IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER DENGAN PHP

Muhammad Dedi Irawan[1]

Program Studi Teknik Informatika, Universitas Asahan,

Jln.Jend. Ahmad Yani Kisaran

[1]temansejati.dedi@gmail.com

Abstrak **- Penelitian ini dilakukan untuk membuat implementasi kriptografi vigenere cipher. Sistem ini dirancang dengan melakukan analisa dengan metode deskriptif, dan metode komperatif. Setelah dilakukan analisa, maka dilakukan pemodelan dengan UML (Unified Modelling Language) dan dilakukan perancangan sistem kriptografi vigenere cipher dengan bentuk enkripsi dan dekripsi text yang dapat diprogram dengan menggunakan software PHP. Hasil penelitian ini adalah sebuah implementasi sistem kriptografi vigenere cipher dengan PHP.**

Kata Kunci **- Kriptografi, Vigenere Cipher, Enkripsi – Dekripsi, Text, PHP.**

Abstract **- This research was conducted to make the implementation of crystalline vigenere cipher. This system is designed by conducting analysis with descriptive method, and comparative method. After analyzing, UML (Unified Modeling Language) is modeled and design of crystallographic vigenere cipher system with encryption and text decryption that can be programmed by using PHP software. The result of this research is an implementation of cryptography system vigenere cipher with PHP.**

Keywords **- Cryptography, Vigenere Cipher, Encryption - Decryption, Text, PHP.**

I. PENDAHULUAN

A. Latar Belakang

Masalah keamanan dan kerahasiaan data merupakan salah satu aspek penting pada sebuah sistem pengiriman informasi. Dalam hal ini, sangat terkait dengan betapa pentingnya informasi tersebut dikirim dan diterima oleh orang yang berkepentingan. Informasi akan tidak berguna lagi apabila di tengah proses pengiriman, informasi itu disadap atau dibajak oleh orang yang tidak berhak.

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi. Ilmu sandi (kriptografi) sendiri telah ada sejak lama. Tercatat dalam sejarah bahwa Julius Caesar, seorang kaisar Romawi menggunakan penyandian untuk menyampaikan pesan rahasia saat perang.

Sandi *Vigenère* sebenarnya merupakan pengembangan dari sandi *Caesar*. Pada sandi *Caesar*, setiap huruf pada teks digantikan dengan huruf lain yang memiliki perbedaan tertentu pada urutan alfabet. Misalnya pada sandi *Caesar* dengan geseran 3, A menjadi D, B menjadi E dan seterusnya. Sandi *Vigenère* terdiri dari beberapa sandi *Caesar* dengan nilai geseran yang berbeda.

Berdasarkan uraian di atas, maka penulis bermaksud untuk mempelajari sandi *Vigenère* dengan merancang suatu perangkat lunak pembelajaran sekaligus mengimplementasikan sandi *Vigenère* dalam sebuah aplikasi. Oleh karena itu, penulis mengambil

penelitian dengan judul "**Implementasi Kriptografi Metode Vigenere Cipher Dengan PHP**".

B. Batasan Masalah

Adapun batasan masalah penulisan skripsi ini adalah sebagai berikut.

1. *Input* pesan dibatasi hanya *file* berekstensi .txt dan hanya mengandung huruf tanpa karakter *enter* dan simbol. Sedangkan *output* hasil penyandian dapat disimpan dalam bentuk *file* berekstensi .txt yang dapat dibuka dengan aplikasi Notepad.
2. Perancangan menggunakan aplikasi XAMPP menggunakan Program HTML, dan PHP.

C. Tujuan dan Manfaat Penelitian

Tujuan dari penelitian ini adalah menghasilkan suatu aplikasi pembelajaran yang memiliki fasilitas untuk mengamankan atau menyembunyikan informasi dan pesan yang akan dikirimkan.

D. Manfaat Penelitian

Adapun manfaat yang dapat diperoleh dan penulisan peneltian adalah sebagai berikut:

1. Bagi penulis, yaitu dapat menambah pemahaman mengenai kriptografi terutama tentang metode sandi *Vigenère*.
2. Bagi pengguna, yaitu dapat menambah pemahaman pengguna mengenai sandi *Vigenère* dan juga pengguna dapat menyandikan pesan rahasia yang hendak dikirimkan tanpa takut dibaca oleh orang yang tidak memiliki hak dengan menggunakan aplikasi ini.

II. LANDASAN TEORI

A. Kriptografi

Kriptografi secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita. Selain pengertian tersebut terdapat pula pengertian ilmu yang mengajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (A. Menezes, P. Van Oorschot and S. Vanstone – Handbook of Applied Cryptography). Sedangkan menurut Kaufman et. al. (2002) menjelaskan bahwa kata Kriptografi berasal dari bahasa yunani dan memiliki makna seni dalam menulis pesan rahasia (*The art of secret writing*), dimana kriptografi terdiri dari 2 kata yaitu $\kappa\rho\upsilon\pi\tau o\ \psi\alpha\nu\gamma$ yang berarti *rahasia* atau *tersembunyi* dan $\gamma\rho\alpha\phi\eta$ yang berarti *tulisan* [2].

