PERANCANGAN APLIKASI PENYANDIAN DATA TEXT MENGGUNAKAN METODE SYMETRIC STREAM CHIPHER PADA FILE MICROSOFT WORD

Disusun sebagai salah satu syarat untuk menempuh ujian akhir memperoleh gelar sarjana komputer pada fakultas sains & teknologi
Universitas Pembangunan panca budi
Medan

SKRIPSI

OLEH

NAMA	: ADITYA KUMARA
NPM	: 1414370339
PROGRAM STUDI	: SISTEM KOMPUTER

FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI
Medan
2020

LEMBAR PENGESAHAN

PERANCANGAN APLIKASI PENYADIAN DATA TEXT MENGGUNAKAN METODE SYMETRIC STREAM CHIPHER PADA FILE MICROSOFT WORD

DISUSUN OLEH

NAMA	: ADITYA KUMARA
N.P.M	: 1414370039
PROGRAM STUDI	: SISTEM KOMPUTER

Skripsi telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal

Dosen Pembimbing I	Dosen Pembimbing II
Eko Hariyanto S.Kom, M.Kom	Saiful Haryanto S.Kom, M.Kom

Mengetahui

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

SURAT PERNYATAAN

Saya Yang Bertanda Tangan Dibawah Ini :

Nama	:	ADITIA KUMARA
N. P. M	:	1414370339
Tempat/Tgl. Lahir	:	Medan / 23 Desember 1996
Alamat	:	Jl. Pinang Baris Gg. Sekata No. 1 K
No. HP	:	08126512671
Nama Orang Tua	:	AINAR NADEN/INDRANI
Fakultas	:	SAINS & TEKNOLOGI
Program Studi	:	Sistem Komputer
Judul	:	Perancangan Aplikasi Penyandian Data Text menggunakan Metode Symmetric Stream Cipher pada File Microsoft Word

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

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

Medan, 29 November 2019

Yang Membuat Pernyataan

ADITIA KUMARA

1414370339

Telah Diperiksa oleh LPMU
dengan Plagiarisme.....51.....%
Medan, 29 November 2019
THARMIZI HAKIM
Calvo Pramono, SE.,MM

FM-BPAA-2012-011

Hal : Permohonan Meja Hijau

Medan, 29 November 2019
Kepada Yth : Bapak/Ibu Dekan
Fakultas SAINS & TEKNOLOGI
UNPAB Medan
Di -
Tempat

Telah di terima berkas persyaratan dapat di proses
Medan, 29/11/2019
Ka. BPAA
CALVO PRAMONO, SE., MM.

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama	: ALVIA KUMARA
Tempat/Tgl. Lahir	: Medan / 23 Desember 1996
Nama Orang Tua	: AINAR HADER
N. P. M	: 1414370339
Fakultas	: SAINS & TEKNOLOGI
Program Studi	: Sistem Komputer
No. HP	: 081265312671
Alamat	: Jl. Pinang Baris Gg. Teluata No. 1 K

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul **Perancangan Aplikasi Penyandian Data Text Menggunakan Metode Symmetric Stream Cipher**, Selanjutnya saya menyatakan :

1. Melampirkan KHS 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 rekap keterangan bebas pustaka
4. Terlampir surat keterangan bebas laboratorium
5. Terlampir pas photo untuk ijazah ukuran 4x6 = 5 lembar dan 3x4 = 5 lembar Hitam Putih
6. Terlampir foto copy STTB SLTA dilegalisir 1 (satu) lembar dan bagi mahasiswa yang lanjutan D3 ke S1 lampirkan ijazah dan transkripnya sebanyak 1 lembar.
7. Terlampir pelunasan kwitansi pembayaran uang kuliah berjalan dan wisuda sebanyak 1 lembar
8. Skripsi sudah dijilid box 7 eksemplar (1 untuk perpustakaan, 1 untuk mahasiswa) dan jilid kertas jeruk 5 eksemplar untuk penguji (bentuk dan warna penjilidan disesuikan 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 masukkan kedalam MAP
12. Bersedia membayarkan biaya-biaya yang dibebankan untuk memproses pelaksanaan ujian dimaksud, dengan perincian sbb :

1.	[102] Ujian Meja Hijau	: Rp.	300.000
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.	~~1,405,000~~
			1.905.000

20/11/2019

Periode Wisuda Ke : **64**

Ukuran Toga : **M**

Diketahui/disetujui oleh :
Sri Suryani, S.T., M.Sc.
Dekan Fakultas SAINS & TEKNOLOGI

Hormat saya
ALVIA KUMARA
1414370339

Catatan :

- 1.Surat permohonan ini sah dan berlaku bila ;
  - a. Telah dicap Nihil Perpustakaan dan 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.

TANDA BEBAS PUSTAKA
No. 1265 / PERP / BP / 2019
Dinyatakan tidak ada sangkut pautnya dengan UPT. Perpustakaan
Medan, 29 NOV 2019
Kepala UPT. Perpustakaan
Nanda Khairidah, S.Ip

Plagiarism Detector v. 1460 - Originality Report

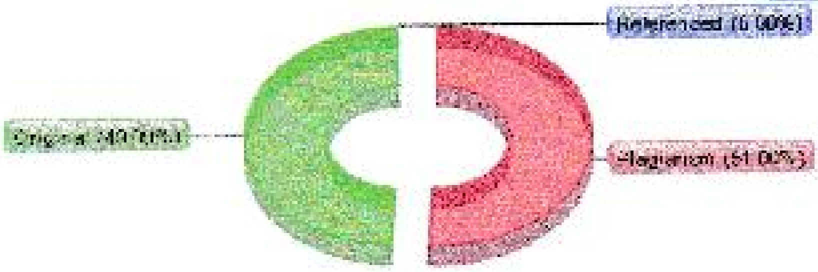
Analyzed document: 11/28/19 10:26:15

"ADITYA KUMARA_14143720339_1414370339_SISTEM KOMPUTER.docx"

Check Type: Internet - via Google and Bing

Licensed to: **Universitas Pembangunan Panca Budi_License3**

Relation chart:



Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

Top sources of plagiarism:

% 10	wrds: 706	http://eprints.umm.ac.id/37532/3/jiptummpp-gdl-nendarizky-50741-3-babii.pdf
% 10	wrds: 668	https://norrianto-erif.blogspot.com/2012/03/kriptografi.html
% 7	wrds: 474	https://www.powershow.com/view/f/54276a-NjQ1O/Kriptografi_powerpoint_ppt_present...

w other Sources:]

Processed resources details:

166 - Ok / 28 - Failed

w other Sources:]

Important notes:

Wikipedia: Google Books: Ghostwriting services: Anti-cheating:

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI

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

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

PERMOHONAN MENGAJUKAN JUDUL SKRIPSI

ya yang bertanda tangan di bawah ini :

ma Lengkap	: Aditya kumara
mpat/Tgl. Lahir	: MEDAN / 23 November 1996
mor Pokok Mahasiswa	: 1414370339
gram Studi	: Sistem Komputer
sentrasi	: Keamanan Jaringan Komputer
lah Kredit yang telah dicapai	: 141 SKS, IPK 3.04

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

Judul SKRIPSI	Persetujuan
Perancangan Aplikasi Pengamanan Pesan Dengan Algoritma Caesar Chiper	
Perancangan Aplikasi Penyembunyian Data Text Menggunakan Metode Symmetric Stream Cipher	
Perancangan Perangkat Lunak Steganografi Menggunakan Algoritma JSTEG	

ul yang disetujui oleh Ketua Program Studi ditandai tanda ☑

Dekan I

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

Medan, 21 Januari 2019

Pemohon,

(Aditya Kumara)

Tanggal : .....

Disetujui oleh :

Dekan I

(Sri Supatmi, S.T., M.Sc.)

Tanggal : .....

Disetujui oleh :

Dosen Pembimbing I :

(.....)

Tanggal : .....

Disetujui oleh:

Ka. Prodi Sistem Komputer

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

Tanggal : .....

Disetujui oleh:

Dosen Pembimbing II :

(.....)

YAYASAN PROF. DR. H. KACIRUN 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	:	Aditya Kurnia
NPM	:	1414310939
Tingkat/Semester	:	4/Vlll
Fakultas	:	SAINS & TEKNOLOGI
Jurusan/Prodi	:	Sistem Komputer

Benar dan telah menyelesaikan urusan administrasi di Laboratorium Komputer Universitas Pembangunan Panca Budi Medan

Medan, 28 November 2015
Ka. Laboratorium
A.n.

Rachmat Fadly, S.Kom

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

iversitas : Universitas Pembangunan Panca Budi
kultas : SAINS & TEKNOLOGI
sen Pembimbing I : Rial Hardian ST., S.Kom., M.Kom.
son Pembimbing II : Suhrah Hatarto, S.Kom., M.Kom
ma Mahasiswa : ADITYA KUMARA
usan/Program Studi : Sistem Komputer
mor Pokok Mahasiswa : 1414370339
jang Pendidikan :
dul Tugas Akhir/Skripsi : Pengembangan Aplikasi Penyewaan Dvd Berbasis Mobile Menggunakan Framework Codeigniter

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
	* Acc Seminar		
9/4 - 19	* Seminar dan rumusan masalah. Dengan latar belakang		BAB I
5/5 - 19	* Acc BAB I		
16 - 19	* perbaiki lumus deskripsi pada program		
19 - 19	* tambah kan fitur deskripsi pesan		
29 - 19	* Acc program		
	* Acc Seminar Hasil		

Medan, 17 Januari 2019
Diketahui/Disetujui oleh :
Dekan,

Hamdani, ST. M.T

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 : Eko Hari Parmadi, Skom. M.kom
Dosen Pembimbing II : Sudhan Hartanto, Skom. M.Kom
Nama Mahasiswa : ADITYA KUMARA
Jurusan/Program Studi : Sistem Komputer
Nomor Pokok Mahasiswa : 1414370339
Bidang Pendidikan : .....
Judul Tugas Akhir/Skripsi : .....

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
10/7-19	Acc Sempro		
18-19	perbaiki latar belakang masalah		BAB 2
10-19	Acc BAB 2		
0-19	perbaiki program-2 error pd metode		
0-19	Acc Program		
0-19	Acc seminar Hasil		
-19	Acc Sidang meja hijau		

17 Juli
Medan, ~~04 November~~ 2019
Diketahui/Disetujui oleh :
Dekan

Hamdani, S.T. M.T.

*) Jika perlu

UNIVERSITAS PEMBANGUNAN PANCA BUDI
FAKULTAS SAINS & TEKNOLOGI
Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8225571
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id
Medan - Indonesia

Universitas : Universitas Pembangunan Panca Budi
Fakultas : SAINS & TEKNOLOGI
Dosen Pembimbing I : Edo Hariyanto S.Kom., M.Kom
Dosen Pembimbing II : Subhan Hariyanto, S.Kom., M.Kom
Nama Mahasiswa : ADITYA KUMARA
Jurusan/Program Studi : Sistem Komputer
Nomor Pokok Mahasiswa : 1414070339
Bidang Pendidikan :
Judul Tugas Akhir/Skripsi : Pengendali data IoT menggunakan

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
7/19	Revisi Bab II		
/19	Revisi Bab III		
/19	Perbaikan Bab III		
/19	Perbaikan Bab III		
/19	Perbaikan Program		
19	ACC Temas		
/19	ACC Ujian		

Medan, 17 Juli 2019
Diketahui/Disetujui oleh :
Dekan

Hamdani, S.T., M.T

Form 3a-1

FM-BPAA-2012-038

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
...an Pembimbing I	: Eko Hadi Santo, S.Kom., M.Kom
...an Pembimbing II	: Syahrul Hidayanto, S.Kom., M.Kom
...a Mahasiswa	: ADITYA KUMARA
...an/Program Studi	: Sistem Komputer
...r Pokok Mahasiswa	: 1414370038
...ang Pendidikan	:
...Tugas Akhir/Skripsi	:

TANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
5/7-19	Acc Seminar		
8-19	perbaiki latar belakang masalah		BAB 2
9-19	Acc BAB I		
-19	perbaiki program TB error pd metode		
-19	Acc program		
-19	Acc seminar Hasil		
19	Acc Sidang meja hijau		

17 Juli
Medan, ~~September~~ 2019
Diketahui/Disetujui oleh :
Dekan,

Hamdani, S.T., M.T

...ak perlu

ABSTRAK

Aditya Kumara

Perancangan Aplikasi Penyandian Data Text Menggunakan Metode Symetric Stream Chipher Pada File Microsoft Word

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 Chiper*. 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 Chiper*.

Kata Kunci: Kriptografi, *Vigenere Chiper*.

KATA PENGANTAR

Puji Syukur penulis panjatkan kepada Tuhan Yang Maha Esa, yang telah memberikan rahmat-Nya kepada penulis, sehingga Skripsi ini dapat diselesaikan oleh penulis tepat pada waktunya dengan judul ***Perancangan aplikasi penyadian data text menggunakan metode symmetric stream chiper pada file Microsoft word***

Skripsi ini dilakukan guna memenuhi salah satu syarat pemenuhan kurikulum dalam menyelesaikan pendidikan pada Program Studi S1 Sistem Komputer Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan. Pada kesempatan ini, penulis menyampaikan rasa terima kasih dan penghargaan yang sebesar-besarnya kepada :

1. Teristimewa kepada Kedua Orang Tua dan Keluarga saya, yang telah banyak memberikan bimbingan dan bantuan baik moril maupun material selama penulis mengikuti pendidikan hingga selesainya Skripsi ini.
2. Bapak Dr. H. Muhammad Isa Indrawan, SE, MM, selaku Rektor Universitas Pembangunan Panca Budi Medan.
3. Bapak Ir. Bhakti Alamsyah, M.T., P.hD, selaku Rektor I Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
4. Dekan Fakultas Sains dan Teknologi , Ibu Sri Shindi Indira, S.T.,M.Sc.
5. Bapak Eko Hariyanto, S.kom, M,Kom Selaku Pembimbing 1 yang juga telah memberikan pengarahan dan petunjuk Skripsi Ini.

6. Bapak Subhan Hartanto , S.Kom., M,Kom, selaku Dosen Pembimbing II yang juga telah memberikan pengarahan dan petunjuk dalam Skripsi ini.
7. Bapak/Ibu Dosen beserta seluruh staf Universitas Pembangunan Panca Budi Medan.
8. Teman-teman dekat penulis khususnya Dayat, Bayu,Karim,Wira,Rusli yang sudah memotivasi dan membantu dalam menyelesaikan skrpsi

Penulis menyadari bahwa Skripsi ini masih kurang sempurna. Oleh karena itu, penulis sangat mengharapkan dan menghargai saran maupun kritikan dari pembaca dan semua pihak yang mengarah kepada perbaikan Tuga Akhir ini.

Medan, 16 Desember 2019
Penulis,

ADITYA KUMARA
NPM. 1414370339

DAFTAR ISI

Halaman

DAFTAR GAMBAR

No Judul **Hal**

DAFTAR TABEL

No Judul **Hal**

BAB I

PENDAHULUAN

1.1 Latar Belakang

Keamanan dan kerahasiaan data merupakan suatu aspek yang sangat penting dalam proses pertukaran pesan atau informasi. Suatu pesan yang sifatnya rahasia membutuhkan suatu sistem penyimpanan dan pengiriman data atau *file* agar tidak mudah terbaca dan diketahui semua orang. Ada berbagai macam cara untuk mengamankan data atau *file*, salah satunya adalah menggunakan metode kriptografi.

