IMPLEMENTASI ALGORITMA *THREE TRANSPOSITION VIGENERE CIPHER* DALAM PENGAMANAN KOMUNIKASI INTERNAL BERBASIS DEKSTOP

SKRIPSI

Oleh
Faizal
150210097

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
2020

IMPLEMENTASI ALGORITMA *THREE TRANSPOSITION VIGENERE CIPHER* DALAM PENGAMANAN KOMUNIKASI INTERNAL BERBASIS DEKSTOP

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Oleh
Faizal
150210097

o

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK DAN KOMPUTER
UNIVERSITAS PUTERA BATAM
TAHUN 2020

SURAT PERNYATAAN ORISINIALITAS

Yang bertanda tangan dibawah ini saya :

Nama	: Faizal
NPM	: 150210097
Fakultas	: Teknik Dan Komputer
Program Studi	: Teknik Informatika

Menyatakan Bahwa "Skripsi" yang saya buat dengan judul :

Implementasi Algoritma *Three Tansposition Vigenere Cipher* Dalam Pengamanan Komunikasi Internal Berbasis Dekstop

Adalah hasil karya sendiri dan bukan "duplikasi" dari karya orang lain. Sepengetahuan saya didalam naskah Skripsi.ini tidak terdapat karya ilmiah atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis dikutip didalam naskah ini dan disebutkan dalam sumber kutipan dan daftar pustaka.

Apabila ternyata di dalam naskah Skripsi. ini dapat dibuktikan terdapat unsur-unsur PLAGIASI, saya bersedia naskah Skripsi. ini digugurkan dan Gelar. yang saya peroleh dibatalkan, serta diproses sesuai dengan peraturan perundang-undangan yang berlaku.

Demikian pernyataan ini saya buat dengan sebenarnya tanpa ada paksaan dari siapapun

Batam, 17 Februari 2020

Faizal

150210097

IMPLEMENTASI ALGORITMA THREE TRANSPOSITION VIGENERE CIPHER DALAM PENGAMANAN KOMUNIKASI INTERNAL BERBASIS DEKSTOP

SKRIPSI

Untuk memenuhi salah satu syarat
guna memperoleh gelar Sarjana

Oleh
Faizal
150210097

Telah disetujui oleh pembimbing pada tanggal

Seperti yang tertera di bawah ini

Batam, 17 Februari 2020

Andi Maslan, S.T.,M.SI
Pembimbing

Abstrak

Berbagi kabar, bertukar informasi, menambahkan informasi, berinteraksi dengan manusia lain, dan sejenisnya, adalah proses yang kita kenal dengan istilah pengiriman pesan. Tidak semua orang berhak untuk mengetahui pesan yang bersifat privasi, sensitif dan sangat rahasia. Ada sebuah metode yang dipergunakan untuk menjaga keamanan pesan, Metode untuk menjaga kerahasiaan pesan ini bernama metode enkripsi. yang merupakan metode dimana dilakukan upaya – upaya memanipulasi pesan sehingga pesan tersebut akan terlihat seperti kumpulan teks yang tidak ada artinya. Teknik enkripsi hadir disaat masa klasik dimana semua pesan masih diubah ke dalam bentuk *ciphertext* yang dituliskan diatas kertas, hingga masa kini yang sudah serba dibumbui penggunaannya dengan teknologi. Keamanan dari pengiriman pesan lintas perangkat akan sangat diperlukan agar setiap informasi yang keluar, baik itu bersifat privasi maupun tidak, dapat sampai kepada pihak yang memang menjadi tujuan pesan itu tanpa bocor kepada pihak lain. Bocor dalam konteks ini tidak selalu dalam artian peretasan digital, namun juga dalam arah ketidak sengajaan dalam peminjaman perangkat teknologi kepada pihak lain yang dipercayai memakainya. Dari kondisi ini ditemui salah solusi enkripsi yang lebih baru bernama algoritma TTVC (*Three transposition vignere cipher)* yang merupakan pengembangan dari algoritma yang sudah ada. Dari kondisi yang dihadapi ini peneliti akan mencoba untuk menerapkan algoritma TTVC terhadap keamanan teks pada era teknologi yang sudah sangat berkembang. Dari penelitian yang dilakukan, algoritma diterapkan berbasis web dan diketahui berhasil menjaga teks yang dikirmkan maupun diterima secara baik dan lancar.

Kata Kunci: Enkripsi, TTVC, Kriptografi

Abstract

Sharing news and exchanging information is the process we known as communication. in communicating with others, some of the messages do not suppose to be exposed to the person who doesn't belong. this case could because of the sensitivity and privacy issue. protecting the privacy of messages through technology devices often called encryption. Encryption is the process of masking real messages into an unreadable message. encryption has been around since the message is sent by primitive technology, and still exist in this advanced technology nowadays. the privacy issue is the most common problem people face every day, and the implementation of encryption could help solve this problem. there is an encryption algorithm called TTVC (Three transposition vignere cipher) which the classic vignere cipher has been modified into held on three times transposition. this research aims to implement the TTVC algorithm and learn if this encryption method still reliable nowadays. result found that TTVC is proven still good to protect privacy from exchanging messages. TTVC algorithm succeeds implemented into a web application and WhatsApp messenger is used as the carrier. TTVC still could protect the message from sender to receiver, vice versa.

Keyword: Encryption, TTVC, Cryptography

KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Program Studi Teknik Informatika Universitas Putera Batam.