Ada empat tujuan mendasar dari ilmu kriptograpi ini juga merupakan aspek keamanan informasi yaitu Kerahasiaan adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi. Integritas data adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubtitusian data lain kedalam data yang sebenarnya. Autentikasi adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasiitu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harusdiautentikasi keaslian isi datanya, waktu pengiriman

dan lain-lain. Non-repudiasi atau penyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman / terciptanya suatu informasi oleh yang mengirimkan atau membuat.

Kriptografi memiliki 4 komponen utama yaitu :

1. *Plaintext,* yaitu pesan yang dapat dibaca.
2. *Ciphertext,* yaitu pesan sandi/ pesan acak yang tidak bisa dibaca.
3. *Key,* yaitu kunci untuk melakukan teknik kriptografi.
4. *Algoritma,* yaitu metode untuk melakukan enkripsi dan dekripsi.

Proses–proses dasar kriptografi dibagi menjadi dua bagian, yaitu Enkripsi (*Encryption*) dan Dekripsi (*Decryption*). Adapun contoh Teknik Kriptografi Klasik, yaitu :

1. Subtitusi yaitu teknik ini mengganti satu atau sekumpulan bit pada blok plainteks tanpa mengubah urutannya.
2. Transposisi yaitu teknik ini memindahkan posisi bit pada blok plainteks berdasarkan aturan tertentu.

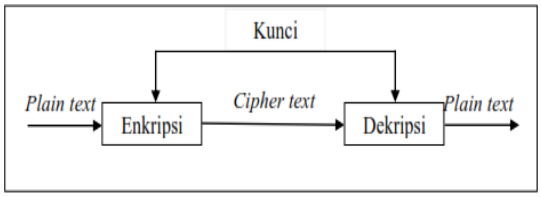
Sedangkan contoh dari Teknik Kriptografi Modern sendiri yaitu :

1. Kriptografi Simetris, yaitu teknik enkripsi dan dekripsi dengan teknik atau metode atau kunci yang sama.
2. Kriptografi Asimetris, yaitu teknik enkripsi dan dekripsi dengan dua kunci yaitu kunci public (*Public key*) dan kunci rahasia (*Private key*).
3. Kriptografi Hibrid, yaitu teknik enkripsi dan dekripsi dua lapis, maksudnya setelah file dienkripsi kemudian dilakukan enkripsi sekali lagi begitu sebaliknya.

1. Algoritma Kriptografi

Algoritma dalam kriptografi dibagi menjadi dua, yaitu:

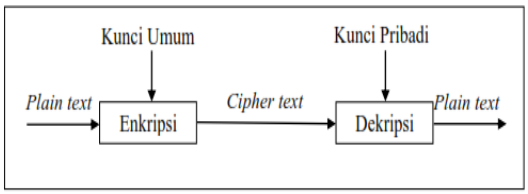
1) Algoritma simetris atau sering disebut algoritma kriptografi konvensional adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses deskripsi. Algoritma kriptografi simetris dibagi menjadi dua kategori yaitu algoritma aliran (*Stream Ciphers*) dan algoritma blok (*Block Ciphers*). Dimana pada algoritma aliran, proses penyandiannya akan beriorientasi pada satu bit/byte data. Sedangkan pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit/*byte* data (per blok). Adapun contoh algoritma kunci simetris adalah *Data Encryption Standard* (DES), Blowfish, Twofish, MARS, *International Data Encryption Algoritm* (IDEA), 3DES (DES diaplikasikan 3 kali), *Advanced Encryption Standard* (AES).



Gambar 1 Proses Enkripsi dan Dekripsi Algoritma Simetris [4].

2) Algoritma asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan deskripsi. Dimana kunci enkripsi dapat disebarkan kepada umum dan dinamakan sebagai kunci publik (*public key*), sedangkan kunci deskripsi disimpan untuk digunakan sendiri dan dinamakan sebagai kunci pribadi (*private key*). Oleh karena itu, kriptografi ini dikenal pula dengan nama kriptografi kunci publik (*public key cryptography*). Adapun contoh algoritma yang menggunakan kunci asimetris adalah *Riverst Shamir Adleman* (RSA) dan *Elliptic Curve Cryptography* (ECC). Adapun pada kriptografi asimetris, dimana setiap pelaku sistem informasi

akan memiliki sepasang kunci, yaitu kunci publik dan kunci pribadi, dimana kunci publik di distribusikan kepada umum, sedangkan kunci pribadi disimpan untuk diri sendiri. Artinya bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca surat tersebut, ia perlu mendeskripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut.



Gambar 2.2 Proses Enkripsi Dan Dekripsi Algoritma Asimetris [4].

2. *Vigenere Cipher*

Vigenère cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1986. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu *Blaise de Vigenère*, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku La Cifra del Sig. Giovan Batista Belaso, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553 [3].

