PENINGKATAN KEAMANAN ALGORITMA VIGENERE CIPHER DENGAN TEKNIK PENGACAKAN TABEL ENCODING MENGGUNAKAN ALGORITMA BLUM-BLUM SHUB

Disusun dan Diajukan sebagai Salah Satu Syarat Pengajuan Judul
Tugas Akhir/Skripsi pada Fakultas Sains Dan Teknologi
Universitas Pembangunan Panca Budi
Medan

SKRIPSI

DISUSUN OLEH :

NAMA : KHAIRUNISYA HOYBAN

NPM : 1514370079

PROGRAM STUDI : SISTEM KOMPUTER

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
MEDAN
2019

LEMBAR PENGESAHAN

PENINGKATAN KEAMANAN ALGORITMA VIGENERE CIPHER DENGAN TEKNIK PENGACAKAN TABEL ENCODING MENGGUNAKAN ALGORITMA BLUM BLUM SHUB

DISUSUN OLEH :

NAMA	**: KHAIRUNISYA P O YHAN**
N.P.M	**: 1514370879**
PROGRAM STUDI	**: SISTEM KOMPUTER**

Skripsi telah disetujui oleh Dosen Pembimbing Skripsi

Pada Tanggal 30 Oktober 2019:

Dosen Pembimbing I

(Andysah P. U. Siahaan, S.Kom, ,M.Kom Ph.D)

Dosen Pembimbing II

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

Mengetahui,

Dekan Fakultas Sains dan Teknologi

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

Ketua Program Studi Sistem Komputer

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

SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama	:	Khairunisya Royhan
NPM	:	1514370079
Prodi	:	Sistem Komputer
Konsentrasi	:	Keamanan Jaringan Komputer
Judul Skripsi	:	Peningkatan Keamanan Algoritma Vignere Cipher dengan Teknik Pengacakan Tabel Encoding Menggunakan Algoritma Blum Blum Shub

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,

Yang membuat pernyataan

Royhan

1514370079

Plagiarism Detector v. 1092 - Originality Report:

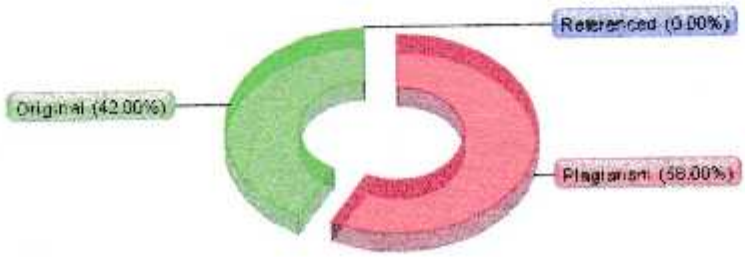
Analyzed document: 15/10/2019 15:21:44

"KHAIRUNISYA ROYHAN_1514370079_SISTEM KOMPUTER.docx"

Licensed to: **Universitas Pembangunan Panca Budi_License4**

UNIVERSITAS PEMBANGUNAN PANCA BUDI

Relation chart:



Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

Top sources of plagiarism:

% 29	wrds: 1664	http://repository.usu.ac.id/bitstream/handle/123456789/20100/Chapter%20II.pdf?sequence=4&a...
% 22	wrds: 1250	https://amindadewisutiasih.blogspot.com/feeds/posts/default
% 22	wrds: 1255	https://amindadewisutiasih.blogspot.com/2011/04/kryptography-classik-dan-vigenere.html

Show other Sources:]

Processed resources details:

242 - Ok / 49 - Failed

Show other Sources:]

Important notes:

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

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	:	KHAIRUNISYA ROYFAN
N.P.M.	:	1514370079
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, 05 Oktober 2019
Ka. Laboratorium

Tschrid Wadly, S. Kom

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI

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

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

PERMOHONAN JUDUL TESIS / SKRIPSI / TUGAS AKHIR*

Saya yang bertanda tangan di bawah ini :

Nama Lengkap	: KHAIRUNISYA ROYHAN
Tempat/Tgl. Lahir	: Binjai / 29 Oktober 1997
Nomor Pokok Mahasiswa	: 1514370079
Program Studi	: Sistem Komputer
Konsentrasi	: Keamanan Jaringan Komputer
Jumlah Kredit yang telah dicapai	: 141 SKS, IPK 3.48
Nomor Hp	: 081263860595
Dengan ini mengajukan judul sesuai bidang ilmu sebagai berikut	:

No.	Judul
1.	Peningkatan keamanan algoritma vigenere chiper dengan teknik pengacakan tabel encoding menggunakan algoritma blum blum shub

Catatan : Diisi Oleh Dosen Jika Ada Perubahan Judul

*Coret Yang Tidak Perlu

Medan, 29 Maret 2019

Pemohon,

(Khairunisya Royhan)

(Rektor)

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

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)

Tanggal : 2 Apr

Disetujui oleh:

Ka. Prodi Sistem Komputer

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

Tanggal : 2 Apr

Disetujui oleh:

Dosen Pembimbing II :

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

Telah Diperiksa oleh LPMU
dengan Plagiarisme.....58 %
Medan, 15 OKTOBER 2019
An Ka. LPMU
HUSNI M. ERONGA, BA., MSC.
Calvin Permana, SE.MM

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau

Medan, 15 Oktober 2019
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di
Tempat

Telah di terima berkas persyaratan dapat di proses
Medan, 16 OCT 2019
An. Ka. BPAA
TEGUH WAHYONO, SE., MM.

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	: KHAIRUNISYA ROYHAN
Tempat/Tgl. Lahir	: Binjai / 29 Oktober 1997
Nama Orang Tua	: DRS RAHMAD SALEH
N. P. M	: 1514370079
Fakultas	: SAINS & TEKNOLOGI
Program Studi	: Sistem Komputer
No. HP	: 081263860595
Alamat	: Jl. Jend. Gatot Subroto, Komp. cekapung indah No.112

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **Peningkatan keamanan algoritma vigenere chiper dengan teknik pengacakan tabel encoding menggunakan algoritma blum blum shub**, 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.	250.000
2.	[170] Administrasi Wisuda	: Rp.	1,500,000
3.	[202] Bebas Pustaka	: Rp.	100,000
4.	[221] Bebas LAB	: Rp.	5,000
Total Biaya		: Rp.	~~1,605,000~~

1.855.000 } Total : Rp. 4.730.000
2.875.000 }

Uk. T. 50 % Rp.

Ukuran Toga : M 16/10-19.

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

Hormat saya
KHAIRUNISYA ROYHAN
1514370079

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.

UKM CENTER 16/10 2019
PANCA BUDI

TANDA BEBAS PUSTAKA
No. 882 / Perp / BP / 2019
Perpustakaan tidak ada sangkut
pautan UPT. Perpustakaan
Medan 15 OCT 2019
UNIVERSITAS PEMBANGUNAN PANCA BUDI
UNPAB INDONESIA
UPT. PERPUSTAKAAN
Elfrida, S.Sos

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

ersitas : Universitas Pembangunan Panca Budi
ultas : SAINS & TEKNOLOGI
en Pembimbing I : ANDYSAH PUTRA UTAMA SIAHAAN, S.KOM, M.KOM
en Pembimbing II : MUHAMMAD IQBAL, S. KOM, M.KOM
ma Mahasiswa : KHAIRUNISYA ROYHAN
usan/Program Studi : Sistem Komputer
mor Pokok Mahasiswa : 1514370079
ang Pendidikan : STRATA (S1)
ul Tugas Akhir/Skripsi : PENINGKATAN KEAMANAN ALGORITMA VIGNERE CHIPER DENGAN TEKNIK PENGACAKAN TABEL ENDCODING MENGGUNAKAN ALGORITMA BLUM-BLUM SHUB

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
6/12	Acc Seminar Judul		
13/1	Revisi Bab I		
15/2	Revisi Bab II		
20/3	Revisi Bab III		
7/4	Revisi Bab IV, V		
8/4	Acc Seminar		
2/10	Acc Sidang		
31/11	Acc Jilid		

Medan, 30 November 2018
Diketahui/Disetujui oleh :
Dekan,

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

yang tidak perlu

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4.5 Telp (061) 8455571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

Universitas : Universitas Pembangunan Panca Budi
Fakultas : SAINS & TEKNOLOGI
Dosen Pembimbing I : ANDYSAH PUTRA UTAMA SIAHAAN S.KOM, M.KOM, Ph.D
Dosen Pembimbing II : DR. MUHAMMAD IQBAL S.KOM, M.KOM
Nama Mahasiswa : KHAIRUNISYA ROYHAN
Jurusan/Program Studi : Sistem Komputer
Nomor Pokok Mahasiswa : 1514370079
Jenjang Pendidikan : STRATA (S1)
Judul Tugas Akhir/Skripsi : PENINGKATAN KEAMANAN ALGORITMA VIGNERE CHIPER DENGAN TEKNIK PENGACAKAN TABEL ENCODING MENGGUNAKAN ALGORITMA BLUM-BLUM SHUB

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
7/12 2018	Acc Judul		
15/9 19	Revisi Latar belakang		
18/9 19	Acc Bab II		
18/9 19	Revisi Bab II		
21/9 19	Acc Bab II & III		
26/9 19	Acc Semua		
14/5 20	Acc Sidang		
1/11 19	Revisi		
24/11 19	Acc Sidang		

Medan, 30 November 2018
Diketahui/Disetujui oleh :
Dekan,

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

yang tidak perlu

ABSTRAK

KHAIRUNISYA ROYHAN

PENINGKATAN KEAMANAN ALGORITMA VIGNERE CHIPER DENGAN TEKNIK PENGACAKAN TABEL ENCODING MENGGUNAKAN ALGORITMA BLUM-BLUM SHUB

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 dan Blum-Blum Shub. 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 dan Blum-Blum Shub.