Penulis menyadari bahwa skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa skripsi ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Rektor Universitas Putera Batam.
2. Ketua Program Studi Teknik Informatika Universitas Putera Batam.
3. Bapak Andi Maslan, S.T.,M.SI selaku pembimbing Skripsi pada Program Studi Teknik Informatika Universitas Putera Batam.
4. Dosen dan Staff Universitas Putera Batam.
5. Ibu Lusiana Sapta, S.H selaku Wakil Dirketur Lembaga Pendidikan dan Pelatihan Madani Batam yang telah memberikan izin tempat penelitian.
6. Rekan-rekan seperjuangan Universitas Putera Batam yang selalu memberikan motivasi baik berupa sharing pendapat, motivasi dan hal-hal lainnya dalam rangka pembuatan skripsi ini.
7. Keluarga yang selalu memberikan do’a dan motivasi yang baik.

Harapan penulis semoga skripsi ini bermanfaat khususnya bagi penulis dan para pembaca pada umumnya. Semoga Allah SWT membalas kebaikan dan selalu mencurahkan hidayah serta taufik-Nya. Akhir kata penulis ucapkan terima kasih.

Batam, 17 Februari 2020

Penulis
Faizal

DAFTAR ISI

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR TABEL

Halaman

BAB I

PENDAHULUAN

1.1 Latar Belakang

Berbagi kabar, bertukar informasi, menambahkan informasi, berinteraksi dengan manusia lain, dan sejenisnya, adalah proses yang kita kenal dengan istilah pengiriman pesan. Untuk melakukan proses pengiriman pesan adalah metode yang paling mudah untuk saling bertukar informasi kesesama manusia lainnya. Banyak faktor yang mendukung dan membelakangi mengapa pengiriman pesan terus terjadi. Dalam bidang psikologi menurut seorang ahli bernama *Homo ludens* Mengatakan bahwa komunikasi dipengaruhi oleh psikologi humanistik yang menyatakan bahwa manusia adalah pelaku aktif dalam interaksi dengan lingkungannya. Sehingga dapat diambil hipotesis bahwa pengiriman pesan dalam menyampaikan informasi akan dan tetap terus terjadi sampai kedepannya.

Manusia telah berikirim pesan sejak dari zaman dahulu, Dimulai sejak proses pertukaran informasi dalam bentuk primitif, bahkan sampai dimasa modern yang membawa segala aspek kehidupan ketingkat yang lebih canggih. Dalam contoh metode pengiriman pesan secara primitif, salah satunya dikenal dengan teknik penyampaian pesan yang digunakan oleh suku *Navajo*, penduduk asli Amerika (suku indian) (TribalDirectory, 2016). Mereka menggunakan api yang diatur asapnya agar dapat dikumpulkan dan dilepaskan diudara dan membentuk

sebuah pola asap tertentu yang merupakan sebuah cara penyampaian pesan pada anggota suku yang lain agar dapat berkomunikasi.

Seiring dengan perkembangan waktu, mulai dirasakan kebutuhan akan sebuah kerahasiaan dari pesan – pesan yang akan dikirimkan, agar tidak dapat diketahui isinya oleh pihak yang tidak berhak mengetahuinya. Tidak semua orang berhak untuk mengetahui pesan yang bersifat privasi, sensitif dan sangat rahasia. Oleh karena itu, pengiriman pesan dalam penyampaian informasi harus diberlakukan dengan sangat khusus dengan menggunakan metode khusus pula. Dapat dibayangkan jika sebuah perusahaan besar yang sedang melakukan transaksi melalui media *online* karena letak perbedaan geografis berbeda dan dalam keadaan mendesak, ternyata transaksinya sedang di dengarkan juga oleh peretas (*Hacker*) dan dijual informasinya pada perusahaan saingan, sehingga perusahaan saingan tersebut dapat memanfaatkan informasi tersebut untuk membuat perusahaan tersebut kalah produksi dan mengalami kerugian.

Itu semua dapat terjadi karena kurangnya metode keamanan dalam pengiriman dan penyampaian pesan yang dipakai. Salah satu kasus kebocoran informasi yang terjadi di negara Indonesia, tepatnya setelah pernyataan Marciano Norman, yang saat itu sedang menjabat sebagai kepala satuan Badan Intelijen Negara (BIN). Marciano mengatakan bahwa “Penyadapan ini memang yang terbuka dari 2007-2009, Tetapi dari informasi yang kita terima bahwa ada data – data yang terjadi pelanggaran pada kurun waktu itu”, beliau mengklarifikasi bahwa telah terjadi penyadapan dari pihak aparat Intelijen Australia terhadap

presiden yang bertugas pada saat itu yaitu Susilo Bambang Yudhoyono, istrinya Ani yudhoyono, dan beberapa pejabat lainnya (BBC, 2013).

Metode untuk menjaga kerahasiaan pesan ini bernama metode enkripsi. yang merupakan metode dimana dilakukan upaya – upaya memanipulasi pesan sehingga pesan tersebut akan terlihat seperti kumpulan teks yang tidak ada artinya. Apabila pembaca tidak tau cara membacanya, Atau Menurut Wahana & Andi "Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca)".

Bermula pada tahun 1900 sebelum masehi, cendikiawan mesir menggunakan *Hieroglyph* yang tidak biasa pada prasasti mereka. Dan ini disebut oleh kahn dalam bukunya *The Codebrekaer* sebagai sebuah dokumen dengan kriptografi pertama (Khan, 1967). Kemudian *Glovan* metode penyajian teks alphabet dengan menggunakan deretan sandi *Caesar* berdasarkan huruf – huruf pada kata kunci. Selanjutnya pada tahun pada sekitar tahun 725-790 sebelum masehi, Abu 'Abdul-Rahman al-Khalil ibnu Ahmad' Amr ibn Tammam al-Farahid ibn al-Zadi al-Yahmadi telah menuliskan sebuah buku terkait kriptografi yang terinspirasi dari kriptogram Yunani yang sering dipakai pada masa kerajaan *byzantine,* yang kemudian oleh ahli pemecah kriptografi untuk membongkar mesin enigma (Jackob, 2020). Mesin Enigma sendiri adalah alat enkripsi yang berbentuk seperti koper dengan isi berupa motor mekanis listrik dan diadopsi oleh kebanyakan Negara yang ikut perang dunia kedua seperti Jerman, Jepang, dan

Italia dalam menyampaikan pesannya agar tidak mudah diketahui oleh pihak musuh.