Cara kerja dari *Vigenère cipher* ini mirip dengan Caesar cipher, yaitu mengenkripsi plainteks pada pesan dengan cara menggeser huruf pada pesan tersebut sejauh nilai kunci pada deret alphabet. *Vigenère cipher* adalah salah satu algoritma kriptografi klasik yang menggunakan metode substitusi abjad majemuk. Substitusi abjad-majemuk mengenkripsi setiap huruf yang ada menggunakan kunci yang berbeda, tidak seperti *Caesar cipher* yang menerapkan metode substitusi abjad-tunggal yang semua huruf disuatu pesan dienkripsi menggunakan kunci yang sama.

Sebagai contoh *Caesar cipher* jika terdapat plainteks:

MAKALAH KRIPTOGRAFI

Maka jika dienkripsi dengan dengan nilai kunci 2 akan didapat cipherteks:

OCMCNCJ MTKRVQITCHK

Dari cipherteks yang didapat dapat kita lihat bahwa huruf M dienkripsi menjadi O, huruf A dienkripsi menjadi huruf C, dan seterusnya dimana huruf pada pesan digeser sejauh nilai kunci. Algoritma *Caesar cipher* sangat sederhana sehingga sanga berisiko untuk dipecahkan karena hanya dibutuhkan pengetahuan satu huruf dari plainteks untuk mengetahui kunci yang digunakan. *Vigenère cipher* yang menerapkan metode substitusi abjad-majemuk tidak memiliki permasalahan tersebut karena setiap huruf pada pesan yang dienkripsi dengan *Vigenère cipher* ini akan digeser dengan nilai yang berbeda tergantung dengan kunci yang diberikan. Kunci yang digunakan pada *Vigenère cipher* berbeda denganyang digunakan pada *Caesar cipher*. Jika pada *Caesar cipher* kuncinya hanya satu nilai saja, maka pada *Vigenère cipher* kunci yang digunakan berbentuk deretan huruf. Kunci yang berbetuk deretan kata tersebut akan memungkinkan setiap huruf plainteks untuk dienkripsi dengan kunci yang berbeda. Jika panjang kunci yang digunakan lebih pendek dari panjang *plainteks* maka kunci akan diulang sampai panjang kunci samdengan panjang *plainteks*. Algoritma ini akanmeminimalkan kemungkinan dipecahkannya *cipherteks* jika satu huruf plainteks diketahui. Model matematika dari enkripsi pada algoritma *Vigenère cipher* ini adalah seperti berikut:

Ci= Ek(Mi) = (Mi + Ki) mod 26

Dan model matematika untuk deskripsinya adalah:

Mi= Dk(Ci) = (Ci - Ki) mod 26

Dengan C memodelkan *cipherteks*, M memodelkan *Plainteks*, dan K memodelkan kunci. Contoh dari penerapan algoritma *Vigenère cipher* adalah jika kita memiliki sebuah *plainteks* yang ingin dienkripsi:

MAKALAH KRIPTOGRAFI

Dan kita menggunakan kunci:

TUGAS

Maka plainteks akan dienkripsi dengan cara:

Plaintext : MAKALAH KRIPTOGRAFI

Kunci : TUGASTU GASTUGASTUG

Ciphertext : FUQADTB QRAINUGJTZO

Huruf pada kunci akan dikonversi menjadi sebuah nilai, misalnya A = 0, B = 1, sampai dengan Z = 25. Setelah itu prosesnya sama seperti pada Caesar cipher dimana setiap huruf pada plainteks akan digeser sejauh nilai kunci yang posisinya bersesuaian. Pergeseran huruf-huruf ini bisa dipetakan dalam bentuk tabel 26x26 yang memetakan antara huruf pada plainteks dengan huruf pada kunci seperti yang diperlihatkan pada Gambar 2.1.

	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
S	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

Gambar 2 Tabel Pemetaan *Vigenere Cipher*

Selain menggunakan Algoritma *Vigenere Cipher* bujur sangkar *Vigenere* untuk melakukan algoritma ini dapat dilakukan dengan menjumlahkan *plaintext* dengan kunci kemudian di modulo 26.

Dengan Asumsi a = 0, b = 1, c = 2, ……, z = 25

3. *Software*

Perangkat Lunak (*Software*) adalah serangkaian instruksi yang dipahami oleh perangkat keras pengolahan data atau komputer, sehingga perangkat keras itu dapat melaksanakan pemrosesan data sesuai dengan yang dikehendaki.

Sistem adalah seperangkat elemen-elemen yang terdiri atas manusia, mesin atau alat dan prosedur serta konsep-konsep yang dihimpun menjadi satu guna mencapai tujuan bersama. Secara tradisional, software terbagi menjadi dua katagori dasar yaitu sistem program dan program aplikasi [3].