Kata Kunci: Kriptografi, Blum-Blum Shub, Vigenere Cipher.

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 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.Dalam proses enkripsi dan deskripsi pada algoritma vigenere chiper ini akan ditambahkan metode algoritma blum-blum shub agar penyandian pesan lebih sulit untuk dipecahkan. 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 "**Peningkatan keamanan algoritma Vigenere Cipher dengan teknik pengacakan tabel encoding menggunakan algoritma blum-blum shub**"**.**

1.2 Rumusan Masalah

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

1. Bagaimana merancang sebuah peningkatan keamaan pada aplikasi *software* menggunakan kriptografi *vigenere chiper* dengan algoritma blum-blum shub sebagai pengaman informasi teks ?
2. Bagaimana membuat aplikasi peningkata keamanan pesan dengan menerapkan kriptografi dan algoritma blum-blum shub sebagai pengamanan aplikasi berbasis *desktop* ?

1.3 Batasan Masalah

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

1. Aplikasi yang dibangun hanya menampilkan proses melakukan enkripsi dan dekripsi informasi dengan menggunakan algoritma *vigenere chiper* dengan algoritma blum-blum shub.
2. Perancangan aplikasi merupakan simulasi pengamanan aplikasi.
3. Program yang digunakan dalam perancangan aplikasi ini adalah *visual basic .net 2010* menggunakan algoritma vigenere cipher dalam proses pengamanan aplikasi.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai penulis dalam perancangan aplikasi pengamanan aplikasi adalah :

a. Merancang keamanan aplikasi dengan menerapkan kriptografi dengan menggunakan algoritma *vigenere cipher* dengan algoritma blum-blum shub .
b. Merancang sistem pengamanan informasi dengan proses enkripsi dan dekripsi menggunakan metode algoritma *vigenere cipher* dengan algoritma blum-blum shub.

1.5 Manfaat Penelitian

Perancangan aplikasi penerapan *algoritma* vigenere dengan algoritma blum-blum shub ini bermanfaat bagi masyarakat luas antara lain :

1. Dengan menggunakan aplikasi ini seseorang dapat mengamankan suatu informasi tanpa takut diketahuin oleh orang lain.

2. Dapat digunakan dalam proses kerahasian data.
3. Proses pertukaran data atau informasi menjadi aman.

BAB II

LANDASAN TEORI

2.1 Aplikasi

Aplikasi adalah sebuah 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.

2.2 *Kriptografi*

1. 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 :

a. Pesan, *Plaintext*, dan *Cipherteks*

Pesan (*message*) adalah data atau in*Form*asi 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 ditrans*Form*asikan kembali menjadi *Plaintext* semula agar dapat diterima dan bisa dibaca.

b. 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*.

c. Enkripsi dan dekripsi

Proses menyandikan *Plainteks* menjadi *Cipherteks* disebut enkripsi (*encryption*) atau *enCiphering*. Sedangkan proses mengembalikan *Cipherteks* menjadi *Plainteks* disebut dekripsi (*decryption*) atau *deCiphering*.

d. *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 trans*Form*asi *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

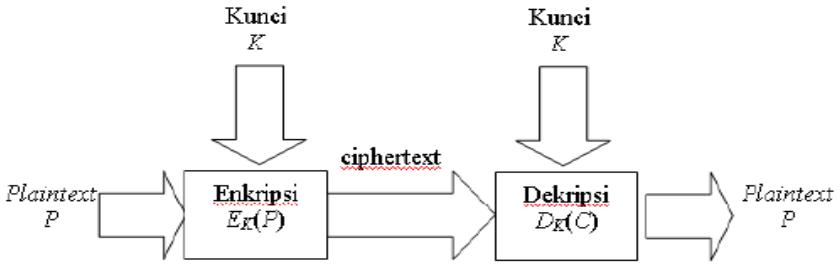
C = Cipherteks

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 2.2.1. Skema enkripsi dan dekripsi menggunakan kunci

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

e. 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.

f. Penyadap

Penyadap (*eavesdropper*) adalah orang yang mencoba menangkap pesan selama ditransmisikan. Tujuan penyadap adalah untuk mendapatkan in*Form*asi sebanyak - banyaknya mengenai sistem *Kriptografi* yang digunakan untuk berkomunikasi dengan maksud untuk memecahkan *Cipherteks*. Nama lain penyadap : *enemy*, *adversary*, *intruder*, *interceptor*, *bad guy*.

g. 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*)

mentrans*Form*asikan *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.

2. Tujuan *Kriptografi*

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

a. 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*.

b. 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)?”.

c. 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.

d. Non-Repudiation

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

e. *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 2.2.1. Konversi *Vigenere* 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

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 *Cipher*textnya adalah tulisan *Plaintext* diubah ke dalam bentuk angka seperti pada tabel konversi di bawah ini

Tabel 2.2.2. 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 *Cipher*textnya adalah:

VPXZGIAXIVWPUBTTMJPWIZITWZT

2) Huruf

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

Tabel 2.2.3. *Vigenere Cipher*

	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

2.3 Metode Blum-Blum Shub

Blum-Blum Shub (BBS) merupakan suatu *Pseudo Random Number Generator* yang diajukan pada tahun 1986 oleh Lenore Blum, Manuel Blum dan Michael Shub. BBS memiliki bentuk persamaan:

$X_{n+1} = X_{n^2} \bmod m$

dengan m merupakan hasil dari perkalian dua buah bilangan prima besar p dan q ,serta output-nya dalam Least Significant Bit dari X_n dimana hal yang sama sebagai parity dari X_n. Dua buah bilangan prima p dan q harus kongruen terhadap 3 mod 4 dan Greatest Common Divisor(GCD) harus kecil. Generator ini sering digunakan untuk aplikasi kriptografi, karena generator ini tidak begitu cepat. Bagaiman pun juga, generator ini mempunyai bukti keamanan yang kuat, dimana berhubungan dengan kualitas generator karena sulitnya faktorisasi integer. Berikut langkah-langkah algoritma dari BBS:

1. Pilih dua bilangan prima p dan q, dimana p dan q keduanya kongruen terhadap 3 modulo 4.

   $p \equiv 3 \bmod 4$ dan $q \equiv 3 \bmod 4$.
2. Hasilkan bilangan bulat Blum ndengan menghitung $n = p \times q$.
3. Pilih lagi sebuah bilangan acak ssebagai umpan, bilangan yang dipilih harus memenuhi kriteria:

a. $2 \leq s < n$.

b. s dan n adalah relatif prima.

4. Hitung nilai $x_o = s^2 \bmod n$.

5. Hasilkan bilangan bit acak dengan cara:

   a. Hitung $x_i = x_{(i-1)}^2 \bmod n$.

   b. Hasilkan z_i = bit-bit yang diambil dari x_i. Bit yang diambil bisa merupakan LSB (Least Significant Bit) atau hanya satu bit atau sebanyak j bit (j tidak melebihi $\log_2 (\log_2 n)$). Bilangan bit acak dapat digunakan langsung atau diformat dengan aturan tertentu, sedemikian hingga menjadi bilangan bulat.

2.4 Serangan Terhadap *Kriptografi*

Serangan ("serangan kriptanalisis") terhadap *Kriptografi* dapat dikelompokkan dengan beberapa cara:

1. Berdasarkan keterlibatan penyerang dalam komunikasi, serangan dapat dibagi atas dua macam, yaitu:
2. 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 in*Form*asi yang digunakan untuk kriptanalisis. Beberapa metode penyadapan antara lain :

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

3. 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 in*Form*asi yang tersimpan, dan sebagainya.

4. Berdasarkan banyaknya in*Form*asi yang diketahui oleh kriptanalis, maka serangan dapat dikelompokkan menjadi lima jenis, yaitu:

   a. *Ciphertext-only attack*

      Ini adalah jenis serangan yang paling umum namun paling sulit, karena in*Form*asi 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 in*Form*asi yang diketahui,dan sebagainya.

b. Known-Plaintext attack

Ini adalah jenis serangan dimana kriptanalis memiliki pasangan *Plainteks* dan *Cipherteks* yang berkoresponden.

c. 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.

d. *Chosen-Ciphertext attack*

Ini adalah jenis serangan dimana kriptanalis memilih *Cipher*text untuk dideskripsikan dan memiliki akses ke *Plaintext* hasil deskripsi.

e. *Chosen text attack*

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

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

a. 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.

b. *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.

c. 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.

d. 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.

6. Kompleksitas serangan

Kompleksitas serangan dapat diukur dengan beberapa cara, yaitu :

a. 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.

b. Kompleksitas waktu (*time complexity*)

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

c. 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.

2.5 Keamanan Algoritma Kriptografi

Doni Ariyus (2005) Menuliskan Lard Knudsen mengelompokkan hasil kriptanalis ke dalam beberapa kategori berdasarkan jumlah dan kualitas in*Form*asi yang berhasil ditemukan :

1. Pemecahan total (*total break*). Kriptanalis menemukan kunci *K*
2. Deduksi (*penarikan kesimpulan*) global (*global deduction*). Kriptanalismenemukan algoritma alternatif, A, yang ekivalen dengan tetapi tidak mengetahui kunci *K*.)
3. Deduksi lokal (*instance*/*local deduction*). Kriptanalis menemukan *Plainteks* dari *Cipherteks* yang disadap.

Deduksi in*Form*asi (*inFormation deduction*). Kriptanalis menemukan beberapa in*Form*asi perihal kunci atau *Plainteks*. Misalnya kriptanalis mengetahui beberapa kunci, kriptanalis mengetahui bahasa yang digunakan untuk menulis *Plainteks*, kriptanalis mengetahui *Form*at *Plainteks*, dan sebagainya. Sebuah algoritma dikatakan aman mutlak tanpa syarat (*unconditionally secure*) bila *Cipherteks* yang dihasilkan oleh algoritma tersebut tidak mengandung cukup in*Form*asi untuk menentukan *Plainteks*.

