BAB II

KAJIAN PUSTAKA

2.1 Teori dasar

Pada Sub Bab ini, Akan diperkenalkan beberapa teori yang dipergunakan dalam penelitian ini, Antara lain Pengantar Jaringan Komputer, UML, Kriptografi, Enkripsi, Deskripsi, *Brute Force, vigenere cipher*, PHP.

2.1.1 Pengantar Jaringan komputer

Dalam konsep sebuah jaringan, ada beberapa komponen pendukung yang ada dan saling terintegrasi, membentuk sebuah kesatuan dimana saling mempengaruhi, sehingga sebuah jaringan tersebut dapat tercipta dan bekerja dengan baik. Beberapa komponen itu dapat dipahami antara lain berupa Standar Jaringan Komputer, Jenis Jaringan Komputer, serta Model OSI Layer didalamnya.

1. Standar Jaringan Komputer

Menurut Indra Riyana didalam jurnalnya mendefinisikan bahwa Jaringan Komputer ialah bagian dari beberapa komputer kemudian dijadikan beberapa alat lalu digabungkan sebagai salah satu standar yang saling terhubung dan menjadi satu kesatuan (Rahadjeng & Puspitasari, 2018). Jaringan Komputer merupakan suatu jaringan komunikasi yang memungkinkan tiap – tiap komputer untuk bisa melakukan rangkaian hubungan jarak jauh berkesempatan agar bisa saling bertukar informasi atau data. Pada jaringan komputer terbagi menjadi dua yaitu

kabel dan nirkabel. Dalam hal jaringan, dikenal juga dengan istilah standarisasi jaringan.

Pada umumnya Jaringan Komputer bisa juga di anggap sebagai *Network Protocols* yaitu sebuah aturan yang dipakai dengan maksud agar sebuah jaringan bisa berfungsi walaupun dengan menggunakan perangkat memakai sumber buatan. Tolak ukur pada sebuah Jaringan Komputer adalah sebuah kelompok sistem yang sudah teruji secara efisien supaya agar bisa menggabungkan ragam pada peralatan keras komputer supaya saling bisa terhubung. Sebelum di sediakan penciptaan standar jaringan utama, tiap *brand* yang membuat komputer menghasilkan standar jaringannya tersendiri, dan hal ini sangat teruji menjadi suatu hal yang mengambat komunikasi pada jaringan saat itu.

Gambar 2.1 Logo ISO

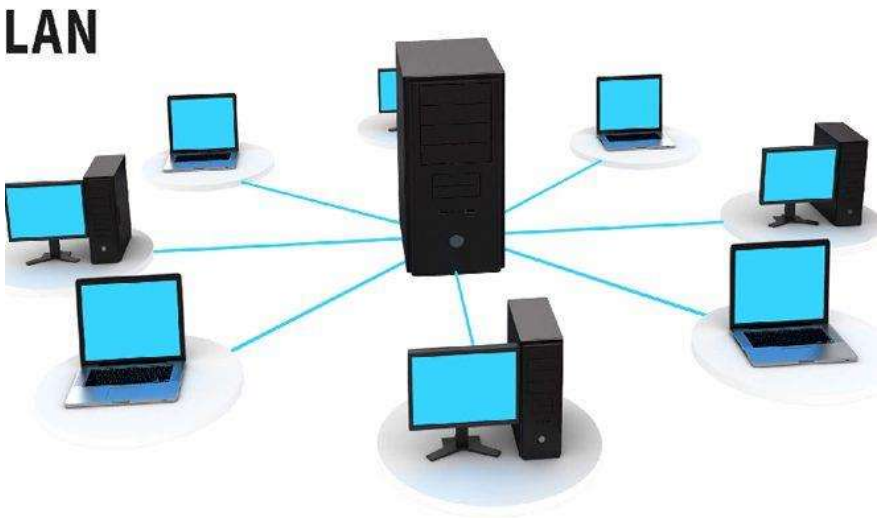
Sumber: Iso.org

Di Dalam sebuah Standar Jaringan Komputer, terdapat dua jenis tipe yang sangat terkenal, berupa TCP/IP (*The Transmission Control Protocol/Internet Protocol*) yang di buat oleh departemen pertahanan Amerika Serikat dan OSI *Reference Model* (7 Lapisan OSI) yang dibuat dari ISO.

2. Jenis Jaringan

Berikut menurut Andi Maslan didalam bukunya ada beberapa jenis bentuk jaringan pada jaringan komputer, antara lain :

A) LAN (*Local Area Network)*



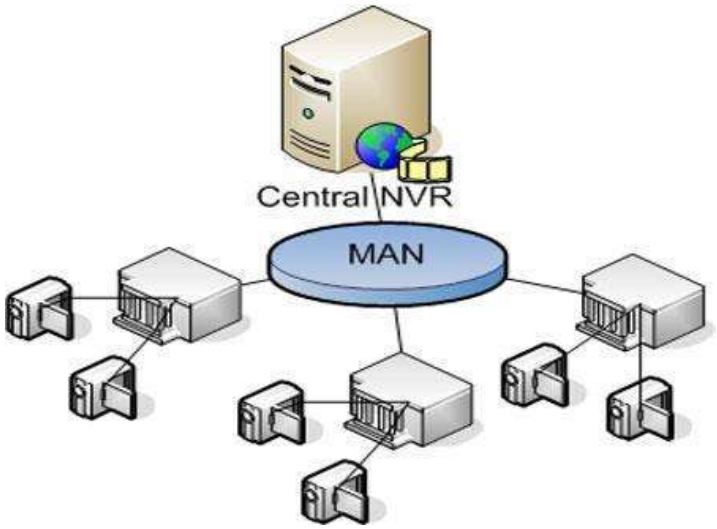
Gambar 2.2 *local Area Network*

Sumber : *pro.co.id*

LAN Ialah sebuah jaringan yang hanya dimiliki oleh individu secara khusus didalam sebuah kampus atau perusahaan yang hanya mencangkup beberapa kilometer.LAN selalu dipakai dalam menyambungkan komputer individu.

B) MAN (*Metropolitan Area Network*)

Ialah tipe LAN dengan jangkauan yang lebih luas, umumnya memakai teknologi yang hampir mirip dengan LAN. MAN memiliki jarak jangkauan pada perusahaan yang letaknya berdekatan serta berguna dalam keperluan sendiri maupun publik.



Gambar 2.3 ilustrasi MAN

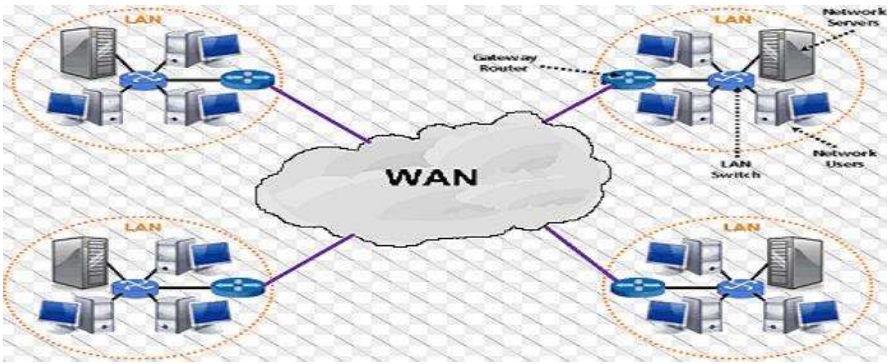
Sumber : *docplayer.info*

C) WAN (*Wide Area Network)*

Merupakan jaringan LAN yang memiliki jarak jangkuan yang sangat luas biasanya antar negara maupun benua. Beberapa jenis teknologi WAN yang memiliki perbedaan intens dengan saudara LAN yang lainnya (maslan, S.Kom. & wangdra, S.Kom., 2012). Pada beberapa aspek seperti berikut :

1) Teknologi yang dibangun yang dikelola oleh beberapa pengelola fasilitas telekomunikasi yang kerap menangani puluhan ribu pelanggan sehingga ukuran komplikasi dapat dengan mudah disesuaikan dengan kebutuhan.
2) Rincian dalam lapisan wujudnya biasanya mempunyai jarak antara 2 sampai 40 mil.
3) Rincian dalam mengartikan berbagai macam kecepatan data, dari 56 Kbps sampai 10 Gbps.