4. *Flowchart*

Menurut Yakub, (2012:162) Bagan alir *(Flowchart)* adalah bagan yang menggambarkan urutan instruksi proses dan hubungan satu proses dengan proses yang lainnya menggunakan simbol-simbol tertentu. Dalam pengoperasian komputer terutama dalam prosess pengolahan data terdapat beberapa simbol yang disebut *Flowchart.*

B. Alat Bantu Perancangan Sistem

Alat bantu perancangan sistem ini adalah UML (Unified Modelling Language). *Unified Modelling Language (UML)* adalah sebuah bahasa yang telah menjadi standar dalam industri untuk visualisasi, merancang dan mendokumentasikan sistem piranti lunak [1]. UML menawarkan sebuah standar untuk merancang model sebuah sistem. Dengan menggunakan UML kita dapat membuat model untuk semua jenis aplikasi piranti lunak, dimana aplikasi tersebut dapat berjalan pada piranti keras, sistem operasi dan jaringan apapun, serta ditulis dalam bahasa pemrograman apapun. Untuk menguasai UML, sebenarnya cukup dua hal yang harus kita perhatikan :

1. Menguasai pembuatan diagram UML

2. Menguasai langkah-langkah dalam analisa dan pengembangan dengan UML

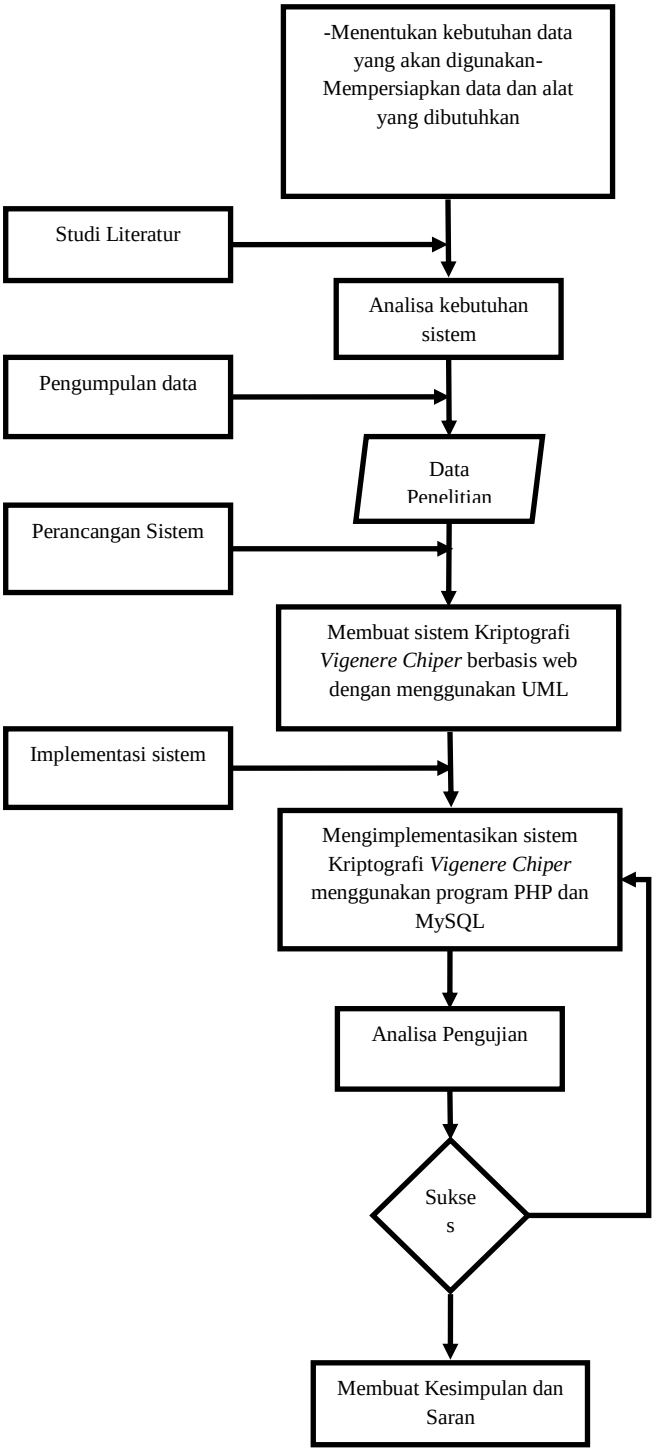
UML menggunakan notasi grafis untuk menyatakan suatu desain. Pemodelan dengan UML berarti menggambarkan yang ada dalam dunia nyata kedalam bentuk yang dapat dipahami dengan menggunakan notasi standart UML. Pemodelan dengan UML terdiri dari 8 tipe diagram yang berbeda untuk memodelkan sistem perangkat lunak. Masing-masing diagram UML didesain untuk menunjukkan satu sisi dari bermacam-macam sudut pandang (perspektif) dan terdiri dari tingkat abstraksi yang berbeda. Ke-8 (delapan) model tersebut adalah :

1. *Use case Diagram*
2. *Class Diagram*
3. *Object Diagram*
4. *State Diagram*
5. *Activity Diagram*
6. *Sequence Diagram*
7. *Collaboration diagram*
8. *Component diagram*
9. *Deployment diagram*

Abstraksi konsep dasar UML yang terdiri dari *structural classification, dynamic behavior,* dan *model management,* bisa kita pahami dengan mudah apabila kita melihat gambar diatas dari diagram. *Main concepts* bisa kita pandang sebagai term yang akan muncul pada saat kita membuat diagram. Dan *view* adalah kategori dari diagram tersebut [1].

