikan pesan menjadi cipherteks.

3. Enkripsi dan dekripsi

Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (*encryption*) atau *enciphering*. Sedangkan proses mengembalikan cipherteks menjadi plainteks disebut dekripsi (*decryption*) atau *deciphering*.

4. Cipher dan kunci

   Algoritma kriptogarfi disebut juga *cipher*, yaitu aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Beberapa *cipher* memerlukan algoritma yang berbeda untuk *enciphering* dan *deciphering*.

   Konsep matematis yang mendasari algoritma kriptografi adalah relasi antara dua buah himpunan yang berisi elemen – elemen plainteks dan himpunan yang berisi cipherteks. Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen- elemen antara dua himpunan tersebut. Misalkan *P* menyatakan plainteks dan *C* menyatakan cipherteks, maka fungsi enkripsi *E* memetakan *P* ke *C*.

   $E(P) = C$

   Dan fungsi dekripsi *D* memetakan *C* ke *P*

   $D(C) = P$

   Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan semula, maka kesamaan berikut harus benar,

   $D(E(P)) = P$

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 *enciphering* dan *deciphering*. Kunci biasanya berupa string atau deretan bilangan. Dengan menggunakan K, maka fungsi enkripsi dan dekripsi dapat ditulis sebagai :

$E_K(P)=C$ *dan* $D_K(C)=P$

Dan kedua fungsi ini memenuhi

$D_K(E_K(P))=P$

Keterangan :

P = plainteks

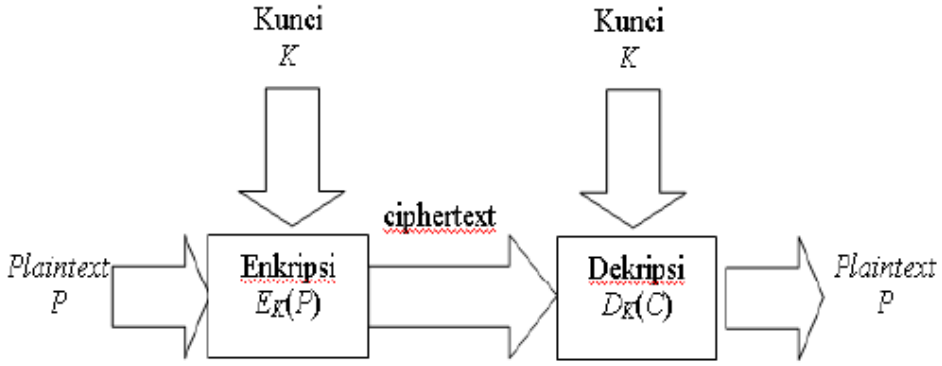
C = cipherteks

K = kunci

EK = proses enkripsi menggunakan kunci *K*

DK = proses dekripsi menggunakan kunci *K*

Skema enkripsi dengan menggunakan kunci diperlihatkan pada gambar dibawah ini :



Gambar 1. Skema enkripsi dan dekripsi dengan menggunakan kunci

Gambar di atas menjelaskan bahwa Plaintext (tulisan asli) disandikan menggunakan kunci sehingga muncul sebagai ciphertext. Kemudian tulisan dideskripsikan untuk mendapatkan tulisan asli atau Plaintext.

5. Sistem kriptografi

   kriptografi membentuk sebuah sistem yang dinamakan sistem Kriptografi. *Sistem kriptografi* (*cryptosystem*) adalah kumpulan yang terdiri dari algoritma kriptografi, semua plainteks dan cipherteks yang mungkin, dan kunci. Di dalam kriptografi, cipher hanyalah salah satu komponen saja.

6. Penyadap

   penyadap (*eavesdropper*) adalah orang yang mencoba menangkap pesan selama ditransmisikan. Tujuan penyadap adalah untuk mendapatkan informasi sebanyak - banyaknya mengenai sistem kriptografi yang digunakan untuk berkomunikasi dengan maksud untuk memecahkan

cipherteks. Nama lain penyadap : *enemy*, *adversary*, *intruder*, *interceptor*, *bad guy*.

7. Kriptanalisis dan kriptologi

   Kriptografi berkembang sedemikian rupa sehingga melahirkan bidang yang berlawanan yaitu kriptanalisis. *Kriptanalisis* (*cryptanalysis*) adalah ilmu dan seni untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalis. Jika seorang kriptografer (*cryptographer*) mentransformasikan plainteks menjadi cipherteks dengan suatu algoritma dan kunci maka sebaliknya seorang kriptanalis berusaha untuk memecahkan cipherteks tersebut untuk menemukan plainteks atau kunci. Kriptologi (*cryptology*) adalah studi mengenai kriptografi dan kriptanalisis.

b. Tujuan kriptografi

   Dari paparan awal dapat dirangkumkan bahwa kriptografi bertujuan untuk memberi layanan keamanan. Yang dinamakan aspek – aspek keamanan sebagai berikut :

   1. Kerahasiaan (*confidentiality*)

      Adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak – pihak yang tidak berhak. Di dalam kriptografi layanan ini direalisasikan dengan menyandikan plainteks menjadi cipherteks. Misalnya pesan “harap datang pukul 8” disandikan menjadi

"trxC#45motyptre!%". istilah lain yang senada dengan confidentiality adalah *secrecy* dan *privacy*.

2. Integritas data (*data integrity*)

   Adalah layanan yang menjamin bahwa pesan masih asli/utuh atau belum pernah dimanipulasi selama pengiriman. Dengan kata lain, aspek keamanan ini dapat diungkapkan sebagai pertanyaan: " apakah pesan yang diterima masih asli atau tidak mengalami perubahan (modifikasi)?".

3. Otentikasi (*authentication*)

   Adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak – pihak yang berkomunikasi (*user autehentication*). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sember pesan.

4. *Non-Repudiation*

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

c. Vigenere Cipher

Teknik dari substitusi Vigenere dapat dilakukan dengan dua cara:

1. Angka

   Teknik substitusi vigenere dilakukan menggunakan angka dengan menukarkan huruf dengan angka.

Tabel 1. Konversi Vigenere ke Angka

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Algoritma Vigenere dengan teknik angka menggunakan tabel pemindahan huruf ke angka dimana huruf yang dimulai dari huruf A akan dipindahkan menjadi angka 0. Sementara huruf B menjadi angka 1 dan selanjutnya akan berakhir pada angka 25.

Contoh :

Plaintext : This cyptosystem is not secure

Kunci : cipher

Maka untuk mendapatkan ciphertextnya adalah tulisan plaintext diubah ke dalam bentuk angka seperti pada tabel konversi di bawah ini

Tabel 2. Konversi Vigenere Contoh Ke Angka

T	H	I	S	C	R	Y	P	T	O	S	Y	S	T	E	M
19	7	8	18	2	17	24	25	19	14	18	24	18	19	4	12
2	8	15	7	4	17	2	8	15	7	4	17	2	8	15	7
21	15	23	25	6	8	0	23	8	21	22	15	20	1	19	19

I	S	N	O	T	S	E	C	U	R	E
8	18	13	14	19	18	4	2	20	17	4
4	17	2	8	15	7	4	17	2	8	15
12	9	15	22	8	25	8	19	22	25	19

Pada baris kedua merupakan hasil konversi plaintext ke dalam bentuk angka. Untuk baris ketiga didapat dari konversi kunci yang diulang sampai tulisan plaintext berakhir. Pada baris keempat merupakan hasil penjumlahan antara baris kedua dan ketiga. Jika hasil penjumlahan berada di atas 26 maka akan diulang kembali ke huruf A. setelah hasil penjumlahan didapat, maka angka kembali dikonversi ke huruf sehingga didapat ciphertextnya adalah:

VPXZGIAXIVWPUBTTMJPWIZITWZT

2. Huruf

   Teknik substitusi vigenere dengan menggunakan huruf dapat dilakukan dengan pada gambar tabel di bawah ini

Tabel 3. Vigenere Chiper

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

3. Serangan terhadap kriptografi

a. Jenis – jenis serangan

Serangan (“serangan kriptanalisis”) terhadap kriptografi dapat dikelompokkan dengan beberapa cara :

1. Berdasarkan keterlibatan penyerang dalam komunikasi, serangan dapat dibagi atas dua macam, yaitu :

   a. Serangan pasif (*passive attack*)

      Pada serangan ini, penyerang tidak terlibat dalam komunikasi antara pengirim dan penerima, namun penyerang menyadap semua pertukaran pesan antara kedua entitas tersebut. Tujuannaya adalah untuk mendapatkan sebanyak mungkin informasi yang digunakan untuk kriptanalisis. Beberapa metode penyadapan antara lain :

      – *Wiretapping* : penyadap mencegat data yang ditransmisikan pada saluran kabel komunikasi dengan menggunakan sambunganperangkat keras.
      – *Electromagnetic Eavesdropping* : penyadap mencegat data yang ditrasnmisikan melalui saluran wireless, misalnya radio dan microwave.
      – *Acoustic Eavesdropping* : menangkap gelombang suara yang dihasilkan oleh suara manusia.

b. Serangan aktif (*active attack*)

Pada jenis serangan ini, penyerang mengintervensi komunikasi dan ikut mempengaruhi sistem untuk keuntungan dirinya. Misalnya penyerang mengubah aliran pesan seperti menghapus sebagian cipherteks, mengubah cipherteks, menyisipkan potongan cipherteks palsu, me-replay pesan lama, mengubah informasi yang tersimpan, dan sebagainya.