4) Teknologi ini selalu digunakan pada teknik *multipexing,* sebagian membawa beberapa sambungan logika sekaligus melalui jalur wujud yang sama.



Gambar 2.4 ilustrasi WAN

Sumber : *dictio.id*

3. Topologi Jaringan

Topologi ialah salah satu cara dalam mengatur alur sebuah jaringan pada komputer. Adapun jenis topologi jaringan menurut made santo didalam bukunya yang sering digunakan dalam perusahaan maupun umum adalah sebagai berikut :

A) Topologi Bus

Topologi ini menggabungkan seluruh komputer yang terhubung di jaringan harus mengkoneksikan dirinya pada kabel utama sebagai lalu lintas data. Di dalam topologi bus mempunyai titik yang saling menyambungkan pada sepanjang kabel kemudian menggabungkan ujung kabel dengan penutupnya, sangat mudah dalam pemasangan karena Cuma menyambungkan antara simpul saja. Beserta sangat murah dalam pembiayaannya. Pengantar data saling bersinggungan pada sebuah kabel maka jika titik yang digabungkan semakin banyak maka kinerja jaringan tentu akan sangat menurun, disebabkan sering terjadinya tabrakan.

B) Topologi Star

Topologi yang berupa seperti bintang secara keseluruhan komputer saling terhubung pada sebuah alat penghubung tunggal (consentrator). Pada topologi star pada setiap titik pengiriman data yang akan melalui jalur tunggal yang kemudian akan dikirimkan pada titik yang terhubung (contohnya menggunakan 32 port), sehingga akan membuat kemampuan jaringan akan semakin lama. Mudah jika ingin mengembangkan, karena setiap titik akan terhubung secara langsung ke consentrator. Apabila ada salah satu kabel yang terputus, maka seluruh jaringan akan tetap bisa berkomunikasi tanpa menyebabkan down pada jaringan secara keseluruhan, beserta tipe kabel yang digunakan ialah jenis UTP.

C) Topologi Ring

Topologi akan terhubung dengan menggunakan komputer disebelahnya sehingga akan membantuk seperti lingkaran. Dalam topologi ini titik – titik yang akan dihubungkan secara berurutan pada tiap – tiap kabel yang akan menghasilkan bentuk jaringan seperti lingkaran. Cukup sederhana dalam pemasangan karena mirip dengan topologi bus. Pada saat pengiriman paket akan dikirimkan melalui jalur 2 arah bisa dari kiri atau dari kanan maka akan membuat tabrakan pada saat pengiriman data dapat dihindarkan. Masalahnya adalah sama dengan Topologi bus, jika salah satu titik mengalami kerusakan akan membuat semua komputer tidak bisa berkomunikasi pada jaringan tersebut. Tipe kabel yang digunakan toplogi Ring ini sama dengan topologi Star.

D) Topologi Mesh

Ialah topologi yang memungkinkan semua titik saling terhubung secara langsung dengan yang lainnya pada sebuah jaringan. Banyaknya jumlah pada jalur harus dipersiapkan dalam membentuk topologi mesh ialah jumlah yang dipusatkan dikurangi 1 (n-1, n = jumlah sentral). pada topologi mesh mempunyai keterikatan yang sangat kuat dengan peralatan yang ada, penyusunannya di tiap peralatan yang sudah ada didalamnya terdapat jaringan yang saling terkoneksi antara yang satu dengan yang lainnya. Di Dalam jumlah perangkat yang sedang terhubung sangat banyak, akibatnya akan sangat sulit untuk diatur bila dibandingkan dengan hanya sedikit perangkat saja yang terhubung (gitakarma, S.T. & ariawan,S., 2014).

E) Topologi Hybrid

Merupakan topologi jaringan klien-server karena dimana jaringan terdapat banyak server yang dibutuhkan oleh pengguna. Akan tetapi pengguna juga dapat melihat serta mengakses data – data yang telah disediakan oleh pengguna yang lain, yang bisa diakses melalui satu jaringan yang sama. Topologi ini bisa meliputi berbagi koneksi antara printer, berbagi file serta menghubungkan koneksi ke internet.

2.1.2 UML

Dalam dunia pemrograman, dikenal istilah pemrograman terstruktur dan pemrograman berbasis objek (OOP). Dalam keberadaannya, terstruktur lebih kepada pemrograman untuk proses belajar dan mengenali pemrograman (karena lebih kepada belajar tentang algoritma). Akan tetapi, untuk pemrograman OOP

lebih kepada pembuatan program yang ditujukan untuk pembuatan aplikasi siap pakai. Namun, apapun program maupun aplikasi yang dibuat, tiap programmer memiliki pilihan kesukaannya tersendiri yang dipakai untuk tujuan memodelkan sistemnya. Salah satu sistem pemodelan yang ada disebut dengan *Unified Modeling Language* (UML). Menurut Kurniawan dalam jurnalnya memaparkan bahwa UML merupakan bahasa untuk pemodelan standar dan digunakan untuk memberikan gambaran terkait perencanaan pengembangan atas sebuah sistem yang akan dibangun (Kurniawan, 2018).

Gambar 2.5 Logo UML

Sumber gambar: *product.microsoft.com*

Dalam UML, ada beberapa bentuk diagram yang bisa dipergunakan untuk merepresentasikan/memberikan gambaran dari sebuah system. Beberapa diagram yang biasa dipergunakan adalah *Use Case*, *Class* diagram, dan *Sequence* diagram. Berikut penjelasan dari beberapa jenis diagram di UML tersebut.

1. *Use Case Diagram*

Use case diagram salah satu bentuk yang ekslusif untuk membuat langkah – langkah melalui sistem informasi yang akan dikerjakan. Pada *Use case* diagram bakal memaparkan hubungan antara satu orang pelaku dengan sebagian pelaku

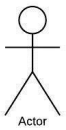
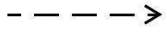
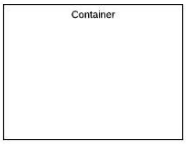
lainnya. Ada 2 kondisi mendasar dalam *use case* yaitu mendeskripsikan pada pemain dan pengertian mengenai *use case.*

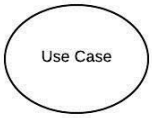
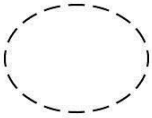
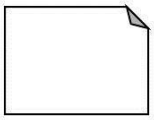
A) pelaku sebagai orang, prosedur ataupun proses yang berhubungan pada aturan yang bakal dikerjakan.

B) *Use case* ialah kegunaan yang telah disediakan dari sistem.

Selanjutnya simbol-simbol pada sistem yang ada di dalam use case diagram.

Tabel 2.1 bagian - bagian dalam *Use Case* Diagram

No	Gambar	Nama	Keterangan
1		Pelaku	Menerangkan/menjabarkan objek maupun yang termasuk pada sebuah system
2		Keterikatan	Korelasi terhadap transisi yang terdiri dari perubahan pada elemen yang terikat serta mempengaruhi elemen yang tidak terikat
3		Generalisasi	Rangkaian tentang sasaran dari bawah mempunyai sifat dan struktur data dari entitas induk
4		*Include*	Menjelaskan awal mula *use case* secara jelas
5		memperpanjang	Bermakna jika *use case* bertujuan meneruskan sifat dari *use case* berawal kepada satu titik khusus.
6		Asosiasi	Mengilustrasikan korelasi antara objek.
7		Sistem	rencananya pengiriman yang menunjuk pada saat sistem sebagai kontribusi secara tertentu.