III. METODOLOGI PENELITIAN

A. Kerangka Kerja Penelitian



Gambar 3. Kerangka Kerja Penelitian

B. Uraian Kerangka Kerja

Berikut ini adalah uraian dari kerangka kerja penelitian ini :

1. Studi literatur
   Melakukan analisa kebutuhan sistem dengan melakukan survei ke lokasi penelitian dan melakukan wawancara, serta observasi.
2. Pengumpulan data
   Dalam penelitian ini pengumpulan data penulis lakukan melalui :
   a. Jurnal
      Jurnal–jurnal yang penulis jadikan sebagai referensi adalah jurnal yang berkaitan dengan Kriptografi *Vigenere Chiper* berbasis web, dan yang berhubungan dengan judul yang penulis angkat.
   b. Buku yang berhubungan dengan penelitian yang dilakukan Buku yang penulis gunakan sebagai referensi adalah buku yang berkaitan dengan judul yang penulis angkat.
3. Perancangan Sistem
   Dalam penelitian ini perancangan Kriptografi *Vigenere Chiper* berbasis web menggunakan UML *(Unified Modelling Language).*
4. Implementasi Sistem
   Dalam penelitian ini implementasi sistem menggunakan bahasa pemrograman PHP dan MySQL.
5. Melakukan Analisa Pengujian apabila masih terdapat *error (debug)* pada program yang diimplementasikan
6. Kalau tidak ada *error (debug),* maka dilanjutkan dengan membuat kesimpulan dan saran

C. Teknik Pengumpulan Data

Data dikumpulkan dengan menggunakan metode *Deskriptif* dan *Komperatif.* Penelitian ini merupakan penelitian yang dilakukan dengan menggunakan tabel pemetaan *vigenere chiper* dengan memberikan file yang ber-extensi .txt yang dibuat oleh penulis untuk mengetahui bagaimana hasil dari *enkripsi* dan *dekripsi* file yang ber-extensi .txt tersebut.

D. *Metode Penelitian*

Metode penelitian yang akan penulis lakukan yaitu menggunakan metode Deskriptif. Metode deskriptif digunakan untuk mengolah rumus-rumus dari metode kriptografi *vigenere cipher* secara manual dan aplikasi yang dibangun dengan menggunakan bahasa pemrograman PHP.

IV. ANALISA DAN PERANCANGAN

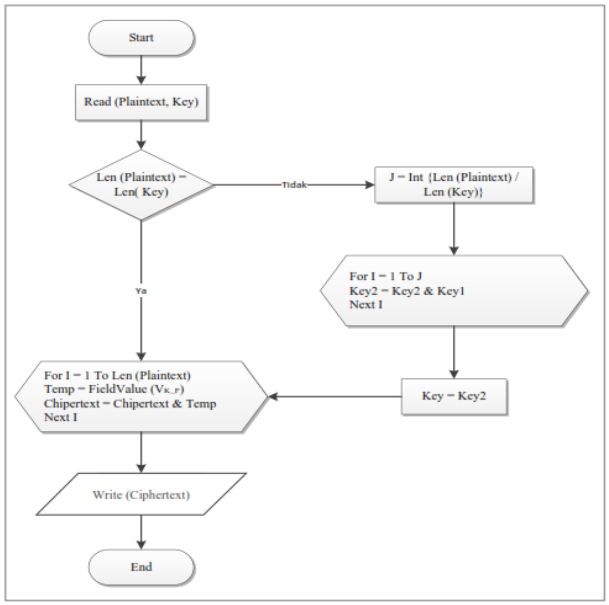
A. Analisa

Analisa sistem sesuai dengan harapan penulis untuk meningkatkan pemahaman pengguna yang ingin belajar kriptografi tentang metode sandi *Vigenère*. Kriptografi saat ini sangat diperlukan agar informasi yang dikirimkan tidak bisa dibaca ataupun disadap oleh orang yang tidak berhak. Oleh karena itu dengan adanya aplikasi kriptografi vigenere cipher dengan PHP, pengguna dapat menambah pemahaman tentang sandi *Vigenère* dan juga dapat menggunakannya untuk mengamankan pesan dari orang yang tidak memiliki hak untuk membacanya.

B. Perancangan

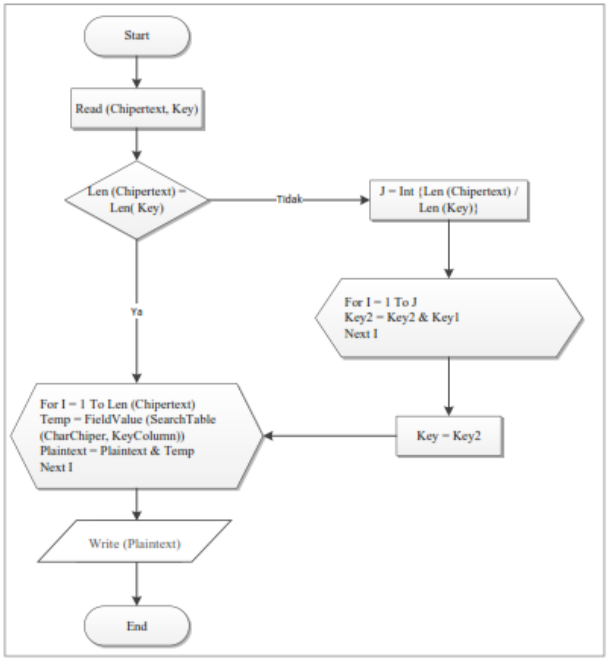
Proses perancangan yang akan digunakan merupakan proses perancangan yang berorientasi pada prosedural, sehingga diperlukan *flowchart* enkripsi, *flowchart* dekripsi, *Use case diagram* aplikasi kriptografi *vigenere cipher*, *activity diagram* aplikasi kriptografi *vigenere cipher, sequence diagram* aplikasi kriptografi *vigenere cipher, flowchart* sistem serta perancangan tampilan. Untuk aplikasi ini, dirancang sistem yang dapat memproses karakter *American*