2.6 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.

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.

2.7 *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:

1. Untuk membuat program aplikasi berbasiskan windows.
2. Untuk membuat obyek-obyek pembantu program, seperti Control Active X, File Help, Aplikasi Internet dan sebagainya.

3. Menguji program (debugging) dan menghasilkan program akhir berakhiran ”EXE” yang bersifat executable atau dapat langsung dijalankan.

   Keistimewaan utama dari *Visual Basic* adalah:

4. Menggunakan plat*Form* pembuatan program yang diberi nama *developer studio*, yang memiliki tampilan seperti C++ dan visual J++.
5. Memiliki kompiler handal yang dapat menghasilkan *File Executable* yang lebih cepat dan efisien.
6. Memiliki tambahan saran wizard yang baru. Tambahan kontrol-kontrol baru dan lebih canggih serta peningkatan kaidah struktur bahasa *Visual Basic*.
7. Kemampuan membuat Active X dan fasilitas internet yang lebih banyak.
8. Sarana akses yang lebih cepat dan andal untuk membuat aplikasi database yang berkemampuan tinggi.
9. *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 sebagai berikut:

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 *Form*1. 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 *Form*ulir (*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 *Form*1. 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.

2.8 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.

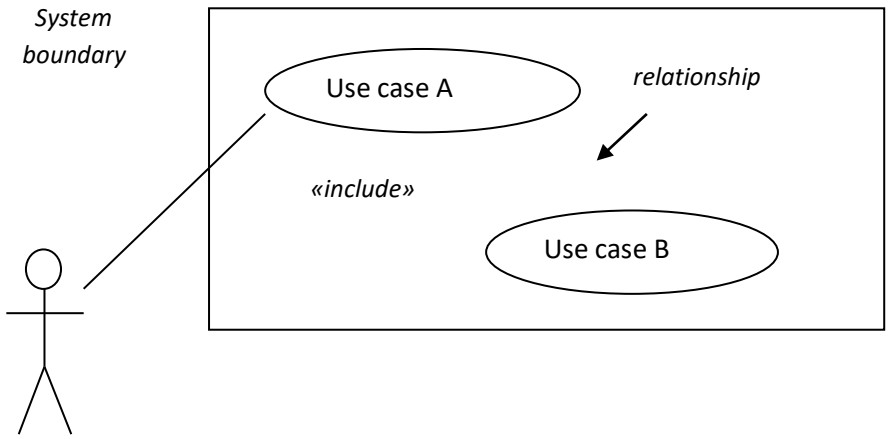
1. *Use Case Diagrams*

   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 in*Form*asi yang akan dibuat. *Use case* mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem in*Form*asi yang akan dibuat. Secara kasar, *use case* digunakan untuk mengetahui fungsi apa saja yang ada di dalam sebuah sistem in*Form*asi 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*.

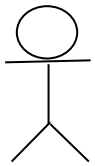


Gambar 2.7.1. *Use Case Diagram*

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

a. Aktor

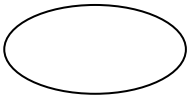
Aktor merupakan orang, proses, atau sistem lain yang berinteraksi dengan sistem in*Form*asi yang akan dibuat di luar sistem in*Form*asi yang akan dibuat itu sendiri, jadi walaupun simbol dari aktor adalah gambar orang, tapi aktor belum tentu merupakan orang.



Gambar 2.7.2. Aktor

b. *Use Case*

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



Gambar 2.7.3. *Use Case*

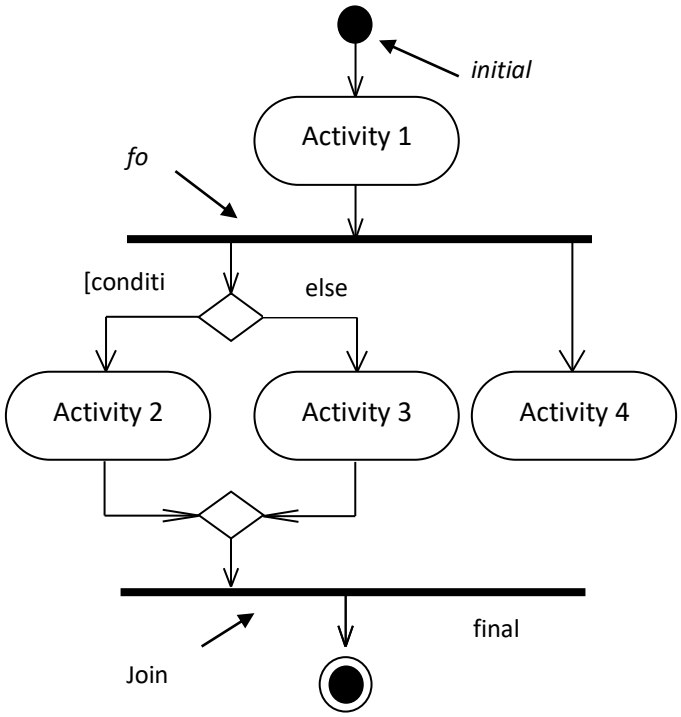
2. Activity Diagrams

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 :

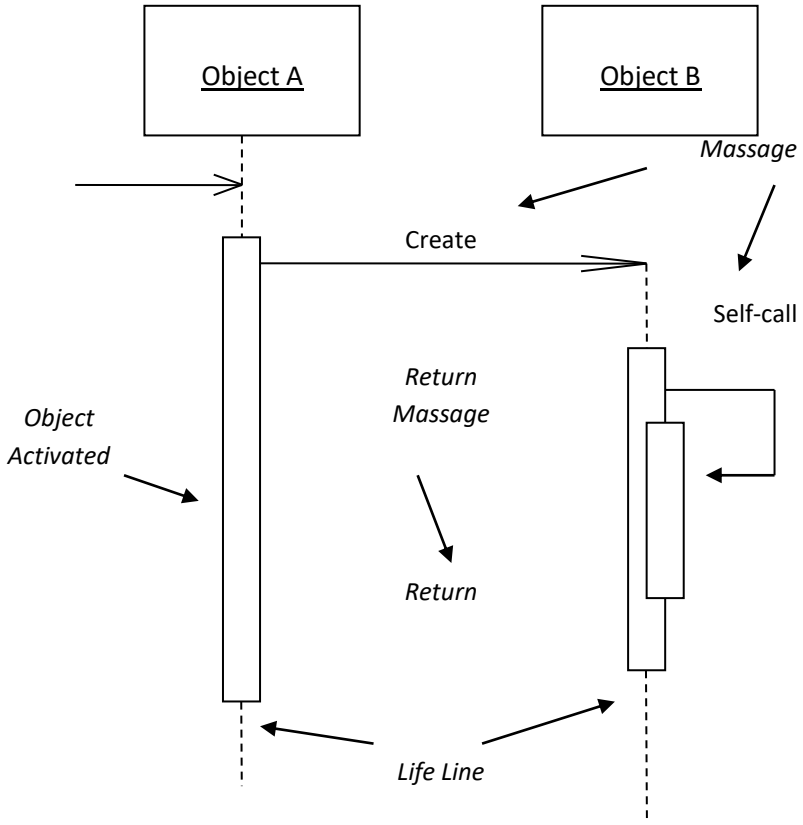
a. Rancangan proses bisnis dimana setiap urutan aktivitas yang digambarkan merupakan proses bisnis sistem yang didefinisikan.
b. Urutan atau pengelompokkan tampilan dari sistem/*user interface* di mana setiap aktivitas dianggap memiliki antarmuka tampilan.
c. Rancangan pengujian di mana setiap aktivitas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



Gambar 2.7.4. *Activity Diagram*

3. Sequence Diagrams

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 2.7.5. *Sequence Diagram*

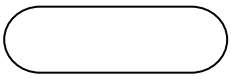
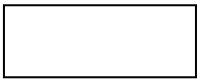
2.9 Pengertian Flowchat

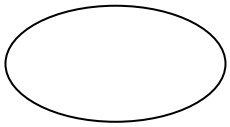
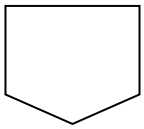
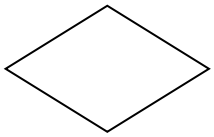
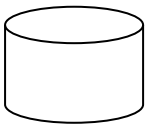
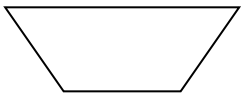
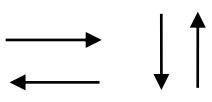
Menurut (Sariadin Siallagan, 2013), Flowchart adalah suatu diagram alir yang mempergunakan simbol atau tanda untuk menyelesaikan masalah. Dalam hal ini, penyelesaian masalah menggunakan simbol-simbol yang telah disepakati.

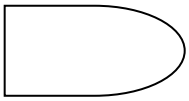
Menurut (Abdillah Baraja, 2012) Flowchart adalah representasi grafik yang menggambarkan setiap langkah yang akan dilakukan dalam suatu proses, yang merupakan alat bantu yang banyak digunakan untuk menggambarkan sistem secara pisikal.

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 2.8.1. 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).