8		*Use Case*	penjabaran pada serangkaian aktivitas yang terlihat pada suatu aturan yang akan menjadikan sebuah *output* yang bernilai.
9		kolaborasi	Keterkaitan antara metode - metode dengan bagian lain yang saling bekerja sama dalam memfasilitasi perilaku yang semakin kuat pada nilai dan bagian – bagian lainnya (sinergi).
10		Catatan	Bagian yang bersifat nyata yang terkenal pada saat aplikasi diproses serta menggambarkan suatu hasil dari komputer

Sumber tabel: Data Peneliti (2019)

2. *Class Diagram*

Class diagram merepresentasikan desain sistem pada aspek dalam menjelaskan kelas-kelas yang bakal dibuat di dalam suatu sistem. Diagram kelas dikerjakan supaya programmer menjadikan kelas-kelas sesuai yang direncanakan yang sudah ada di dalam diagram kelas supaya antar dokumentasi serta implementasi dalam pembuatan sistem terdapat kesamaan. Urutan pada diagram kelas yang efektif ialah diagram kelas seharusnya mempunyai kategori kelas sebagai berikut.

A) Kelas main

Kelas yang mempunyai kegunaan awal pada saat sistem dijalankan.

B) Kelas view

Kelas yang mengerjakan bentuk desain yang akan digunakan oleh pemakai sistem.

C) Kelas controller

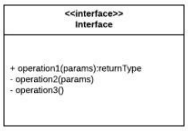
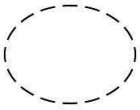
Kelas yang memproses peranan - peranan yang harus siap dipakai dari penjelasan *use case*.

D) Kelas *model*

Kelas yang akan dipakai dalam menyimpan atau mempesatukan data supaya menjadi satu kesatuan yang utuh atau mengarsipkan di dalam database.

Selanjutnya ada simbol-simbol yang ad pada diagram kelas.

Tabel 2.2 Elemen dalam *Class* Diagram

No	Gambar	Nama	Keterangan
1		Generaslisasi	Korelasi dimana pada saat objek keturunan berbagi perilaku dengan metode data pada objek yang terdapat di atasnya objek yang sudah ada lebih dahulu.
2		Asosiasi nary	Cara supaya dapat menghindari ikatan yang melebihi dari jenis 2 objek.
3		Kelas	kumpulan dari beberapa objek-objek yang saling berbagi sifat serta proses yang sama.
4		Colaborasi	Deskripsi ialah urutan dari tindakan yang muncul pada sistem yang peroleh bila suatu hasil yang terukur bagi suatu aktor
5		Realisasi	aktivitas yang akan benar-benar dilakukan oleh suatu objek.
6		Ketergantungan	keterikatan dimana saat perubahan yang terjadi pada suatu komponen mandiri akan membuat suatu konsekuensi

			komponen yang saling bergantung pada yang lain atau elemen yang tidak mandiri
7	———————	asosiasi	Yang menyatukan antar objek satu beserta objek lainnya

Sumber tabel: Data Peneliti (2019)

3. *Activity Diagram*

Diagram aktivitas yang dipakai dalam membuat jalur kegiatan atau pekerjaan pada sebuah sistem atau proses usaha ataupun jadwal yang ada di dalam perangkat lunak. Pusat pada diagram aktivitas ini ialah aktivitas pada suatu metode yang ada bukan pada aktivitas dari peram aktor yang diperoleh dalam sistem. Diagram aktivitas sering dipakai dalam menjelaskan faktor - faktor sebagai berikut.

A) perancangan pada saat suatu proses bisnis yang terpakai dimana setiap aktivitas bisnis yang diperkirakan ialah proses bisnis pada sistem yang dirumuskan.

B) kumpulan pada tampilan dari sistem interface dimana pada setiap aktivitas yang telah terjadi memiliki tampilan sendiri.

C) skema pengetesan dimana pada setiap aktivitas dianggap membutuhkan sebuah pengetesan yang butuh dijelaskan kasus pengujiannya.

D) skema menu yang akan ditampilkan pada *software*.

selanjutnya ialah metode - metode yang terdapat pada sebuah diagram aktivitas.

Tabel 2.3 Elemen dalam *Activity* Diagram

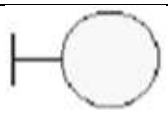
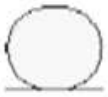
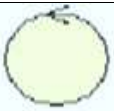
No	Gambar	Nama	Keterangan
1		Aktivitas	Menunjukkan betapa tiap kelas berinteraksi secara antarmuka satu sama lain
2		Tindakan	*State* pada sistem yang menggambarkan keputusan dalam suatu aksi
3		Node awal	Suatu titik objek untuk awal permulaan
4		Aktivitas final	Suatu akhiran pada tahapan objek
5		*Fork Node*	Merupakan suatu aliran yang pada tahapan tertentu yang akan terbagi menjadi beberapa aliran

Sumber tabel: Data Peneliti (2019)

4. *Sequence Diagram*

Sequence diagram yang menjelaskan tentang kerja sama dinamis antar beberapa objek. Berguna dalam menunjukkan kumpulan pesan yang disebarkan antara objek serta hubungan antar objek. Entitas yang terdiri pada suatu titik tertentu saat pengeksekusian sistem. Kuantitas diagram *sequence* yang wajib digambar sama dengan minimal sejumlah penjabaran *use case* yang mempunyai suatu proses individu atau yang paling utama ialah semua *use case* yang sudah di rumuskan korelasi disaat jalannya pesan sudah sangat cukup pada diagram *sequence* sehingga yang seharus di buat juga semakin banyak. bagian – bagian yang dimiliki oleh Squence diagram adalah sebagai berikut.

Tabel 2.4 Elemen dalam *Sequence* Diagram

No	Gambar	Nama	Keterangan
1		Admin	Interface yang saling berinteraksi dengan yang lain
2		Batas	Sistem yang menggambarkan suatu keputusan
3		Kesatuan	Suatu permulaan objek
4		*Lifeline*	Suatu objek yang dibuat dan bisa dihapus
5		*Fork Node*	Suatu tahapan khusus yang terbagi menjadi beberapa bagian

Sumber tabel: Data Peneliti (2019)

2.1.3 Kriptografi

Berdasarkan kutipan yang telah disampaikan oleh Rifki Sadikin dalam Bukunya yang berjudul "Kriptografi untuk Keamanan Jaringan", Kriptografi menjelaskan tentang pengetahuan bagaimana cara menyembunyikan pesan. Sedangkan didalam pemahaman modern, Kriptografi dikenal sebagai pengetahuan yang mengarahkan kepada teknik matematika dengan tujuan pengamanan informasi berupa kerahasiaan. Kelengkapan dan kemananan yang unik. Bahwa penjelasan kriptografi modern ialah bukan hanya beruhubungan saja sebagai menutupi pesan akan tetapi makin atas kelompok proses untuk mempersiapkan kententraman data (Sadikin, 2012).

Selanjutnya definisi dari kriptografi menurut Angga AP Dan Desi dalam jurnal penelitiannya yang berjudul "Rancangan Aplikasi Pengamanan Data

Dengan Algoritma *Advanced Enciptyon Standard (AES)*", Kriptografi sebenarnya merupakan gambaran pengetahuan sekaligus dengan keterampilan dalam menjaga sebuah kerahasiaan pesan. Kriptografi juga dapat dipahami sebagai pengetahuan mengenai metode-metode ilmu hitung yang berkenaan pada bagian keamanan informasi seperti kerahasiaan, karakter data, dan verifikasi (Nurnaningsih & Permana, 2018).

Berdasarkan dari dua kutipan jurnal diatas, Dapat disimpulkan bahwa kriptografi adalah ilmu yang mempelajari teknik-teknik perhitungan yang berhubungan dengan aspek keamanan informasi yang bersumber dari zaman tradisional hingga modern. Di zaman peperangan romawi kuno, informasi bocor maka sama dengan ribuan nyawa akan melayang.

Sering kali pengirim pesan di masa itu masih mengandalkan tenaga kurir yang berlari/menunggangi kuda, sehingga masih mudah untuk ditangkap dan dicuri informasinya. Sehingga kaisar Julius *Caesar* menemukan teknik kriptografi klasik pertama kali, dan dengan seni menyembunyikan informasinya, pihak musuh tidak serta-merta dapat mengetahui rencananya meski sang pembawa pesan ditangkap dan suratnya dibaca sekalipun oleh pihak musuh.