Saat ini *kriptografi* terbagi menjadi dua yaitu kriptografi klasik dan kriptografi modern. Pada *kriptografi* klasik terdapat algoritma *Vigenere Chiper*. *Vigenere Chiper* ini mempunyai 26 kemungkinan karena menggunakan alfabet. *Vigenere Chiper* merupakan algoritma klasik untuk menyandikan sebuah *plaintext* dengan cara substitusi sehingga dalam memecahkan pesan tersebut akan terasa susah. Penelitian ini menggunakan pemrograman *Visual Basic.Net* 2010. (Halim Agung; 2015)

Algoritma Vigenere Chiper merupakan salah satu metode kriptografi berbasis protokol. Protokol adalah aturan yang berisi tentang langkah-langkah yang melibatkan dua kunci yang dibuat untuk menyelesaikan suatu kegiatan. Dalam kriptografi, protokol digunakan oleh orang-orang yang terlibat, seperti untuk proses otentifikasi, pengaktifan bilangan acak, bahkan untuk berbagi dan bertukar informasi yang bersifat rahasia. Pengirim dan penerima pesan melakukan

penukaran sebanyak tiga tahap untuk mengekripsikan pesan tersebut. Pada dasarnya, *Algoritma Vigenere Chiper* di implementasikan dengan menggunakan satu algoritma enkripsi dan dekripsi yang telah disepakati oleh kedua belah pihak.

Berdasarkan latar belakang yang telah penulis uraikan di atas, maka penulis tertarik untuk memilih judul **"*Perancangan Aplikasi Penyandian Data Text Menggunakan Metode Symetric Stream Chipher Pada File Microsoft Word*".**

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas dapat penulis simpulkan bahwa yang menjadi pokok permasalahan dalam pembahasan ini adalah sebagai berikut:

1. Bagaimana membuat sistem penyandian file menggunakan algoritma *vigenere chiper*?
2. Bagaimana merancang sistem keamanan file dengan algoritma *Vigenere Chiper* pada pesan singkat?

1.3 Batasan Masalah

Berdasarkan perumusan masalah diatas maka penulis melakukan pembatasan masalah yang akan dibahas sebagai berikut:

1. Implementasi enkripsi dan dekripsi hanya berupa teks yang berada dalam file.
2. Program yang dibahas menggunakan pemrograman *Visual Basic.Net 2010.*

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini dengan menggunakan algoritma *Vigenere Chiper* ini yang ingin dicapai adalah sebagai berikut:

1. Merancang aplikasi massenger dengan keamanan data teks dengan algoritma *Vigenere Chiper*.
2. Memperkuat keamanan pesan pada aplikasi pesan singkat di aplikasi massenger.

1.4 Manfaat Penelitian

Adapun manfaat dalam penelitian ini yang diperoleh dari penerapan algoritma *Vigenere Chiper* adalah sebagai berikut:

1. Memiliki aplikasi massenger dengan keamanan data data menggunakan algoritma *Vigenere Chiper*.

2. Menjadi Sarana media pembelajaran dalam bidang keamanan informasi pada mata kuliah keamanan data bagi mahasiswa Universitas Pembangunan Pancabudi.

BAB II

LANDASAN TEORI

2.1 *Kriptografi*

Kriptografi merupakan kata dari bahasa *Yunani* yaitu *cryptography*, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Sehingga, bila digabungkan akan menjadi kata yang berarti menyembunyikan/merahasiakan tulisan. *Kriptografi* adalah suatu ilmu ataupun seni mengamankan pesan dan dilakukan oleh *cryptographer* (**Anonim, 2014**).

Kriptografi digunakan untuk memastikan privasi dan autentifikasi data dalam komunikasi antar sistem komputer. Terdapat dua proses dasar dalam *kriptografi* yaitu: (**Rhee, 2013**).

1. *Enkripsi*, adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). (**Pabokory, 2015:11**).
2. *Deskripsi*, adalah kebalikan dari *Enkripsi* yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. (**Pabokory, 2015**.)

Sebuah pesan atau data yang masih asli dan belum mengalami penyandian dikenal dengan istilah *plaintext*. Kemudian setelah disamarkan dengan suatu cara penyandian, maka *plaintext* ini disebut sebagai chipertext. Proses penyamaran dari *plaintext* ke *Ciphertext* disebut *Enkripsi* (*encryption*), dan proses pengembalian dari *Ciphertext* menjadi *plaintext* kembali disebut dekripsi (*decryption*). (Pabokory,

2015). *File* yang dapat di *Enkripsi* dapat berupa teks, gambar maupun audio dan video.

2.1.1 *Kriptografi Klasik*

Kriptografi klasik adalah *kriptografi* yang disebut juga sebagai *kriptografi* kunci tunggal atau *kriptografi* simetris yang menggunakan kunci yang sama untuk *Enkripsi* maupun *Deskripsi*. *Kriptografi* klasik merupakan *kriptografi* yang digunakan pada zaman dahulu sebelum komputer ditemukan atau sudah ditemukan namun belum secanggih sekarang. *Kriptografi* ini melakukan pengacakan huruf pada kata terang / *plaintext*. (**Bishop, 2014**).

Algoritma kriptografi klasik digunakan sejak sebelum era komputerisasi dan kebanyakan menggunakan teknik kunci simetris. Metode menyembunyikan pesannya adalah dengan teknik substitusi atau transposisi atau keduanya. Teknik substitusi adalah menggantikan karakter dalam *plaintext* menjadi karakter lain yang hasilnya adalah *Cipher*text. Sedangkan transposisi adalah teknik mengubah *plaintext* menjadi *Cipher*text dengan cara permutasi karakter. Kombinasi keduanya secara kompleks adalah yang melatarbelakangi terbentuknya berbagai macam algoritma kriptografi modern. Contoh algoritma kriptografi klasik yaitu: *Caesar Cipher, Vigenere Cipher,* dan *Hill Cipher.*

2.1.2 *Kriptografi Modern*

Algoritma kriptografi modern merupakan suatu perbaikan yang mengacu pada kriptografi klasik. Algoritma ini menggunakan pengolahan simbol biner yang dibentuk dari kode *ASCII* (*American Standard Code for Information Interchange*)

karena berjalan mengikuti operasi komputer digital, sehingga membutuhkan pengetahuan dasar matematika untuk menguasainya . Algoritma ini memiliki tingkat kesulitan yang kompleks yang menyebabkan kriptanalis sangat sulit memecahkan *Cipher*text tanpa mengetahui kuncinya. Adapun jenis kunci dalam kriptografi modern terdiri dari 3 yaitu: *simetri*, *asimetri*, dan hibrida. Pada kriptogarfi modern terdapat berbagai macam algoritma yang dimaksudkan untuk mengamankan informasi yang dikirim melalui jaringan komputer. Contoh kriptografi modern yaitu *MD5, RC4, AES* dan lain-lain. (**Bishop, 2014**).

2.1.3 Proses *Enkripsi* dan *Deskripsi*

Enkripsi yaitu suatu proses pengaman suatu data yang disembunyikan atau proses konversi data (*plaintext*) menjadi bentuk yang tidak dapat dibaca/ dimengerti. Enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara, namun, hanya organisasi-organisasi tertentu dan individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan yang menggunakan enkripsi. Di pertengahan tahun 1970an enkripsi kuat dimanfaatkan untuk pengamanan oleh sekretariat agen pemerintah Amerika Serikat pada domain publik, dan saat ini enkripsi telah digunakan pada sistem secara luas, seperti Internet, e-commerce, jaringan telepon bergerak dan ATM pada bank. Enkripsi dapat digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk membuat komunikasi yang aman, terutama untuk memastikan integrasi dan autentikasi dari sebuah pesan. Untuk menampilkan enkripsi dan kebalikannya dekripsi, digunakan algoritma yang biasa disebut *Cipher* dengan menggunakan metode serangkaian langkah yang

terdefinisi yang diikuti sebagai prosedur. Alternatif lain ialah *Enchiperment.* Informasi yang asli disebuh sebagai *plaintext,* dan bentuk yang sudah dienkripsi disebut sebagai chiphertext. Pesan chipertext berisi seluruh informasi dari pesan *plaintext,* tetapi tidak dalam format yang didapat dibaca manusia ataupun komputer tanpa menggunakan mekasnisme yang tepat untuk melakukan dekripsi. (**Bishop, 2014**).

Sedangkan Dekripsi yaitu kebalikan dari proses enkripsi yaitu proses konversi data yang sudah dienkripsi (*ciphertext*) kembali menjadi data aslinya (*Original Plaintext*) sehingga dapat dibaca/ dimengerti kembali.Pesan yang akan dienkripsi disebut plaintext yang dimisalkan plaintext (P), proses enkripsi dimisalkan enkripsi (E), proses dekripsi dimisalkan dekripsi (D), dan pesan yang sudah dienkripsi disebut *ciphertext* yang dimisalkan ciphertext (C). (**Bishop, 2014**).

2.2 Algoritma Kriptografi *Vigenere Chiper*

Teknik dari substitusi *Vigenere* dapat dilakukan dengan dua cara:

1. Angka

Teknik substitusi *Vigenere* dilakukan menggunakan angka dengan menukarkan huruf dengan angka.

Tabel 2.1. 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 2.2. 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

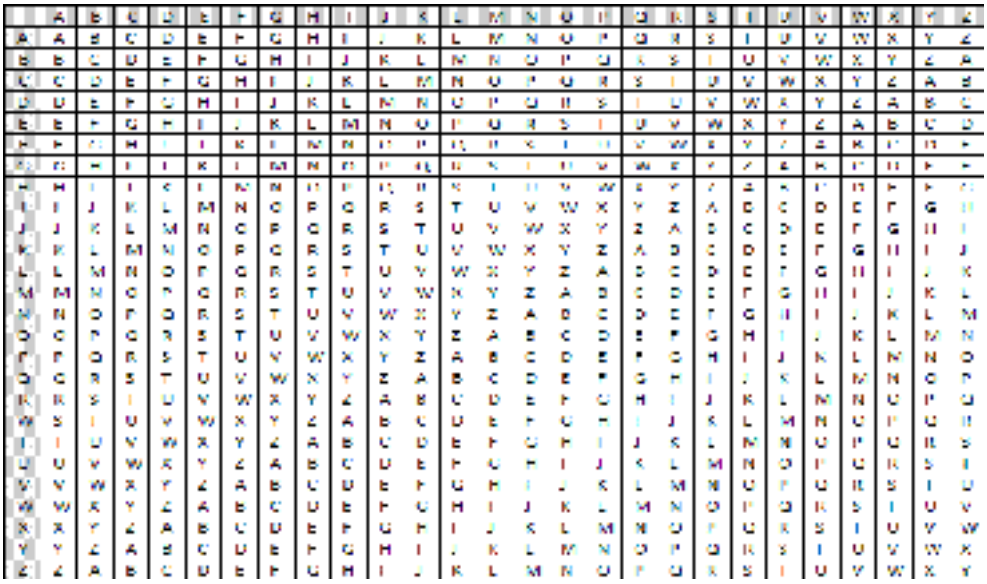
kembali ke huruf A. setelah hasil penjumlahan didapat, maka angka kembali dikonversi ke huruf sehingga didapat ciphertextnya adalah:

VPXZGIAXIVWPUBTTMJPWIZITWZT

2. Huruf

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

Tabel 2.3. *Vigenere* Cipher



2.3 Pengertian *One Time Pad (OTP)*

Algoritma *One Time Pad* (OTP) merupakan algoritma berjenis *Symetric key* yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan cara *stream Cipher* yang berasal dari hasi XOR antara *bit plaintext* dan *bit key*. Pada metode ini *plain text* diubah kedalam kode ASCII dan kemudian dikenakan operasi

XOR terhadap kunci yang sudah diubah ke dalam kode ASCII. (**Hamokwarong, 2014**)

One-time pad adalah salah satu stream *Cipher* klasik yang secara matematis terbukti sempurna aman. *Cipher* teksnya tidak mungkin dapat dipecahkan. Keamanan algoritma *one-time pad* terletak pada penggunaan barisan bilangan acak sejati (*trully random*) sebagai kunci enkripsi, panjang kunci sama dengan panjang pesan dan tidak ada perulangan kunci sebagaimana pada pada *Vernam Cipher* atau *Vigenere Cipher*. (**Munir, 2014**)

Sayangnya *one-time pad* tidak dapat diimplementasikan secara praktis sebab pembangkitan bilangan acak sejati tidak dapat diulang kembali di sisi penerima pesan. Oleh karena itu kunci (*pad*) harus dikirim melalui saluran komunikasi yang kedua (misalnya melalui kurir), sayangnya saluran kedua itu umumnya lambat dan ongkosnya mahal. One-time pad masih dapat diterapkan namun kunci yang berupa barisan bilangan acak diganti dengan barisan bilangan semi-acak (*pseudo-random*) dengan syarat barisan kunci itu tidak boleh berulang. (**Munir, 2014**)

2.4 Pengertian Algoritma

Penyelesaian permasalahan dengan menggunakan alat bantu system computer paling tidak akan melibatkan lima tahapan, yaitu:

1. Analisis masalah
2. Merancang algoritma
3. Membuat program computer

4. Menguji hasil program computer
5. Dokumentasi

Algoritma adalah Sistem kerja komputer memiliki *brainware, hardware,* dan *software*. Tanpa salah satu dari ketiga sistim tersebut, komputer tidak akan berguna. Kita akan lebih fokus pada *software* komputer. Software terbangun atas susunan program (silahkan baca mengenai pengertian program) dan *syntax* (cara penulisan/pembuatan program). Untuk menyusun program atau syntax, diperlukannya langkah - langkah yang sistematis dan logis untuk dapat menyelesaikan masalah atau tujuan dalam proses pembuatan suatu *software*. Maka, Algoritma berperan penting dalam penyusunan program atau *syntax* tersebut.

Pengertian Algoritma adalah susunan yang logis dan sistematis untuk memecahkan suatu masalah atau untuk mencapai tujuan tertentu. Dalam dunia komputer,Algoritma sangat berperan penting dalam pembangunan suatu software. Dalam dunia sehari-hari, mungkin tanpa kita sadari Algoritma telah masuk dalam kehidupan kita.

Algoritma adalah kunci dari bidang ilmu komputer, dan pada dasarnya setiap hari kita melakukan aktivitas algoritma. Kata algoritma berasal dari sebutan Algorizm (Abu Abdullah Muhammad Ibn Musa Al Khwarizmi, ahli matematika Uzbeki

a. Algoritma adalah urutan langkah-langkah berhingga untuk memecahkan masalah logika atau matematika
b. Algoritma adalah logika, metode dan tahapan (urutan) sistematis yang digunakan untuk memecahkan suatu permasalahan.

c. Algoritma adalah urutan langkah-langkah logis penyelesaian masalah yang disusun secara sistematis dan logis.
d. Algoritma adalah urutan logis pengambilan keputusan untuk pemecahan masalah.

Pembuatan algoritma harus selalu dikaitkan dengan:

a. Kebenaran algoritma
b. Kompleksitas (lama dan jumlah waktu proses dan penggunaan memori)

Kriteria Algoritma yang baik:

a. Tepat, benar, sederhana, standar dan efektif
b. Logis, terstruktur dan sistematis
c. Semua operasi terdefinisi
d. Semua proses harus berakhir setelah sejumlah langkah dilakukan
e. Ditulis dengan bahasa yang standar dengan format pemrograman agar mudah untuk diimplementasikan dan tidak menimbulkan arti ganda.

2.5 Keamanan Data

Pada zaman teknologi informasi sekarang, data atau informasi merupakan suatu asset yang sangat berharga dan harus dilindungi. Hal ini juga diikuti oleh kemajuan teknologi komputer. Kemajuan teknologi komputer membantu semua aspek kehidupan manusia. Dengan adanya kemajuan dalam teknologi informasi, komunikasi dan komputer maka kemudian muncul masalah baru, yaitu masalah keamanan akan data dan informasi dan dalam hal ini akan membuka peluang bagi orang-orang yang tidak bertanggung jawab untuk menggunakannya sebagai tindak

kejahatan. Dan tentunya akan merugikan pihak tertentu. Dalam keamanan data ada beberapa aspek yang berkaitan dengan persyaratan kemanan yaitu (**Pabokory, 2015:2**):

1. *Secrecy*. Berhubungan dengan akses membaca data dan informasi. Data dan informasi di dalam suatu sistem komputer hanya dapat diakses dan dibaca oleh orang yang berhak.
2. *Integrity*. Berhubungan dengan akses merubah data dan informasi. Data dan informasi di dalam suatu sistem komputer hanya dapat diubah oleh orang yang berhak.
3. *Availability*. Berhubungan dengan ketersediaan data dan informasi. Data dan informasi yang berada dalam suatu sistem komputer tersedia dan dapat dimanfaatkan oleh orang yang berhak. (Pabokory, 2015:2)[.
4. Lebih lanjut menurut (Pabokory, 2015:2), terdapat lima langkah kemanan komputer yang baik untuk diperhitungkan yaitu; aset, analisis resiko, perlindungan, alat dan prioritas.