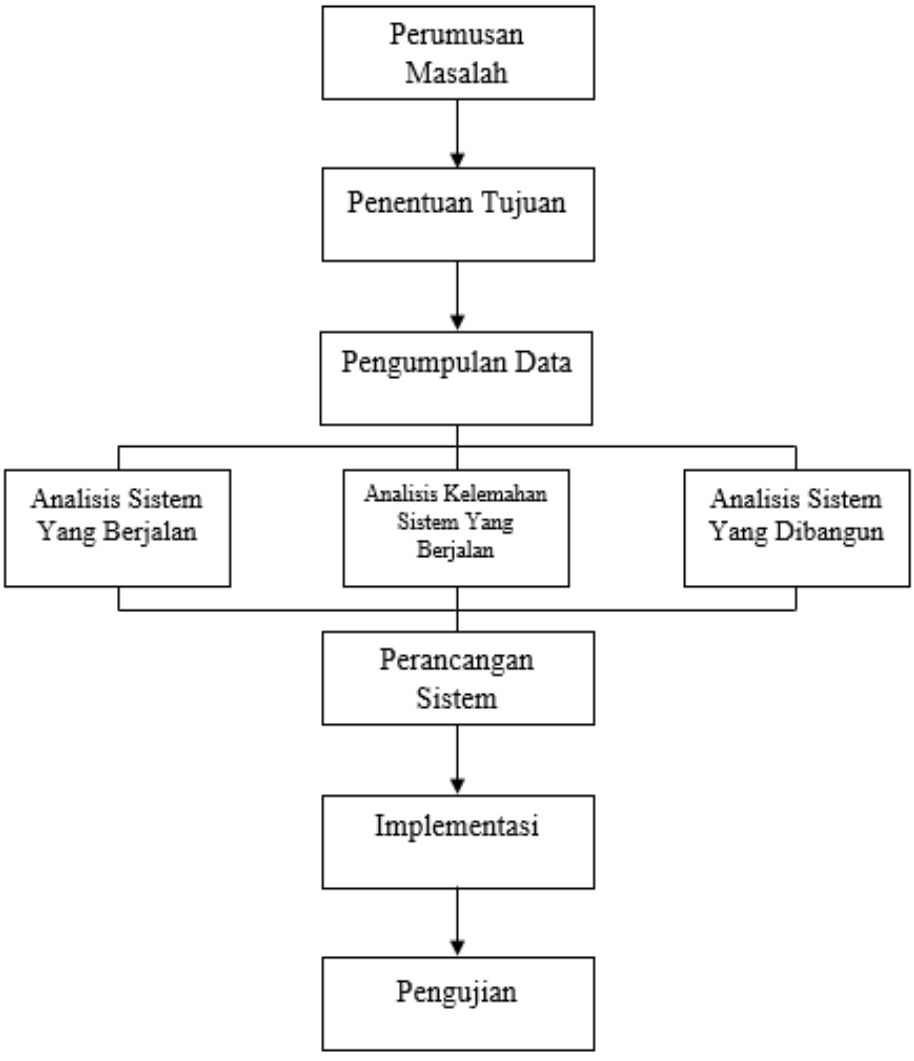
Sumber : Abdillah Baraja, 2012

BAB III

METODOLOGI PENELITIAN

3.1 Tahapan Penelitian

Adapun tahapan penelitian yang dilakukan oleh penulis yaitu sebagai berikut:



Gambar 3.1 : Tahapan penelitian
Sumber : Berdasarkan Rancangan Penulis (2019)

3.2 Metode Pengumpulan Data

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

1. Studi literature

   Pengumpulan data dengan cara mengumpulkan *literature*, jurnal, *paper* dan bacaan-bacaan yang ada kaitannya dengan judul penelitian.

2. 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.

3.3 Analisis Sistem

1. Analisis sistem yang berjalan

   Dalam materi perkuliahan Keamanan komputer terdapat bab mengenai enkripsi. Salah satu bentuk metode keamanan komputer adalah menggunakan metode *Vigenere Cipher*. 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 *Ciphertext*nya harus menggunakan penghitungan seperti di bawah ini:

Langkah Pertama membuat tabel konversi ASCII.

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 255 1

Dalam hal ini plaintext adalah *Ciphertext* 1 yang didapat.

C1 = S + K mod 255

= 83 + 75 mod 255

= 158 = ž

C2 = E + A mod 255

= 69 + 65 mod 255

= 134 = †

C3 = L + M mod 255

= 76 + 77 mod 255

= = ™

C4 = A + P mod 255

= 65 + 80 mod 255

= 145 = ‘

C5 = M + U mod 255

= 77 + 85 mod 255

= 162 = ¢

C6 = A + S mod 255

= 65 + 83 mod 255

= 148 = ”

C7 = T + K mod 255

= 84 +75 mod 255

= 159 = Ÿ

C8 = D + A mod 255

= 68 + 65 mod 255

= 133 = a

C9 = A + M mod 255

= 65 + 77 mod 255

= 142 = ‘

C10 = T + P mod 255

= 84 + 80 mod 255

= 164 = ‘

C11 = A + U mod 255

= 65 + 85 mod 255

= 150 = ©

C12 = N + S mod 255

= 78 + 83 mod 255

= 161 = ”

C13 = G + K mod 255

= 71 + 74 mod 255

= 145 = ™

Sehingga *Ciphertext* kedua yang didapat adalah:

Ciphertext = **ž†™‘¢”Ÿa‘‘©”™ˆ**

2. Kelemahan sistem yang berjalan

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

a. Harus melihat tabel untuk proses penyandian teks
b. Jika tulisan terlalu banyak, menambah kesulitan pada proses penyandian.
c. Memungkinkan kesalahan pada proses penyandian

3. Analisis Sistem yang Dibangun

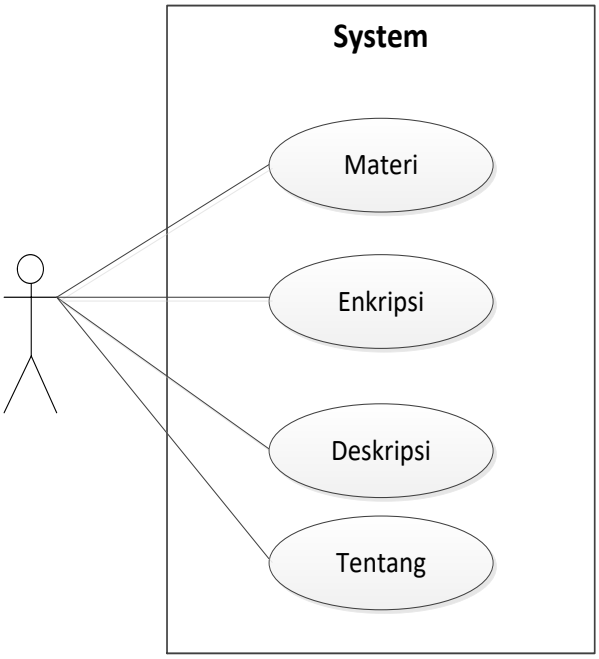
Perancangan sistem yang akan dibangun dilakukan setelah menganalisis permasalahan yang ada dari sistem berjalan. Sistem baru yang akan dibangun ini merupakan perubahan dari sistem yang dilakukan secara manual yang akan dijadikan secara komputerisasi dengan menggunakan aplikasi visual studio.

3.4 Rancangan Penelitian

1. *Unified Modeling Language*

a. *Use case* Diagram

Berikut adalah *use case diagram* yang menggambarkan kegiatan.



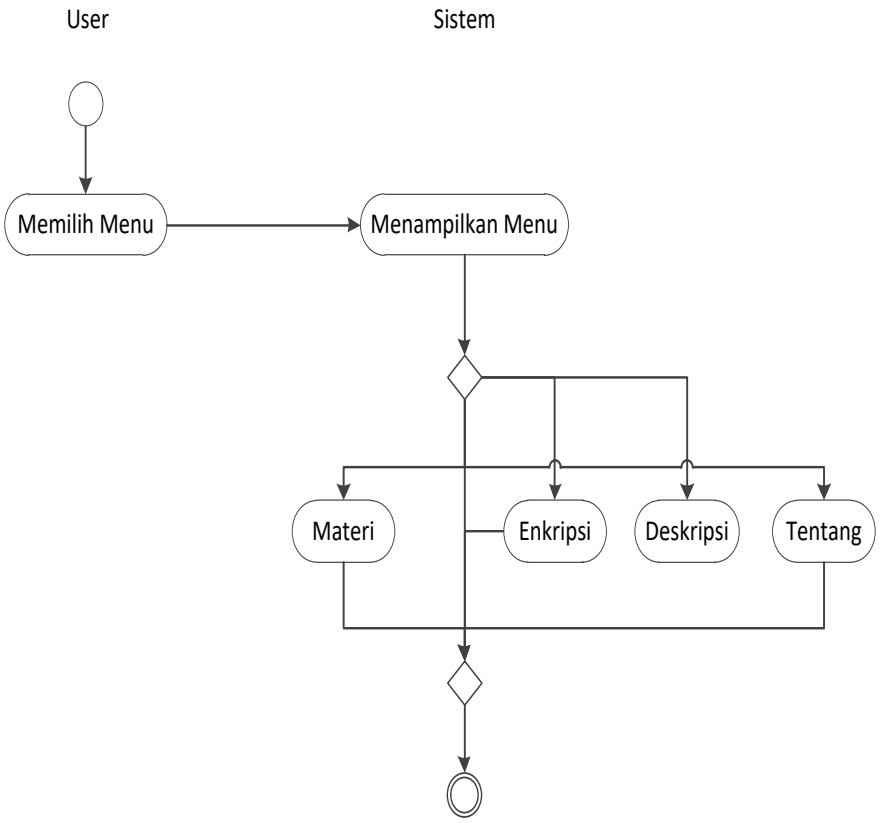
Gambar 3.4.1. *Use Case Diagram*
Sumber : Berdasarkan Rancangan Penulis (2019)

Keterangan :