2.1.4 Enkripsi

Enkripsi Menurut Kurniawan Y yang dikutip oleh M. Miftahul Amin dalam jurnalnya memaparkan bahwa enkripsi merupakan sesuatu yang melambangkan kondisi dimana ada sebuah perubahan kode dan sejenisnya yang masih bisa dibaca, diubah agar tidak lagi mudah untuk dibaca. Proses pada mengubah kode agar tidak bisa dibaca (*ciphertext)* menjadi bisa dibaca kembali (*plaintext)* disebut

dengan dekripsi (Amin, 2016). Seringkali pada saat bertukar pesan kedua pihak mengabaikan fakta bahwa pesan yang dikirim atau diterimanya dapat dengan mudah bocor dan diketahui oleh pihak yang tidak berwenang, sehingga enkripsi yang terjadi dipihak pengirim akan meminimalisir kebocoran pesan yang dikirimkan.

Selanjutnya menurut Muhammad Yasin S, Enkripsi merupakan suatu metode untuk melaksanakan pertukaran sandi yang masih mudah dipahami menjadi suatu sandi yang tidak lagi bisa dipahami (Simargolang, 2017). Terkadang yang terjadi pada dunia nyata saat melakukan pertukaran pesan sering terjadi kejadian bahwa pesan yang dikirimkan sangat mudah diketahui oleh pihak yang tidak seharusnya mendapatkan informasi tersebut, sehingga diberilah enkripsi. Dan walaupun kejadian ini terjadi, jika sebelumnya sudah dienkripsi dan pihak lain tidak tahu cara membukanya, kemungkinan kebocoran data dapat diminimalisir.

Maka dapat disimpulkan dari dua sumber referensi diatas bahwa Enkripsi merupakan sesuatu yang melambangkan kondisi dimana ada sebuah perubahan kode dan sejenisnya yang kemudian dikonversi menjadi suatu sandi yang tidak bisa dipahami. Hal ini merupakan proses pertama dalam kriptografi, karena proses ini hanya mengubah *plaintext* menjadi *chipertext*. Adapun proses lanjutannya disebut dengan Dekripsi dan dijelaskan pada bagian selanjutnya.

2.1.5 Dekripsi

M. Azman M dan Nyoman PS memaparkan didalam jurnalnya “Efektivitas Pesan Teks dengan *Cipher* Substitusi, *Vigenere Cipher*, dan *Cipher* Transposisi”,

bahwa Dekripsi merupakan sebuah metode ataupun teknik konversi untuk sebuah pertukaran pesan yang mulanya tidak bisa dipahami (karena berbentuk *ciphertext*) dan kemudian dapat dibaca kembali dengan menggunakan petunjuk khusus (Maricar & Sastra, 2018). Ada banyak metode dalam dekripsi sebuah pesan yang terenkripsi, dan itu semua berasarkan pada algoritma dasarnya. Akan tetapi, keberadaan dari dekripsi merupakan hal penting karena jika sebuah pesan yang sudah terenkripsi sampai pada pihak yang menerimanya namun tidak bisa diubah kembali untuk menjadi pesan yang dapat dimengerti, maka tugas dan fungsi sebuah kriptografi dikatakan gagal karena tidak dapat menuntaskan/memenuhi tujuan dasarnya.

Selanjutnya berdasarkan penjelasan Nirla Laila Dan Anita Sindar RMS didalam jurnal mereka yang berjudul "Implementasi Steganografi LSB Dengan Enkripsi *Vigenere Cipher* Pada Citra", Menjelaskan bahwa deskripsi ialah transisi huruf ataupun kalimat yang tidak bisa dimengerti (*ciphertext*) kemudian menjadi boleh dibaca kembali (*plaintext*) (Laila & Rms, 2018). Sebaliknya yang sering terjadi pengirim tidak mengetahui bagaimana cara agar pesan yang dikirimkannya tidak mudah dimengerti oleh orang lain yang tidak seharusnya tau, oleh karena itu dilakukanlah dengan cara mendeskripsikan isi pesan agar penerima dengan mudah bisa membacanya kembali dengan menggunakan aturan yang telah disepakati bersama.

Dari penjelasan diatas bisa disimpulkan bahwa deskripsi merupakan proses pengubahan kembali dari pesan yang mulanya tiada boleh dimengerti (*ciphertext*)

kemudian ditransisi menjadi (*plaintext*) sehingga boleh dibaca oleh penerima yang seharusnya menerima pesan tersebut.

2.1.6 Brute Force

Sebagaimana yang dijelaskan oleh Indra Gunawan didalam jurnalnya *Brute force* merupakan aturan untuk melakukan pemecahan kode dengan memposisikan serta mencari segala kemungkinan dengan memakai panjang kode dan karakter spesifik. dan dikombinasikan dengan beragam kode yang digunakan. Dengan begitu *bruce force* ialah penyerangan yang menggunakan penjebolan menggunakan berbagai kemungkinan password hingga menemukan password yang tepat (Gunawan, Sumarno, Tambunan, & Irawan, 2018).

Berikutnya *Brute Force* yang dijelaskan oleh Amin Siddiq Sumi dengan Purnawansyah beserta dengan yang lain. *Brute Force* dapat diartikan sebagai suatu strategi tepat dalam menyelesaikan sebuah masalah kebanyakan ditemui dari latar permasalahan dan penjelasan motif yang dilibatkan. *Brute force* mengatasi masalah dengan sangat simpel, tepat dan sangat jelas. *Brute Force* umumnya biasa disebut teknik *hacking* dalam sebuah server yang menjaga jaringan atau website ekslusif. *Brute Froce* sendiri merupakan salah satu teknik *hacking* dalam meretas suatu *password* pada server.

Dari penjelasan diatas bisa disimpulkan bahwa *Brute Force* itu sendiri ialah aturan untuk melakukan pemecahan kode dengan memposisikan serta mencari segala kemungkinan dengan mencari latar permasalahan dan penjelasan motif yang dilibatkan. *Brute Force* sendiri merupakan sebuah teknik *hacking* dalam meretas suatu *password* (atau bisa juga kombinasi tertentu).

2.1.7 Jenis Algoritma dalam Kriptografi

1. Vigenere Cipher

Berdasarkan apa yang dijabarkan oleh Angga Aditya Permana, *Vignere cipher* dapat dipahami sebagai suatu algoritma yang memproses melaksanakan kode memakai indeks diagram mengunakaan abjad secara berurutan (Permana, 2018). Ada beberapa algoritma kriptografi yang tersebar dan dapat digunakan, salah satunya adalah *vignere cipher* yang juga dipilih untuk diimplementasikan dalam penelitian ini. *Vignere cipher* memanfaatkan sebuah diagram yang berisi distribusi huruf dan pemakaiannya sesuai dengan baris yang disediakan. Adapun diagram *vignere* dapat dilihat pada gambar 2.6 berikut.

	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 2.6 Tabel Distribusi *Vigenere Cipher*

Sumber : data penelitian (2019)

Pada gambar diatas dapat dijelaskan sebagai contoh, pertama-tama akan dipilihlah *plaintext*nya berupa kalimat asli yang belum diubah, kemudian dilakukanlah subtitusi (pergeseran huruf) terhadap *plaintext* tersebut. Syarat substitusi dapat dilakukan yaitu memiliki sebuah basis geser, yaitu memilih letak

dari patokan posisi penggeser posisi alphabet asli ke posisi abjad baru (dari A-Z menjadi E-D, lihat gambar 2.6) Kemudian pada simulasi dalam melakukan enkripsi yaitu diawali dengan memasukan *plaintext* yang ingin di enkripsi lalu lakukan pergeseran huruf sesuai basis geser yang diinginkan, adapun pedoman melakukannya ada pada Gambar 2.6 sebelumnya. Peneliti akan memilih contoh kalimat berupa UNIVERSITAS PUTERA BATAM sebagai *Plaintext* lalu urutan E sebagai basis gesernya untuk melakukan enkripsi *vigenere.* Lihat gambar berikut ini untuk memahami posisi perubahan baru dari abjad A-Z normal menjadi E-D sebagai urutan barunya.