Teknik enkripsi hadir disaat masa klasik dimana semua pesan masih diubah ke dalam bentuk *ciphertext* yang dituliskan diatas kertas, hingga masa kini yang sudah serba dibumbui penggunaannya dengan teknologi. Manusia modern kini hidupnya dipenuhi dengan *smartphone* yang memiliki kedudukan sebagai alat primer pemuas kebutuhnnya. Menurut data lembaga penghitung digital, akan ada 2,53 milyar total manusia pengguna smartphone ditahun 2018 ini (Statista.com, 2020). Namun sepertinya kenyataan ini juga tidak menggeser penggunaan dari *desktop* PC dan *Notebook* yang sudah melegenda kebutuhan pemakaiannya. Pemakaian *desktop* PC dan *Notebook* tetap bertambah dan tidak mengalami penurunan karena meskipun *smartphone* sudah menjamur, masih banyak hal yang lebih nyaman dikerjakan menggunakan *desktop* maupun *Notebook* pada beberapa kondisi dan waktu tertentu. Sehingga, keamanan dari pengiriman pesan baik secara messenger maupun *email* akan sangat diperlukan agar setiap informasi yang keluar, baik itu bersifat privasi maupun tidak, dapat sampai kepada pihak yang memang menjadi tujuan pesan itu tanpa bocor kepada pihak lain. Bocor dalam konteks ini tidak selalu dalam artian peretasan digital, *Desktop* dan *Notebook* biasanya bisa saja dipinjamkan kepada pihak yang pemiliknya sudah dipercayai. Seperti kerabat, keluarga, maupun pihak berwajib. Untuk mencegah informasi tertentu yang dimiliki pesan tersebut dapat diketahui orang lain, maka penulis berkeinginan untuk mengajukan penelitian berupa pembuatan aplikasi yang dapat melakukan enkripsi pesan menggunakan metode *vigenere* dan

menggunakan algoritma *three transposition VC* yang berbasis *Windows desktop* sebagai solusi masalah yang ada ini dengan judul "**Impelementasi Algoritma *Three Transposition Vigenere cipher* Dalam Pengamanan komunikasi Internal Berbasis Dekstop** ".

1.2 Identifikasi masalah

Berdasarkan latar belakang yang sudah dikemukakan sebelumnya, maka identifikasi masalah yang akan dijadikan bahan pembuatan skripsi adalah sebagai berikut :

1. Terjadinya kebocoran informasi terhadap pesan teks yang ingin disampaikan.
2. Isi pesan teks yang diketahui oleh pihak lain selain tujuannya sangat beresiko tinggi.
3. Banyak orang yang menyampaikan pesan sensitif tanpa perlindungan enkripsi.

1.3 Pembatasan masalah

Agar pembuatan penelitian skripsi ini akan terarah dan sesuai tujuan, maka akan dibatasi masalahnyanya pada :

1. pembuatan aplikasi enkripsi berbasis *windows* desktop
2. perancangan program mengggunakan PHP
3. metode *vigenere* yang digunakan adalah algoritma *three transposition*
4. enkripsi hanya terjadi pada angka dan huruf
5. aplikasi berguna sebagai *plain-text* menjadi *ciphertext,* begitu sebaliknya.

1.4 Perumusan masalah

Berdasarkan penjelesan latar belakang diatas, maka akan dirumuskan masalahnya berupa :

1. Bagaimana cara merancang aplikasi berbasis *Three transposition vigenere cipher*?
2. Bagaimana Algoritma *Three transposition vigenere cipher* bekerja?
3. Bagaimana implementasi *Three transposition vigenere cipher* untuk melindungi pesan?

1.5 Tujuan Penelitian

Berdasarkan dengan apa yang sudah dijelaskan sebelumnya, maka tujuan penelitian ini antara lain adalah :

1. Menerapkan metode *vigenere cipher* dalam mengenkripsi pesan teks
2. Membuktikan bahwa enkripsi klasik masih bermanfaat

1.6 Manfaat penelitian

Manfaat dari penelitian ini merupakan imbas positif yang dapat dirasakan oleh pihak tertentu atas dilakukannya penelitian ini setelah selesai nantinya. Adapun manfaaat penelitian berupa teoritis dan praktis.

1.6.1 Manfaat teoritis

Manfaat dari hasil skripsi ini adalah menghasilkan output yang dapat menerapkan fungsi dan prinsip – prinsip yang dimiliki oleh *vigenere cipher* yang dapat mengenkripsi teks.

1.6.2 Manfaat praktis

Manfaat praktis yang dapat dihasilkan dari skripsi ini antara lain:

1. Bagi pengguna aplikasi, dapat lebih mengamankan lagi teks pesan yang akan dibuat agar tidak terjadi kebocoran informasi.
2. Bagi peneliti akan lebih memahami algoritma *vigenere cipher* serta lebih memahami ilmu tentang kriptografi.