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

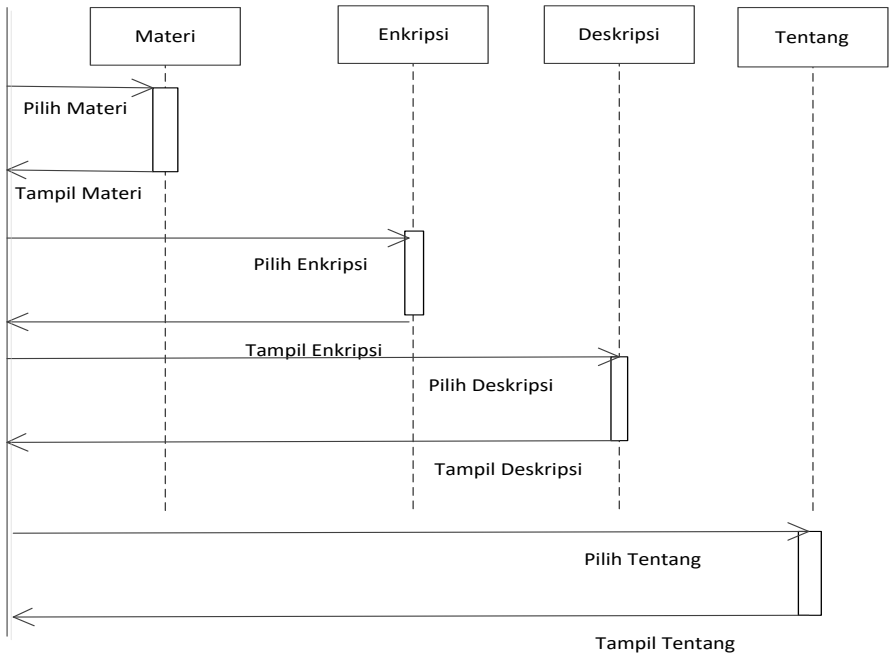
b. Activity Diagram

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



Gambar 3.4.2. *Activity Diagram*
Sumber : Berdasarkan Rancangan Penulis (2019)

c. Sequence Diagram



Gambar 3.4.3. *Sequence Diagram*
Sumber : Berdasarkan Rancangan Penulis (2019)

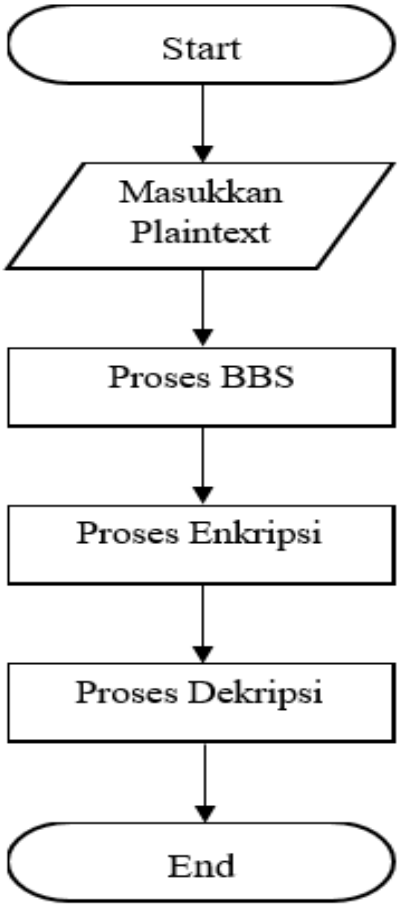
Keterangan Gambar :

1) Diagram di atas menjelaskan bahwa user memilih materi kemudian Sistem menampilkan menu 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.

2. *Flowchart* Sistem

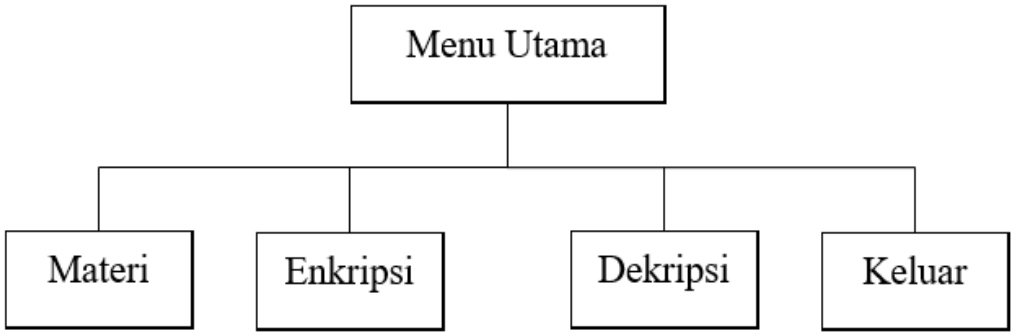
Rancangan flowchart sistem ini dibuat untuk menggambarkan cara kerja sistem yang akan dibangun. Dimulai dengan memasukkan pesan yang akan dienkripsi, kemudian memilih kunci acak menggunakan bantuan metode *Blum-blum Shub*. Setelah itu bari isi pesan dapat dienkripsi maupun didekripsikan kembali. Adapun bentuk *flowchart* sistem yang akan dibuat ialah sebagai berikut:



Gambar 3.4.4. *Flowchart* Sistem
Sumber : Berdasarkan Rancangan Penulis (2019)

3.5 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.

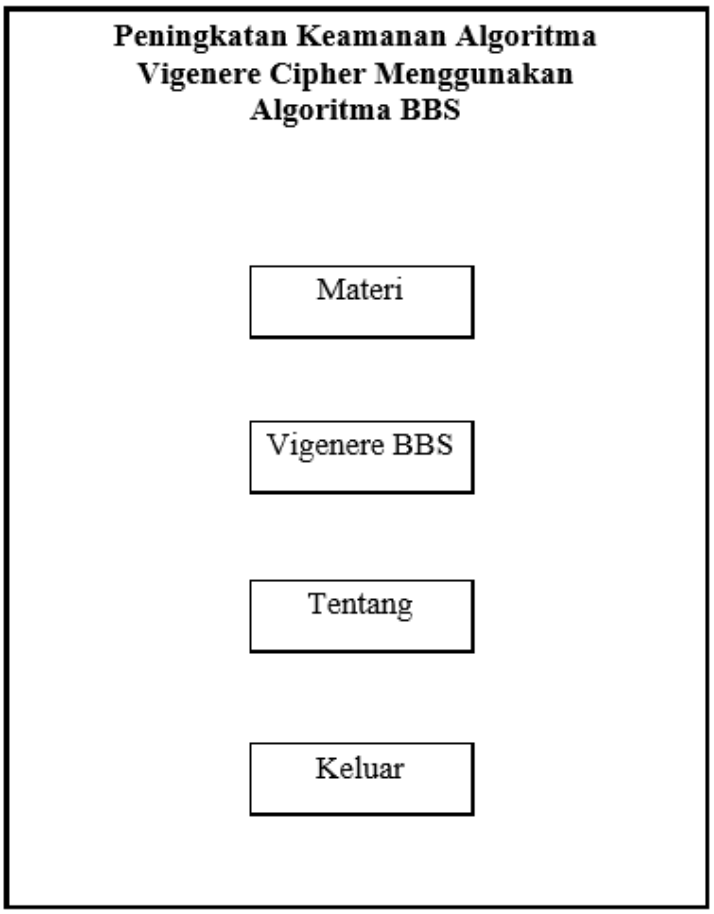


Gambar 3.5. Struktur Navigasi Enkripsi
Sumber : Berdasarkan Rancangan Penulis (2019)

3.6 Perancangan Antarmuka

1. Rancangan Halaman Menu Utama

   Form ini berisi tombol-tombol seperti menu Materi, Vigenere BBS, Tentang, dan Keluar.



Gambar 3.6.1. Rancangan Halaman Menu Utama
Sumber : Berdasarkan Rancangan Penulis (2019)

Pada tampilan di atas terdapat 4 tombol yaitu Materi, Vigenere BBS, Deskripsi, Tentang dan keluar.

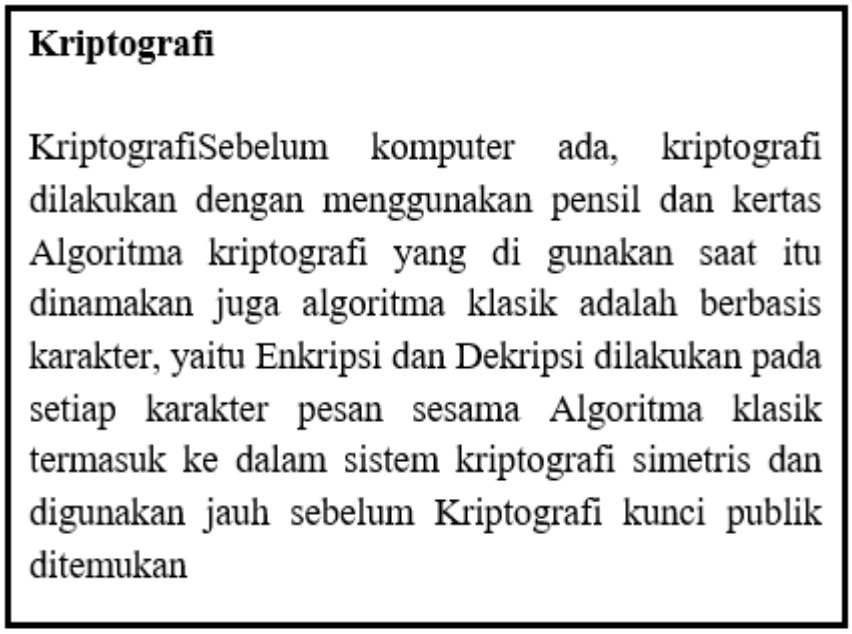
a. Tombol Materi berfungsi untuk menghubungkan pengguna ke form materi.
b. Tombol Vigenere BBS berfungsi untuk menghubungkan pengguna ke form Vigenere BBS.

c. Tombol Tentang berfungsi untuk menghubungkan pengguna ke form tentang.

d. Tombol Keluar berfungsi untuk keluar dari program.