Gambar 2.7 basis geser yang dipilih

Sumber : Data penelitian (2019)

Cara memakai tabel *Vigenere Cipher* :

A) Lakukan pergeseran huruf yang di inginkan, tapi sebelum itu untuk mempermudah prosesnya, sisipkan disetiap bawah huruf dengan bilangan angka yang mewakilinya, misalnya A = 1, B = 2 dan seterusnya.

B) Masukan *plaintext* yang akan di enkripsi UNIVERSITAS PUTERA BATAM

C) Lalu lakukan pergeseran plaintext sebelumnya hingga selesai dengan basis geser barunya.

D) Ubah hasil dari subtitusi geser tadi menjadi angka yang mewakili dari posisi hurufnya.

E) Setelah itu enkripsikan secara vignere menggunakan kunci yang sudah dibuat (kunci yang dipilih berupa SAYA).

F) Setelah mendapatkan hasilnya, lakukan penjumlahan antara plaintext tersubtitusi tadi dengan angka pada kunci tersebut (UNIVERSITAS PUTERA BATAM vs SAYA).

E	F	G	H	I	J	K	L	M	N	O	P	Q
4	5	6	7	8	9	10	11	12	13	14	15	16

R	S	T	U	V	W	X	Y	Z	A	B	C	D
17	18	19	20	21	22	23	24	25	0	1	2	3

Gambar 2.8 Subtitusi baru dari A-Z ke E-D beserta angka yang mewakilinya

Sumber : data penelitian (2019)

Maka, apabila dijabarkan, langkahnya sebagai berikut.

Plaintext : UNIVERSITAS PUTERA BATAM
Ciphertext 1: YRMZIVWMXEW TYXIVE FEXEQ

Vigenere Cipher
Ciphertext 1: YRMZIVWMXEW TYXIVE FEXEQ
Key : SAYASAYASAY ASAYAS AYASA
Ciphertext 2 : QRKZAVUMPEU TQXGVW FCXWQ

Proses Enkripsi

Plaintext	20	13	8	21	4	17	18	8	19	0	18	15	20	19	4	17	0	1	0	19	0	12
Key	18	0	24	0	18	0	24	0	18	0	24	18	0	24	0	18	0	24	0	18	0	24
Hasil	38	13	32	21	22	17	42	8	37	0	42	33	20	43	4	35	0	25	0	37	0	36
Ciphertext	N	N	G	V	W	R	R	I	M	A	R	I	U	S	E	K	A	Z	A	M	A	L

Proses Dekripsi

Ciphertext	38	13	32	21	22	17	42	8	37	0	42	33	20	43	4	35	0	25	0	37	0	36
Key	18	0	24	0	18	0	24	0	18	0	24	18	0	24	0	18	0	24	0	18	0	24
Hasil	20	13	8	21	4	17	18	8	19	0	18	15	20	19	4	17	0	1	0	19	0	12
Plaintext	U	N	I	V	E	R	S	I	T	A	S	P	U	T	E	R	A	B	A	T	A	M

Gambar 2.9 proses Enkripsi dan Deskripsi

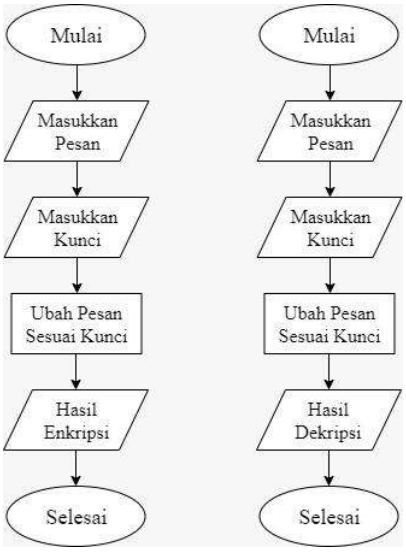
Sumber : Data penelitian (2019)

Pada saat mengenkripsi kita akan mencari hasil dari angka yang kemudian diubah menjadi huruf,dengan catatan *Plaintextnya* ditambah dengan *key*, setelah itu kita akan mendapatkan hasilnya berupa angka yang akan diganti menjadi huruf berdasarkan **Gambar 2.9** tetapi jika hasil dari enkripsi melebihi dari angka abjad 25 maka akan dimulai dari huruf A dengan aturan angkanya tetap dihitung lebih dari 25, contohnya 38 sama dengan huruf M tetapi yang akan ditulis berupa angka bukan huruf.

Sebaliknya jika kita akan mendekripsikan *Ciphertext* yang akan menjadi *Plaintext*nya, kita akan mengurangi angka dari *Plaintext* dengan *key*, yang kemudian mendapatkan hasil yang akan diubah menjadi sebuah *Plaintext*nya. Kriptografi klasik yang tidak menggunakan kode ASCII pada dasar pembentuknya akan ditemui kondisi dimana hasil melebihi jumlah pada abjad. Pada teks sebelumnya ialah (UNIVERSITTAS PUTERA BATAM) maka setelah di enkripsi menjadi (YRMZIVWMXEW TYXIVE FEXEQ).

Kemudian, Berdasarkan pemaparan yang ditulis oleh Muhammad Anas Fauzi didalam jurnalnya “Perancangan Aplikasi Keamanan Pesan Teks dengan menggunakan Algoritma *Triple Transposition Vigenere Cipher*”, Menjelaskan *vigenere cipher* atas penggunaan panduan persegi panjang guna membuat sebuah kode (Fauzi, 2019). Dapat diketahui juga bahwa *vignere cipher* secara mendasar merupakan sebuah algoritma kriptografi yang memanfaatkan sebuah tabel distribusi untuk melakukan enkripsinya. Namun tidak berhenti sampai disitu, dibutuhkan sebuah kunci unik yang dipersiapkan oleh pengirim pesan yang juga diketahui oleh penerima pesan agar nantinya ketika sudah sampai, kedua belah

pihak bisa memanfaatkan *vignere cipher* dengan menyamakan kunci itu yang dipergunakan pengirim sebagai alat enkripsinya (dari *plaintext*) maupun penerima sebagai alat dekripsinya (dari *ciphertext*). konsep dasar dari algoritma *Vignere* dapat dilihat pada *flowchart* dibawah ini.



Gambar 2.10 *Flowchart Vigenere Cipher*

Sumber : data penelitian (2019)

Sesuai dengan simulasi sebelumnya, pada *flowchar*t keduanya diawali dengan mempersiapkan pesan yang akan diubah, baik itu yang sudah terenkripsi maupun ingin di dekripsi. Kemudian dengan memanfaatkan sebuah program krpiptografi *vignere* yang dijalankan, pengguna dapat memasukkan pesan yang sudah diterima/dipersiapkannya. Selanjutnya, dengan mengetahui kuinci yang benar, maka pesan *plaintext* tadi akan dikonversi berdasarkan diagram distribusi *Vignere cipher*, sehingga akan keluar hasil pesan yang diinginkan.

Jika yang dimasukkan itu sebuah pesan terenkripsi, maka hasilnya adalah pesan yang dapat dibaca kembali. Begitu juga sebaliknya. Dan itu adalah konsep

kerja dari *vignere cipher*. Dan *vignere cipher* dapat disimpulkan sebagai sebuah metode enkripsi berbasis diagram distribusi yang dimana kuncinya akan dicocokkan dengan diagram tersebut, dan menghasilkan sebuah teks terenkripsi maupun terdekripsi.