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

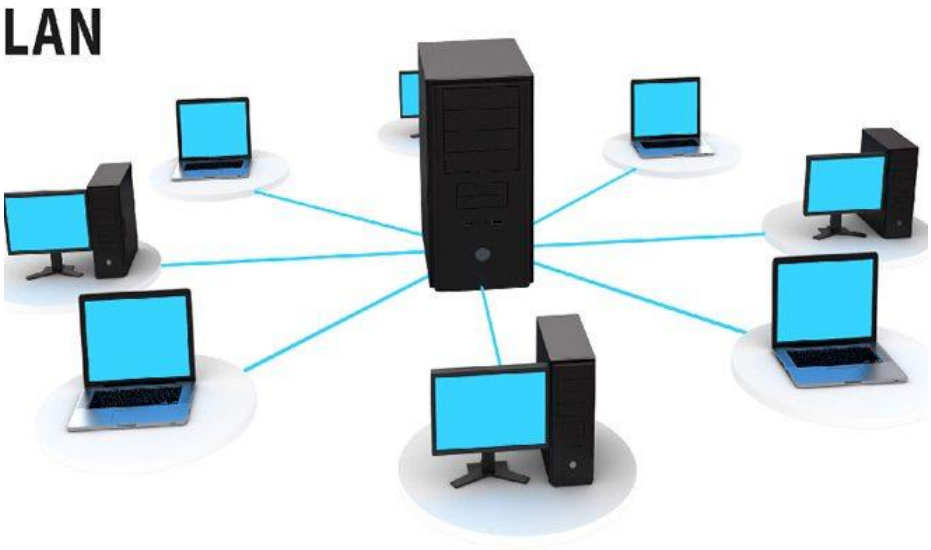
Sumber: Iso.org

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)*



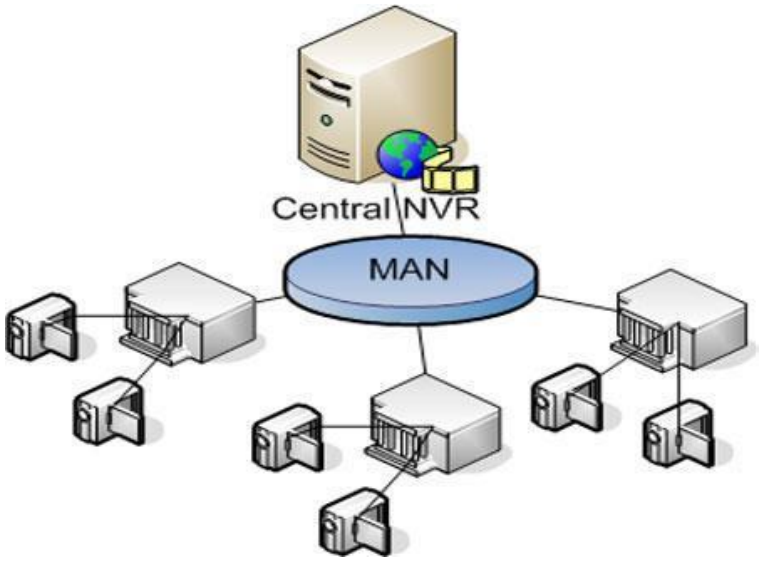
Gambar 2.2 *local Area Network*

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

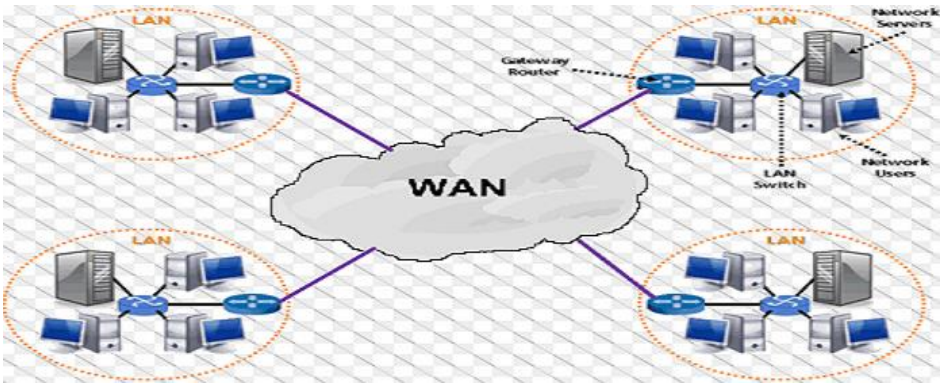
Sumber : *docplayer.info*

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

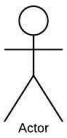
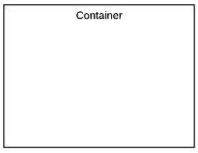
lainnya. Ada 2 kondisi mendasar dalam *use case* yaitu mendeskripsikan pada pemain dan pengertian mengenai *use case.*

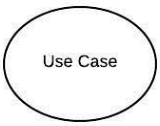
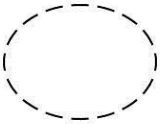
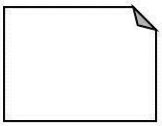
A) pelaku sebagai orang, prosedur ataupun proses yang berhubungan pada aturan yang bakal dikerjakan.

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

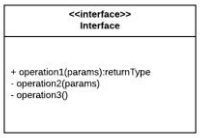
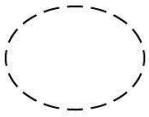
Kelas yang memproses peranan - peranan yang harus siap dipakai dari penjelasan *use case*.

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.

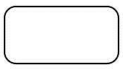
B) kumpulan pada tampilan dari sistem interface dimana pada setiap aktivitas yang telah terjadi memiliki tampilan sendiri.