2. Rancangan Halaman Materi

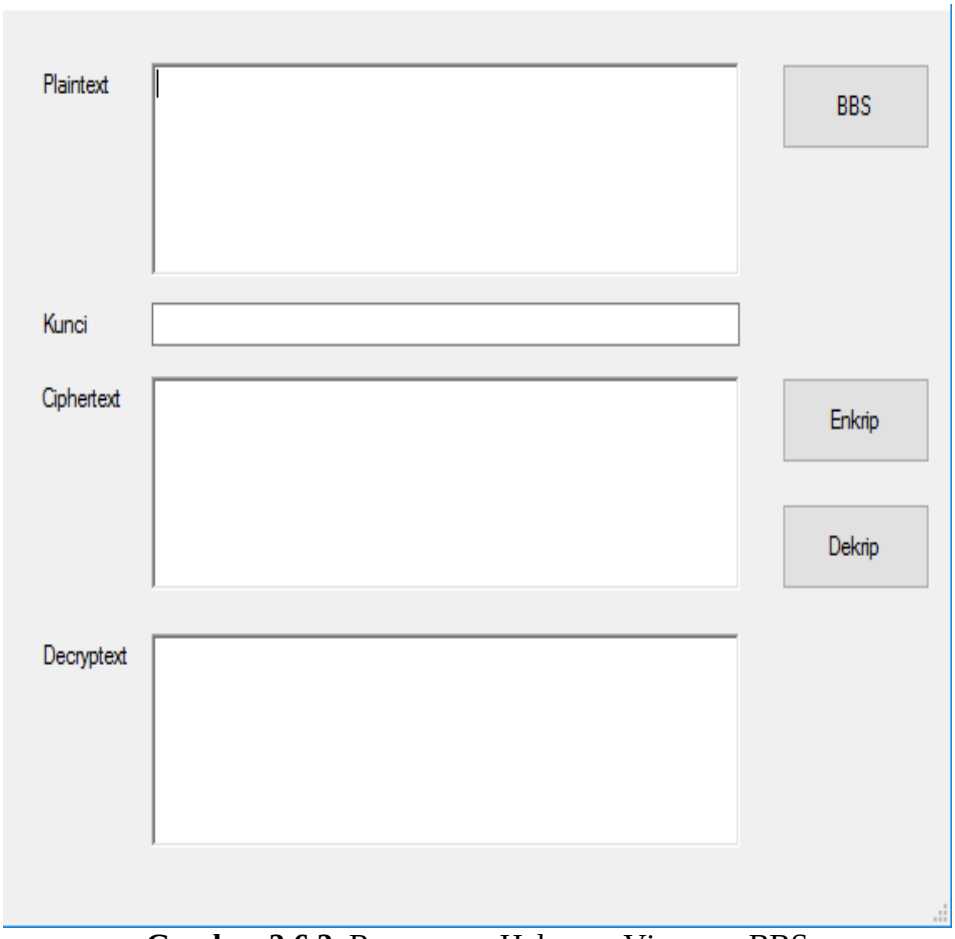
Form ini digunakan untuk menjelaskan cara kerja penyandian, dimulai dari plaintext kemudian kunci yang dikonversikan dalam bentuk angka. Setelah itu dilakukan proses penjumlahan dan jika hasil penjumlahan maka akan dikurangi 6 lalu hasilnya akan dikembalikan lagi ke dalam bentuk huruf.



Gambar 3.6.2. Rancangan Halaman Materi
Sumber : Berdasarkan Rancangan Penulis (2019)

3. Rancangan Halaman Vigenere BBS

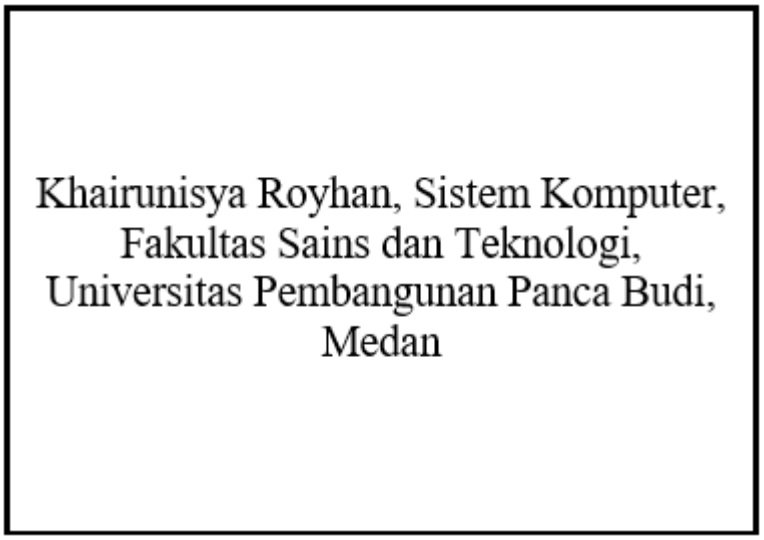
Berisi penjelasan mengenai Vigenere BBS. Pengguna memasukkan tulisan asli atau *plaintext* ke dalam kolom *plaintext* kemudian tekan tombol BBS untuk membentuk kunci, setelah itu pilih tombol Enkripsi untuk mengacak pesan dengan bantuan kunci yang telah dibuat sebelumnya, dan tekan tombol Dekripsi untuk mengembalikan isi pesan kebentuk awal.



Gambar 3.6.3. Rancangan Halaman Vigenere BBS
Sumber : Berdasarkan Rancangan Penulis (2019)

4. Rancangan Halaman Tentang

Berisi mengenai versi program dan pembuat program.



Gambar 3.6.4. Rancangan Halaman Tentang
Sumber : Berdasarkan Rancangan Penulis (2019)

BAB IV

HASIL DAN PEMBAHASAN

4.1 Kebutuhan Spesifikasi Minimum Hardware dan Software

1. Kebutuhan Hardware
    a. Processor berkecepatan 2.0 Ghz
    b. RAM 2 Gb
    c. Keyboard dan Mouse
    d. Monitor 14
2. Kebutuhan Software
    a. Microsoft Windows 7 , Windows XP
    b. Visual Studio 2010

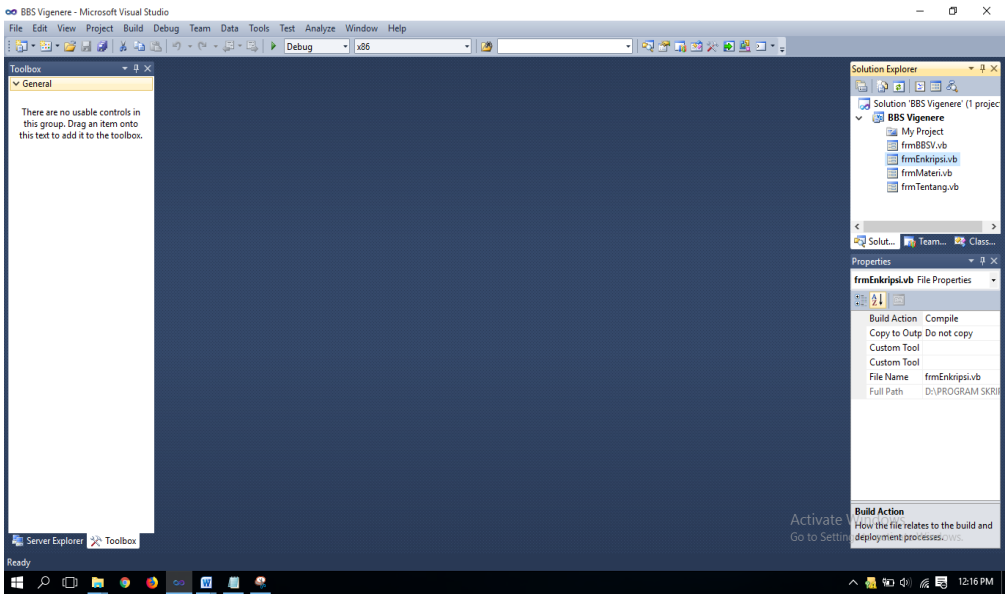
4.2 Pengujian Sistem

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.

1. 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

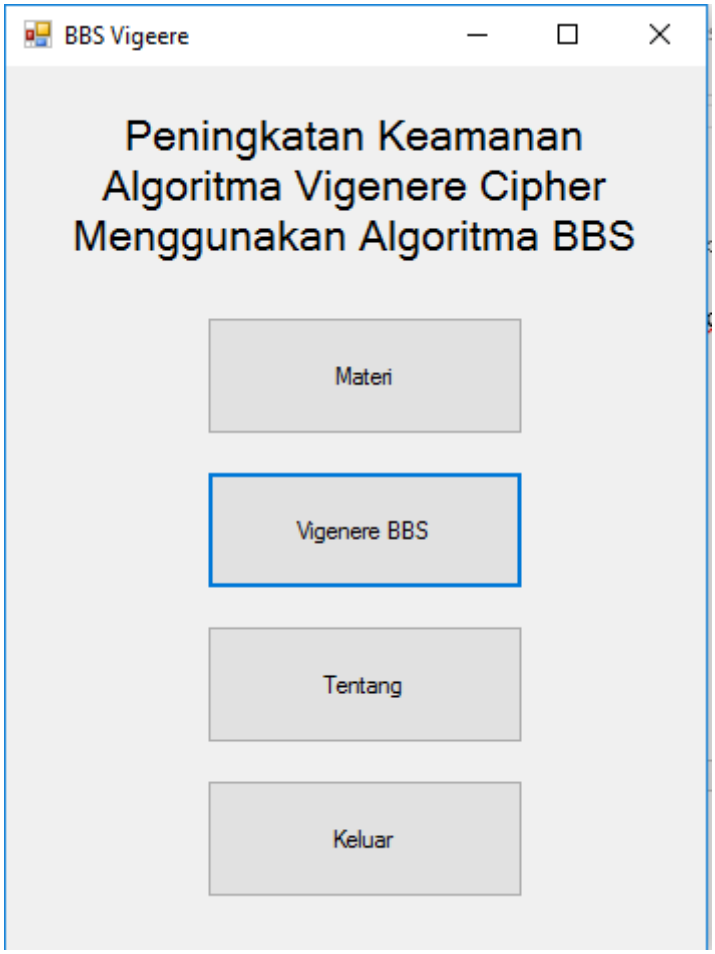
dan tombol pengaturan yang akan mengarahkan pengguna ke form yang menjelaskan tata cara penggunaan dari aplikasi ini.