2.6 *Unified Modeling Language* (UML)

2.6.1 Pengenalan UML

Unified Modelling Language (UML) adalah suatu alat untuk memvisualisasikan dan mendokumentasikan hasil analisis dan desain yang berisi sintak dalam memodelkan sistem secara visual (Haviluddin : 2015 : 1). Banyak orang yang telah membuat bahasa pemodelan pembangunan perangkat lunak sesuai dengan teknologi pemrograman yang berkembang pada saat itu, misalnya yang

sempat berkembang dan digunakan oleh banyak pihak adalah *Data Flow Diagram* (DFD) untuk memodelkan perangkat lunak yang menggunakan pemrograman prosedural atau struktur, kemudian juga ada *State Transition Diagram* (STD) yang digunakan untuk memodelkan *real time* (waktu nyata).

Pada perkembangan teknik pemrograman berorientasi objek, muncullah sebuah standarisasi bahasa pemodelan untuk pembangunan perangkat lunak yang dibangun dengan menggunakan teknik pemrograman berorientasi objek, yaitu *Unified Modeling Language* (UML).

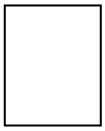
2.6.2 *Use Case Diagram*

Diagram yang menggambarkan *actor, use case* dan relasinya sebagai suatu urutan tindakan yang memberikan nilai terukur untuk aktor. Sebuah *use case* digambarkan sebagai elips horizontal dalam suatu diagram *use case diagram* (Haviluddin : 2015 : 4).

Tabel 2.4 Simbol *Use Case Diagram*

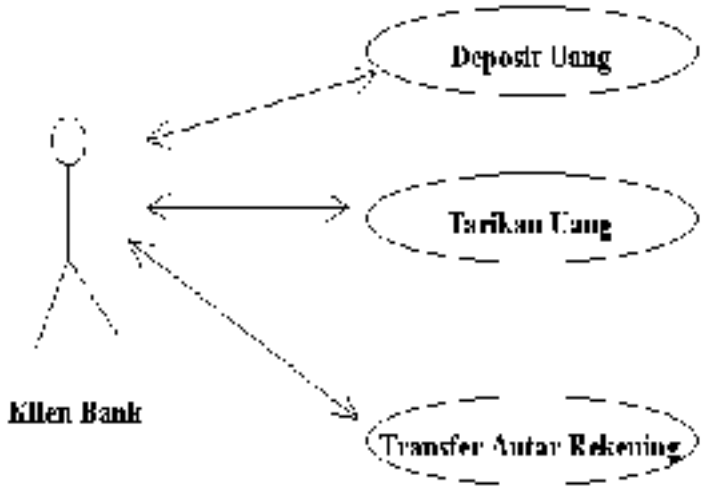
NO	GAMBAR	NAMA	KETERANGAN
1		*Actor*	Menspesifikasikan himpuan peran yang pengguna mainkan ketika berinteraksi dengan *use case*.
2		*Dependency*	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri *(independent)* akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri (*independent*).

Tabel 2.4 Simbol *Use Case Diagram* (Lanjutan)

NO	GAMBAR	NAMA	KETERANGAN
3		*Generalization*	Hubungan dimana objek anak (*descendent*) berbagi perilaku dan struktur data dari objek yang ada di atasnya objek induk (*ancestor*).
4		*Include*	Menspesifikasikan bahwa *use case* sumber secara *eksplisit*.
5		*Extend*	Menspesifikasikan bahwa *use case* target memperluas perilaku dari *use case* sumber pada suatu titik yang diberikan.
6		*Association*	Apa yang menghubungkan antara objek satu dengan objek lainnya.
7		*System*	Menspesifikasikan paket yang menampilkan sistem secara terbatas.
8		*Use Case*	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu aktor
9		*Collaboration*	Interaksi aturan-aturan dan elemen lain yang bekerja sama
10		*Note*	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi

Sumber : (Gellysa Urva, 94 : 2015)

Contoh Use Case Diagram :



Gambar 2.1. Contoh *Use Case Diagram*
Sumber : (Haviluddin : 2015 : 4)

2.6.3 *Activity Diagram*

Diagram aktivitas atau *activity diagram* menggambarkan *workflow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis atau *menu* yang ada pada perangkat lunak. Yang perlu diperhatikan disini adalah bahwa diagram aktivitas menggambarkan aktivitas sistem bukan apa yang dilakukan aktor, jadi aktivitas yang dapat dilakukan oleh sistem.

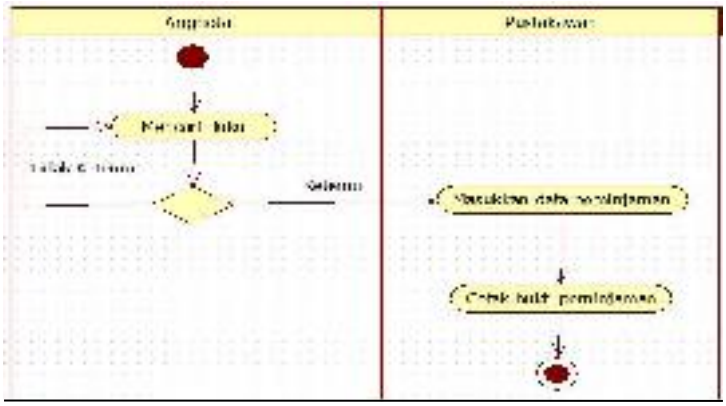
Tabel 2.5. Simbol *Activity Diagram*

NO	GAMBAR	NAMA	KETERANGAN

1		*Activity*	Memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain
2		*Action*	*State* dari sistem yang mencerminkan eksekusi dari suatu aksi
3		*Initial Node*	Bagaimana objek dibentuk atau diawali.
4		*Actifity Final Node*	Bagaimana objek dibentuk dan dihancurkan
5		*Fork Node*	Satu aliran yang pada tahap tertentu berubah menjadi beberapa aliran

Sumber : (Gellysa Urva, 94 : 2015)

Contoh Activity Diagram :



Gambar 2.3. Contoh *Activity Diagram*

Sumber : (Gellysa Urva, 94 : 2015)

2.6.4 *Sequence Diagram*

Diagram sekuen menggambarkan kelakuan objek pada *use case* dengan mendeskripsikan waktu hidup objek dan *message* yang dikirimkan dan diterima

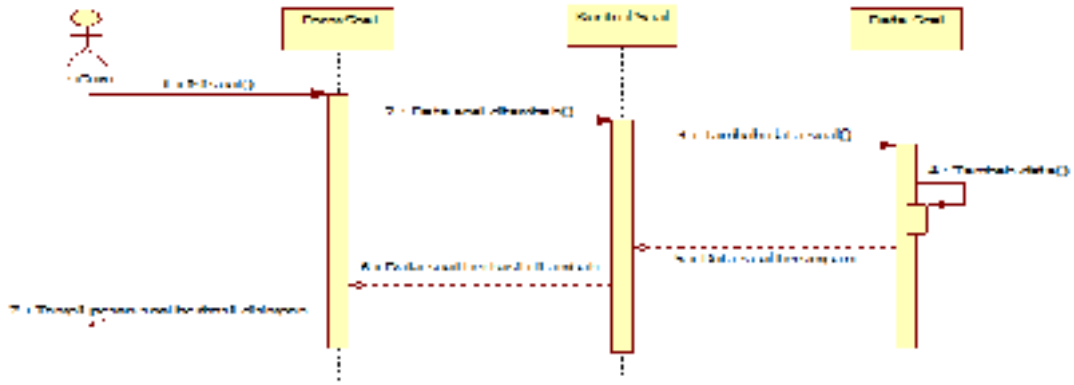
antar objek. Oleh karena itu untuk menggambar diagram sekuen maka harus diketahui objek-objek yang terlibat dalam sebuah *use case* beserta metode-metode yang dimiliki kelas yang diinstansiasi menjadi objek itu. Membuat diagram sekuen juga dibutuhkan untuk melihat skenario yang ada pada *use case.*

Tabel 2.6. Simbol *Sequence Diagram*

NO	GAMBAR	NAMA	KETERANGAN
1		*LifeLine*	Objek *entity*, antarmuka yang saling berinteraksi.
2		*Message*	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi
3		*Message*	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi

Sumber : (Gellysa Urva, 95 : 2015)

Contoh Squence Diagram :

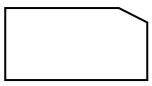


Gambar 2.3. Contoh *Squence Diagram*
Sumber : (Gellysa Urva, 95 : 2015)

2.6.5 *Class Diagram*

Class diagram menggambarkan struktur statis dari kelas dalam sistem anda dan menggambarkan atribut, operasi dan hubungan antara kelas. Class diagram membantu dalam memvisualisasikan struktur kelas-kelas dari suatu sistem dan merupakan tipe diagram yang paling banyak dipakai. Selama tahap desain, class diagram berperan dalam menangkap struktur dari semua kelas yang membentuk arsitektur sistem yang dibuat.

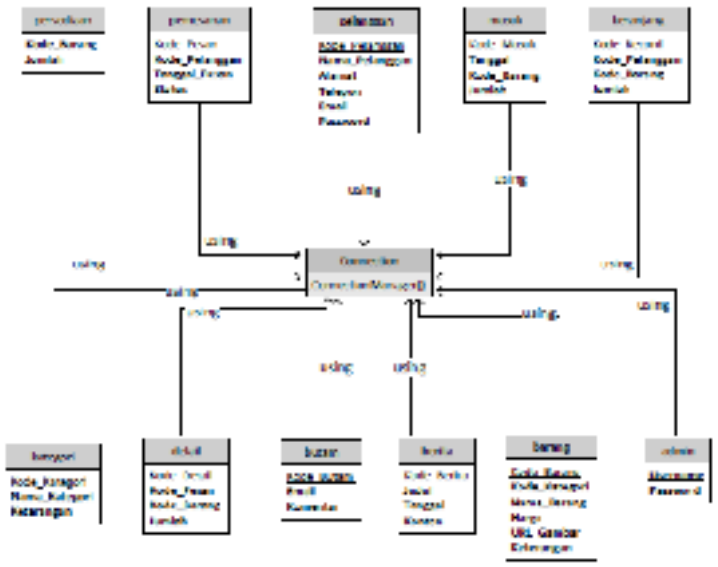
Tabel 2.7. Simbol *Class Diagram*

NO	GAMBAR	NAMA	KETERANGAN
1		*Note*	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi

2	⟶	*dependency*	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri akan mempengaruhi elemen yang bergantung padanya
3	⟵	*extend*	Menspesifikasikan bahwa use case target memperluas prilaku dari use case sumber pada suatu titik yang diberikan.

Sumber : (Gellysa Urva, 95 : 2015)

Contoh *Class* Diagram :



Gambar 2.4 Contoh *Class Diagram*

Sumber : (Gellysa Urva, 95 : 2015)

2.7 Pengertian Informasi

Secara Etimologi, kata informasi ini berasal dari kata bahasa Perancis kuno *informacion* (tahun 1387) mengambil istilah dari bahasa Latin yaitu *informationem*

yang berarti “konsep, ide atau garis besar”. Informasi ini merupakan kata benda dari *informare* yang berarti aktivitas dalam “pengetahuan yang dikomunikasikan”.

Informasi adalah hasil pemrosesan data yang diperoleh dari setiap elemen sistem menjadi bentuk yang mudah dipahami dan merupakan pengetahuan yang relevan dan berguna (Yulansari, 6 : 2013).

Informasi bisa menjadi fungsi penting dalam membantu mengurangi rasa cemas pada seseorang. Menurut pendapat Notoatmodjo (2018) bahwa semakin banyak memiliki informasi dapat memengaruhi atau menambah pengetahuan terhadap seseorang dan dengan pengetahuan tersebut bisa menimbulkan kesadaran yang akhirnya seseorang itu akan berperilaku sesuai dengan pengetahuan yang dimilikinya.

Informasi adalah data yang telah diolah melalui proses tertentu menjadi sesuatu yang menambah pengetahuan atau temuan yang mempunyai arti baru bagi pemakainya (Melina, 38 : 2014).

Adapun fungsi-fungsi informasi adalah sebagai berikut:

1. Untuk meningkatkan pengetahuan bagi si pemakai.
2. Untuk mengurangi ketidakpastian dalam proses pengambilan keputusan pemakai.
3. Menggambarkan keadaan yang sebenarnya dari sesuatu hal.Informasi yang berkualitas harus akurat, tepat dan relevan.

Sumber dari informasi adalah data. Data adalah kenyataan yang menggambarkan suatu kejadian-kejadian dan kesatuan nyata. Data merupakan bentuk yang masih mentah, belum dapat bercerita banyak sehingga perlu diolah

lebih lanjut. Data diolah melalui suatu metode untuk menghasilkan informasi. Data dapat berbentuk simbol-simbol semacam huruf, angka, bentuk suara, sinyal, gambar, dan sebagainya.

2.8 Pengertian *Visual Studio*

Visual Studio .Net merupakan salah satu *tool development Microsoft* yang dapat digunakan untuk membuat aplikasi di lingkungan kerja berbasis sistem operasi *Windows. Visual Studio .NET* menyediakan tools bagi para *developer* untuk membangun aplikasi yang berjalan di *.Net Framework* (Safik : 2015 : 2).

Visual Studio (*Beginners All-Purpose Symbolic Instruction Code*) merupakan Bahasa pemrograman *Integrated Development Environment* (IDE), yaitu bahasa pemrograman *visual* yang digunakan untuk membuat program aplikasi atau *software* berbasis sistem operasi *Microsoft Windows*, dengan menggunakan model pemrograman "*Common Object Model* (COM)".

Visual Studio merupakan turunan bahasa pemrograman *STUDIO* yang menawarkan pengembangan perangkat lunak komputer bebasis grafik dengan cepat. Dengan menggunakan bahasa pemrograman VB, para progammer dapat membangun aplikasi dengan menggunakan komponen-komponen yang di sediakan VB.

Microsoft Visual Studio (sering disingkat sebagai VB saja) merupakan sebuah bahasa pemrograman yang menawarkan *Integrated Development Environment* (IDE) visual untuk membuat program perangkat lunak berbasis sistem operasi Microsoft Windows dengan menggunakan model pemrograman (*COM*),

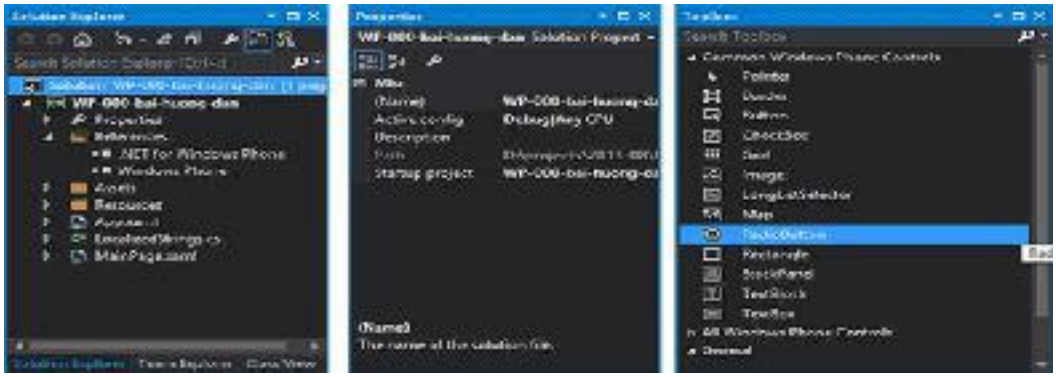
Visual Studio merupakan turunan bahasa pemrograman *STUDIO* dan menawarkan pengembangan perangkat lunak komputer berbasis grafik dengan cepat, Beberapa bahasa skrip seperti *Visual Studio for Applications* (*VBA*) dan *Visual Studio Scripting Edition* (*VBScript*), mirip seperti halnya *Visual Studio*, tetapi cara kerjanya yang berbeda.