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

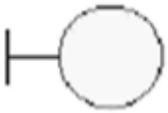
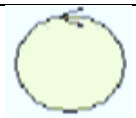
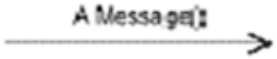
No	Gambar	Nama	Keterangan
1		Aktivitas	Menunjukkan betapa tiap kelas berinteraksi secara antarmuka satu sama lain
2		Tindakan	*State* pada sistem yang menggambarkan keputusan dalam suatu aksi
3		Node awal	Suatu titik objek untuk awal permulaan
4		Aktivitas final	Suatu akhiran pada tahapan objek
5		*Fork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

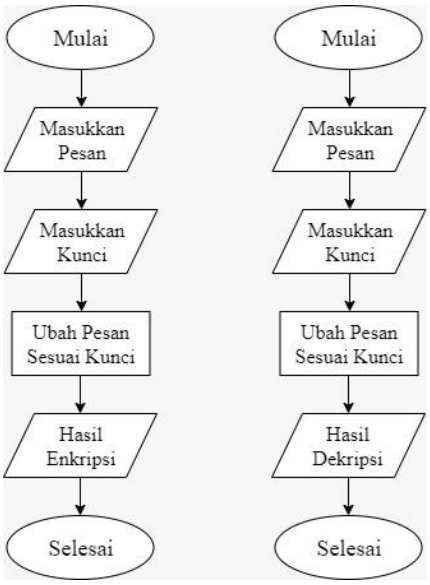
Sumber : Data penelitian (2019)

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.

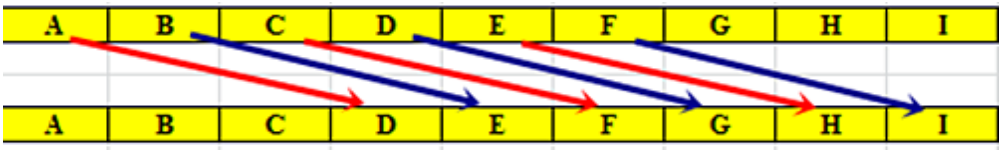
2. Caesar Cipher

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.

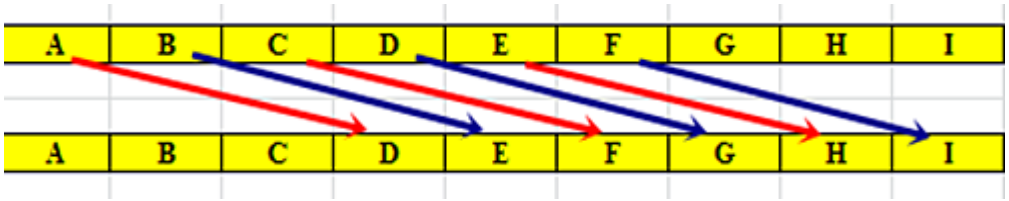
Dalam *Caesar Cipher*, menggunakan pergeseran 3 huruf dalam enkripsi-dekripsinya. Sehingga apabila hurupf awalnya A, menjadi D, B menjadi E, dan begitu seterusnya.



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.

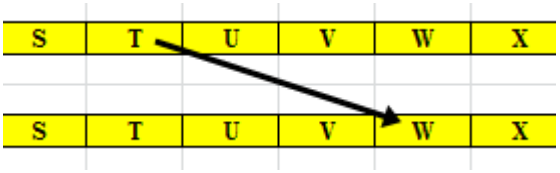


Gambar 2.12 Pergeseran 3 langkah

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*.

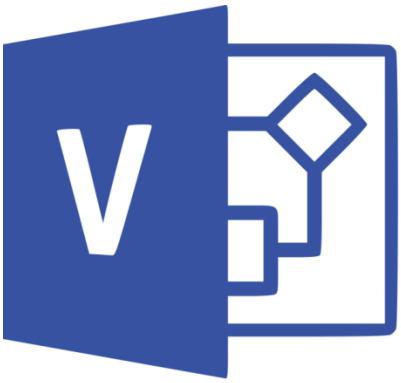
Gambar 2.14 Logo *Guballa.de*

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

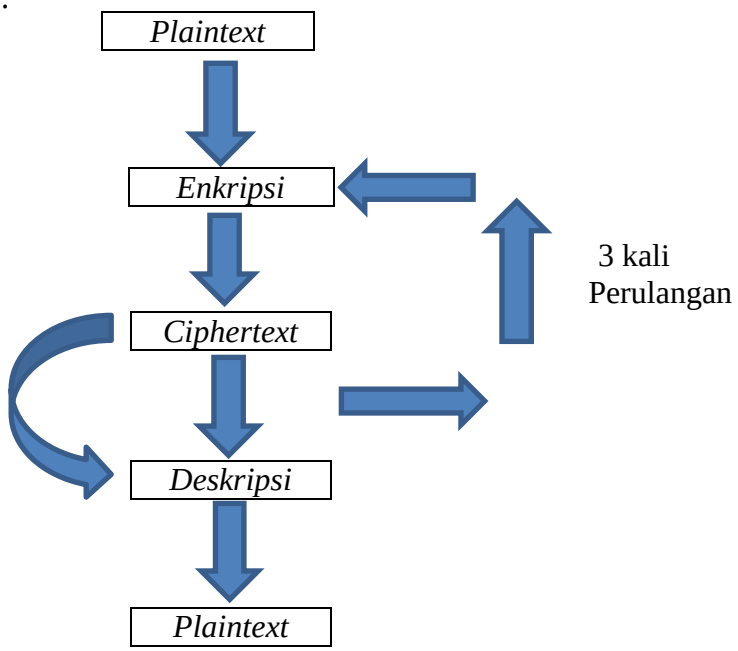
Berdasarkan pendapat yang dikemukakan oleh Yu beserta yang lain menjelaskan tentang *microsoft visio* mempunyai bermacam kelebihan saat memilih untuk menjadi perangkat lunak dalam permodelan tertentu, contohnya dalam dukungan operasi matematis dan logis. Dalam perubahan manual pada bentuk diagram berdasarkan 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 :