2. Berdasarkan banyaknya informasi yang diketahui oleh kriptanalis, maka serangan dapat dikelompokkan menjadi lima jenis, yaitu:

1. *Ciphertext-only attack*

Ini adalah jenis serangan yang paling umum namun paling sulit, karena informasi yang tersedia hanyalah cipherteks saja. Kriptanalis memiliki beberapa cipherteks dari beberapa pesan, semuanya dienkripsi dengan algoritma yang sama. Untuk itu kriptanalis menggunakan beberapa cara, seperti mencoba semua kemungkinan kunci secara *exhaustive search*. Menggunkan analis frekuensi, membuat terkaan berdasarkan informasi yang diketahui,dan sebagainya.

2. *Known-plaintext attack*

Ini adalah jenis serangan dimana kriptanalis memiliki pasangan plainteks dan cipherteks yang berkoresponden.

3. *Chosen-plaintext attack*

   Serangan jenis ini lebih hebat dari pada *known-plaintext attack*, karena kriptanalis dapat memilih plainteks yang dimilikinya untuk dienkripsikan, yaitu plainteks-plainteks yang lebih mengarahkan penemuan kunci.

4. *Chosen-ciphertext attack*

   Ini adalah jenis serangan dimana kriptanalis memilih ciphertext untuk dideskripsikan dan memiliki akses ke plaintext hasil deskripsi.

5. *Chosen text attack*

   Ini adalah jenis serangan yang merupakan kombinasi *chosen-plaintext attack* dan *chosen-chiphertext attack*.

3. Berdasarkan teknik yang digunakan dalam menemukan kunci, maka serangan dapat dibagi menjadi dua, yaitu :

   1. *Exhaustive attack* atau *brute force attack*

      Ini adalah serangan untuk mengungkap plainteks atau kunci dengan menggunakan semua kemungkinan kunci. Diasumsikan kriptanalis mengetahui algoritma kriptografi yang digunakan oleh pengirim pesan. Selain itu kriptanalis memiliki sejumlah cipherteks dan plainteks yang bersesuaian.

2. *Analytical attack*

   Pada jenis serangan ini, kriptanalis tidak mencoba-coba semua kemungkinan kunci tetapi menganalisis kelemahan algoirtma kriptografi untuk mengurangi kemungkinan kunci yang tidak ada. Diasumsikan kriptanalis mengetahui algoritma kriptografi yang digunakan oleh pengirim pesan. Analisis dapat menggunakan pendekatan matematik dan statistik dalam rangka menemukan kunci.

3. *Related-key attack*

   Kriptanalis memiliki cipherteks yang dienkripsi dengan dua kunci berbeda. Kriptanalis tidak mengetahui kedua kunci tersebut namun ia mengetahui hubungan antara kedua kunci, misalnya mengetahui kedua kunci hanya berbeda 1 bit.

4. *Rubber-hose cryptanalysis*

   Ini mungkin jenis serangan yang paling ekstrim dan paling efektif. Penyerang mengancam, mengirim surat gelap, atau melakukan penyiksaan sampai orang yang memegang kunci memberinya kunci untuk mendekripsi pesan.

4. Kompleksitas serangan

Kompleksitas serangan dapat diukur dengan beberapa cara, yaitu :

1. Kompleksitas data (*data complexity*)

Jumlah data (plainteks dan cipherteks) yang dibutuhkan sebagai masukan untuk serangan. Semakin banyak data yang dibutuhkan untuk melakukan serangan, semakin kompleks serangan tersebut, yang berarti semakin bagus sistem kriptografi tersebut.

2. Kompleksitas waktu (*time complexity*)

Waktu yang dibutuhkan untuk melakukan serangan. Semakin lama waktu yang dibutuhkn untuk melakukan serangan, berarti semakin bagus kriptografi tersebut.

3. Kompleksitas ruang memori (*space/storage complexity*)

Jumlah memori yang dibutuhkan untuk melakukan serangan. Semakin banyak memori yang dibutuhkan untuk melakukan serangan, berarti semakin bagus sistem kriptografi tersebut.

4. Keamanan Algoritma Kriptografi

Menurut Doni Ariyus (2005) Menuliskan Lard Knudsen mengelompokkan hasil kriptanalis ke dalam beberapa kategori berdasarkan jumlah dan kualitas informasi yang berhasil ditemukan :

– Pemecahan total (*total break*). Kriptanalis menemukan kunci *K*

- Deduksi (*penarikan kesimpulan*) global (*global deduction*). Kriptanalis menemukan algoritma alternatif, A, yang ekivalen dengan tetapi tidak mengetahui kunci *K*.)
- Deduksi lokal (*instance*/*local deduction*). Kriptanalis menemukan plainteks dari cipherteks yang disadap.

Deduksi informasi (*information deduction*). Kriptanalis menemukan beberapa informasi perihal kunci atau plainteks. Misalnya kriptanalis mengetahui beberapa kunci, kriptanalis mengetahui bahasa yang digunakan untuk menulis plainteks, kriptanalis mengetahui format plainteks, dan sebagainya. Sebuah algoritma dikatakan aman mutlak tanpa syarat (*unconditionally secure*) bila cipherteks yang dihasilkan oleh algoritma tersebut tidak mengandung cukup informasi untuk menentukan plainteks.

5. Algortima Kriptografi Klasik

Sebelum komputer ada, kriptografi dilakukan dengan menggunakan pensil dan kertas. Algoritma kriptografi (*cipher*) yang digunakan saat itu, dinamakan juga algoritma klasik, adalah berbasis karakter, yaitu enkripsi dan dekripsi dilakukan pada setiap karakter pesan. Semua algoritma klasik termasuk ke dalam sistrm kriptografi simetris dan digunakan jauh sebelum kriptografi kunci publik ditemukan.

Kriptogarfi klasik memiliki beberapa ciri :

a. Berbasis karakter
b. Menggunakan pena dan kertas saja, belum ada komputer

c. Termasuk ke dalam kriptografi kunci simetris.

Tiga alasan mempelajari algoritma klasik :

a. Memahami konsep dasar kriptografi

b. Dasar algoritma kriptografi modern

c. Memahami kelemahan sistem kode.

(*Ariyus, Dony. 2005*)

Pada dasarnya, algoritma kriptografi klasik dapat dikelompokkan ke dalam dua macam cipher, yaitu :

1. Cipher substitusi (*substitution cipher*)

   Di dalam cipher substitusi setiap unit plainteks diganti dengan satu unit cipherteks. Satu "unit" di isini berarti satu huruf, pasanga huruf, atau dikelompokkan lebih dari dua huruf. Algoritma substitusi tertua yang diketahui adalah *Caesar cipher* yang digunakan oleh kaisar Romawi , Julius Caesar (sehingga dinamakan juga *casear cipher*), untuk mengirimakan pesan yang dikirimkan kepada gubernurnya.

2. Cipher transposisi (*transposition cipher*)

   Pada cipher transposisi, huruf-huruf di dalam plainteks tetap saja, hanya saja urutannya diubah. Dengan kata lain algoritma ini melakukan transpose terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah permutasi atau pengacakan (*scrambling*) karena transpose setiap karakter di dalam teks sama dengan mempermutasikan karakter-karkater tersebut.

6. Visual Basic Net 2010

Merupakan sebuah bahasa pemograman dan sebagai sarana (tool) untuk menghasilkan program-program aplikasi berbasiskan windows. Beberapa kemampuan atau manfaat dari Visual Basic diantaranya:

a. Untuk membuat program aplikasi berbasiskan windows.
b. Untuk membuat obyek-obyek pembantu program, seperti Control Active X, File Help, Aplikasi Internet dan sebagainya.
c. Menguji program (debugging) dan menghasilkan program akhir berakhiran ”EXE” yang bersifat executable atau dapat langsung dijalankan.