Gambar 4.2.1. Tampilan Awal/ Home
Sumber : Hasil pengujian Aplikasi (2019)

2. Tampilan Halaman Menu Utama

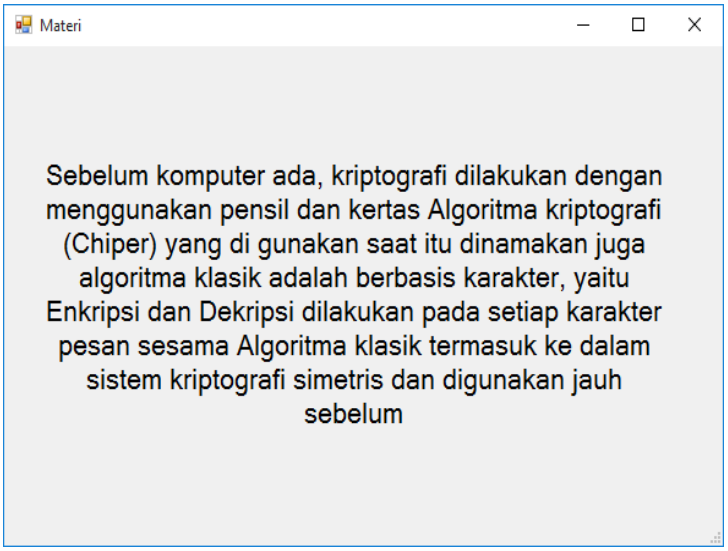
Tampilan berikut ini menampilakan halaman atau form yang berisi tentang profil dari aplikasi ini. Di dalamnya terdapat judul dari aplikasi beserta maksud dari pembuatannya beserta nama dan nomor pokok mahasiswa penulis.



Gambar 4.2.2. Tampilan Halaman Menu Utama
Sumber : Hasil pengujian Aplikasi (2019)

3. Tampilan Materi

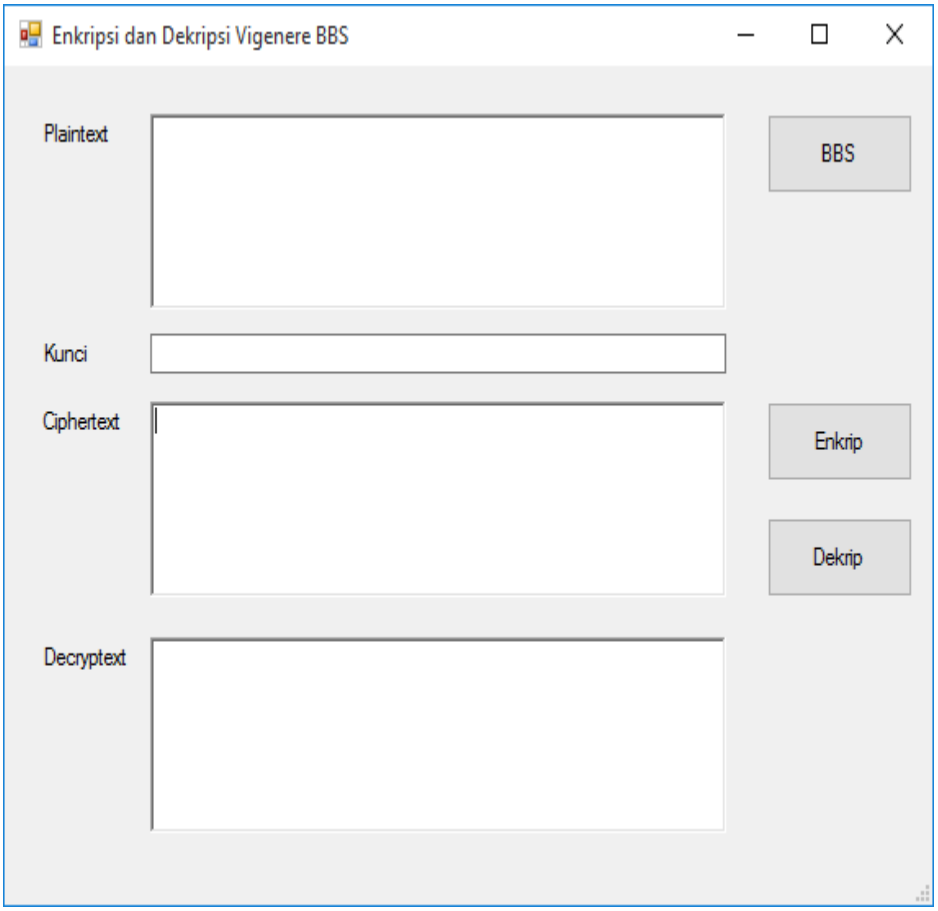
Tampilan materi merupakan tampilan halaman atau form yang berisi tentang materi yang dijalankan. Pada halaman tersebut dijelaskan apa-apa saja yang menjadi kewajiban bagi pengirim dan penerima saat menjalankan simulasi algoritma vigenere.



Gambar 4.2.3. Tampilan Materi
Sumber : Hasil pengujian Aplikasi (2019)

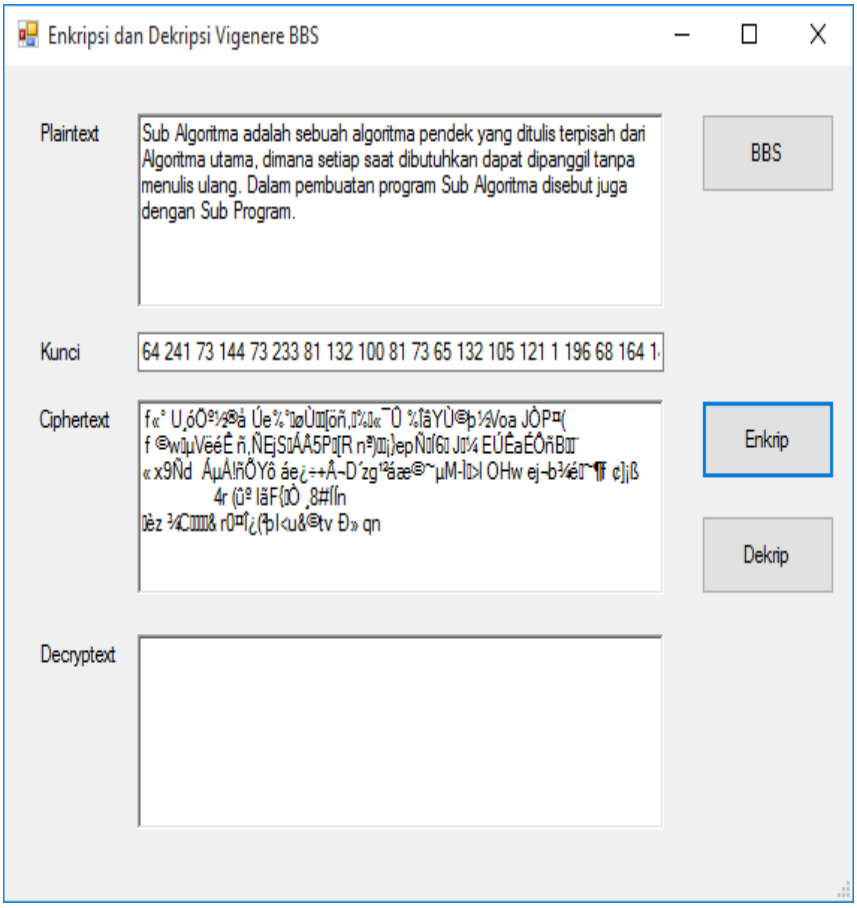
4. Tampilan Halaman Utama Algoritma Vigenere

Tampilan berikut merupakan tampilan utama pada aplikasi ini. Algoritma vigenere merupakan protokol yang menjamin tidak adanya pertukaran kunci antara pihak-pihak yang melakukan enkripsi dan dekripsi. Kedua belah pihak menggunakan kunci mereka masing-masing untuk mengenkripsi pesan dan kemudian untuk mendekripsi pesan tanpa perlu mengetahui kunci yang lainnya.



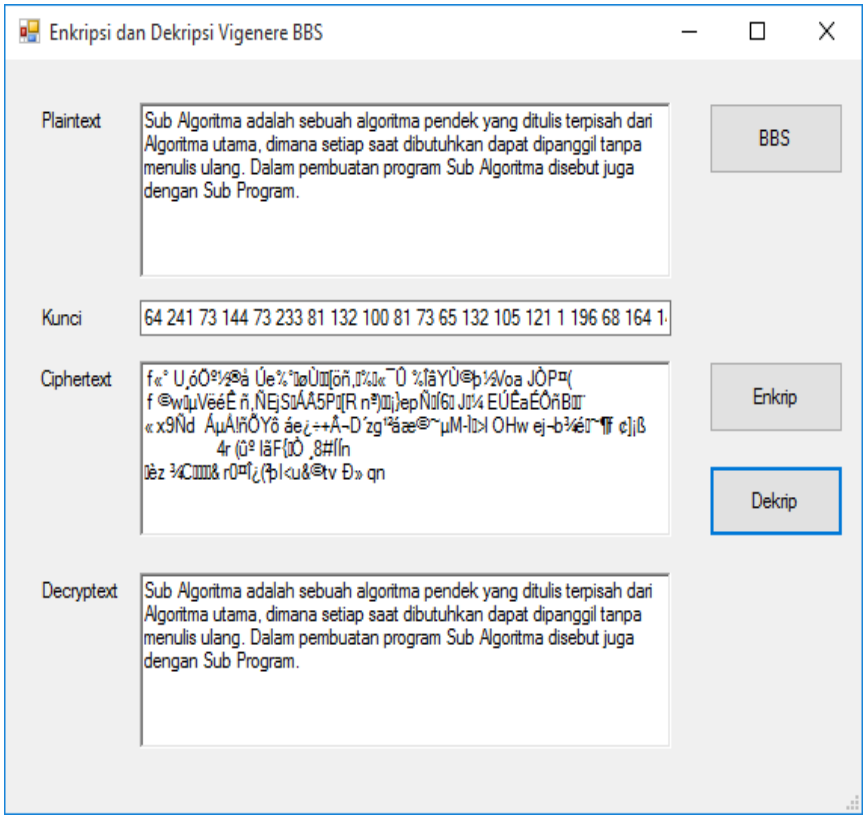
Gambar 4.2.4. Tampilan Halaman Utama Algoritma Vigenere
Sumber : Hasil pengujian Aplikasi (2019)

Uji coba ini dilakukan dengan memasukkan pesan teks kedalam kolom *Plaintext* untuk kemudian dilakukan pemrosesan.