Para *programmer* dapat membangun aplikasi dengan menggunakan komponen-komponen yang disediakan oleh *Microsoft Visual Studio* Program-program yang ditulis dengan *Visual Studio* juga dapat menggunakan *Windows* API, tapi membutuhkan deklarasi fungsi luar tambahan.

Dalam pemrograman untuk bisnis, *Visual Studio* memiliki pangsa pasar yang sangat luas. Dalam sebuah survey yang dilakukan pada tahun 2005, 62% pengembang perangkat lunak dilaporkan menggunakan berbagai bentuk *Visual Studio*, yang diikuti oleh *C++, JavaScript, C#,* dan *Java*.

Beberapa komponen kerja program *visual Studio 2015* telah ditampilkan sebagai tampilan standard. Masih banyak lagi komponen yang masih tersembunyi sehingga memerlukan perintah tertentu untuk menampilkannya. Kita dapat mengatur komponen di dalam program visual Studio 2015 sesuai dengan yang kita butuhkan. Berikut ini adalah beberapa komponen kerja dari visual Studio 2015 adalah :

Berikut ini adalah *table* yang berisi nama tombol yang terdapat didalam *toolbox* beserta fungsinya.



Gambar 2.5. Tampilan *Toolbox*
Sumber : (Safik : 2015 : 2).

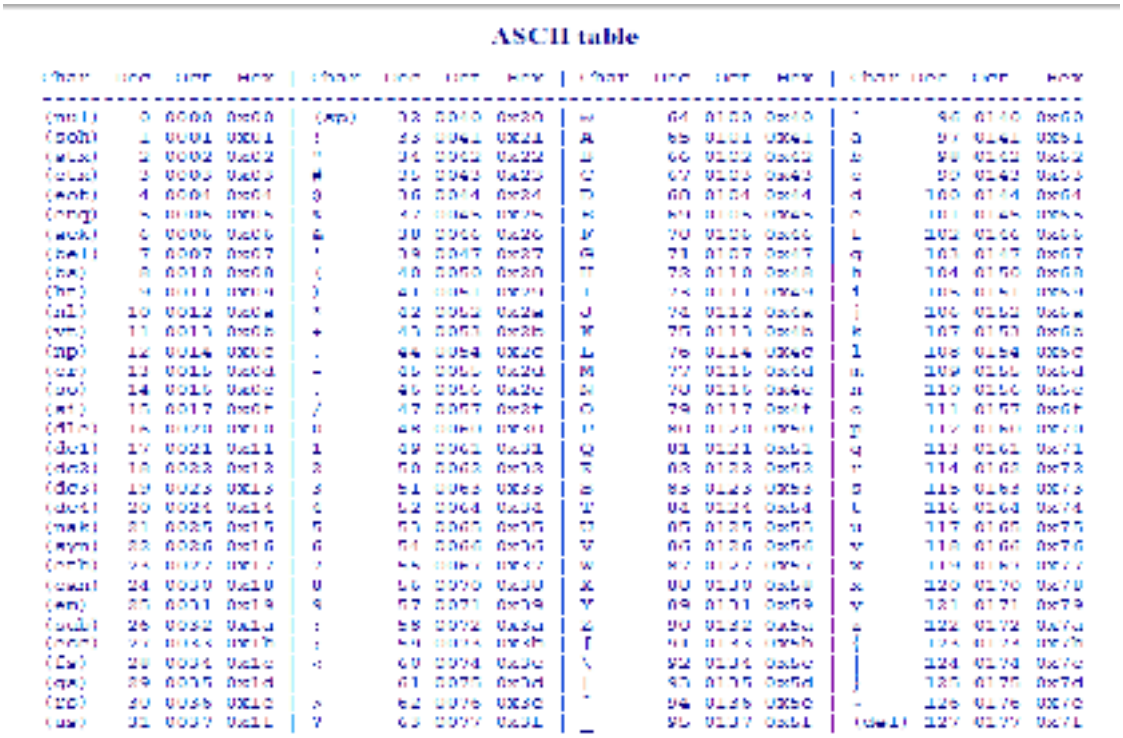
Table 2.8. *Toolbox Visual Studio*

Nama tombol	fungsi
Pointer	Memilih, mengatur ukuran dan memindahkan posisi yang terpasang di bagian form.
Bindingsources	Untuk mengkoneksikan program ke database
Label	Menampilkan teks, dimana pengguna program tidak bisa mengubah teks tersebut
Groupbox	Untuk mengelompokkan item yang ada di form
Checkbox	Membuat kotak periksa, dimana pengguna program dapat memilih sekaligus
Listbox	Membuat daftar pilihan
Timer	Membuat control waktu dan interval yang diperlukan
Image	Menampilkan gambar pada form dalam format *bit*map, icone, atau metafile
Picturebox	Menampilkan gambar dari sebuah file
Textbox	Membuat teks, dimana teks tersebut dapat diubah oleh pembuat program
Button	Membuat tombol perintah
Combobox	Menambahkan control kotak combo yang merupakan control gabungan antara textbox dan listbox

Sumber : (Safik : 2015 : 2).

2.9 Tabel ASCII

ASCII merupakan kepanjangan dari (American Standard Code for Information Interchange), dan pengertian dari ASCII sendiri adalah suatu standar internasional dalam kode huruf dan simbol seperti Hex dan Unicode tetapi ASCII lebih bersifat universal.



Gambar 2.6. Tabel ASCII

https://www.asciitable.com/

2.10 Pengertian *Flowchat*

Flowchart merupakan gambar atau bagan yang memperlihatkan urutan dan hubungan antar proses beserta instruksinya (Nuraini, 2015). Gambaran ini dinyatakan dengan simbol. Dengan demikian setiap simbol menggambarkan proses tertentu. Sedangkan hubungan antar proses digambarkan dengan garis penghubung.

Flowchart ini merupakan langkah awal pembuatan program.

Dengan adanya *flowchart* urutan proses kegiatan menjadi lebih jelas. Jika ada penambahan proses maka dapat dilakukan lebih mudah. Setelah flowchart selesai disusun, selanjutnya pemrogram (programmer) menerjemahkannya ke bentuk program dan bahasa pemrograman.

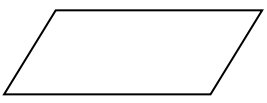
1. *Flowchart* Sistem *(System Flowchart)*

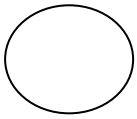
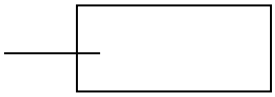
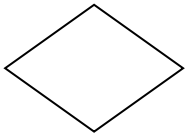
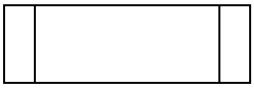
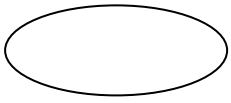
Sistem *Flowchart* merupakan bagian yang menunjukkan alur kerja atau apa yang sedang dikerjakan di dalam sistem secara keseluruhan dan menjelaskan urutan dari prosedur-prosedur yang ada di dalam sistem. Dengan kata lain, flowchart ini merupakan deskripsi secara frafik dari urutan prosedur-prosedur yang terkombinasi yang membentuk suatu sistem.

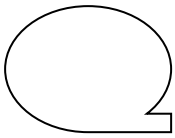
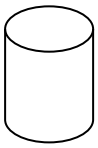
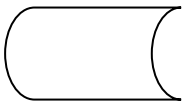
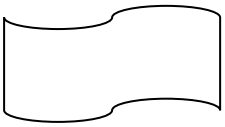
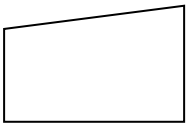
Flowchart Sistem terdiri dari data yang mengalir melalui system dan proses yang mentransformasikan data itu. Data dan proses dalam flowchart sistem dapat digambarkan secara *online* (dihubungkan langsung dengan computer) atau offline(tidak dihubungkan langsung denan computer, misalnya mesin tik, cash register atau kalkulator).

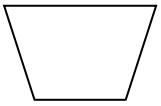
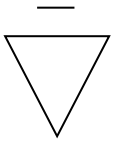
Simbol-simbol yang digunakan dalam system flowchart antara lain :

Tabel 2.1. Simbol-simbol *flowchart*.

SIMBOL	NAMA SIMBOL / ARTI
	INPUT / OUTPUT Mempresentasikan input data atau output data yang diproses atau informasi

	PROSES Mempresentasikan operasi
	PENGHUBUNG Keluar atau masuk dari bagian lain flowchart khususnya halaman yang sama
	ANAK PANAH Mempresentasikan alur kerja
	PENJELASAN Digunakan untuk komentar tambahan
	KEPUTUSAN Keputusan dalam program
	PREDEFINED PROCESS Rincian operasi berada di tempat lain.
	PREPARATION Pemberian harga awal
	TERMILAN POINTS Awal / akhir flowchart
	PUNCHED CARD Input / output yang menggunakan kartu berulang

	DOKUMEN Input / output dalam format yang dicetak
	MAGNETIC TAPE Input / output yang menggunakan pita magnetic
	MAGNETIC DISK Input / Output yang menggunakan disk magnetic
	ON-LINA STORAGE Input / output yang menggunakan penyimpanan akses langsung
	PUNCHED TAPE Input / output yang menggunakan pita kertas berlubang
	MANUAL INPUT Input yang dimasukkan secara manual dari keyboard
	DISPLAY Output yang ditampilkan pada terminal

	MANUAL OPERATION Operasi manual
	OFF – LINE STORAGE Penyimpanan yang tidak dapat diakses oleh komputer secara langsung
	COMMUNICATION LINK Transmisi data melalui channel komunikasi, Seperti telepon

(Sumber : Blauch, 2012)

2.12 Metode-Metode *Kriptografi*

Kriptografi berasal dari bahasa Yunani, "*kryptós*" yang berarti tersembunyi dan "gráphein" yang berarti tulisan. Sehingga kata kriptografi dapat diartikan menjadi "tulisan tersembunyi". kriptografi adalah ilmu matematika yang berhubungan dengan transformasi data agar arti dari data tersebut menjadi sulit untuk dipahami, mencegahnya dari perubahan tanpa izin, atau mencegahnya dari penggunaan yang tidak sah. (Zelvina, 57 : 2012)

Jika transformasinya dapat dikembalikan, kriptografi juga dapat diartikan sebagai proses mengubah kembali data yang terenkripsi menjadi bentuk yang mudah dipahami. Sehingga, kriptografi juga dapat diartikan sebagai proses untuk melindungi data dalam arti yang luas. Pengertian Kriptografi dalam kamus bahasa

Inggris *Oxford* adalah Sebuah teknik rahasia dalam penulisan, dengan karakter khusus, dengan mengguanakan huruf dan karakter di luar bentuk aslinya, atau dengan metode-metode lain yang hanya dapat dipahami oleh pihak-pihak yang memproses kunci, juga semua hal yang ditulis dengan cara seperti ini. Jadi, secara umun kriptografi diartikan sebagai seni menulis atau memecahkan *cipher*.

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 cipherteksPesan (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 (ciphertext) atau kriptogram (cryptogram). Cipherteks harus dapat ditransformasikan 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*.Kriptografi Asimetri (Asymetric Cryptography) . 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 di jaga 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 $D\ K\ (C) = P$

Keterangan :

P = plainteks

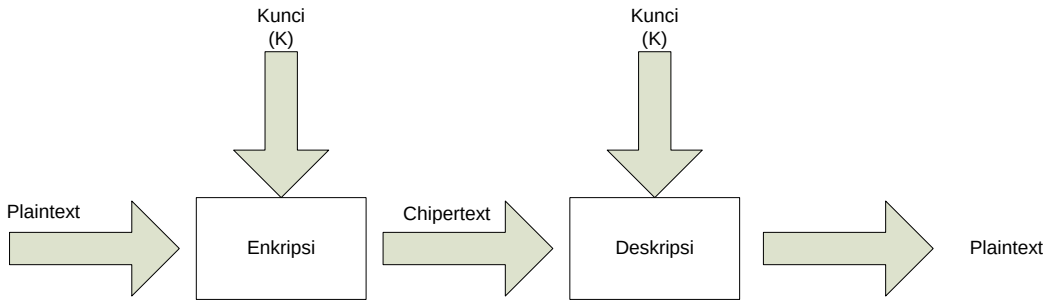
C = cipherteks

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

Sumber : *Dony Ariyus, 2015*

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 (*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*.

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.

a. Tujuan kriptografi

Tujuan dari kriptografi yang juga merupakan aspek keamanan informasi adalah sebagai berikut: (Zelvina, 58 : 2012)

1) Kerahasiaan (*confidentiality*) adalah layanan yang digunakan untuk menjaga isi informasi dari semua pihak kecuali pihak yang memiliki otoritas terhadap informasi. Ada beberapa pendekatan untuk menjaga kerahasiaan, dari pengamanan secara fisik hingga penggunaan algoritma matematika yang membuat data tidak dapat dipahami. Istilah lain yang senada dengan *confidentiality* adalah *secrecy* dan *privacy*.
2) Integritas data adalah layanan penjagaan pengubahan data dari pihak yang tidak berwenang. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam pesan yang sebenarnya. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (*digital signature*). Pesan yang telah ditandatangani menyiratkan bahwa pesan yang dikirim adalah asli.
3) Otentikasi adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi juga harus diotentikasi asalnya. Otentikasi

sumber pesan secara implisit juga memberikan kepastian integritas data, sebab jika pesan telah dimodifikasi berarti sumber pesan sudah tidak benar. Oleh karena itu, layanan integritas data selalu dikombinasikan dengan layanan otentikasi sumber pesan. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (*digital signature*). Tanda-tangan digital menyatakan sumber pesan.

4) Nirpenyangkalan (*non-repudiation*) adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

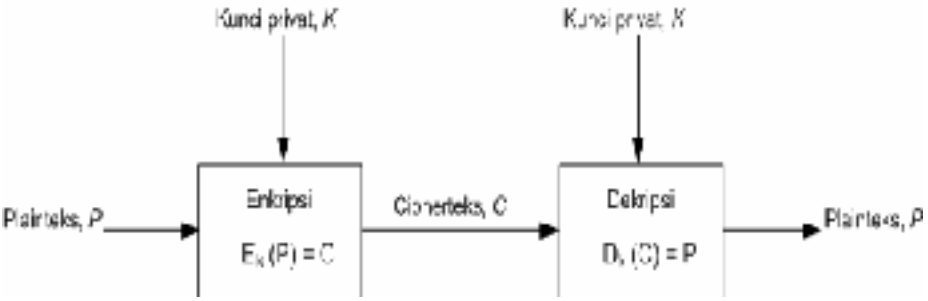
b. Jenis - jenis Kriptografi

Berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi 2 macam, yaitu kriptografi simetri(*symetriccryptography*) dan kriptografi asimetri (*asymetric cryptography)*.

1. Kriptografi Simetri (Symetric Cryptography)

   Pada sistem kriptografi simetri, kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Keamanan sistem kriptografi simetri terletak pada kerahasiaan kunci. Istilah lain untuk kriptografi simetri

adalah kriptografi kunci privat (private key cryptography) atau kriptografi konvensional (conventional cryptography).



Gambar 2 Kriptografi Simetri (Symetric Cryptography)

Sumber : Zelvina, 58 : 2012

Algoritma kriptografi simetri dapat dikelompokkan menjadi dua kategori antara lain :

a. Cipher aliran (stream cipher)

   Algoritma kriptografi beroperasi pada plainteks/cipherteks dalam bentuk bit tunggal yang dalam hal ini rangkaian bit dienkripsikan/didekripsikan bit per bit. Cipher aliran mengenkripsi satu bit setiap kali.