Standard Code for Information Interchange (ASCII). Berikut ini adalah gambar 3 *flowchart* enkripsi dari metode *vigenere cipher*.



Gambar 4. *Flowchart* Enkripsi *Vigenere Cipher*

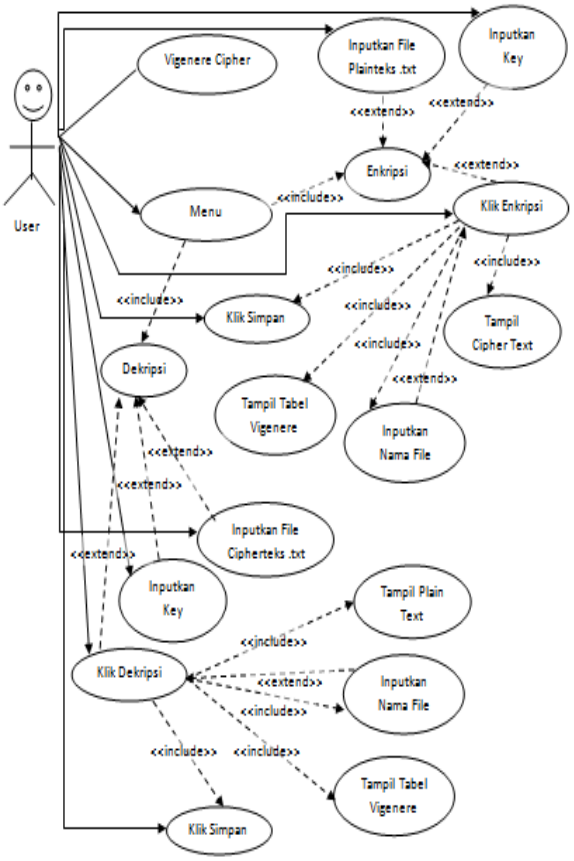
Sedangkan *flowchart* dekripsi *vigenere cipher* dapat dilihat pada gambar 5 berikut ini.



Gambar 5 *Flowchart* Dekripsi *Vigenere Cipher*

C. Use Case Diagram

Seperti yang telah dijelaskan sebelumnya *use case diagram* menggambarkan fungsionalitas yang diharapkan dari sebuah sistem. Pada diagram ini menekankan "apa" yang diperbuat sistem, dan bukan "bagaimana" membuat sistem. Sebuah *use case* merepresentasikan sebuah interaksi antara aktor dengan sistem. Gambar 4.3 memodelkan interaksi antara user dengan sistem kriptografi *vigenere cipher*.



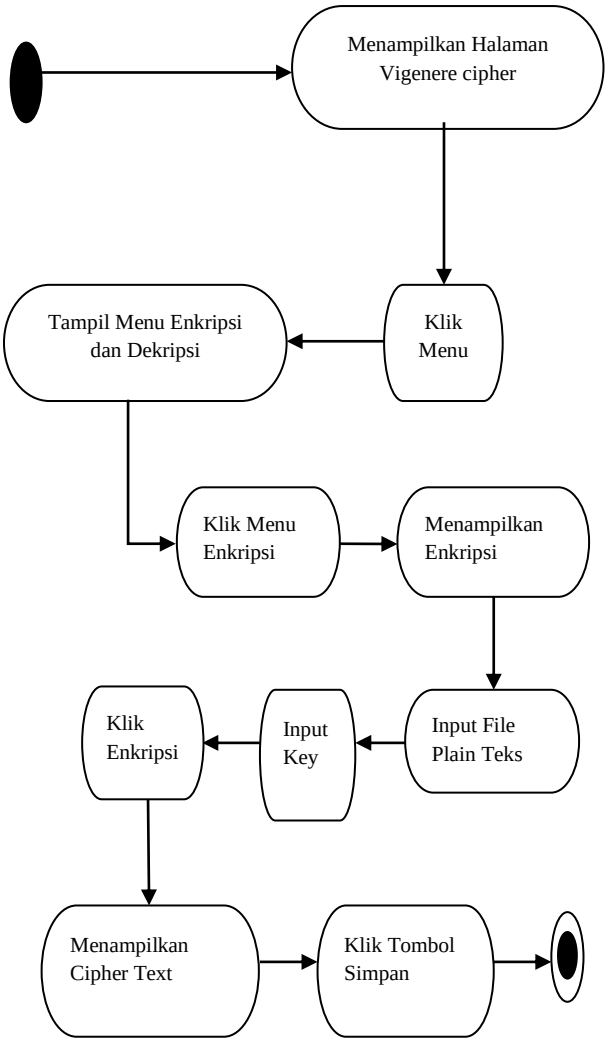
Gambar 6 *Use Case Diagram* Aplikasi Kriptografi *Vigenere Cipher*