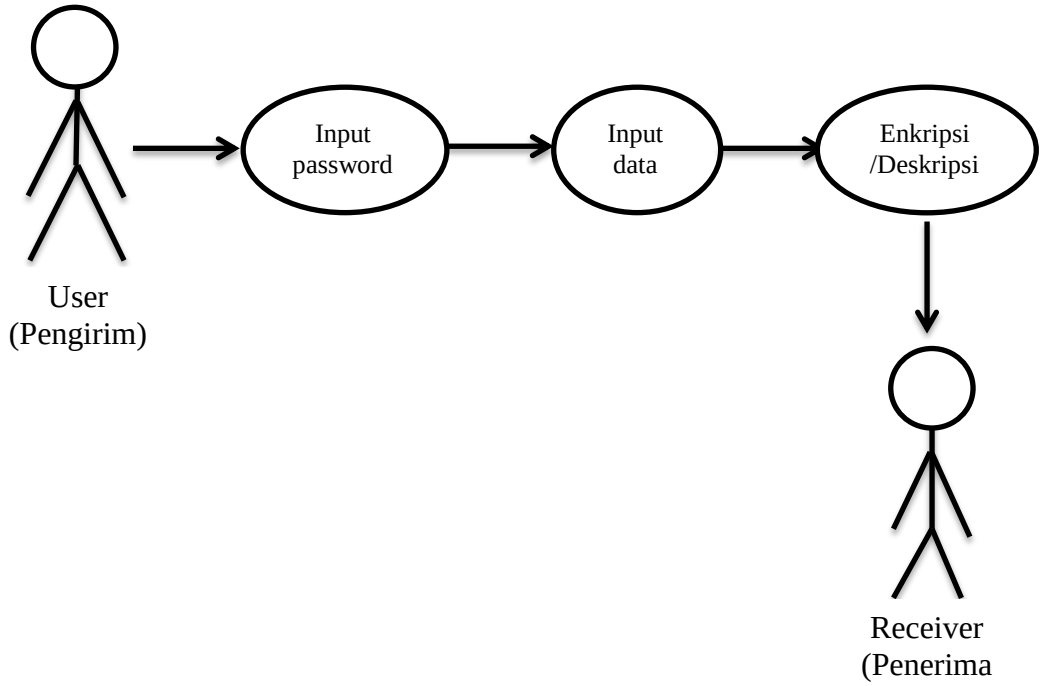


Gambar 2.16 Proses *Three Transpositiin Vigenere Cipher*

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

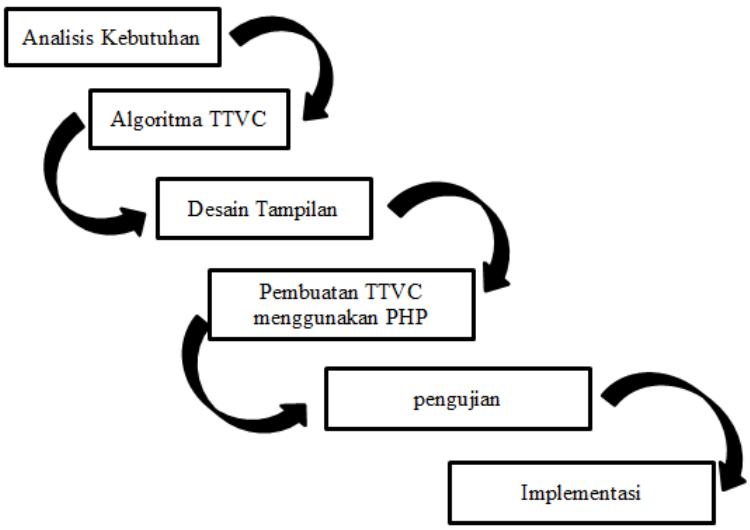
aplikasikan menjadi sebuah *windows* dekstop. Untuk melihat seberapa kuat algoritma TTVC ini dipakai untuk mengamankan pesan teks pada zaman sekarang.

BAB III

METODE PENELITIAN

3.1 Desain Penelitian

Desain penelitian merupakan sebuah penggambaran secara langkah dan tahap yang dipilih peneliti dari sudut pandang peneliti untuk melakukan penelitiannya dari awal hingga akhir. Desain penelitian akan terdiri dari sebuah ilustrasi grafik dan diikuti oleh penjelasan dibawahnya. Tujuan dari dibuatnya desain penelitian adalah membuat peneliti dapat memvisualkan secara sederhana namun ringkas dan lengkap terkait alur penelitian yang dilakukannya. Adapun desain dari penelitian ini adalah sebagai berikut.



Gambar 3.19 Desain Penelitian

Sumber: Data olahan Peneliti (2019)

Adapun desain penelitian diatas dapat dijabarkan sebagai berikut :

1. Analisis Kebutuhan

Pada tahapan pertama, peneliti melakukan analisis terhadap sistem yang berada pada lokasi penelitian yang dipilih. Hal ini membawa peneliti untuk mencoba memahami keberadaan sistem yang berjalan, potensi ancaman yang bisa terjadi, dan sekaligus permasalahan yang sudah pernah terjadi, agar ditemukan permasalahan yang bersifat mendesak (urgensi) untuk diteliti. Setelah melakukan observasi langsung ke tempat yang dipilih, ditemui permasalahan yang bersifat penting untuk diteliti adalah kebocoran data. kebocoran data sudah pada lokasi penelitian pernah terjadi pada tahun 2018 silam, dan disebabkan karena pengamanan data yang masih rentan (tidak memiliki keamanan sama sekali). Peneliti melakukan analisis kebutuhan yang ada di perusahaan Lembaga Pendidikan dan Pelatihan Madani yang ditemukan tidak adanya pengamanan pesan teks apabila pimpinan perusahaan mengirimkan memo (pesan singkat) kepada karyawannya. Untuk itu pengamanan teks sangat diperlukan agar karyawan lain tidak mengetahui isi memo tersebut.