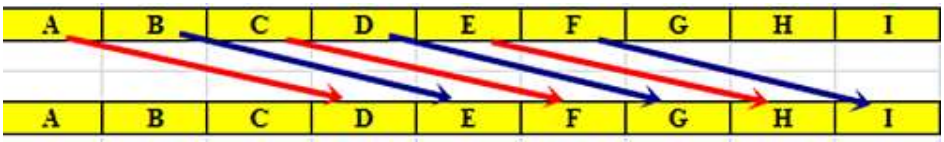
2. Caesar Cipher

Caesar cipher menurut Agustin Siburian dan Andi Paul Harianja di dalam jurnalnya "Perancangan Aplikasi Pengamanan Basis Data menggunakan Alogritma *Caesar Cipher* "menegaskan *caesar cipher* adalah penggantian sebuah karakter dalam teks sederhana kemudian mengubah menjadi karakter yang lain mempunyai letak perbedaan khusus (Siburian et al., 2017). Namun saat ini pergantian karakter dalam sebuah pesan itu sangat jarang dilakukan karena bagi pengirim menganggap mengubah isi pesan itu tidak mudah dibaca oleh penerima. Karena itu dibutuhkan tata cara untuk bisa membaca yang dikirimkan oleh pengirim dengan menggunakan metode *caesar cipher.*

Lalu menurut Adnan Buyung Nasution pada jurnalnya "Implementasi Pengamanan Data Dengan Menggunakan Algoritma *caesar cipher* dan transposisi *cipher*", *caesar cipher* yakni seluruh huruf dalam naskah awal kemudian akan di transformasi menggunakan aturan khusus lalu mempunyai perbedaan pada huruf (Nasution, 2019). Sebaliknya jika pengirim tidak memahami bagaimana mana cara untuk merubah teks yang sebelumnya akan di ganti agar isi teks tersebut orang lain tidak bisa membacanya. Diperlukan metode *caesar cipher* untuk memperhitungkannya agar tidak mudah untuk dimengrti oleh orang umum.

Oleh sebab itu dapat disimpulkan *caesar cipher* mengambarkan penggantian sebuah karakter dalam teks sederhana lalu bertransformasi menggunakan aturan khusus lalu mempunyai perbedaan pada huruf aslinya. Untuk bisa lebih memahami konsep dari *caesar cipher*, maka dapat dilihat berikut contoh simulasinya.

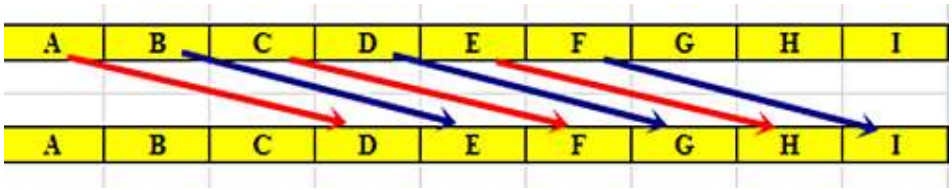
Dalam *Caesar Cipher*, menggunakan pergeseran 3 huruf dalam enkripsi-dekripsinya. Sehingga apabila hurupf awalnya A, menjadi D, B menjadi E, dan begitu seterusnya.



Gambar 2.11 Aturan geseran pada *Caesar Cipher*

Sumber: Data penelitian (2019)

Diasumsikan jika ada pesan yang ingin dikirimkan berupa kalimat "TEMUI SAYA DI KANTOR" ingin disampaikan pada seseorang namun tidak ingin agar diketahui oleh selain orang yang dituju tersebut, maka bisa dipergunakan metode *caesar cipher* ini untuk mengamankannya.

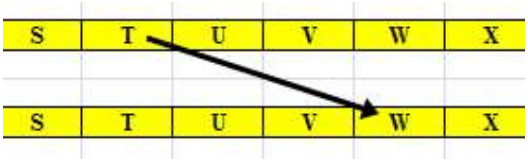


Gambar 2.12 Pergeseran 3 langkah

Sumber: Data penelitian (2019)

1. Lakukan pergesean huruf yang dinginkan, contohnya Geser ke D (pergeseran 3 langkah)

2. Selanjutnya jika sudah selesai melakukan pergeseran masukan kalimat sumber (*Plaintext).*
3. Maka dilakukanlah transposisi, contoh T = X (Nggak sinkron sm gambarnya)
4. Maka hasil akhirnya adalah hasil *ciphertext*nya



Gambar 2.13 contoh huruf T digeser kekanan sebanyak 3 langkah

Sumber: Data penelitian (2019)

Plaintext (Kalimat sumber) *:* TEMUI SAYA DI KANTOR
Ciphertext (Hasil Enkripsi) : WHPXL UDBD GL NDPWRU

2.2 *Tools*

2.2.1. PHP

Bersumber pada penelitian yang dilakukan oleh Penda, yang mengutip pemaparan dari Anhar bahwa PHP merupakan singkatan dari *Hypertext preprocessor* yang memiliki fungsi sebagai salah satu bahasa pemrograman web yang dapat disandingkan dengan HTML (Hasugian, 2018).

Kemudian menurut palevi menjelaskan PHP ialah sebuah bahasa pemrograman yang menjalankan dengan menggunakan beranda web. (Palevi, Mulyani, & Khoir, 2018).

Dapat di tarik kesimpulan bahwa PHP adalah suatu bahasa pemrograman web yang terhubung dengan server.

Contoh kode program sederhana dari PHP :

```
1  <html>
2    <body>
3        <?php
4                echo “Hello world!”;
5        ?>
6    </body>
7  </html>
```

2.2.2. XAMPP

Berdasarkan penelitian menurut Ninuk wiliani dan syadid zambi, XAMPP merupakan sekumpulan halaman web yang terhubung dengan server menggunakan aplikasi open source yang didalamnya terdapat server MySQL yang didukung dengan bahasa pemrograman PHP untuk membuat website yang dapat diubah – ubah (Syadid Zambi, 2017).

Selanjutnya pada penelitian yang dilakukan oleh Fitri ayu dan Nia permata sari, yang mengutip dari penjabaran dari Madcoms XAMPP merupakan sekumpulan paket *software* seperti *Apache, MySQL, PHPMyAdmin, FileZilla,* dan lain sebagainya. XAMPP beroperasi guna memudahkan instalisasi dibagian PHP, yang mana lazimnya digunakan pada pengembangan web (Ayu Fitri, 2018).

Dari penjelasan diatas dapat disimpulkan XAMPP adalah halaman web yang terhubung dengan server menggunakan aplikasi *open source* yang didalamnya terdapat beberapa *software* seperti *Apache, MySQL, PHPMyAdmin, FileZilla,* dan lain sebagainya agar memudahkan instalisasi dibagian PHP.

2.2.3. HTML

Menurut Imzen Sitorus didalam bukunya HTML merupakan bahasa dasar pemograman yang digunakan untuk membuat suatu tampilan website (Sitorus, 2012). HTML merupakan kepanjangan dari (*Hypertext Markup Language*) yang memungkinkan pengguna untuk menyusun dan membuat judul, paragraf dan tautan dihalaman website. HTML merupakan konfersi dari bahasa ASCII atau bahasa komputer yang dibuat untuk mempermudah dalam pembuatan tampilan website. HTML juga merupakan standar yang digunakan dalam pembuatan suatu website. Dengan adanya halaman website informasi dapat disebar luaskan kepada penggunanya di seluruh dunia, sehingga HTML sangat efektif dalam penggunaan dan pemanfaatanya pada penyebaran suatu informasi.

Selanjutnya menurut Besus Maula Sulthon HTML bisa dikatakan tolak ukur dari sebuah pembuatan website yang akan diakses dari internet, tidak temasuk dari sebuah bahasa pemrograman. Akan tetapi HTML ialah sebuah aturan penulisan yang membuat aplikasi (*sofware)* bisa memahaminya, agar bisa ditampilkan serta dilihat oleh pembaca supaya dengan mudah bisa mengerti. HTML dirangkai menggunakan simbol dan kode eksluif untuk dimasukkan kesebuah dokumen atau file. Sedangkan *Hypertext* sama dengan sebuah proses yang dipakai dalam memindahkan halaman website (Sulthon, 2018).