Keistimewaan utama dari Visual Basic adalah:

d. Menggunakan platform pembuatan program yang diberi nama developer studio, yang memiliki tampilan seperti C++ dan visual J++.
e. Memiliki kompiler handal yang dapat menghasilkan File Executable yang lebih cepat dan efisien.
f. Memiliki tambahan saran wizard yang baru. Tambahan kontrol-kontrol baru dan lebih canggih serta peningkatan kaidah struktur bahasa Visual Basic.
g. Kemampuan membuat Active X dan fasilitas internet yang lebih banyak.
h. Sarana akses yang lebih cepat dan andal untuk membuat aplikasi database yang berkemampuan tinggi.
i. Visual Basic.net memiliki beberapa versi baru edisi yang disesuaikan dengan kebutuhan pemakainya.

Dalam pemograman berbasiskan OOP (Object Oriented Programming), sebuah program dibagi menjadi bagian-bagian kecil yang disebut dengan obyek. Setiap obyek memiliki entiti terpisah dengan entiti-entiti lain dalam lingkungannya. Obyek-obyek yang terpisah ini dapat diolah sendiri-sendiri, dan setiap obyek memiliki sekumpulan sifat dan metode yang melakukan fungsi tertentu sesuai dengan yang telah diprogramkan kepadanya.

Adapun obyek-obyek yang dipergunakan dalam program ini adalah:

1. Project

   Project adalah sekumpulan modul. Jadi project merupakan aplikasi itu sendiri. Project disimpan dalam file yang berakhiran VBP. Jika kita akan melaksanakan pembuatan program aplikasi, akan terdapat jendela project yang berisi semua file yang dibutuhkan menjalankan program aplikasi Visual Basic.net pada saat pembuatan program aplikasi baru maka jendela project otomatis akan berisi object form1. Pada jendela project terdapat tiga icon yaitu View Code, View Object, dan Toggle Folders. Icon View Code dipakai untuk menampilkan jendela editor kode program. Icon View Object dipakai untuk menampilkan bentuk formulir (form) dan icon Toggle Folders digunakan untuk menampilkan folder

2. Form

   Form adalah jendela yang dipakai untuk membuat user interface/tampilan. Secara otomatis akan tersedia form yang baru jika membuat suatu program

aplikasi yang baru, dengan nama Form1. pada umumnya dalam suatu form terdapat garis titik-titik yang disebut dengan Grid. Untuk lebih memahami form ini maka di bawah ini terdapat gambar jendela form.

3. Toolbox

   Toolbox adalah kumpulan dari obyek yang digunakan untuk membuat user interface (tampilan) serta control bagi program aplikasi. Untuk menempatkan control pada suatu form dapat dilakukan dengan klik ganda control dalam toolbox, kemudian mengubah besar dan ukurannya serta memindahkannya dengan metode Drag and Drop atau dengan cara mengklik kontrol toolbox, kemudian pindahkan pointer mouse jendela form. Kursor berubah menjadi Crosshair lalu tempatkan pada sudut kiri atas dimana kita inginkan kontrol tersebut diletakkan, tekan tombol mouse kiri dan tahan ketika menyeret kursor ke arah sudut kanan bawah.

4. Properties

   Properties berisikan daftar struktur setting properti yang digunakan pada sebuah object terpilih. Kotak drop-down pada bagian atas jendela berisi daftar semua object pada form yang aktif. Ada tab tampilan, yaitu alphabetic (urut abjad) dan categorized (urut berdasarkan kelompok).

5. Kode Program

   Kode program adalah serangkaian tulisan perintah yang akan dilaksanakan jika suatu obyek dijalankan. Kode program ini mengkontrol dan menentukan jalannya suatu obyek.

6. Event

   Event adalah peristiwa atau kejadian yang diterima suatu obyek, misalnya klik, seret, tunjuk, dan lain sebagainya.

7. Metode (Methods)

   Metode adalah serangkaian perintah yang sudah tersedia pada suatu obyek yang dapat diminta untuk mengerjakan tugas khusus.

8. Module

   Module dapat disejajarkan dengan form, tetapi module tidak mengandung obyek. Module berisikan prosedur umum, deklarasi variabel dan definisi konstanta yang digunakan oleh aplikasi.

7. Pengertian UML

Unified Modelling Language (UML) adalah sebuah bahasa yang telah menjadi standar dalam industri untuk visualisasi, merancang 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, di mana 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 (Prastuti Sulistyorini, 2012).

Unified Modeling Language (UML) adalah kumpulan notasi grafis yang didukung oleh sebuah model tunggal, yang membantu dalam menjelaskan dan merancang sistem perangkat lunak, khususnya sistem perangkat lunak dibangun menggunakan gaya berorientasi objek. UML terdiri atas banyak elemen-elemen grafis yang digabungkan membentuk diagram. Tujuan representasi elemen-elemen grafis ke dalam diagram adalah untuk menyajikan beragam sudut pandang dari sebuah sistem berdasarkan fungsi masing-masing diagram tersebut. Kumpulan dari beragam sudut pandang inilah yang kita sebut sebuah model (Andy Prasetyo Utomo, 2013).

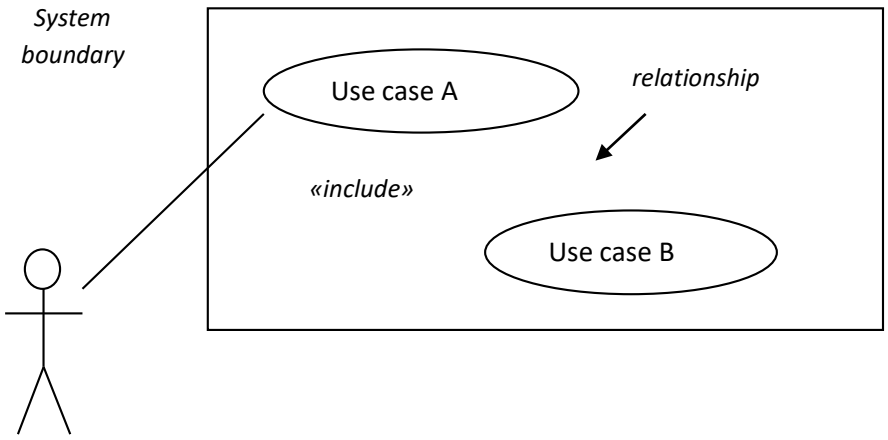
Dengan menggunakan model ini diharapkan pengembangan piranti lunak dapat memenuhi semua kebutuhan pengguna dengan lengkap dan tepat, termasuk faktor-faktor seperti *scalability*, *robustnees*, *security*, dan sebagainya. Untuk melakukan pemodelan sistem perangkat lunak secara visual digunakan UML (*Unified Modelling Language*) yang digambarkan secara elektronik lewat sarana perangkat lunak *Rational Rose*. Sebagai mana telah diterapkan oleh Gufran (2012) di mana UML diterapkan untuk mengukur kinerja mahasiswa menggunakan pendekatan berorientasi objek. Kemudian UML diterapkan juga oleh Sunguk (2012) untuk menerapkan sistem *database* dan aplikasi komputer. Selanjutnya Jakimi dan Koutbi (2009) menerapkan pendekatan UML untuk sekenario rekayasa dan kode generasi.

a. Use Case Diagram

Use case merupakan teknik menangkap kebutuhan-kebutuhan fungsional dari sistem baru atau sistem yang diubah. Setiap *use case* terdiri dari satu atau lebih skenario yang menerangkan bagaimana sistem berinteraksi dengan pengguna atau sistem yang lain untuk mencapai suatu sasaran bisnis tertentu. Dalam tehnik ini tidak diterangkan cara kerja sistem secara internal maupun implementasinya. Yang ditunjukkan adalah langkah-langkah yang dilakukan pengguna dalam menggunakan perangkat lunak (Nyimas Artina, 2006).

Diagram *Use Case* merupakan diagram yang menggambarkan fungsi berupa komponen, kelas, atau kejadian yang ada dalam *system* (Ade Sutedi *et al*, 2015). *Use case* atau diagram *use case* merupakan pemodelan untuk kelakuan (*behavior*) sistem informasi yang akan dibuat. *Use case* mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem informasi yang akan dibuat. Secara kasar, *use case* digunakan untuk mengetahui fungsi apa saja yang ada di dalam sebuah sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi itu (Rosa A.S dan M. Shalahuddin, 2014).

Syarat penamaan pada *use case* adalah nama didefinisikan sesimpel mungkin dan dapat dipahami. Ada dua hal utama pada *use case* yaitu pendefinisian apa yang disebut aktor dan *use case*.

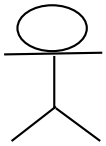


Gambar 2. *Use Case Diagram*

Terdapat 2 bagian utama dalam *use case modeling* sebagaimana dijelaskan sebagai berikut:

- Aktor

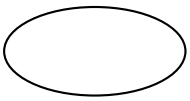
  Aktor merupakan orang, proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat di luar sistem informasi yang akan dibuat itu sendiri, jadi walaupun simbol dari aktor adalah gambar orang, tapi aktor belum tentu merupakan orang.