2. Algoritma TTVC

Kebocoran data yang terjadi pada lokasi penelitian berupa data peserta ujian yang pernah mengikuti pelatihan ditempat tersebut. Data yang berbentuk teks dicuri oleh pihak yang tidak bertanggung jawab, dan menimbulkan kerugian bagi pihak pemilik tempat penelitian tersebut (lembaga pelatihan swasta). Kondisi permasalahan ini dapat diberikan solusi dari sudut pandang teknologi (informatika) dengan cara pengamanan kriptografi (berbasis teks). Peneliti

menggunakan Algoritma *Three Transposition Vigenere Cipher* sebagai keamanan dari pesan teks yang akan dikirim sehingga menghasilkan enkripsi dan dekripsi pada teks tersebut. Untuk itu yang hanya boleh membuka pesan hanya orang yang mempunyai kunci (pengguna).

3. Desain Tampilan

Pada tahapan ini Peneliti membuat desain tampilan program agar mudah digunakan oleh Perusahaan Lembaga Pendidikan Dan Pelatihan Madani. Adapun tampilan dari desain tersebut terdapat *form login*, *form input*, *form* pengiriman pesan, dan *form* input data member.

4. Pembuatan TTVC Menggunakan PHP

Algoritma TTVC merupakan salah satu dari sekian banyak algoritma kriptografi yang ditujukan untuk pengamanan teks. Alasan pemilihan dari metode ini dikarenakan peneliti menyadari bahwa metode ini sudah pengembangan dari algoritma serupa, yaitu *vignere cipher*, akan tetapi TTVC merupakan versi yang sudah dikembangkan. Cara kerja dari TTVC adalah mengenkripsi/mendekripsi teks yang ingin diubah, memanfaatkan algortima *vignere* sebanyak 3 kali pengulangan. Sehingga keamanan yang ditawarkan metode ini semakin meningkat. Nantinya algoritma TTVC ini akan diimplementasikan dalam bentuk program desktop berbasis PHP, sehingga dapat dipakai oleh pihak pemilik lokasi penelitian untuk mengamankan data teksnya sehingga tidak terjadi kembali pencurian data dengan cara yang sama. Peneliti membuat program menggunakan HTML dikarenakan penggunaannya bisa digunakan pada hp, PC, atau leptop.

5. Pengujian

Pada tahapan terakhir dari penelitian, hasil program yang dibuat tidak langsung diserahkan kepada pemilik lokasi peneltian, namun dilakukan pengujian (meneliti potensi kemampuan program) pada penerapan TTVC yang dimiliki oleh program tersebut. Bentuk pengujian yang dilakukan adalah percobaan *brute force* (pembobolan paksa) terhadap hasil enkripsi menggunakan aplikasi pembobol kriptografi. Tujuan pengujjian ini adalah bentuk penelitian yang dilakukan peneliti terhadap permasalahan yang ditemui, agar bermanfaat dan memberi sumbangsih bagi kalangan akademisi dan peneliti (terlepas manfaat praktis bagi pemilik lokasi penelitian). Peneliti melakukan tahap pengetesan agar program tersebut sempurna sebelum diimplementasikan dan tidak terjadi eror. Hasil laporan pengujian yang dilakukan akan dilaporkan dalam hasil penelitian, dan barulah program diserahkan kepada pemilik lokasi penelitian.

6. Implementasi

Algoritma TTVC merupakan salah satu dari sekian banyak algoritma kriptografi yang ditujukan untuk pengamanan teks. Alasan pemilihan dari metode ini dikarenakan peneliti menyadari bahwa metode ini sudah pengembangan dari algoritma serupa, yaitu *vignere cipher*, akan tetapi TTVC merupakan versi yang sudah dikembangkan. Cara kerja dari TTVC adalah mengenkripsi/mendekripsi teks yang ingin diubah, memanfaatkan algortima *vignere* sebanyak 3 kali pengulangan. Sehingga keamanan yang ditawarkan metode ini semakin meningkat. Nantinya algoritma TTVC ini akan diimplementasikan dalam bentuk program desktop berbasis PHP, sehingga dapat dipakai oleh pihak pemilik lokasi

penelitian untuk mengamankan data teksnya sehingga tidak terjadi kembali pencurian data dengan cara yang sama. Setelah melakukan tahapan semua diatas peneliti melakukan tahapan implementasi di perusahaan Lembaga Pendidikan Dan Pelatihan madani.

Pada perancangan ini menggunakan metode waterfall. Seperti yang dikemukakan oleh Rosa A.S dan M.Salahuddin didalam bukunya. Model waterfall merupakan sebuah aturan klasik dimana biasanya disebut model alur terjun, menyediakan strategi dalam sebuah aturan hidup perangkat lunak secara teratur dimulai dengan menganalisis desain, pengujian, tahap pendukung, serta pengkodean(M.shalahuddin, 2013). Bisa disimpulkan bahwa waterfall merupakan aturan yang harus dipenuhi oleh pembuat perancangan dalam penelitian agar hasil yang diperoleh bisa sesuai dengan yang diinginkan.