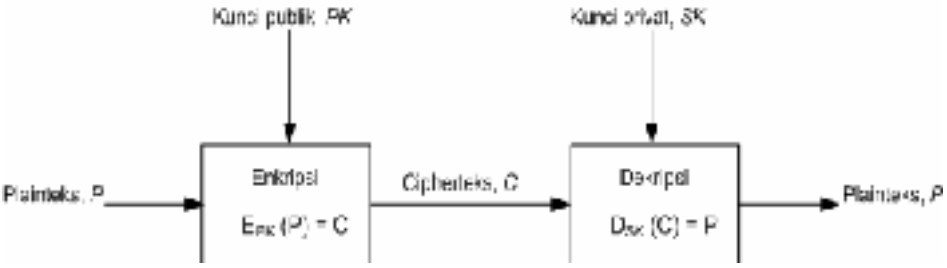
b. Cipher blok (block cipher)

   Algoritma kriptografi beroperasi pada plainteks/cipherteks dalam bentuk blok bit, yang dalam hal ini rangkaian bit dibagi menjadi blok-blok bit yang panjangnya sudah ditentukan sebelumnya. Cipher blok mengenkripsi satu blok bit setiap kali.

2. Kriptografi Asimetri (Asymetric Cryptography)

   Pada sistem kriptografi asimetri, kunci untuk proses enkripsi tidak sama dengan kunci untuk proses dekripsi. Istilah lain untuk kriptografi asimetri

adalah kriptografi kunci publik (public key cryptography), sebab kunci untuk enkripsi tidak rahasia dan dapat diketahui oleh siapapun, sementara kunci untuk dekripsi hanya diketahui oleh penerima pesan.



Gambar 3. Kriptografi Asimetri (*Asymetric Cryptography*)

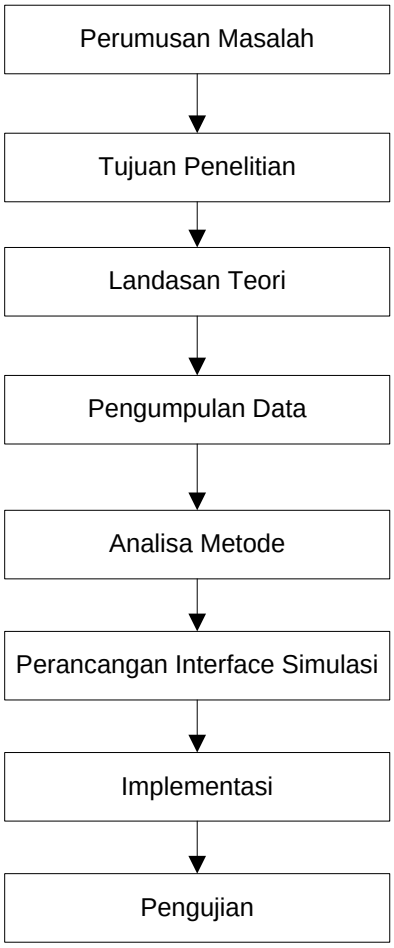
Sumber : Zelvina, 58 : 2012

BAB III

ANALISA DAN PERANCANGAN SISTEM

3.1 Tahapan Penelitian

Adapun tahapan penelitian yang dilakukan oleh penulis ini dengan judul Perancangan Aplikasi Penyandian Data Text Menggunakan Metode Symetric Stream Chipher Pada File Microsoft Word adalah sebagai berikut:



Gambar 3.1 Tahapan Penelitian

3.2 Metode Pengumpulan Data

Pengumpulan data adalah pencarian terhadap susuatu kerena ada perhatian dan keinginan terhadap hasil suatu aktivitas. Metode pengumpulan data dalam penulisan ini dibagi menjadi 2, yaitu :

1. Pengamatan (*Observation*)

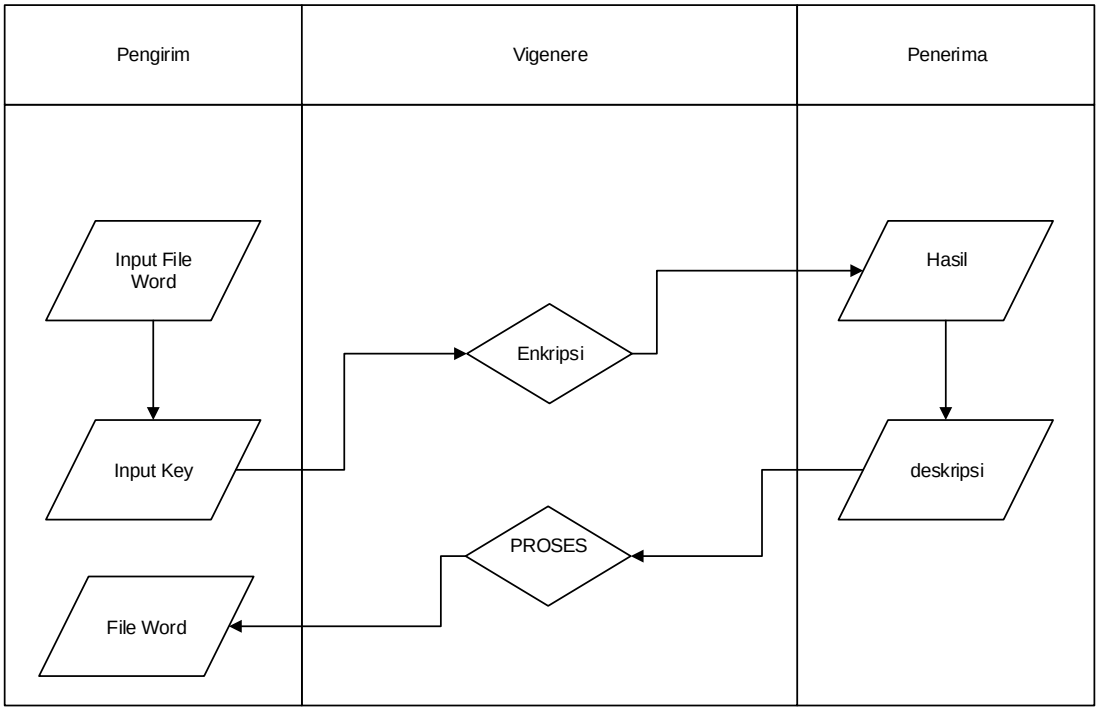
   Penulis melakukan pengamatan langsung pada setiap penggunan aplikasi chating yang sudah ada seperti WA, BBM dan Line untuk mengamati proses keamanan yang sudah dibuat sebelumnya.

2. Penelitian Kepustakaan (*Library Research*)

   Merupakan cara untuk mencari referensi dengan mengumpulkan bahan-bahan pustaka yang dilakukan di perpustakaan kampus, maupun perpustakaan umum, juga melakukan pencarian lewat internet, dengan mengunjungi situs-situs seperti *google Book online* yang dapat membantu pembahasan materi.

3.3 Analisis Sistem Yang Sedang Berjalan

Pertukaran data dalam hal ini pesan rahasia berbentuk teks dengan menggunakan metode tradisional yaitu dengan cara bertukar kata kunci tunggal. Diagram dibawah adalah penggambaran bagaimana pertukaran pesan rahasia menggunakan kunci tunggal terjadi.



Gambar 3.2 Analisis Sistem Yang Berjalan

Pemberitahuan kata kunci dari pengirim ke penerima menggunakan media yang umum digunakan oleh banyak orang.

3.3.1 Analisa Kelemahan yang Berjalan

1. Penggunaan kata kunci tunggal berpotensi terjadinya salah pemahaman. Dalam hal ini kemungkinan penerima salah mengartikan kunci yang diberikan oleh pengirim adalah hal yang dapat terjadi.
2. Pemberitahuan atau pertukaran kata kunci yang dikirimkan oleh pengirim ke penerima memiliki potensi dapat diketahui oleh orang lain sehingga pesan rahasia dapat terbongkar.

3.3.2 Solusi Pemecahan Masalah

Pemecahan masalah yang penulis lakukan adalah dengan melakukan penerapan metode ini yang didalamnya terdapat Algoritma *Vigenere Cipher*. Penggunaan metode ini dapat digunakan sebagai solusi agar pengirim dan penerima tidak lagi harus bertukar kunci tunggal untuk membuka pesan melainkan dapat memiliki kata kunci masing-masing.

Tabel 3.1 Perencanaan Rancangan

No	Sistem yang Berjalan	Sistem yang Diusulkan	Hasil yang Ingin Dicapai
1.	Penggunaan kunci tunggal yang harus diketahui oleh pengirim dan penerima untuk membuka pesan.	Pengirim dan penerima memiliki kunci masing-masing untuk membuka pesan	Tidak ada lagi kesalahan pemahaman atau salah tafsir kunci tunggal karena pengirim dan penerima memiliki kunci yang dapat ditetapkan masing-masing pihak.
2	Pertukaran kunci tunggal menggunakan media komunikasi yang rentan untuk	Pengirim dan penerima dapat menentukan sendiri kunci yang ingin	Kemungkinan bocornya kunci saat proses pertukaran informasi kunci

	dapat diketahui orang lain.	digunakan untuk membuka pesan.	tunggal dapat dihindari.

3.4 Rancangan Penelitian

Visual basic 2010 akan menjadi sarana untuk menciptakan perangkat lunak ini. Pada analisa proses ini penggunaan digunakan sebagai metode yang didalamnya terdapat kombinasi dari algoritma *Vigenere Cipher*. Algoritma *Vigenere Cipher* digunakan oleh pengirim untuk mengenkripsi pesan yang akan dikirimkan..

Perhitungan secara matematis dilakukan sebagai penggambaran proses yang akan terjadi pada metode ini yang didalamnya terdapat algoritma *Vigenere Cipher*. Berikut tahapannya:

Proses Enkripsi Pesan Asli oleh Pengirim

Adapun perhitungannya proses three pass protocol adalah sebagai berikut:

Sebagai contoh:

Diketahui:

Ciphertext : ADYSA

Kunci : 123

Selanjutnya akan di enkripsi dengan formula Algoritma Vigenere Cipher yaitu:

C = P + K mod 255

A = 65 + 1 Mod 255

= 66

= 66 = B

D = 68 + 2 Mod 255

= 70

= 70 = F

Y = 89 + 3 Mod 255

= 92

= 92 = \

S = 83 + 1 Mod 255

= 84

= 84 = T

A = 65 + 2 Mod 255

= 67

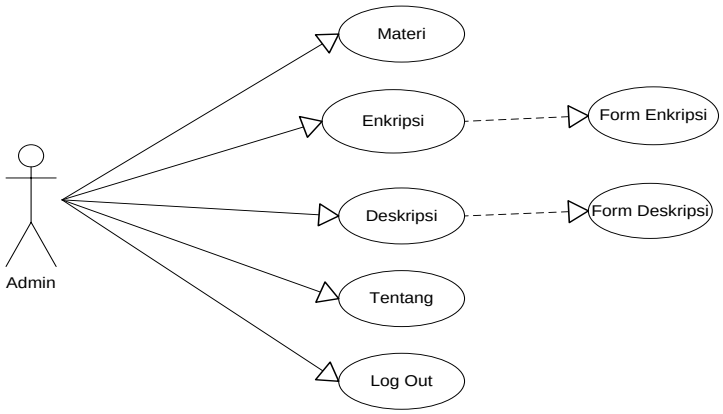
= 67 = C

Sehingga ciphertext kedua yang didapat adalah:

Ciphertext = BF\TC

3.5 UML Yang Diusulkan

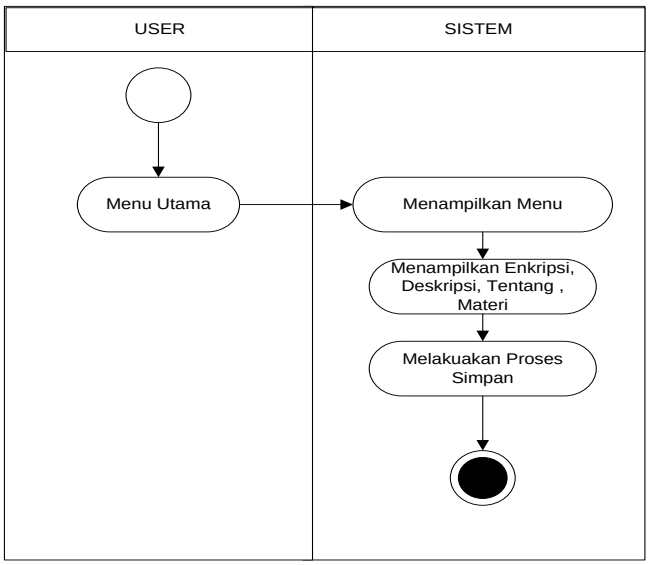
3.5.1. Use Case Diagram



Gambar 3.4 Use Case Diagram

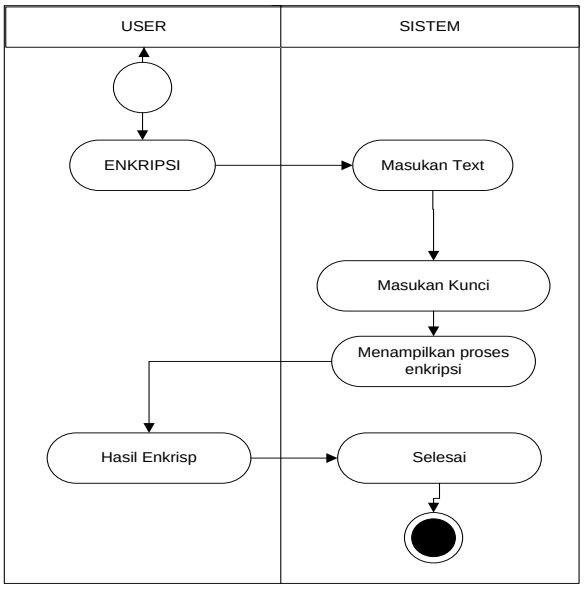
3.5.2 Desain Sistem Secara Detail

1. Activity Diagram Menu Utama



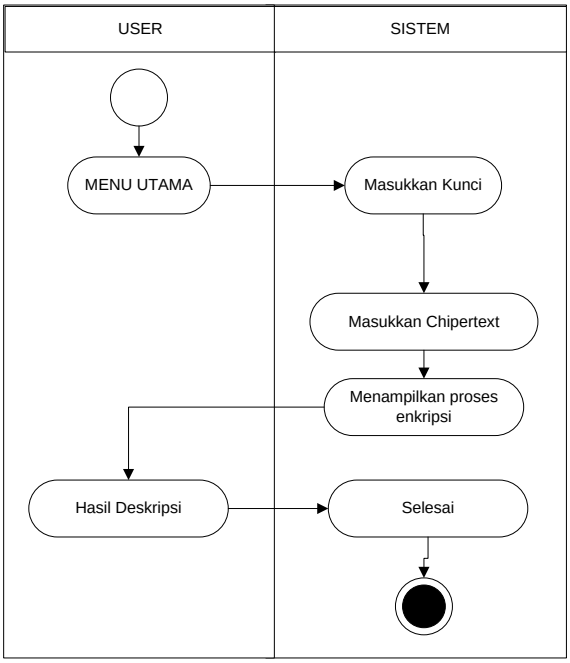
Gambar 3.6 Activity Diagram Menu Utama

2. Activity Diagram Enkripsi



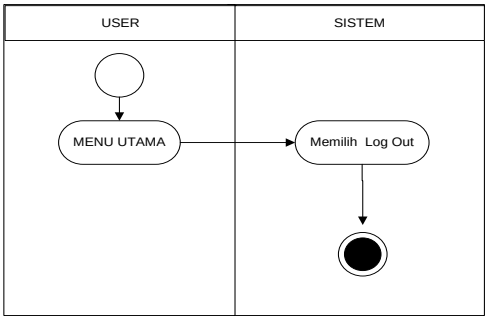
Gambar 3.7 Activity Diagram Enkripsi

3. Activity Diagram Deskripsi



Gambar 3.8 Activity Diagram Deskripsi

4. Activity Diagram Log Out

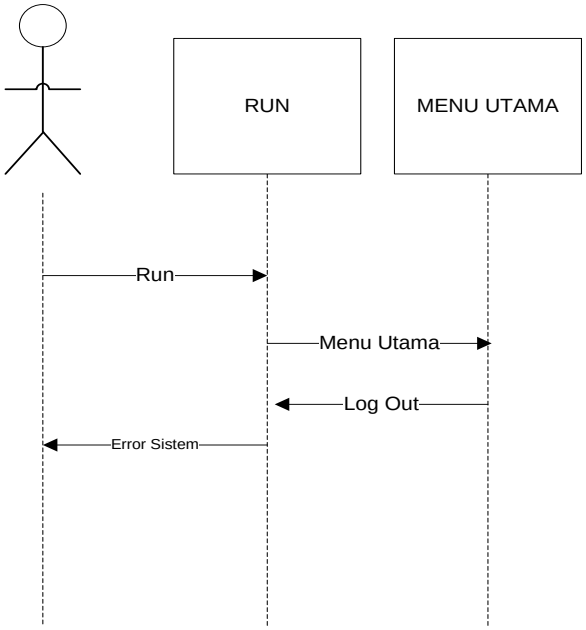


Gambar 3.11 Activity Diagram Log Out

3.5.3 Sequence Diagram

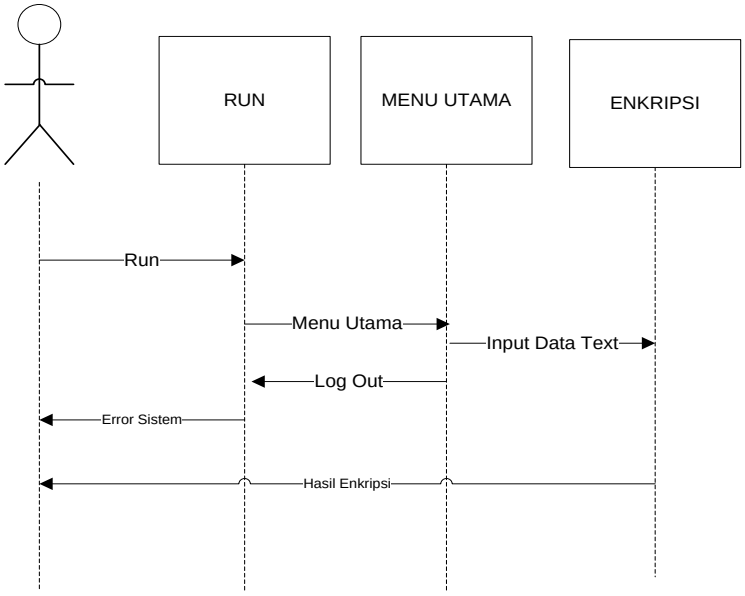
Adapaun sequence digram sistem usulan yang dilakukan oleh penulis adalah sebagai berikut:

1. Sequence Diagram Menu Utama



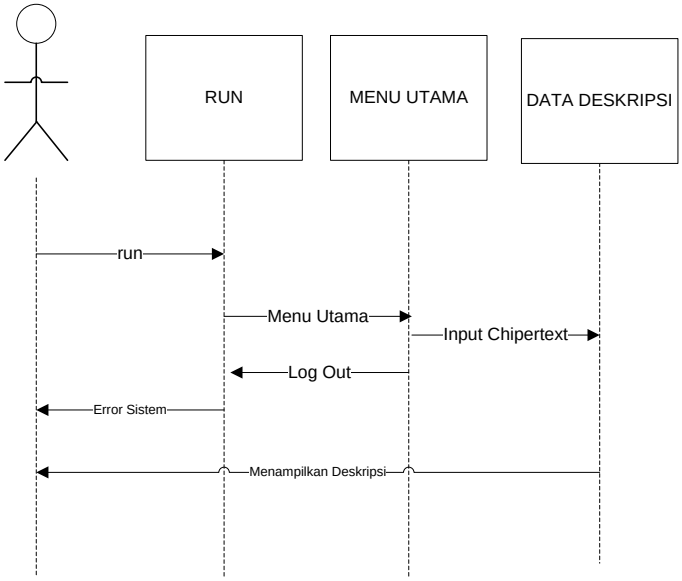
Gambar 3.12 Sequence Diagram Menu Utama

2. Sequence Diagram Enkripsi



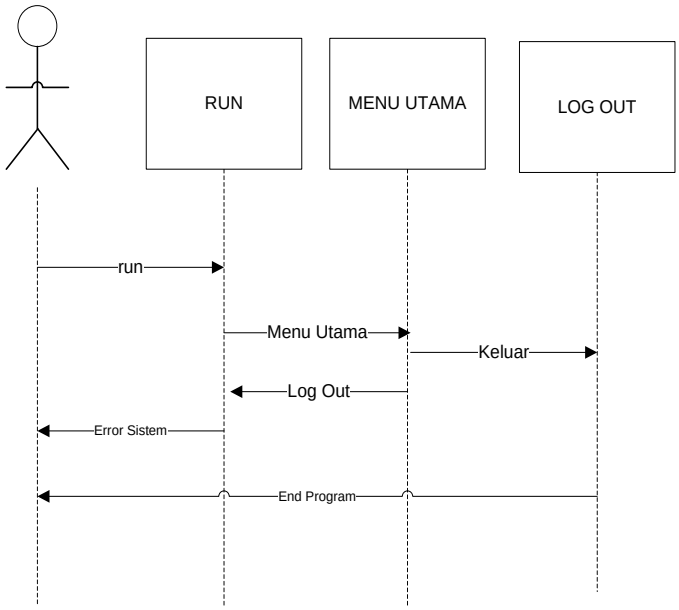
Gambar 3.13 Sequence Diagram Enkripsi

3. Sequence Diagram Deskripsi



Gambar 3.14 Sequence Diagram Deskripsi

4. Sequence Diagram Log Out

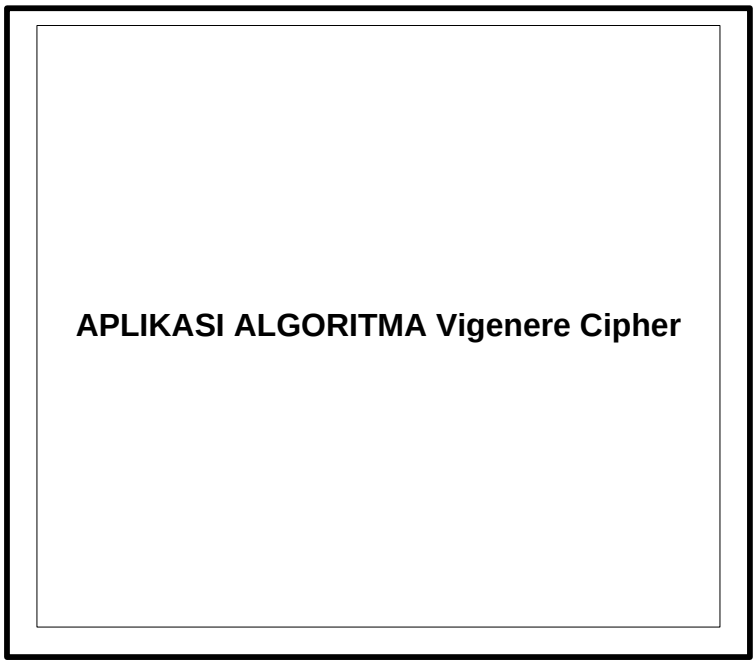


Gambar 3.17 Sequence Diagram Log Out

3.6 Perancangan Interface

1. Rancangan Halaman Judul

   Halaman judul merupakan halaman yang pertama muncul pada saat program dijalankan

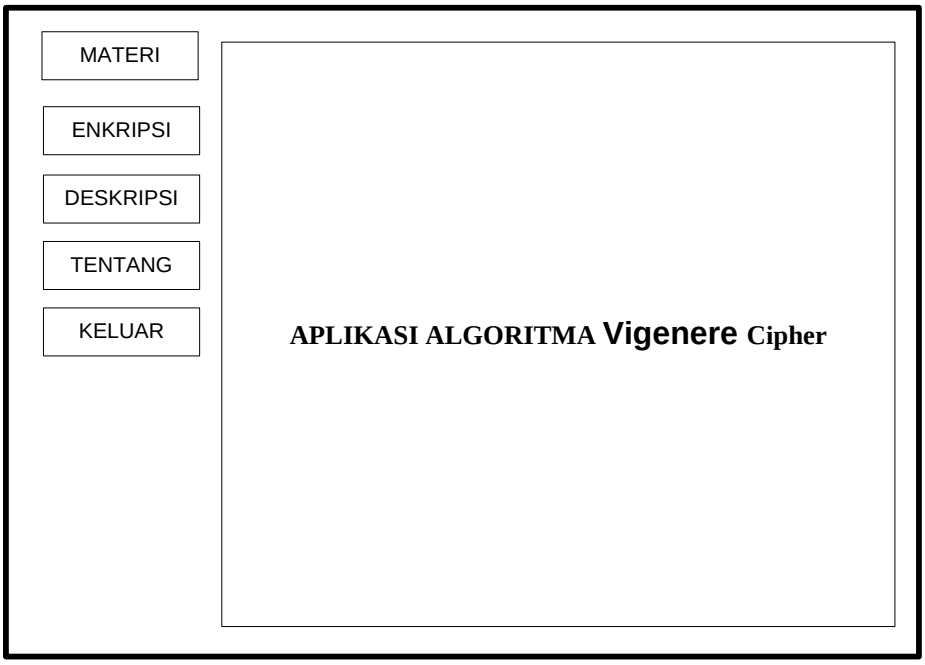


Gambar 3.4 Rancangan Halaman Judul

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

2. Rancangan Halaman Menu Utama

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



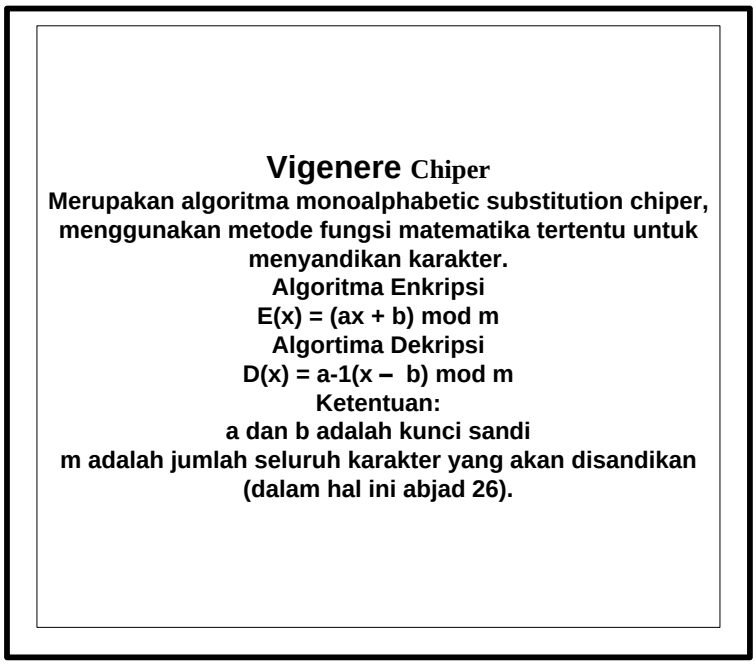
Gambar 3.5 Rancangan Halaman Menu Utama

Pada tampilan di atas terdapat 5 tombol yaitu Materi, Enkripsi, Deskripsi, Tabel Vigenere, 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.

3. Rancangan Halaman Materi

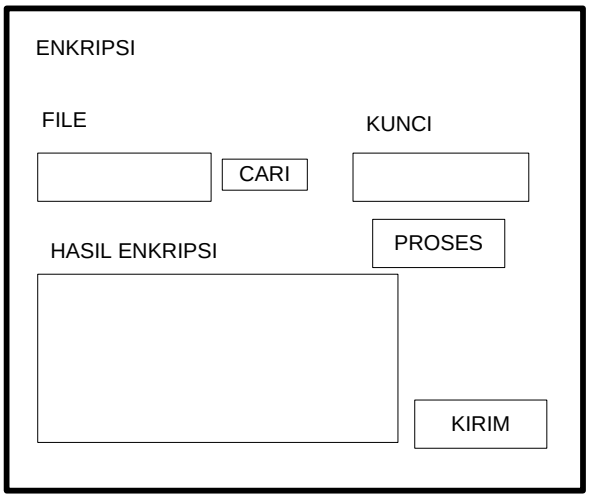
   Form ini digunakan untuk menjelaskan cara kerja penyandian, dimulai dari plaintext kemudian kunci yang dikonversikan dalam bentuk angka. Setelah itu dilakukan proses penjumlahan dan jika hasil penjumlahan maka akan dikurangi 6 lalu hasilnya akan dikembalikan lagi ke dalam bentuk huruf.



Gambar 3.6 Rancangan Halaman Materi

4. Rancangan Halaman Enkripsi

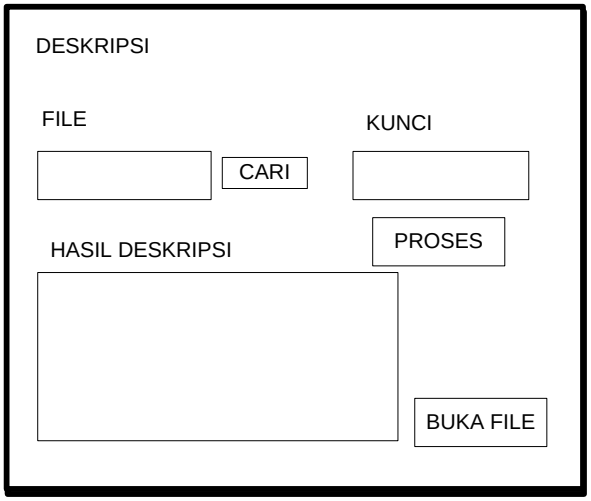
   Berisi penjelasan mengenai Enkripsi. Pengguna memasukkan tulisan asli atau *plaintext* ke dalam tombol masukan *plaintext* kemudian dimasukkan juga kunci. Setelah itu, ditekan tombol Proses Enkripsi yang kemudian akan menampilkan ciphertext atau tulisan yang telah disandikan.



Gambar 3.7 Rancangan Halaman Enkripsi

5. 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.



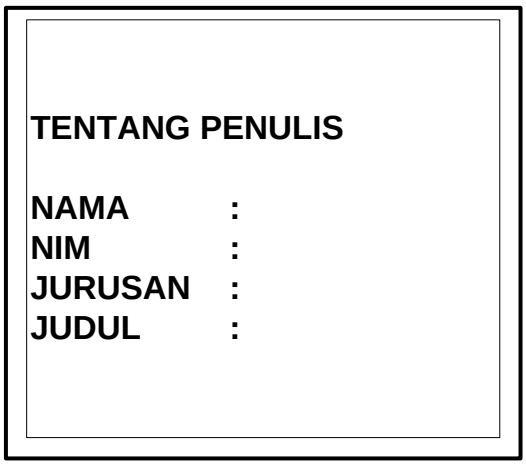
Gambar 3.8 Rancangan Halaman Deskripsi

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.

6. Rancangan Halaman Tentang

Berisi penjelasan mengenai tentang biodata penulis. Isi dari form tentang ini adalah berisikan data dari penulis yang ada menganggkat judul ini.



Gambar 3.9 Rancangan Halaman Tentang

BAB IV

HASIL DAN PEMBAHASAN

4.1 Pengujian Sistem

Pengujian system 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 three-pass protocol 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 .