Gambar 3. Aktor

- *Use Case*

  Use case merupakan fungsional yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antar unit atau aktor.



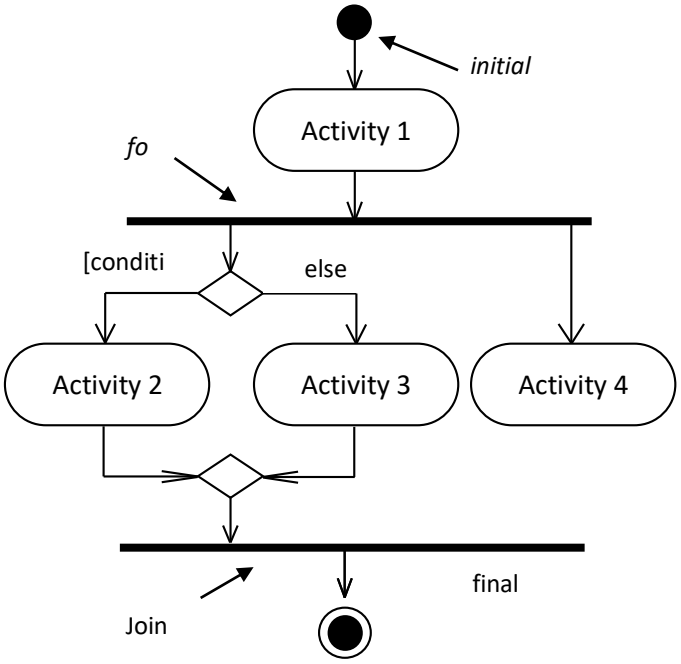
Gambar 4 *Use Case*

b. Activity Diagram

Activity diagrams menggambarkan *workflow* (aliran kerja) atau aktivitas sari sebuah sistem atau proses bisnis. Yang perlu diperhatikan di sini adalah bahwa diagram aktivitas menggambarkan aktivitas sistem bukan apa yang dilakukan aktor, jadi aktivitas yang dapat dilakukan oleh sistem (Rosa A.S dan M. Shalahuddin, 2014).

Diagram aktivitas juga banyak digunakan untuk mendefinisikan hal-hal berikut :

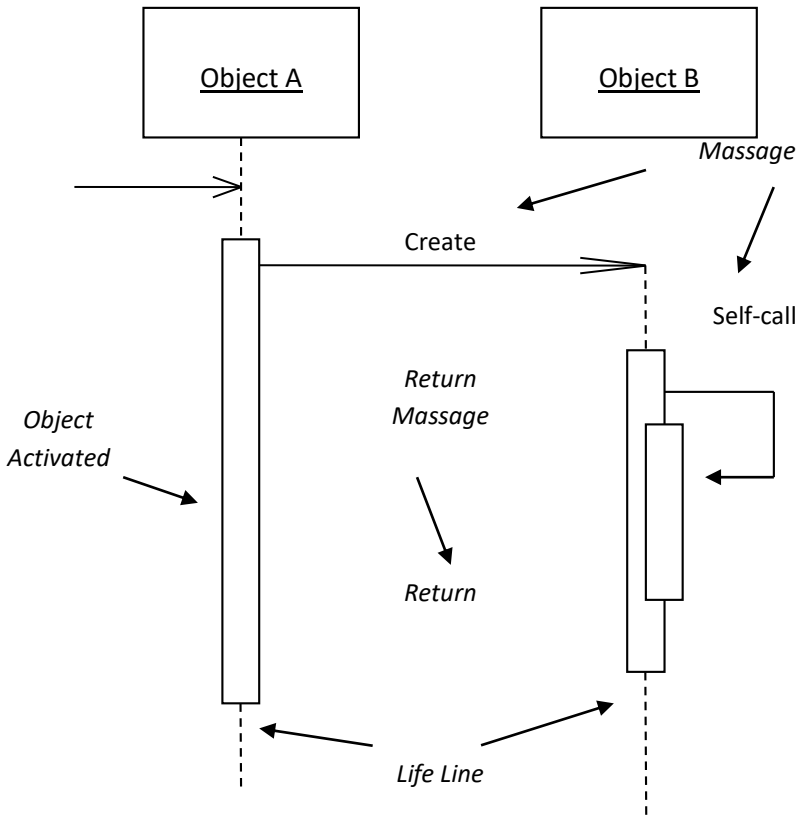
1. Rancangan proses bisnis dimana setiap urutan aktivitas yang digambarkan merupakan proses bisnis sistem yang didefinisikan.
2. Urutan atau pengelompokkan tampilan dari sistem/*user interface* di mana setiap aktivitas dianggap memiliki antarmuka tampilan.
3. Rancangan pengujian di mana setiap aktivitas dianggap memerlukan sebuah pengujian yang perlu didefinisikan kasus ujinya.



Gambar 5. ***Activity Diagram***

c. Sequence Diagram

Sequence diagram menggambarkan kelakuan objek pada *use case* dengan mendeskripsikan waktu hidup objek dan *message* yang dikirimkan dan diterima antar objek. Oleh karena itu 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 (Rosa A.S dan M. Shalahuddin, 2014).



Gambar 6. ***Sequence Diagram***

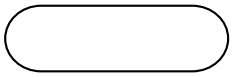
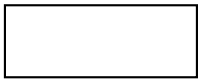
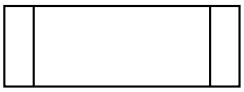
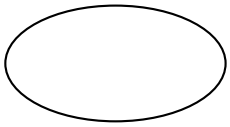
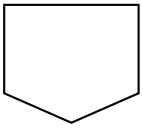
8. Pengertian Flowchat

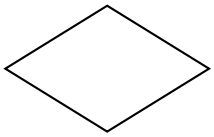
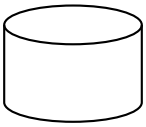
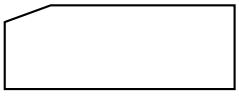
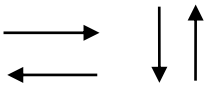
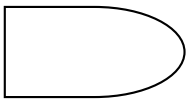
Menurut (Sariadin Siallagan, 2013), Flowchart adalah suatu diagram alir yang mempergunakan simbol atau tanda untuk menyelesaikan masalah. Dalam hal ini, penyelesaian masalah menggunakan simbol-simbol yang telah disepakati.

Menurut (Abdillah Baraja, 2012) Flowchart adalah representasi grafik yang menggambarkan setiap langkah yang akan dilakukan dalam suatu proses, yang merupakan alat bantu yang banyak digunakan untuk menggambarkan sistem secara pisikal.

Bagan alir (flowchart) adalah bagan (chart) yang menunjukkan alir (flow) di dalam program atau prosedur system secara logika. Digunakan terutama untuk alat bantu komunikasi dan untuk dokumentasi.

Tabel 4. Simbol-Simbol Flowchart

NO	SIMBOL	FUNGSI
1.		Terminal menyatakan awal atau akhir dari suatu logaritma.
2.		Menyatakan proses.
3.		Proses yang terdefenisi atau sub program.
4.		Persiapan yang digunakan untuk memberi nilai awal suatu besaran.
5.		Menyatakan masukan dan keluaran (input/output).
6.		Menyatakan penyambung ke simbol lain dalam satu halaman.
7.		Menyatakan penyambung ke halaman lainnya.

8.		Menyatakan pencetakan (dokumen) pada kertas.
9.		Menyatakan *decision* (keputusan) yang digunakan untuk penyeleksian kondisi didalam program.
10.		Menyatakan media prnyimpanan drum magnetik.
11.		Menyatakan input/output menggunakan disket.
12.		Menyatakan operasi yang dilakakukan secara manual.
13.		Menyatakan input/output dari kartu plong.
14.		Menyatakan aliran pekerjaan (proses).
15.		Multidocument (banyak dokumen).
16.		Delay (penundaan atau kelambatan).

Sumber : Abdillah Baraja, 2012

BAB III

METODE PENELITIAN

1. Analisa Permasalahan

a. Analisa sistem yang berjalan

Dalam materi perkuliahan Keamanan komputer terdapat bab mengenai enkripsi. Salah satu bentuk enkripsi adalah menggunakan metode vigenere. Untuk mendapatkan hasil teks yang diubah (*ciphertext)*, menggunakan angka dan tabel untuk konversi. Penggunaan angka jauh lebih sulit dibandingkan dengan menggunakan tabel.

Contoh soal:

Diketahui Plaintext " Selamat Datang" dengan kunci "Kampus". Maka untuk mendapatkan ciphertextnya harus menggunakan penghitungan seperti di bawah ini:

Langkah Pertama membuat tabel konversi vigenere.