Gambar 4.2.5. Tampilan Enkripsi dengan Algoritma Vigenere
Sumber : Hasil pengujian Aplikasi (2019)

Tombol enkripsi yang ditekan setelah memasukkan kunci berupa karakter angka selanjutnya akan mengeksekusi rangkaian karakter pesan asli yang selanjutnya akan dipanggil plaintext. Hasil enkripsi didapatkan pada textbox dibawahnya.Tombol kirim yang ditekan oleh penerima berfungsi untuk meneruskan pesan kembali pada pengirim. Selanjutnya ciphertext yang merupakan enkripsi dari ciphertext yang diterima dari pengirim akan diteruskan ke pengirim.



Gambar 4.2.6. Tampilan Dekripsi dengan Algoritma Vigenere
Sumber : Hasil pengujian Aplikasi (2019)

4.3 Validasi Sistem

1. Hasil Perhitungan Manual Proses Enkripsi.

Char	Dec	Oct	Hex	Char	Dec	Oct	Hex	Char	Dec	Oct	Hex	Char	Dec	Oct	Hex
(nul)	0	0000	0x00	(sp)	32	0040	0x20	@	64	0100	0x40	`	96	0140	0x60
(soh)	1	0001	0x01	!	33	0041	0x21	A	65	0101	0x41	a	97	0141	0x61
(stx)	2	0002	0x02	"	34	0042	0x22	B	66	0102	0x42	b	98	0142	0x62
(etx)	3	0003	0x03	#	35	0043	0x23	C	67	0103	0x43	c	99	0143	0x63
(eot)	4	0004	0x04	$	36	0044	0x24	D	68	0104	0x44	d	100	0144	0x64
(enq)	5	0005	0x05	%	37	0045	0x25	E	69	0105	0x45	e	101	0145	0x65
(ack)	6	0006	0x06	&	38	0046	0x26	F	70	0106	0x46	f	102	0146	0x66
(bel)	7	0007	0x07	'	39	0047	0x27	G	71	0107	0x47	g	103	0147	0x67
(bs)	8	0010	0x08	(	40	0050	0x28	H	72	0110	0x48	h	104	0150	0x68
(ht)	9	0011	0x09	)	41	0051	0x29	I	73	0111	0x49	i	105	0151	0x69
(nl)	10	0012	0x0a	*	42	0052	0x2a	J	74	0112	0x4a	j	106	0152	0x6a
(vt)	11	0013	0x0b	+	43	0053	0x2b	K	75	0113	0x4b	k	107	0153	0x6b
(np)	12	0014	0x0c	,	44	0054	0x2c	L	76	0114	0x4c	l	108	0154	0x6c
(cr)	13	0015	0x0d	-	45	0055	0x2d	M	77	0115	0x4d	m	109	0155	0x6d
(so)	14	0016	0x0e	.	46	0056	0x2e	N	78	0116	0x4e	n	110	0156	0x6e
(si)	15	0017	0x0f	/	47	0057	0x2f	O	79	0117	0x4f	o	111	0157	0x6f
(dle)	16	0020	0x10	0	48	0060	0x30	P	80	0120	0x50	p	112	0160	0x70
(dc1)	17	0021	0x11	1	49	0061	0x31	Q	81	0121	0x51	q	113	0161	0x71
(dc2)	18	0022	0x12	2	50	0062	0x32	R	82	0122	0x52	r	114	0162	0x72
(dc3)	19	0023	0x13	3	51	0063	0x33	S	83	0123	0x53	s	115	0163	0x73
(dc4)	20	0024	0x14	4	52	0064	0x34	T	84	0124	0x54	t	116	0164	0x74
(nak)	21	0025	0x15	5	53	0065	0x35	U	85	0125	0x55	u	117	0165	0x75
(syn)	22	0026	0x16	6	54	0066	0x36	V	86	0126	0x56	v	118	0166	0x76
(etb)	23	0027	0x17	7	55	0067	0x37	W	87	0127	0x57	w	119	0167	0x77
(can)	24	0030	0x18	8	56	0070	0x38	X	88	0130	0x58	x	120	0170	0x78
(em)	25	0031	0x19	9	57	0071	0x39	Y	89	0131	0x59	y	121	0171	0x79
(sub)	26	0032	0x1a	:	58	0072	0x3a	Z	90	0132	0x5a	z	122	0172	0x7a
(esc)	27	0033	0x1b	;	59	0073	0x3b	[	91	0133	0x5b	{	123	0173	0x7b
(fs)	28	0034	0x1c	<	60	0074	0x3c	\	92	0134	0x5c	|	124	0174	0x7c
(gs)	29	0035	0x1d	=	61	0075	0x3d	]	93	0135	0x5d	}	125	0175	0x7d
(rs)	30	0036	0x1e	>	62	0076	0x3e	^	94	0136	0x5e	~	126	0176	0x7e
(us)	31	0037	0x1f	?	63	0077	0x3f	_	95	0137	0x5f	(del)	127	0177	0x7f

Gambar 4.3 Tabel Konversi Karakter Ke ASCII

Pada tabel diatas berfungsi untuk memindahkan huruf dalam bentuk angka.

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

Plaintext	M	E	D	A	N
	77	69	68	65	78

Langkah selanjutnya, masukan kunci BBS ”241 41 64 57 0”

Plaintext	M	E	D	A	N
	77	69	68	65	78
Key	241	41	64	57	0

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	M	E	D	A	N
	77	69	68	65	78
Key	241	41	64	57	0
Kode CT	62	110	132	122	78
Ciphertext	>	n	„	z	N

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

Maka diketahui ciphertext dari plaintext ”MEDAN” dengan kunci BBS adalah >n zN.

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.

2. Hasil perhitungan manual proses deskripsi.

Setelah dienkripsi, maka *plaintext* ”MEDAN” akan berubah menjadi ”>n zN” berdasarkan kunci yang telah ditetapkan.

Chipertext	>	N		z	N
	62	110	132	122	78

Kunci yang diinputkan adalah sebagai berikut.

Chipertext	>	N		z	N
	62	110	132	122	78
Key	241	41	64	57	0

Berdasarkan langkah diatas maka diperoleh hasil sebagai berikut.

Chipertext	>	N		z	N
	62	110	132	122	78
Key	241	41	64	57	0
Kode PT	77	69	68	65	78
Plaintext	M	E	D	A	N

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

5.1 Kesimpulan

Berdasarkan pembahasan dalam Penerapan Kriptografi Sebagai Alternatif Pengamanan Pada Aplikasi, maka dapat diambil kesimpulan sebagai berikut :

1. Perangkat lunak ini dirancang untuk menampilkan simulasi pengamanan aplikasi menggunakan kriptografi.
2. Penggunaan Algoritma Vigenere memiliki manfaat bagi pengguna aplikasi.
3. Pengamanan aplikasi menggunkan kriptografi dengan algoritma vigenere chiper ini sangat berguna dikarenakan proses enkripsi dan deskripsinya sulit untuk ditebak dan di bobol.

5.2 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 komputer.

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.

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.

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

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

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

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

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

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.

Fachri, B. (2018). Perancangan Sistem Informasi Iklan Produk Halal Mui Berbasis Mobile Web Menggunakan Multimedia Interaktif. Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika), 3, 98-102.

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

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

Fachri, Barany. "Perancangan Sistem Informasi Iklan Produk Halal Mui Berbasis Mobile Web Menggunakan Multimedia Interaktif." Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika) 3 (2018): 98-102.

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

FACHRI, Barany. Perancangan Sistem Informasi Iklan Produk Halal Mui Berbasis Mobile Web Menggunakan Multimedia Interaktif. Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika), 2018, 3: 98-102.

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

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).

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

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

M.Barja Sanjaya, Patrick Adolf Telnoni. (2015). Implementasi Blum-Blum Shub dan *Chaotic Fuction* untuk Modifikasi *Key Genrating* pada AES, *Jurnal Elektro Telekomunikasi Terapan.* 164-165.

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

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

Muttaqin, Muhammad. "Analisa Pemanfaatan Sistem Informasi E-Office Pada Universitas Pembangunan Panca Budi Medan Dengan Menggunakan Metode Utaut." Jurnal Teknik Dan Informatika 5.1 (2018): 40-43.

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

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.

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).

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.

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

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

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

Rio Irawan, Ilhamsyah, Yulrio Brianorman. (2015). Aplikasi Enkripsi Dan Dekripsi Pesan Singkat Menggunakan Algoritma *Knapsack* Berbasis Android. *Jurnal Coding Sistem Komputer Untan.* 3. 57-66.

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

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

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

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

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

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

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

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

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