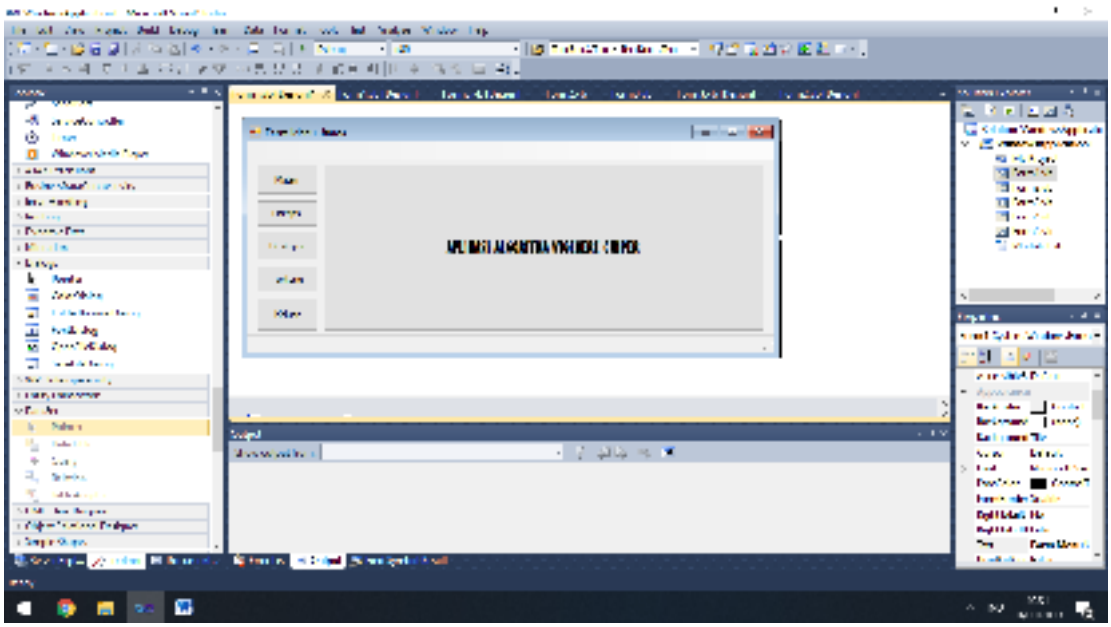
Proses yang akan dilakukan pengujian dalam aplikasi ini adalah simulasi pengiriman pesan dengan menggunakan metode algoritma *Vigenere Cipher* antara pengirim kepada penerima dengan kunci yang dimiliki masing-masing pihak tanpa perlu bertukar kunci tunggal hingga pada akhirnya pesan asli yang dikirimkan oleh pengirim dapat dibaca oleh penerima.

Tahap implementasi system 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.

1. Tampilan Awal/ Home

Tampilan pada gambar 4.1 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 *read me!* yang akan mengarahkan pengguna ke form yang menjelaskan tata cara penggunaan dari aplikasi ini.



Gambar 4.1 Tampilan Awal/ Home

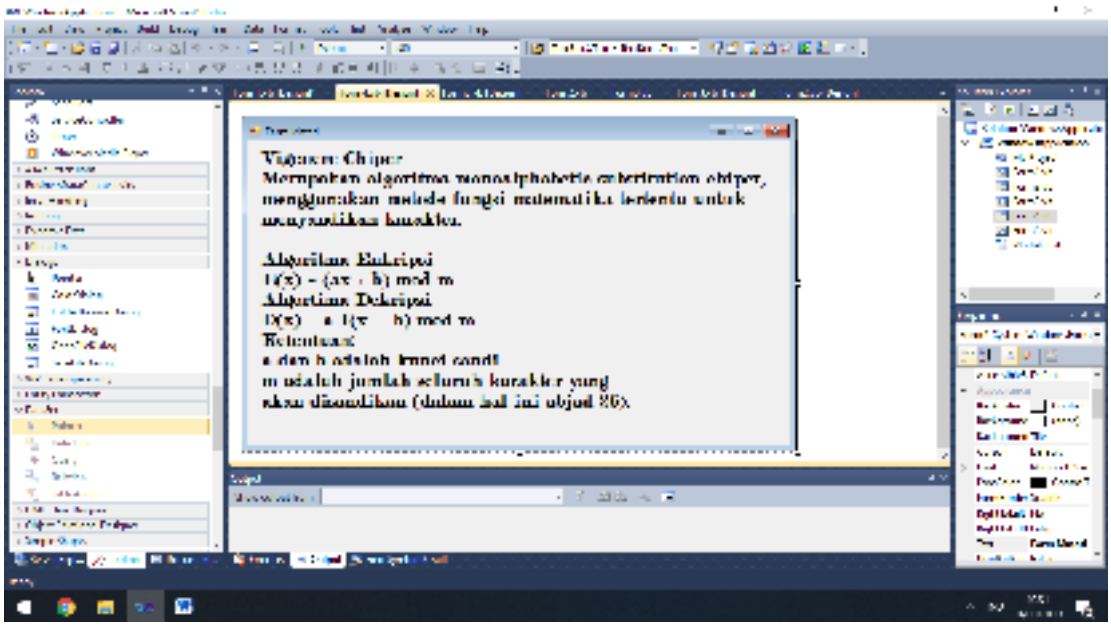
Keterangan Gambar :

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.

2. Tampilan Aturan Materi

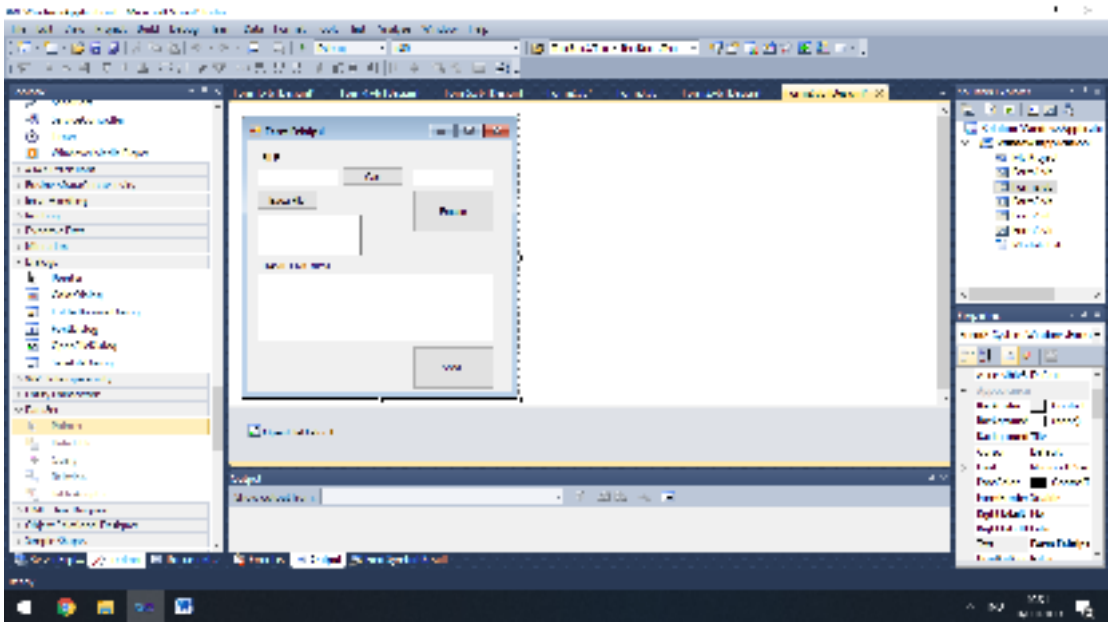
Tampilan aturan penggunaan aplikasi merupakan tampilan halaman atau form yang berisi tentang tata cara penggunaan aplikasi yang dijalankan. Pada halaman tersebut dijelaskan apa-apa saja yang menjadi kewajiban bagi pengirim dan penerima saat menjalankan simulasi algoritma *Vigenere Cipher*.



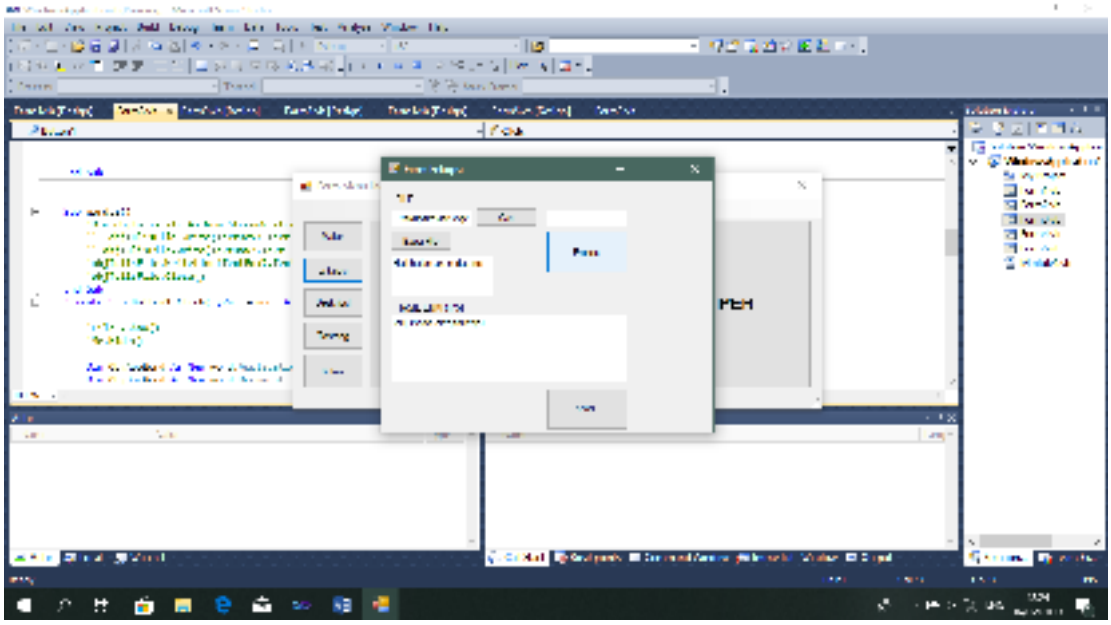
Gambar 4.2 Tampilan Form Mater

3. Tampilan Halaman Enkripsi

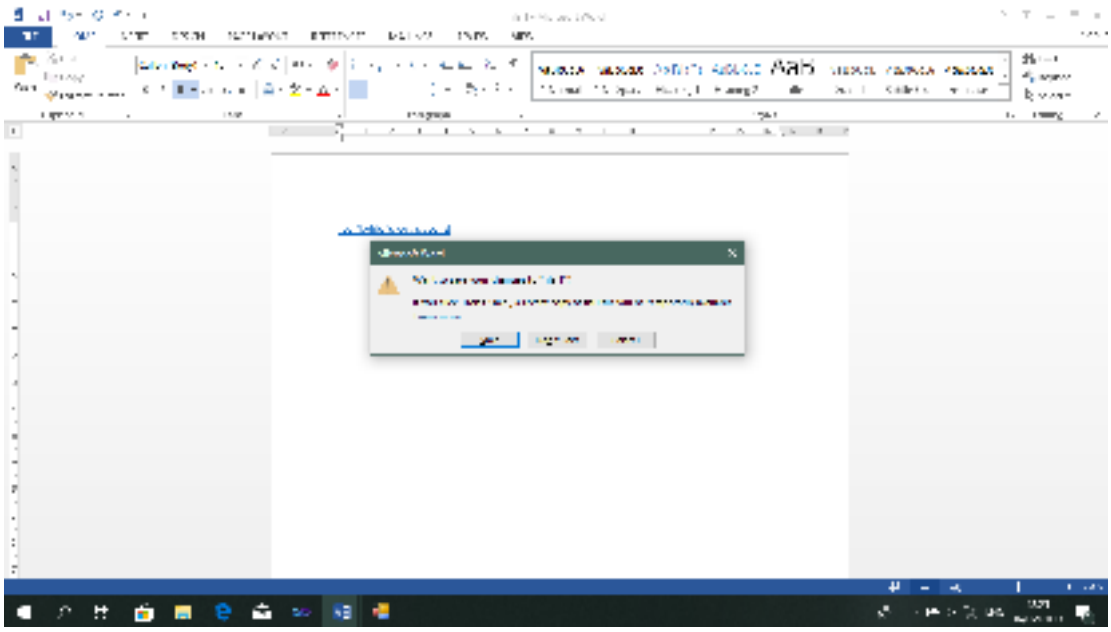
Tampilan berikut merupakan tampilan pengiriman pesan pada aplikasi ini. algoritma *Vigenere Cipher* merupakan protokol yang menjamin tidak adanya pertukaran kunci antara pihak-pihak yang melakukan enkripsi dan dekripsi. Kedua belah pihak menggunakan kunci mereka masing-masing untuk mengenkripsi pesan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



Gambar 4.3 Tampilan Halaman Enkripsi



Gambar 4.4 Tampilan Halaman Enkripsi



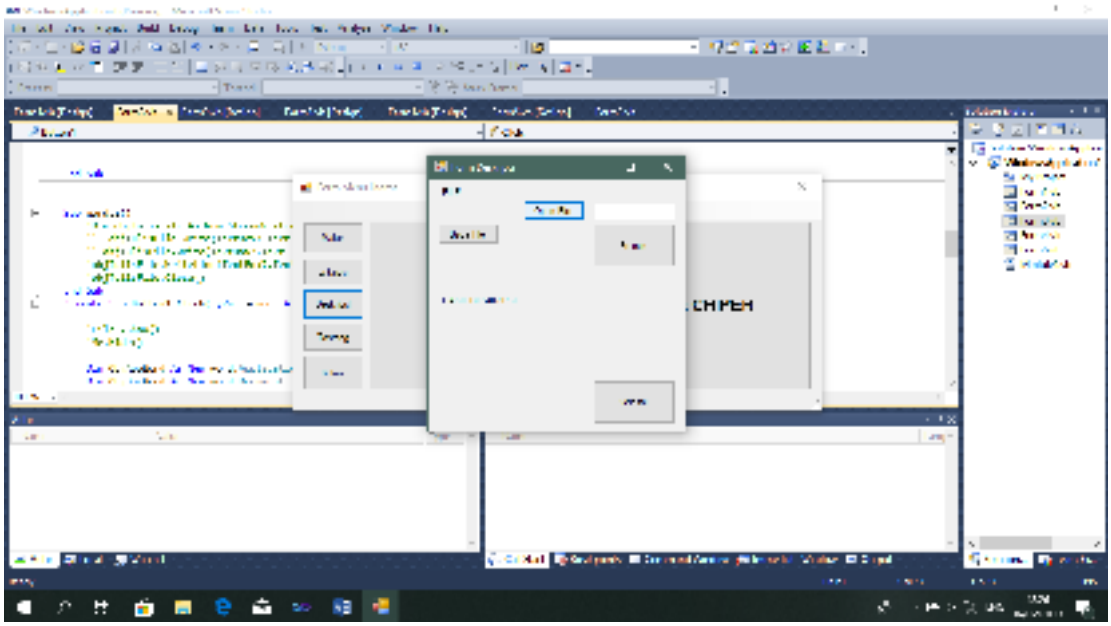
Gambar 4.5 Tampilan Hasil dari Enkripsi

Keterangan Gambar :

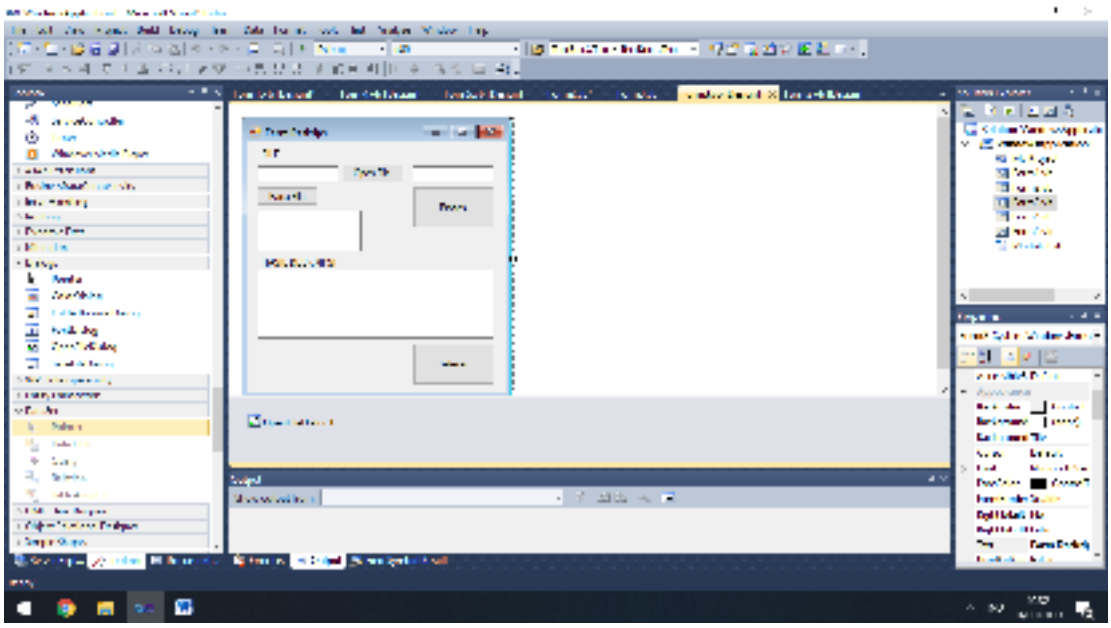
1. Dalam diagram di atas menjelaskan bahwa user memilih materi kemudian Sistem menampilkan materi yang berkaitan dengan materi
2. User merequest Enkripsi kemudian Sistem menampilkan menu Enkripsi
3. User merequest Deskripsi kemudian Sistem menampilkan menu Deskripsi
4. User merequest Menu Tentang kemudian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