Ciphertext : SELAMAT DATANG

Kunci : KAMPUS

Penerima memilih kata KAMPUS sebagai kunci yang akan ia gunakan untuk melakukan proses enkripsi menggunakan Algoritma Vigenere Cipher, sehingga pada prosesnya kata KAMPUS akan mengikuti banyak karakter ciphertext 1 yang didapat.

Ciphertext : SELAMAT DATANG

Kunci : KAMPUS

Selanjutnya akan di enkripsi dengan formula Algoritma Vigenere Cipher yaitu:

C = P + K mod 26

Dalam hal ini plaintext adalah ciphertext 1 yang didapat.

C1 = S + K mod 26

= 83 + 75 mod 26

= 158 = ž

C2 = E + A mod 255

= 69 + 65 mod 26

= 134 = †

C3 = L + M mod 255

= 76 + 77 mod 26

= = ™

C4 = A + P mod 255

= 65 + 80 mod 26

= 145 = ‘

C5 = M + U mod 255

= 77 + 85 mod 26

= 162 = ¢

C6 = A + S mod 255

= 65 + 83 mod 26

= 148 = ”

C7 = T + K mod 255

= 84 +75 mod 26

= 159 = Ÿ

C8 = D + A mod 255

= 68 + 65 mod 26

= 133 = a

C9 = A + M mod 255

= 65 + 77 mod 26

= 142 = ‘

C10 = T + P mod 255

= 84 + 80 mod 26

= 164 = ‘

C11 = A + U mod 255

= 65 + 85 mod 26

= 150 = ©

C12 = N + S mod 255

= 78 + 83 mod 26

= 161 = ”

C13 = G + K mod 26

= 71 + 74 mod 26

= 145 = ™

Sehingga ciphertext kedua yang didapat adalah:

Ciphertext = ž†™‘¢”Ÿa‘‘©”™ˆ

b. Kelemahan sistem yang berjalan

Berdasarkan hasil dari analisa yang diperoleh penulis dapat menguraikan beberapa kelemahan pada sistem yang sedang berjalan, diantaranya :

1) Harus melihat tabel untuk proses penyandian teks
2) Jika tulisan terlalu banyak, menambah kesulitan pada proses penyandian.
3) Memungkinkan kesalahan pada proses penyandian

c. Analisa Sistem yang Dibangun

Perancangan sistem yang akan dibangun dilakukan setelah menganalisa permasalahan yang ada dari sistem berjalan. Sistem baru yang akan dibangun ini merupakan perubahan dari sistem yang dilakukan secara manual yang akan dijadikan secara komputerisasi dengan menggunakan aplikasi visual studio.

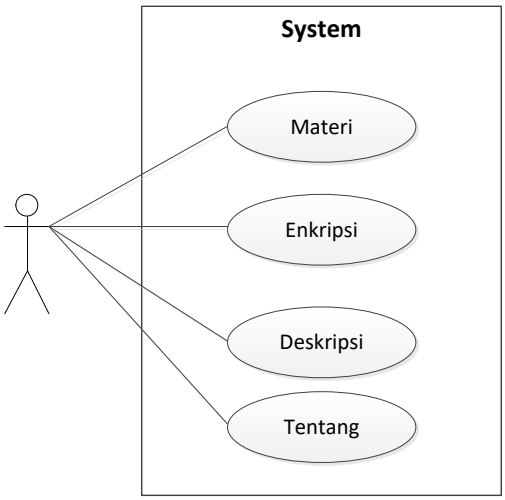
2. Perancangan Berorientasi Objek

Perancangan atau Pemodelan Berorientasi Ojek merupakan proses mendapatkan informasi dari model dan menampilkannya secara grafik dengan menggunakan sebuah standar elemen grafik. Tujuan dari perancangan berorientasi ojbek ini memungkinkan adanya komunikasi yang lebih berkualitas antara pengguna,

pengembang penganalisis, tetster, manajer dan siapapun yang terlibat dalam proyek pengembangan sistem informasi.

a. Use case Diagram

Berikut adalah *use case diagram* yang menggambarkan kegiatan.



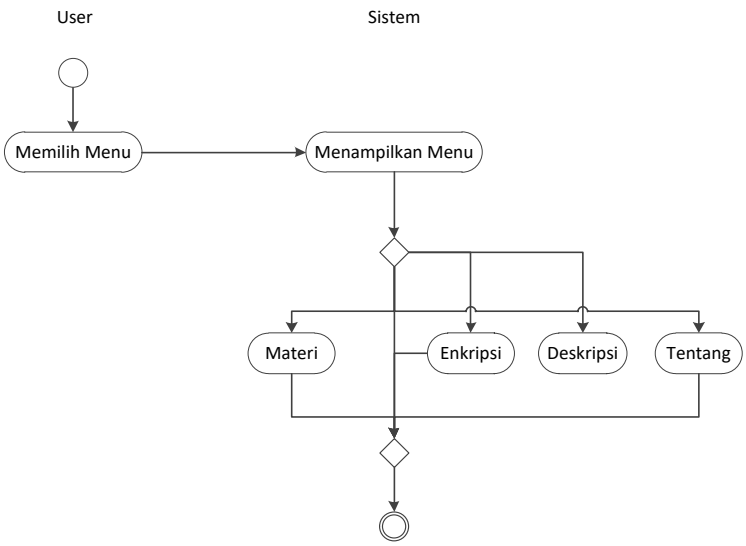
Gambar 13. *Use Case Diagram*

Keterangan :

Dalam *use case* diagram di atas, *user/*pengguna sebagai *actor* yang mempunyai *use case* Materi, Enkripsi dan Tentang.

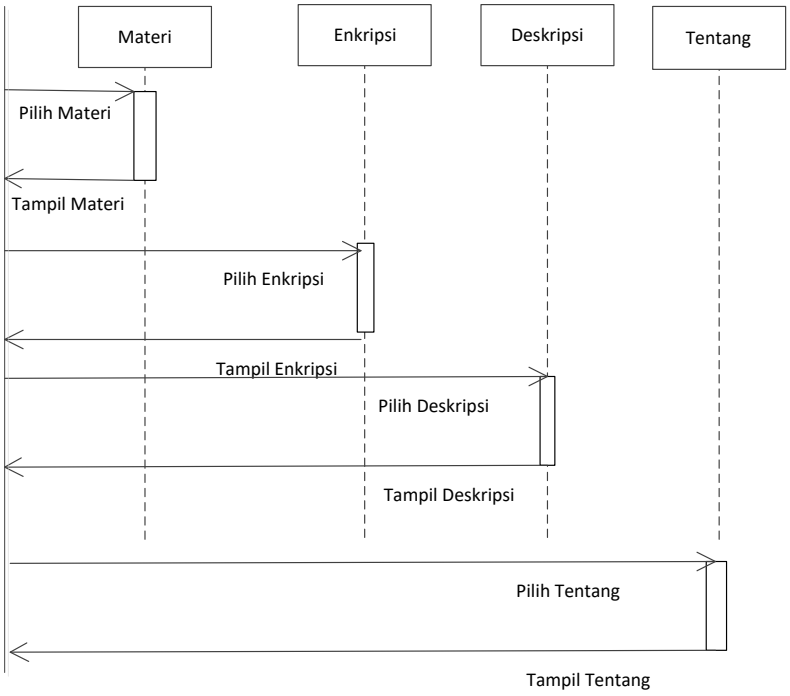
b. Pembuatan Activity Diagram

Activity diagram menggambarkan aktifitas-aktifitas yang terjadi dalam aplikasi dari aktivitas dimulai sampai aktivitas berhenti.



Gambar 14. ***Activity Diagram***

c. Sequence Diagram



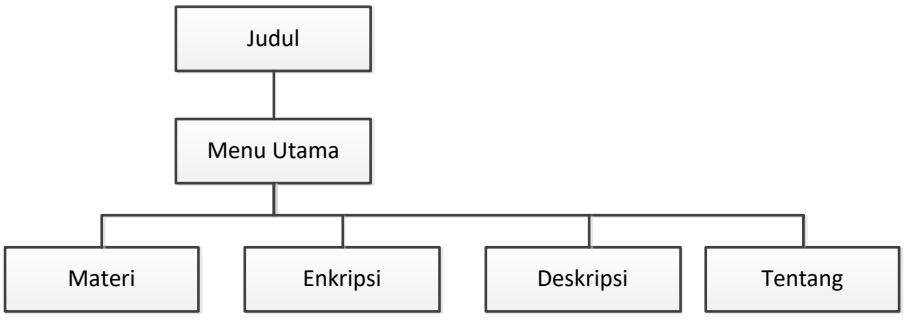
Gambar 15. ***Sequence Diagram***

Keterangan Gambar :

1. Dalam diagram di atas menjelaskan bahwa user memilih materi kemudian Sistem menampilkan materi yang berkaitan dengan materi
2. User merequest Enkripsi kemudian Sistem menampilkan menu Enkripsi
3. User merequest Deskripsi kemudian Sistem menampilkan menu Deskripsi
4. User merequest Menu Tentang kemudian Sistem menampilkan Form Tentang.