Pada aplikasi ini hanya terdapat seorang aktor yang dinamakan *user*. Hanya ada 1 (satu) *user* yang bisa mengoperasikan aplikasi. Terdapat 3 (tiga) menu data yang dapat dilakukan oleh *user*, dengan terlebih dahulu *user* harus memilih menu enkripsi ke aplikasi. Agar dapat memasukkan file *plainteks* yang bertipe .txt serta *key*-nya sehingga di dapatkan pesan

cipherteks-nya. Kemudian pesan *cipherteks* dapat disimpan sebagai file yang bertipe .txt di komputer. Begitu juga dengan dekripsi dari file *cipherteks*-nya. Cara yang dilakukan sama seperti memasukkan file *plainteks* yang bertipe .txt.

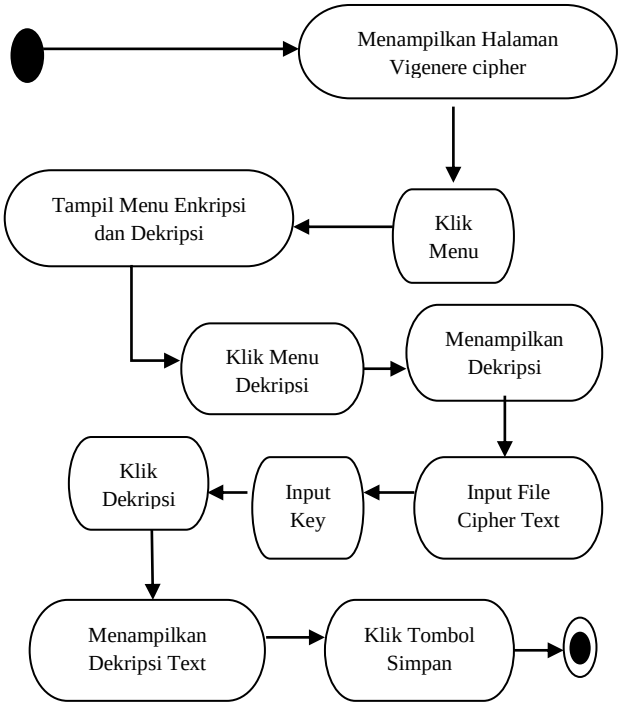
D. Activity Diagram Enkripsi

Berdasarkan *use case* yang telah didefinisikan sebelumnya, dihasilkanlah *Activity Diagram* aplikasi kriptografi teks dengan modifikasi *vigenere cipher* yang dapat dilihat pada Gambar 4.4 dan 4.5.



Gambar 7 *Activity Diagram* Enkripsi

E. Activity Diagram Dekripsi

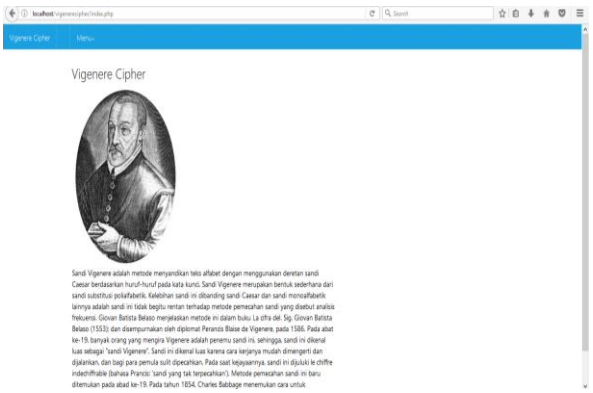


Gambar 8 *Activity Diagram* Dekripsi

V. IMPLEMENTASI SISTEM

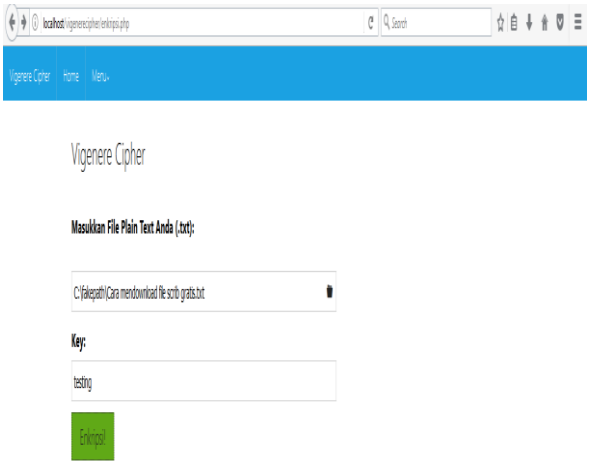
A. Halaman Utama

Halaman ini digunakan sebagai *outer frame* dari seluruh fitur yang dapat digunakan diaplikasi ini. Tampilan halaman utama aplikasi kriptografi teks dengan modifikasi *vigenere cipher* dapat dilihat pada Gambar 9 berikut :