4. Tampilan Halaman Deskripsi

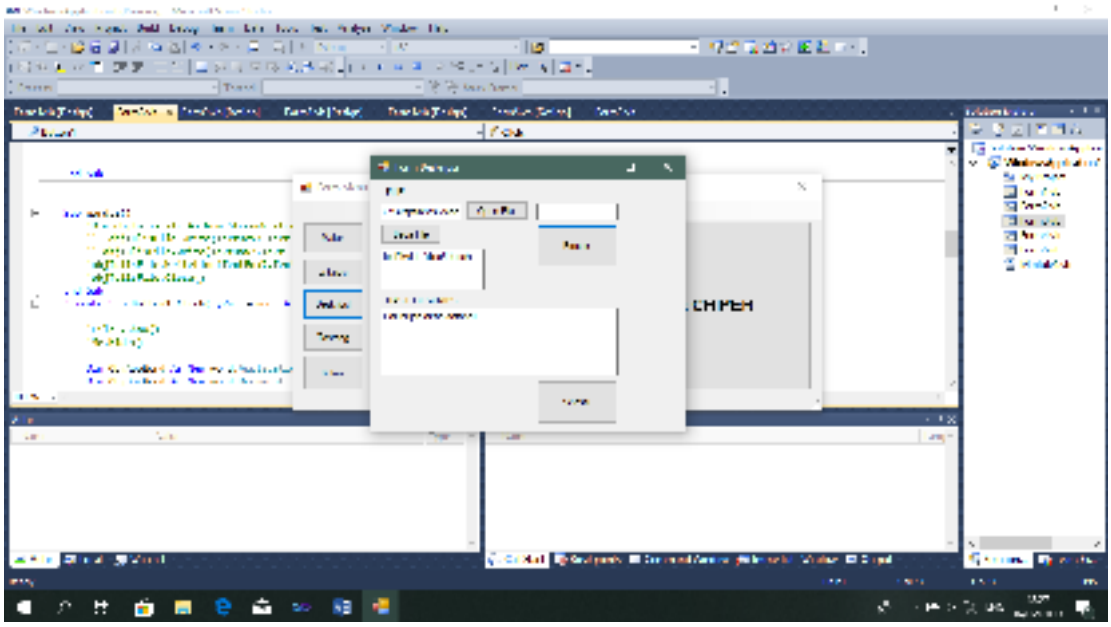
Tampilan berikut merupakan tampilan penerima pesan pada aplikasi ini.



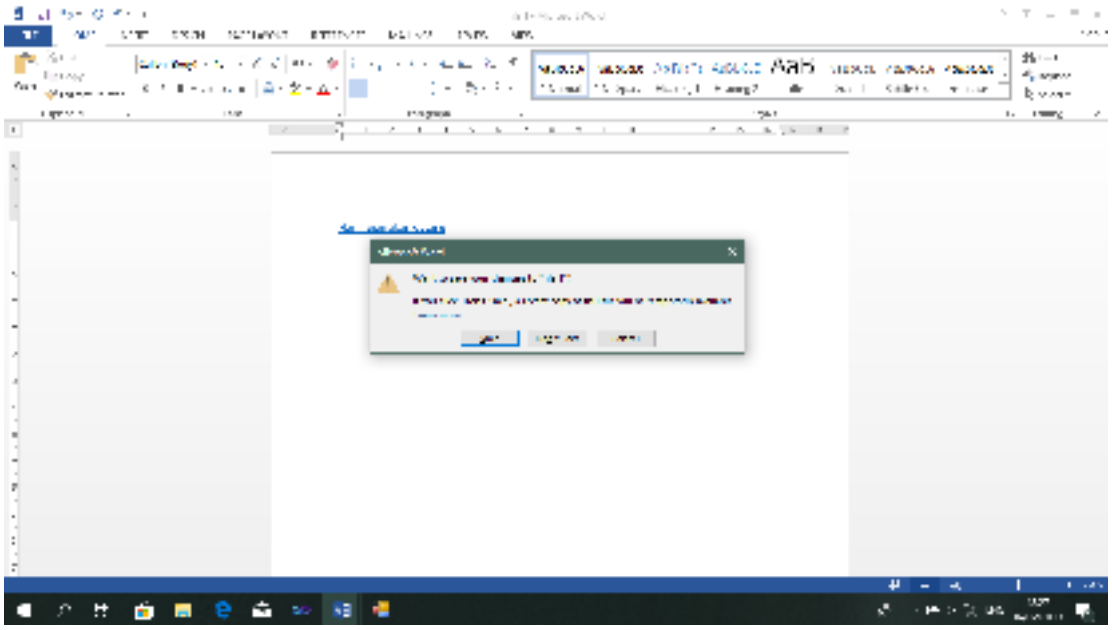
Gambar 4.6 Tampilan Halaman Deskripsi



Gambar 4.7 Tampilan Halaman Deskripsi



Gambar 4.6 Tampilan Halaman Deskripsi



Gambar 4.6 Tampilan Hasil dari Deskripsi

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.

4.3 Pengujian Black Box

Perangkat lunak adalah elemen kritis dari jaminan kualitas perangkat lunak dan merepresentasikan kajian pokok dari spesifikasi, perancangan, dan pengkodean. Pengujian yang digunakan untuk menguji sistem ini adalah metode pengujian *black-box*. Pengujian *black-box* berfokus pada persyaratan fungsional perangkat lunak.

1. Rencana Pengujian

Pengujian fungsi Penerapan Matrix Persegi Pancajang Dalam Pengembangan Algoritma Hill Chiper dilakukan dengan menggunakan metode Black Box. Pengujian dilakukan pada fungsi-fungsi sistem untuk menentukan apakah fungsi tersebut telah berjalan sesuai dengan yang diharapkan.

1) Bangkitkan Kunci

Tabel 4.1 . Rencana Pengujian Tombol Cari

Menu yang diuji	**Detail pengujian**	**Kesimpulan**
Bankitkan Kunci	Melakukan random kunci pada proses hill chiper.	*Diterima*

2) Proses Enkripsi

Tabel 4.2. Rencana Pengujian Pengguna (*User*)

Menu yang diuji	**Detai pengujian**	**Jenis uji**
Proses	Melakukan proses enkripsi	*Diterima*
Kirim	Proses pengiriman file enkripsi	*Diterima*
Clear All	Menghapus seluruh text yang ada pada text box	*Diterima*

3) Proses Deskripsi

Tabel 4.3. Rencana Pengujian Pengguna (*User*)

Menu yang diuji	**Detai pengujian**	**Jenis uji**
Dekripsi	Melakukan proses deskripsi atau pengembalian pesan asli	*Diterima*
Close	Menutup semua program	*Diterima*
Clear All	Menghapus seluruh text yang ada pada text box	*Diterima*

2. Pengujian Proses

Pengujian proses yang telah disusun, maka dapat dilakukan pengujian sebagai berikut :

Tabel 4.4. Proses Pengujian Enkripsi dan Deskripsi (*User*)

Data Pengujian Proses					**Hasil**
Nomor	**Isi Pesan**	**Kunci**	**Enkripsi**	**Deskripsi**	
1	*VIGENERE*CIPHER	5 8	BIGLOHDKJSFU	*VIGENERE*CIPHER	Berhasil

3. Kesimpulan Dan Hasil Pengujian Sistem

Hasil pengujian dari pengujian alpha telah selesai, menunjukkan bahwa sistem sudah memenuhi syarat fungsional. Secara fungsional sistem yang sudah dibangun sudah dapat menghasilkan keluaran sesuai yang diharapkan.

Tabel 4.5. Kesimpulan Pengujian Alpha

Nama fungsi	**Hasil**
Tombol Cari	Fungsi berjalan dengan baik
Proses	Fungsi berjalan dengan baik
Enrkipsi	Fungsi berjalan dengan baik
Deskripsi	Fungsi berjalan dengan baik
Clear All	Fungsi berjalan dengan baik

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan dalam Perancangan Aplikasi Penyandian Data Text Menggunakan Metode *Symetric Stream Chipher* Pada *File Microsoft Word*, maka dapat diambil kesimpulan sebagai berikut :

1. Perangkat lunak ini dirancang untuk menampilkan simulasi pengiriman pesan berekstensi yang diinputkan kedalam textbox antara pengirim dan penerima.
2. Pengirim mengirimkan pesan menggunakan dua kunci yang ditentukan sendiri oleh pengirim.
3. Penerima pesan menggunakan kunci yang diberikan oleh pengirim pesan, agar bisa membuka pesan asli yang dikirimkan oleh pengirim.

5.2 Saran

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

1. Diharapkan adanya kombinasi algoritma keamanan data lainnya.
2. Proses pengamanan data yang dilakukan oleh penulis masih menggunakan visual studio, diharapkan ada yang menggunakan diandroid agar bisa digunakan pada mobile.

DAFTAR PUSTAKA

Anonim, Ariyus, Kadir. 2006. *Computer Security*. Yogyakarta: Penerbit Andi.

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

Bishop, Matt. 2005. *Introduction To Computer Security. Boston: Addison-Wesley*.

Christensen, Chris. 2006. Steganografi And LSB. Http:/Www.Nku.Edu/~Christensen/Section%2014%20steganografi.Pdf.

Leong, Marlon. 2006. *Dari Programmer Untuk Proggrammer Visual Basic*. Yogyakarta: Penerbit Andi.

Martin, Keith. 2012. *Everyday Cryptography*. Oxford: Oxford University Press.

Mulyana, Teady. 2012. *Steganografi Citra Digital Menggunakan Spreadsheet*. Vol: 8 No 2 Agustus 2012.

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

Badawi, A. (2018). Evaluasi Pengaruh Modifikasi Three Pass Protocol Terhadap Transmisi Kunci Enkripsi.

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.

Bahri, S. (2018). Metodologi Penelitian Bisnis Lengkap Dengan Teknik Pengolahan Data SPSS. Penerbit Andi (Anggota Ikapi). Percetakan Andi Ofsset. Yogyakarta.

Diantoro, M., Maftuha, D., Suprayogi, T., Iqbal, M. R., Mufti, N., Taufiq, A., ... & Hidayat, R. (2019). Performance of Pterocarpus Indicus Willd Leaf Extract as Natural Dye TiO2-Dye/ITO DSSC. Materials Today: Proceedings, 17, 1268-1276.

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

Fitriani, W., Rahim, R., Oktaviana, B., & Siahaan, A. P. U. (2017). Vernam Encypted Text in End of File Hiding Steganography Technique. Int. J. Recent Trends Eng. Res, 3(7), 214-219.

Hardinata, R. S. (2019). Audit Tata Kelola Teknologi Informasi menggunakan Cobit 5 (Studi Kasus: Universitas Pembangunan Panca Budi Medan). Jurnal Teknik dan Informatika, 6(1), 42-45.

Hariyanto, E., Lubis, S. A., & Sitorus, Z. (2017). Perancangan prototipe helm pengukur kualitas udara. KOMIK (Konferensi Nasional Teknologi Informasi dan Komputer), 1(1).

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.

Harumy, T. H. F., & Sulistianingsih, I. (2016). Sistem penunjang keputusan penentuan jabatan manager menggunakan metode mfep pada cv. Sapo durin. In Seminar Nasional Teknologi Informasi dan Multimedia (pp. 6-7).

Iqbal, M., Siahaan, A. P. U., Purba, N. E., & Purwanto, D. (2017). Prim's Algorithm for Optimizing Fiber Optic Trajectory Planning. Int. J. Sci. Res. Sci. Technol, 3(6), 504-509.

Marlina, L., Muslim, M., Siahaan, A. U., & Utama, P. (2016). Data Mining Classification Comparison (Naïve Bayes and C4. 5 Algorithms). Int. J. Eng. Trends Technol, 38(7), 380-383.

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.

Ramadhan, Z., Zarlis, M., Efendi, S., & Siahaan, A. P. U. (2018). Perbandingan Algoritma Prim dengan Algoritma Floyd-Warshall dalam Menentukan Rute Terpendek (Shortest Path Problem). JURIKOM (Jurnal Riset Komputer), 5(2), 135-139.

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.

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

Rhee, Man Young. 1994. *Library of Congress Cataloging-in-Publication Data*. Singapore: McGraw-Hill Book Co.

Sutanto, Edhy. 2004. *Algoritma:Teknik Penyelesaian Permasalahan Untuk Komputasi*. Yogyakarta : Graha Ilmu.

Wahana Komputer. 2003. *Memahami Model Enkripsi dan Security Data*. Yogyakarta: Penerbit Andi.

Listening program

```
Imports word = Microsoft.Office.Interop.Word
Public Class Form2
    Dim strFileName As String
    Dim doc As word.Document
    Dim app As word.Application
    Private Sub BtSelect_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles BtSelect.Click
        doc = New word.Document
        app = New word.Application
            Me.TextBox1.Text = Me.OpenFileDialog1.FileName
            TextBox5.Text = doc.Range.Text
            app.Quit()
        End If

        'Dim AmbilFile As New OpenFileDialog
        'AmbilFile.CheckFileExists = True
        'AmbilFile.Filter = "DOC File (*.doc) | *.docx"
        'AmbilFile.Title = "Hanya file berformat DOC"
        'AmbilFile.Multiselect = False
        'AmbilFile.ShowDialog()
        'strFileName = AmbilFile.FileName
        'TextBox1.Text = strFileName
    End Sub

    Private Sub btbaca_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles btbaca.Click
        'Dim mystream As New System.IO.StreamReader(strFileName)
        'Dim BacaString As String
        'Dim TextPerBaris As String = ""
        " Me.TextBox5.ad.Clear()
        'While Not (mystream.EndOfStream)
        '    BacaString = mystream.ReadLine
        '    Me.TextBox5.Text = BacaString
        'End While

    End Sub


        Dim j As Integer
        Dim jum As Integer
        Dim skey As String
        Dim nkata As Integer
        Dim nkunci As Integer
```

```
    Dim skata As String
    Dim splain As String = ""
    Dim nenc As Integer
    j = 0
    skata = TextBox5.Text
    jum = Len(skata)
    skey = TextBox6.Text
    For i = 1 To jum
       If j = Len(skey) Then
          j = 1
       Else
          j = j + 1
       End If
       nkata = Asc(Mid(skata, i, 1)) - 65
       nkunci = (Mid(skey, j, 1))
       nenc = ((nkata + nkunci) Mod 256)
       splain = splain & Chr((nenc) + 65)
    Next i
    TextBox7.Text = splain
Sub yy()
    Dim j As Integer
    Dim jum As Integer
    Dim skey As String
    Dim nkata As Integer
    Dim nkunci As Integer
    Dim skata As String
    Dim splain As String = ""
    Dim nenc As Integer
    j = 0
    skata = TextBox5.Text
    jum = Len(skata)
    skey = TextBox6.Text
    For i = 1 To jum
       If j = Len(skey) Then
          j = 1
       Else
          j = j + 1
       End If
       nkata = Asc(Mid(skata, i, 1)) - 65
       nkunci = (Mid(skey, j, 1))
       nenc = ((nkata + nkunci) Mod 256)
       splain = splain & Chr((nenc) + 65)
    Next i
    TextBox5.Text = splain

End Sub
```