3. Struktur Program

Struktur program mempresentasikan organisasi komponen program (modul) serta mengimplementasikann suatu hirarki kontrol. Hirearki kontrol tidak mengimplementasikan aspek prosedural dari perangkat lunak seperti urutan proses, kejadian atau urutan dari keputusan atau perulangan operasi.



Gambar 16. Struktur Navigasi Enkripsi

4. Perancangan Antarmuka

a. Rancangan Halaman Judul

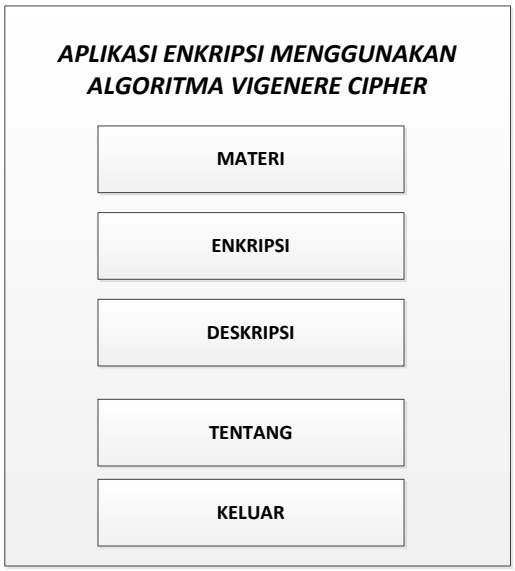
Halaman judul merupakan halaman yang pertama muncul pada saat program

Gambar 17. Rancangan Halaman Judul

Pada rancangan di atas akan menampilkan judul yang kemudian akan pindah ke form menu utama dengan menggunakan timer.

b. Rancangan Halaman Menu Utama

Form ini berisi tombol-tombol seperti menu Materi, Enkripsi, Deskipsi, tentang, dan Keluar.



Gambar 17. Rancangan Halaman Menu Utama

Pada tampilan di atas terdapat 5 tombol yaitu Materi, Enkripsi, Deskripsi, Tentang dan keluar.

- Tombol Materi berfungsi untuk menghubungkan pengguna ke form materi.
- Tombol Enkripsi berfungsi untuk menghubungkan pengguna ke form Enkripsi.
- Tombol Deskripsi berfungsi untuk menampilkan form Deskripsi.
- Tombol Tentang berfungsi untuk menghubungkan pengguna ke form tentang.
- Tombol Keluar berfungsi untuk keluar dari program.

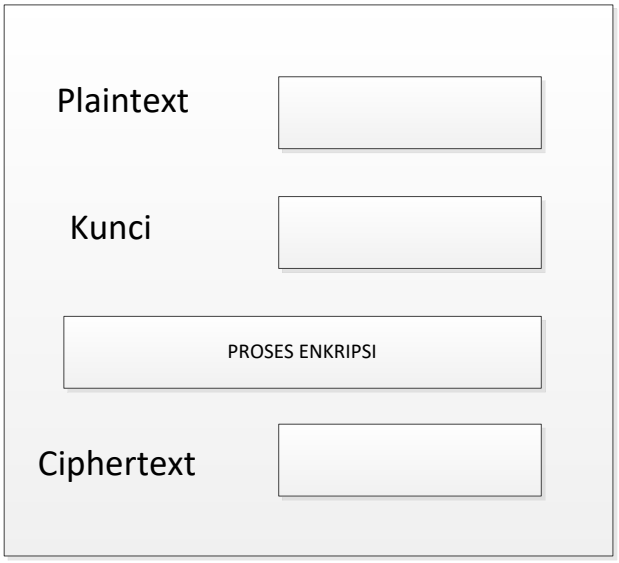
c. Rancangan Halaman Materi

Form ini digunakan untuk menjelaskan cara kerja penyandian, dimulai dari plaintext kemudian kunci yang dikonversikan dalam bentuk angka. Setelah itu dilakukan proses penjumlahan dan jika hasil penjumlahan maka akan dikurangi 6 lalu hasilnya akan dikembalikan lagi ke dalam bentuk huruf.

Gambar 19. Rancangan Halaman Materi

d. Rancangan Halaman Enkripsi

Berisi penjelasan mengenai Enkripsi. Pengguna memasukkan tulisan asli atau *plaintext* ke dalam tombol masukan *plaintext* kemudian dimasukkan juga kunci. Setelah itu, ditekan tombol Proses Enkripsi yang kemudian akan menampilkan ciphertext atau tulisan yang telah disandikan.



Gambar 20. Rancangan Halaman Enkripsi

e. Rancangan Halaman Deskripsi

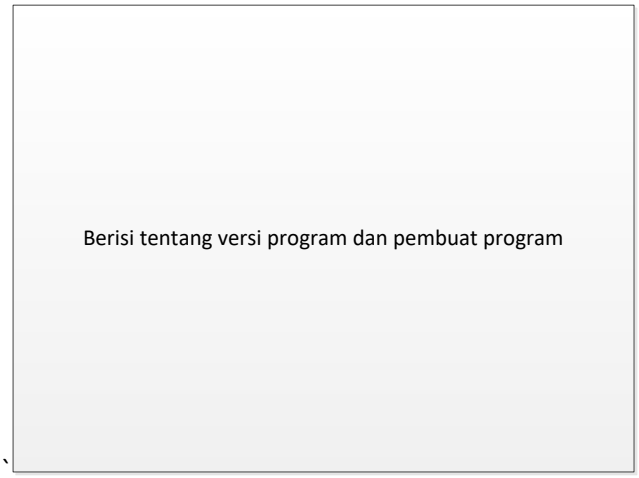
Berisi penjelasan mengenai Enkripsi. Pengguna memasukkan tulisan asli atau *plaintext* ke dalam tombol masukan *plaintext* kemudian dimasukkan juga kunci. Setelah itu, ditekan tombol Proses Enkripsi yang kemudian akan menampilkan ciphertext atau tulisan yang telah disandikan.

Gambar 21. Rancangan Halaman Deskripsi

Pada gambar di atas terdapat kotak input Deskripsi berfungsi untuk memasukkan tulisan yang telah disandikan. Kemudian terdapat tombol Proses Deskripsi untuk mengembalikan ke tulisan asli jika kunci yang dimasukkan sama dengan kunci pada saat penggunaan plaintext.

f. Rancangan Halaman About

Berisi mengenai versi program dan pembuat program.



Gambar 22. Menu About

BAB IV

HASIL DAN PEMBAHASAN

1. Implementasi Sistem

Tahap implementasi sistem merupakan tahap dimana aplikasi yang telah dirancang dijalankan. Tahap ini menunjukkan apakah setiap proses dapat berjalan dengan baik dan mampu memberikan hasil yang diharapkan. Proses perancangan aplikasi menggunakan *visual basic NET 2010* ditampilkan dalam bentuk form-form yang menjadi sarana bagi pengguna untuk melakukan proses implementasi.

2. Pengujian Sistem

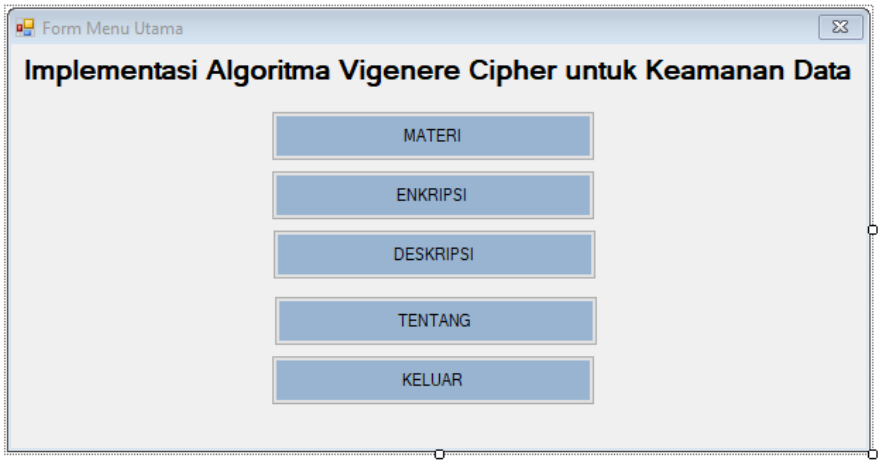
Pengujian sistem dilakukan untuk menunjukkan apakah sistem yang telah dirancang dapat berjalan sesuai harapan. Selain itu tujuan pengujian adalah untuk dapat menemukan kesalahan fungsi pada aplikasi yang dibangun dan memperbaikinya.