Dari kesimpulan diatas maka dapat disimpulkan bahwa HTML ialah bahasa dasar pemrograman yang digunakan untuk membuat suatu tampilan website dengan menggunakan aturan penulisan yang membuat aplikasi (*software*) bisa memahaminya, HTML dirangkai menggunakan simbol dan kode ekslusif untuk

dimasukkan ke sebuah dokumen atau file, sedangkan *hypertext* sama dengan sebuah proses yang dipakai dalam memindahkan halaman website.

2.2.4 *Guballa.de*

Guballa.de merupakan sebuah alamat website yang dikembangkan oleh developer web asal jerman yang bertujuan untuk membuat program berbasis web. Dalam program berbasis web tersebut, pengembang menyediakan tools untuk melakukan *solving* (pemecahan) berbasis *Brute-force* pada beberapa jenis kriptografi tertentu, seperti *polyalphabetic solver*, *substitution cipher solver*, dan juga *vignere cipher*.

Gambar 2.14 Logo *Guballa.de*

Sumber gambar: *guballa.de*

2.2.5 Microsoft visio

Microsoft visio adalah perangkat lunak yang dibuat oleh *microsoft* yang hadir sebagai alternatif untuk pembuatan permodelan suatu sistem. Pada penelitian yang telah di buat oleh xianho beserta teman-temanya memaparkan bahwa *microsoft visio* ialah suatu perangkat yang berfungsi untuk melakukan pembuatan desain diagram grafis pada pemodelan hubungan diagram yang diperlukan dengan data beserta sumber daya yang mewakili secara grafis menggunakan *microsoft visio*. Dalam ide utama dengan perangkat pemodelan

yang komplit. Semua keperluan dalam melakukan pemodelan dipersiapkan oleh *microsoft* supaya pengguna lebih terpuaskan (Lin, Liu, & Lei, 2016).

Gambar 2.15 Logo *Microsoft Visio*

Sumber: Product.microsoft.com

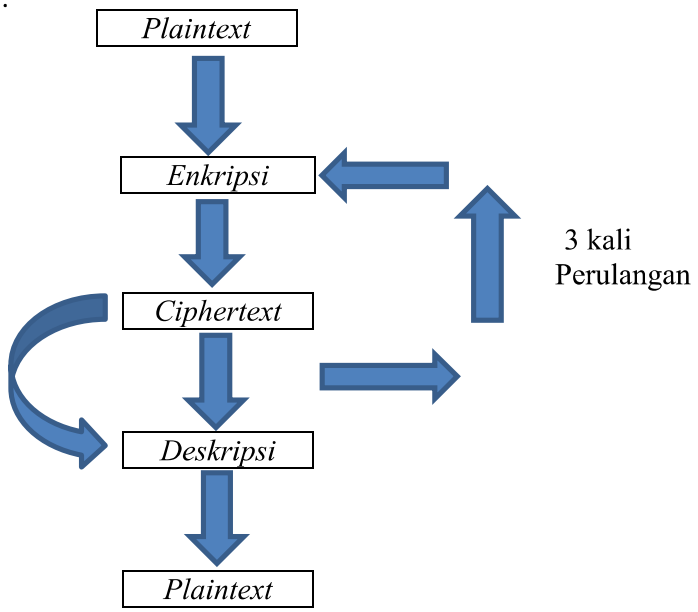
Berdasarkan pendapat yang dikemukakan oleh Yu beserta yang lain menjelaskan tentang *microsoft visio* mempunyai bermacam kelebihan saat memilih untuk menjadi perangkat lunak dalam permodelan tertentu, contohnya dalam dukungan operasi matematis dan logis. Dalam perubahan manual pada bentuk diagram berdasarkan keinginan pemakai, otomatis pada penggunaan atribut diagram pada saat pemodelan digunakan dengan jumlah yang sangat banyak, beserta masih banyak lagi. Fakta lainnya, *microsoft visio* merupakan bagian dari keluarga besar *microsoft*, diciptakan agar mudah untuk digabungkan ke banyak aplikasi *microsoft* lainnya, dan akan melatih pengguna semakin optimal dalam penggunaan waktu pada saat penggunaanya karena semuanya dapat saling berkaitan pemakaiannya (aplikasi lintas *software*).

2.3 Teori Khusus

Menerangkan ide tertentu melalui pengamat penelitian yang diambil, yakni ide tentang bahasan tambahan yang akan dijelaskan. Prinsip Ekslusif yang akan

dikembangkan beserta membawa rujukannya. Ialah jurnal yang telah sah mempunyai standar ISSN. Adapun teori khusus dalam penelitian ini mengarah pada penjelasan dari Algoritma TTVC yang dipilih sebagai solusi dari Kriptografi yang akan dibuat.

Three Transposition Vigenere Cipher adalah tata cara penyandian melalui menyalin proses *vigenere cipher* dimana *plaintextnya* dilakukan *Transposisi* sebelumnya sebanyak tiga kali menggunakan memanfaatkan kunci berbeda antara yang satu dengan yang lainnya. Cara kerja teknik *Three Transpoisition Vigenere Cipher* sebagai berikut :

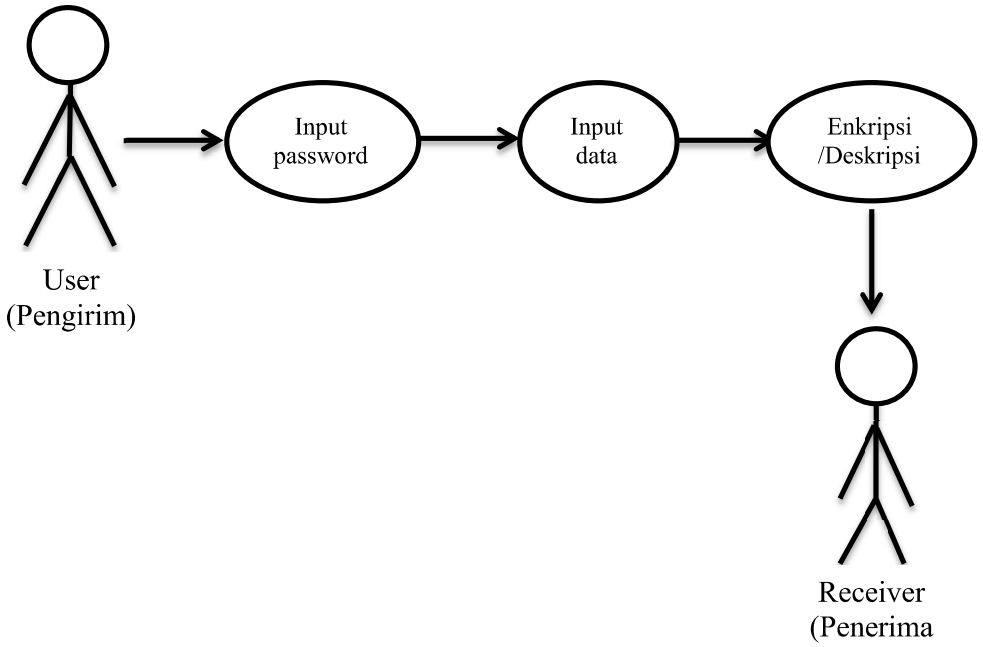


Gambar 2.16 Proses *Three Transpositiin Vigenere Cipher*

Sumber: Data olahan (2019)

Dijelaskan metode *Three Transposition Vigenere Cipher* sangat terkait dengan hasil *Ciphertext* atas kunci amat besar. Jika terjadi kesalahan salah satu huruf saja, dan mengakibatkan kekeliruan pada *Ciphertext*. Langkah – langkahnya:

1. *Plaintext* adalah pesan teks asli.
2. Enkripsi adalah perubahan pesan asli menjadi pesan yang tidak bisa dibaca atau berkode.
3. *Ciphertext* adalah hasil dari proses enkripsi pesan kemudian bisa dibaca.
4. Deskripsi adalah perubahan kembali pesan teks yang sebelumnya tidak bisa dibaca menjadi pesan teks asli.