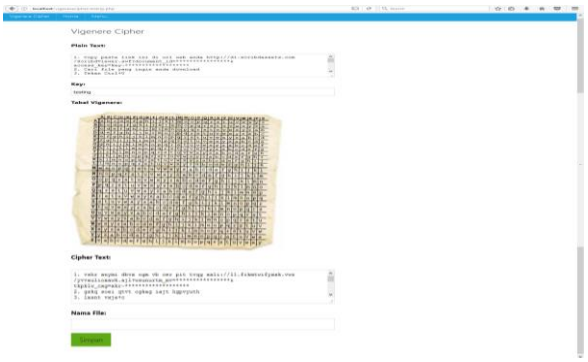
Gambar 9 Halaman Utama Aplikasi Kriptografi *Vigenere Cipher*

B. Halaman Enkripsi



Gambar 10 Halaman Enkripsi Aplikasi Kriptografi *Vigenere Cipher*

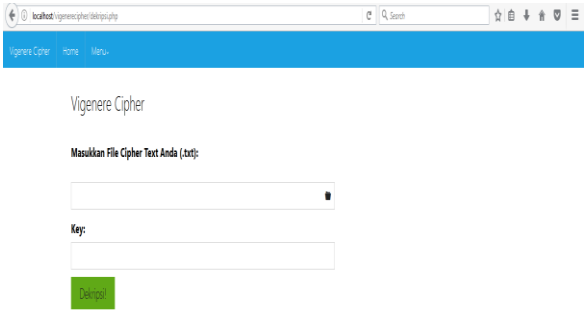
Halaman enkripsi ini akan muncul setelah mengklik menu enkripsi. Kemudian inputkan file *plain text* yang bertipe .txt serta inputkan *key* dalam bentuk teks. Setelah itu klik tombol enkripsi sehingga tampil gambar 11 berikut ini.



Gambar 11 Hasil Enkripsi Dari *Plain Text*

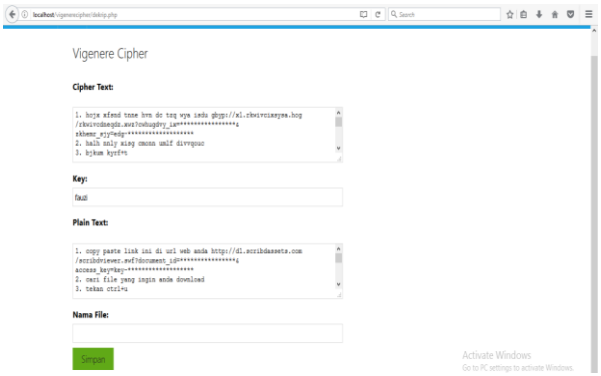
Setelah tampil hasil enkripsi dari *plain text* seperti diatas, maka simpan hasilnya dengan meng-inputkan nama *file* kemudian klik tombol simpan. Sehingga *file* akan disimpan di dalam *folder cipher* yang sudah disiapkan di dalam *folder vigenere cipher*.

C. Halaman Dekripsi



Gambar 12 Halaman Dekripsi Aplikasi Kriptografi *Vigenere Cipher*

Halaman dekripsi ini akan muncul setelah mengklik menu dekripsi. Kemudian inputkan file *cipher text* yang bertipe .txt yang telah disimpan sebelumnya serta inputkan *key* sebelumnya dalam bentuk teks. Setelah itu klik tombol dekripsi sehingga tampil gambar 5.5 berikut ini.



Gambar 13 Hasil Dekripsi Dari *Cipher Text*

Setelah tampil hasil dekripsi dari *cipher text* seperti diatas, maka simpan hasilnya dengan meng-inputkan nama *file* kemudian klik tombol simpan. Sehingga *file* akan disimpan di dalam *folder dekrip* yang sudah disiapkan di dalam *folder vigenere cipher*.

DAFTAR PUSTAKA

[1] Abdul Jabbar, 2011, Pemodelan dan Simulasi Dinamis Pendeteksi Dini Gempa Pada Gedung, *Tesis*, Program Pasca Sarjana Ilmu Komputer, Universitas Putra Indonesia YPTK, Padang.

[2] Apriandala, Rio, 2013, *Sistem Keamanan Menggunakan Rubik Dengan Algoritma Kriptografi Encryption*, Tugas Besar I Makalah Kriptografi, Universitas Bengkulu. 375 Hal.

[3] Efrandi, *et al*, 2014, Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher, *Jurnal Media Infotama*, Vol. 10, No.2, 120 – 128.

[4] *http://www.erdisusanto.com/2012/10/konsep-dasar-kriptografi-simetris-dan.html*, tanggal akses 26 Maret 2015.

[5] Yakub. 2012. *Pengantar Sistem Informasi*. Yogyakarta : Graha Ilmu