Pengujian dilakukan dengan memasukkan karakter atau huruf dari file berformat .txt selanjutnya diproses oleh aplikasi apakah aplikasi tersebut dapat memberikan hasil yang sesuai. Proses yang akan dilakukan pengujian dalam aplikasi ini adalah simulasi pengiriman pesan dengan menggunakan metode algoritma vigenere antara pengirim kepada penerima dengan kunci yang dimiliki masing-

masing pihak tanpa perlu bertukar kunci tunggal hingga pada akhirnya pesan asli yang dikirimkan oleh pengirim dapat dibaca oleh penerima .

a. Tampilan Awal/ Home

Tampilan pada gambar dibawah merupakan tampilan awal ketika aplikasi dijalankan. Pada form ini pengguna dapat memilih untuk membuka beberapa form lainnya seperti tombol tentang yang akan mengarahkan pengguna menuju form yang menjelaskan profil aplikasi ini, tombol materi dan tombol pengaturan yang akan mengarahkan pengguna ke form yang menjelaskan tata cara penggunaan dari aplikasi ini.



Gambar 23. Tampilan Awal/ Home

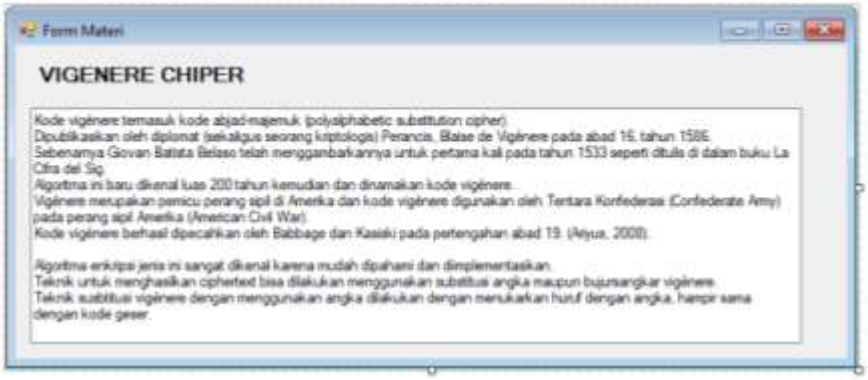
b. Tampilan Halaman Judul

Tampilan berikut ini menampilakan halaman atau form yang berisi tentang profil dari aplikasi ini. Di dalamnya terdapat judul dari aplikasi beserta maksud dari pembuatannya beserta nama dan nomor pokok mahasiswa penulis.

Gambar 24. Tampilan Halaman Tentang

c. Tampilan Materi

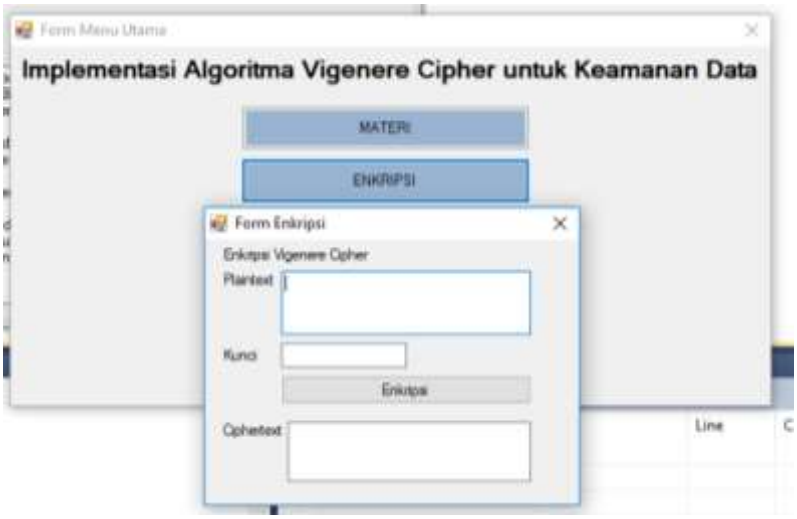
Tampilan materi merupakan tampilan halaman atau form yang berisi tentang materi yang dijalankan. Pada halaman tersebut dijelaskan apa-apa saja yang menjadi kewajiban bagi pengirim dan penerima saat menjalankan simulasi algoritma vigenere.



Gambar 25. Tampilan Materi

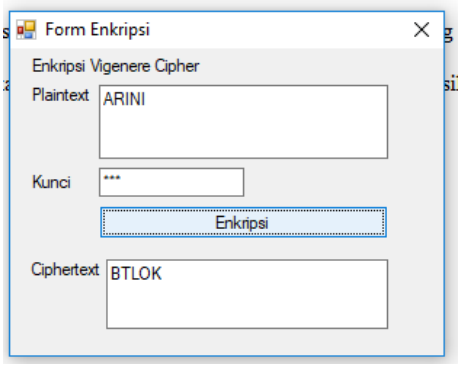
d. Proses Enkripsi dan Deskripsi

Untuk melakukan proses enkripsi, klik button enkripsi pada halaman awal di aplikasi sehingga muncul seperti gambar dibawah ini:



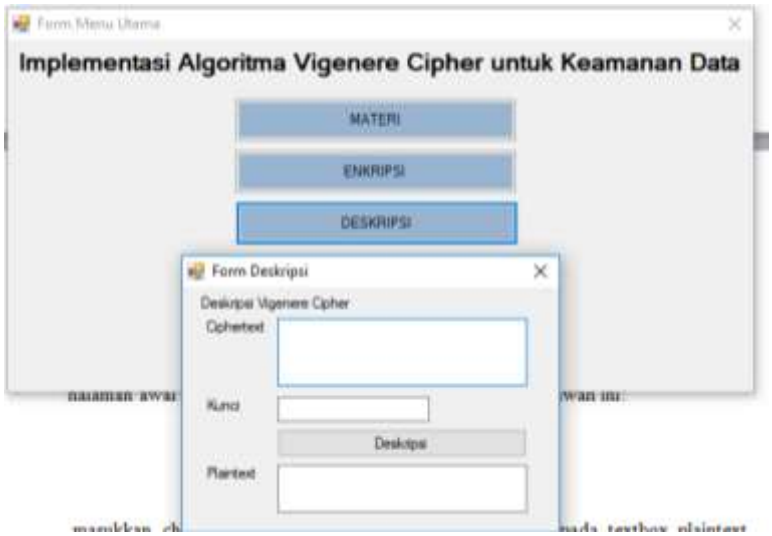
Gambar 26. Tampilan Proses Enkripsi

Selanjutnya masukkan plaintext dan kunci pada masing-masing button, pada textbox plaintext berisikan pesan berformat text dan textbox kunci berisikan angka. Setelah itu klik button enkripsi sehingga muncul chipertext yang sudah disandikan.



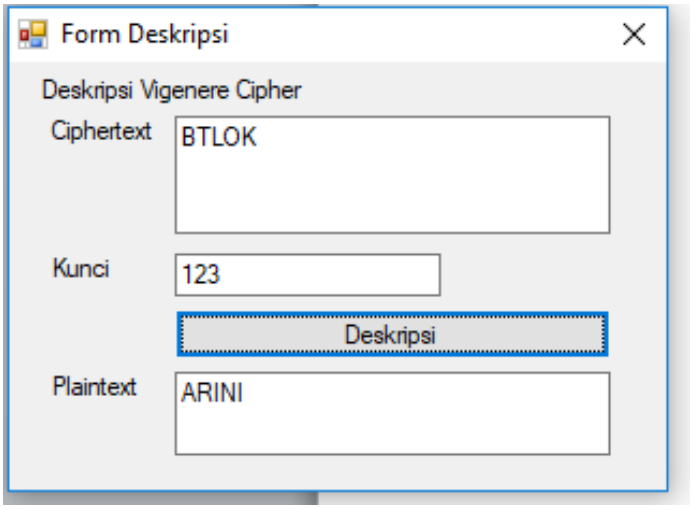
Gambar 27. Tampilan Hasil Enkripsi

Selanjutnya, Untuk melakukan proses deskripsi, klik button deskripsi pada halaman awal di aplikasi sehingga muncul seperti gambar dibawah ini:



Gambar 28. Tampilan Proses Deskripsi

masukkan chipertext dan kunci pada masing-masing button, pada textbox chipertext berisikan pesan berformat text dan textbox kunci berisikan angka. Setelah itu klik button deskripsi sehingga muncul plaintext yang asli seperti dibawah ini.



Gambar 29. Tampilan Hasil Deskripsi

3. Validasi Sistem

a. Hasil Perhitungan Manual Proses Enkripsi.

Langkah pertama membuat sebuah tabel yang bertujuan memindahkan huruf ke dalam bentuk angka.

Tabel 5. Tabel Konversi Huruf Ke Angka

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Pada tabel diatas berfungsi untuk memindahkan huruf dalam bentuk angka.

Langkah kedua membuat sebuah tabel yang bertujuan memindahkan huruf ke dalam bentuk angka.