Gambar 2.17 *Use Case Diagram* pengaman teks

Sumber: Data penelitian (2019)

Three Transposition Vigenere Cipher merupakan suatu teknik enkripsi dengan mengulangi teknik *Vigenere Cipher* sebanyak tiga kali dengan kunci yang berbeda. Teknik *Vigenere Cipher* dimana setiap *Plaintextnya* dilakukan transposisi sebanyak tiga kali dengan membuat kunci dimana disetiap kuncinya itu berbeda – beda. Berdasarkan pada Gambar. 2.17 diatas cara kerja dari sistem

keamanan pesan teks dimana ketika setelah melakukan *input password*. Jika didapati *password* tidak sesuai dengan urutan maka pesan tidak bisa di enkripsi atau di dekripsikan selanjutnya dilakukan penginputan data yang akan di enkripsi, setelah itu maka akan diproses oleh *receiver*.

2.4 Penelitian terdahulu

Dalam pembuatan sebuah penelitian dan perkembangan, dicantumkan beberapa penelitian terkait yang pernah dilakukan sebelumnya oleh penelitian lain dengan tujuan menunjukkan ulasan singkat terkait penelitian tersebut, Dalam penelitian ini akan memaparkan sebanyak lima penelitian terdahulu yang relevan dengan permasalahan yang diteliti

1. Berdasarkan penelitian yang dilakukan oleh Ahmad Rico Santoso, Abdul Riski, Dan Ahmad Kamsyakawuni yang berjudul **"Implementasi Algoritma *Reversed Vigenere Encryption* pada Pengamanan Citra" ISSN 2339 - 0069** peneliti mencoba mengimplementasi menggunakan Algoritma *Reversed Vigenere Engcryption* pada penyandian RGB tujuannya adalah untuk memahami bagaimana tahap – tahap enkripsi dan deskripsi beserta hasil keamanan berawal penyandian citra atas gempuran kriptonalisis. Di dalam jurnalnya tersebut, peneliti menganalisis hasil analisis histogram dan analisis differensial untuk menghasilkan sebuah enkripsi. Perolehan hasil bermula dari proses enkripsi dengan deskripsi agar menghasilkan *cipher image* membentuk setengah pola dari citra asli dapat dengan mudah ditebak, bila menggunakan analisis histogram. Karena nilai – nilai *pixels* dari *Cipher image* bisa menyebar secara keseluruhan sehingga hasil dari enkripsi citra

masih memiliki kelemahan terhadap serangan kriptonalisis. berbeda dengan analisis diffrensial dimana setiap *pixels* citra dapat berubah dari bentuk total.

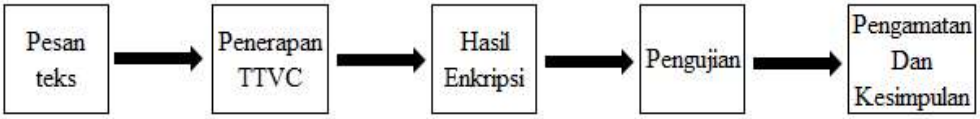
2. Selanjutnya pada penelitian yang berjudul **"Implementasi algoritma transposisi *cipher* pada sistem pengamanan data pada jaringan LAN" ISSN 25649 – 015X** yang dilakukan oleh melivarina Tamba yang memberikan hasil sebuah pemrograman pengaman pesan mengaplikasikan sistem transposisi dengan menggunakan cara transposisi kriptografi dan steganografi bermaksud mengatasi subtansi data rahasia apapun dengan cara menyembunyikan ke dalam perangkat tertentu.
3. Kemudian berdasarkan penelitian yang dilakukan oleh Yuza Reswan, ujang juhardi beserta teman – teman didalam jurnalnya **"Implementasi kompilasi Algoritma Kriptografi Transposisi *Columnar* Dan RSA untuk Pengamanan Pesan Rahasia" ISSN 2247 - 6645** menjelaskan bahwa untuk mengamankan sebuah pesan rahasia diperlukan algoritma kriptografi transposisi columnar dan RSA. Algoritma transposisi columnar ialah salah satu bagian *cipher* transposisi serupa teknik kriptografi dimana pesan dituliskan berurut melalui satu panjang yang diterapkan, kemudian ditaksirkan ulang berdasarkan jalur urutan pembacaan bersumber pada satu kunci. Sedangkan Algoritma RSA yakni merupakan tipe kriptografi yang memakai dua kunci yang berbeda, yaitu satu *key public* dan satunya lagi menggunakan *private key*. Jadi bisa disimpulkan menggabungkan dua algoritma transposisi columnar dengan RSA menguatkan kemanan data dalam sebuah bentuk pesan amat efisien demi mengunci data agar lebih baik.

4. Lalu Daurat Sinaga dan Chaerul Umam melakukan sebuah penelitian dengan judul berupa **"Implementasi Kriptografi *Vigenere Cipher* pada Media Teks Dengan Kombinasi Transposisi Kolom" ISBN 978 – 979** yang memasukkan Algoritma *vigenere cipher* dengan kombinasi Algoritma transposisi kolom. Didalam penelitiannya membuktikan jika pesan *plaintext* dapat di proses menggunakan enkripsi dengan baik memakai sebentuk gabungan algoritma yang dapat dikembalikan seperti awal. Untuk tentukan tingkat keamanan pesan data memakai *avalanhce effect* dengan lima kali percobaan untuk mendapatkan nilai tertinggi. Salah satu elemen *avalanhce effect* ialah bit *flipping* atau perubahan bit dalam sebuah metode enkripsi. Bit flipping bermanfaat menentukan perubahan bit sebelum dan sesudah proses enkripsi. Sehingga sangat berpengaruh untuk meningkatkan proses keamanan kriptografi.
5. Dan menurut Irfan anas, Putra arya nanda dengan yang lain di dalam jurnalnya "**Implementasi Algoritma *Vigenere Cipher* Dan Gost dalam Keamanan Data**" **ISSN 2541 – 044X** menerangkan algoritma *vigenere cipher* yang digabungkan dengan Algoritma *gost* akan menghasilkan sistem keamanan pesan teks yang lebih aman menggunakan 2 kunci untuk mengenkripsi maupun mendeskripsikannya, bukan hanya menggunakan kunci dari alogritma *vigenere cipher* saja akan tetapi menggunakan algoritma gost.

2.5 Kerangka Pemikiran

Kerangka pemikiran adalah penjelasan sementara terhadap suatu gejala yang menjadi objek permasalahan dalam sebuah penelitian. Dalam penelitian ini, dapat dilihat kerangka berfikirnya seperti gambar berikut ini.

Gambar 2.18 Kerangka Berpikir Penelitian



Sumber: Data penelitian (2019)

Pada gambar diatas dapat dilihat bahwa kerangka pemikiran dalam skripsi penelitian ini diawali dari ditemukan sebuah masalah dimana kebanyakan pengguna pada saat mengirimkan pesan berupa teks, dimana mereka sering kali mengabaikan keamanan informasi berupa teks seperti yang dijabarkan sebelumnya pada bab 1. Dan kejadian ini berpotensi mengakibatkan terjadinya kebocoran informasi yang ingin disampaikan kepada pengguna lainnya yang akan membuka membuka pesan tersebut. Padahal ada sebuah metode kriptografi memakai algoritma TTVC, menggunakan kriptografi *vigenere cipher.*

Dalam Metode TTVC terdapat berbagai macam jenis algoritma enkripsi yang telah ditemukan, salah satunya adalah algoritma *vigenere cipher,* yang nantinya akan menjadi hasil dari enkripsi. Berbekal dengan hasil enkripsi menggunakan Algoritma TTVC ini. Diketahui bahwa algoritma ini bukan sekedar algoritma subtitusi biasa, karena sudah ada pengembangan. Jadi peneliti berniat untuk menguji kekuatannya dimasa sekarang, yang akan di

aplikasikan menjadi sebuah *windows* dekstop. Untuk melihat seberapa kuat algoritma TTVC ini dipakai untuk mengamankan pesan teks pada zaman sekarang.