Plaintext	A	R	I	N	I
	0	17	8	13	8

Langkah selanjutnya, masukan kunci ”1 2 3”

Plaintext	U	N	P	A	B
	0	17	8	13	8

Key	1	2	3	1	2

Pada baris tabel yang ketiga, kunci dimasukan berulang sampai cell pada tabel terpenuhi. Pada langkah selanjutnya dilakukan penjumlahan antara baris kedua dan ketika. Jika hasil penjumlahan melebihi 25, maka hasil penjumlahan dikurangi 26 dimana jumlah alfabet ada 26.

Plaintext	A	R	I	N	I
	0	17	8	13	8
Key	1	2	3	1	2
Kode CT	1	19	11	14	10

Setelah dilakukan perjumlahan maka langkah terakhir adalah mengembalikan hasil nilai angka ke dalam bentuk huruf.

Perhitungan manual

	Plaintext	A	R	I	N	I
		0	17	8	13	8
ENKRIPSI	Key	1	2	3	1	2
	Kode CT	1	19	11	14	10
	Chipertext	B	T	L	O	K

Maka diketahui ciphertext dari plaintext ”ARINI” dengan kunci ”123” adalah BTLOK.

Kesimpulan : Berdasarkan proses enkripsi menggunakan aplikasi dan proses perhitungan manual, hasil yang didapat yaitu: proses yang diaplikasi sama dengan hasil yang ada pada perhitungan manual.

b. Hasil perhitungan manual proses deskripsi.

Setelah dienkripsi, maka *plaintext* ”BTLOK” akan berubah menjadi ”ARINI” berdasarkan kunci yang telah ditetapkan.

Chipertext	B	T	L	O	K
	1	19	11	14	10

Kunci yang diinputkan adalah sebagai berikut.

Chipertext	V	P	S	B	D
	1	19	11	14	10
Key	1	2	3	1	2

Berdasarkan langkah diatas maka diperoleh hasil sebagai berikut.

Chipertext	V	P	S	B	D
	1	19	11	14	10
Key	1	2	3	1	2
Kode PT	0	17	8	13	8

Setelah dilakukan perjumlahan dari enkripsi ke dekripsi maka hasil akhirnya adalah sebagai berikut.

Perhiungan manual

	Chipertext	V	P	S	B	D
		1	19	11	14	10
DEKRIPSI	Key	1	2	3	1	2
	Kode PT	0	17	8	13	8
	Plaintext	A	R	I	N	I

Kesimpulan:

Berdasarkan proses deskripsi menggunakan aplikasi dan proses perhitungan manual, hasil yang didapat yaitu: proses yang diaplikasi sama dengan hasil yang ada pada perhitungan manual.

BAB V

PENUTUP

1. Kesimpulan

Berdasarkan pembahasan dalam perancangan Penerapan Algoritma Vigenere Cipher dalam Meningkatkan Keamanan Data, maka dapat diambil kesimpulan sebagai berikut :

1. Perangkat lunak ini dirancang untuk menampilkan simulasi pengiriman pesan berekstensi *txt antara pengirim dan penerima.
2. Penggunaan Algoritma Vigenere memiliki manfaat bagi pengirim dan penerima pesan tanpa harus menukar kunci tunggal.
3. Tidak ada lagi kesalahan pemahaman atau salah tafsir kunci tunggal karena pengirim dan penerima memiliki kunci yang dapat ditetapkan masing-masing pihak.
4. Kemungkinan bocornya kunci saat proses pertukaran informasi kunci tunggal dapat dihindari.

2. Saran

Adapun saran-saran yang dapat dilakukan penelitian ataupun pengembangan selanjutnya adalah sebagai berikut:

1. Perangkat lunak ini dapat dikembangkan dengan menggunakan kombinasi metode-metode lain.

2. Perangkat lunak ini dapat dikembangkan dan terhubung ke jaringan sehingga dapat dijalankan di lebih dari satu computer.
3. Perangkat lunak ini dapat dikembangkan menggunakan algoritma-algoritma lain yang lebih kompleks.

DAFTAR PUSTAKA

Abhirama. D, 2013, Keystream Vigenere Cipher: Modifikasi Vigenere Cipher dengan Pendekatan Keystream Generator, Program Studi Teknik Informatika ITB, Bandung.

Akbar, A. (2018). Pembangunan Model Electronic Government Pemerintahan Desa Menuju Smart Desa. Jurnal Teknik dan Informatika, 5(1), 1-5.

Arjana, Putu H. dkk. 2012. Implementasi Enkripsi Data Dengan Algoritma Vigenere Chiper. Yogyakarta: Seminar Nasional Teknologi Informasi dan Komunikasi 2012 (SENTIKA 2012).

Batubara, S., Wahyuni, S., & Hariyanto, E. (2018, September). Penerapan Metode Certainty Factor Pada Sistem Pakar Diagnosa Penyakit Dalam. In Seminar Nasional Royal (SENAR) (Vol. 1, No. 1, pp. 81-86).

Darma. S. N, 2013, Penerapan Metode Linier Kongruendan Algoritma Vigenère Chiper Pada Aplikasi Sistem Ujian Berbasis LAN, Pelita Informatika Budi Darma, Volume : IV, Nomor: 1, ISSN: 2301-9425.

Dhany, H. W., Izhari, F., Fahmi, H., Tulus, M., & Sutarman, M. (2017, October). Encryption and decryption using password based encryption, MD5, and DES. In International Conference on Public Policy, Social Computing and Development 2017 (ICOPOSDev 2017) (pp. 278-283). Atlantis Press.

Hariyanto, E., & Rahim, R. (2016). Arnold's cat map algorithm in digital image encryption. International Journal of Science and Research (IJSR), 5(10), 1363-1365.

Hendrawan, J. (2018). Rancang Bangun Aplikasi Mobile Learning Tuntunan Shalat. INTECOMS: Journal of Information Technology and Computer Science, 1(1), 44-59.

Khairul, K., Haryati, S., & Yusman, Y. (2018). Aplikasi Kamus Bahasa Jawa Indonesia dengan Algoritma Raita Berbasis Android. Jurnal Teknologi Informasi dan Pendidikan, 11(1), 1-6.

Kurnia, D. (2017). Analisis QoS Pada Pembagian Bandwidth Dengan Metode Layer 7 Protocol, PCQ, HTB Dan Hotspot Di SMK Swasta Al-Washliyah Pasar

Senen. CESS (Journal of Computer Engineering, System and Science), 2(2), 102-111.

Kurnia, D., Dafitri, H., & Siahaan, A. P. U. (2017). RSA 32-bit Implementation Technique. Int. J. Recent Trends Eng. Res, 3(7), 279-284.

Mariance, U. C. (2018). Analisa dan Perancangan Media Promosi dan Pemasaran Berbasis Web Menggunakan Work System Framework (Studi Kasus di Toko Mandiri Prabot Kota Medan). Jurnal Ilmiah Core IT: Community Research Information Technology, 6(1).

Munir, Rinaldi. Diktat Kuliah IF5054 Kriptografi. Sekolah Teknik Elektro dan Informatika Intsititut Teknologi Bandung. 2006.

Pabokory, Fresly Nandar dkk. 2015. Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard.Vol: 10 No 1 Februari 2015.

Putri, N. A. (2018). Sistem Pakar untuk Mengidentifikasi Kepribadian Siswa Menggunakan Metode Certainty Factor dalam Mendukung Pendekatan Guru. INTECOMS: Journal of Information Technology and Computer Science, 1(1), 78-90.

Rahim, R., Aryza, S., Wibowo, P., Harahap, A. K. Z., Suleman, A. R., Sihombing, E. E., ... & Agustina, I. (2018). Prototype file transfer protocol application for LAN and Wi-Fi communication. Int. J. Eng. Technol., 7(2.13), 345-347.

Ruwaida, D., & Kurnia, D. (2018). Rancang Bangun File Transfer Protocol (FTP) dengan Pengamanan Open SSL pada Jaringan VPN Mikrotik di SMK Dwiwarna. CESS (Journal of Computer Engineering, System and Science), 3(1), 45-49.

Sarif, M. I. (2017). Penemuan Aturan yang Berkaitan dengan Pola dalam Deret Berkala (Time Series).

Sarif, M. I. Classification Of Feasibility Of Basic Food Recipients In Kelurahan Tanjung Morawa A, Tanjung Morawa Sub-District Using Naïve Bayes Classifier Algorithm.

Setiawan. I, 2006, Programmable Logic Controller Dan Teknik Perancangan Sistem Kontrol, Penerbit Andi Yogyakarta, ISBN 979-763-099-4.

Sumartono, I., Siahaan, A. P. U., & Mayasari, N. (2016). An overview of the RC4 algorithm. IOSR J. Comput. Eng, 18(6), 67-73.