3.2 Perancangan Sistem

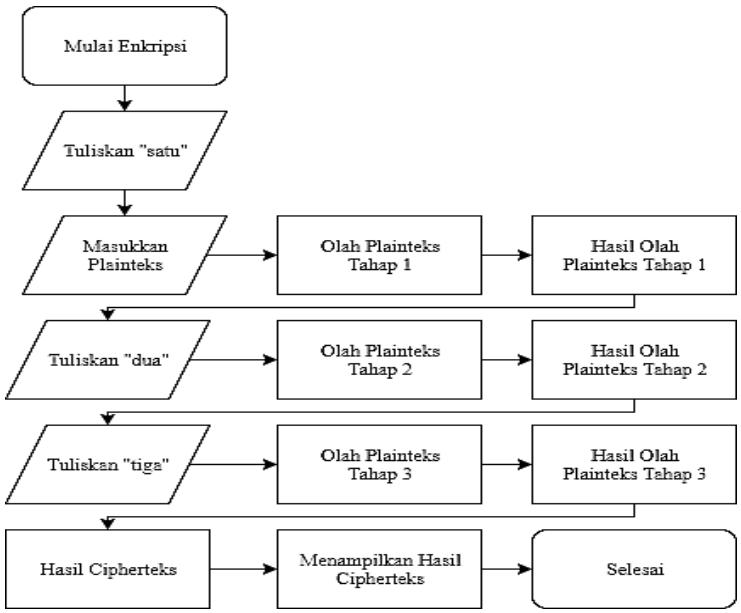
Perancangan dari sistem merupakan tahapan dari pemberian ilustrasi atas sistem yang akan dibuat beserta dengan bentuk perencanaan yang akan dieksekusi saat kegiatan membangun sistemnya (aplikasi enkripsi). Pada sub-bab ini akan dipaparkan terkait algoritma yang akan dipergunakan, pemodelan UML yang akan menggambarkan program didalamnya, serta penjabaran atas spesifikasi yang dibutuhkan untuk bisa menjalankan program tersebut.

3.2.1 Algoritma yang Dipakai

Algoritma merupakan sebuah logika dinamis yang dirumuskan untuk bisa dipakai dalam memecahkan suatu permasalahan yang ada. Algortima sering kali dikaitkan dengan pemrograman, akan tetapi algoritma nyatanya sangat

independen, karena suatu algoritma bisa tercipta dan dapat diimplementasikan ke banyak bahasa pemrograman berbeda. Dalam penelitian ini, seperti yang telah dibahas pada bab 2, akan menggunakan algoritrma *Three Transposition Vignere Cipher* (TTVC) untuk dijadikan bahan integrasi sistem yang dibuat dalam kriptografi pengamanan teks.

TTVC merupakan sebuah algoritma pengembangan dari algoritma pendahulunya, yaitu *Vignere Cipher*. *Vignere Cipher* merupakan sebuah algoritma kriptografi untuk teks dengan konsep pergesar caesar yang berpedoman pada kata kunci yang dibariskan secara simultan. Seperti algoritma kriptografi klasik lainnya, *vignere cipher* akan membuat sebuah plainteks menjadi aman dengan substitusi posisi dengan aturan dinamis dari posisi kata kuncinya. Namun dengan perkembangan dari teknologi yang menuntut banyak untuk terus berevolusi, menjadikan algoritma *vignere* mengalami pengembangan juga menjadi TTVC.



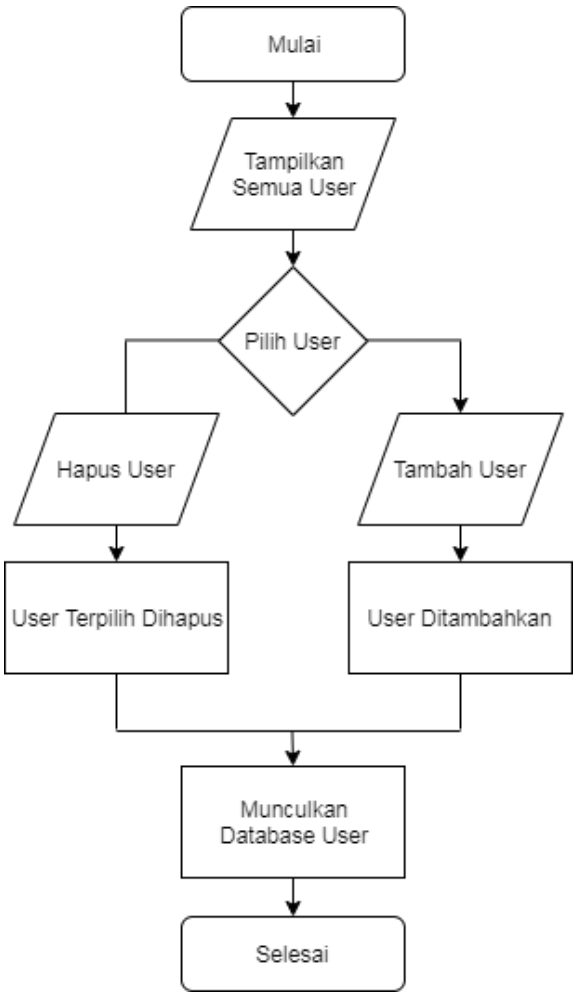
Gambar 3.20 Flowchart algoritma TTVC yang akan diimplementasikan

Sumber: Data olahan (2019)

Masih dengan aturan *vignere* yang asli, kini TTVC bekerja dengan penambahan tahapan, yaitu melakukan enkripsi ataupun dekripsinya yang diulang dengan tiga kali (*Three transposition* = pergeseran posisi tiga kali). Dengan keberadaan dari pengembangan algoritma ini, menjadikan pengamanan dari teks semakin lebih meyakinkan lagi. Sesuai dengan konsep TTVC yang orisinil, dalam penelitian ini juga masih mengadopsi metode yang sama. Dari segi sistem akan dibuat secara sistem dengan proses yang linear berbasis *vignere* (namun dimodifikasikan). Pada segi sistem, perencanaan implementasi pada proses enkripsi diilustrasikan seperti pada gambar 3.20 diatas, dimana pengguna akan bertemu dengan halaman yang telah diprogram untuk bisa melakukan enkripsi-dekripsi berbasis vignere, dan meminta pengguna untuk turut berpartisipasi memasukkan kalimat kunci (satu-dua-tiga) agar kalimat *input* yang diinginkan dapat dikonversi dan menjadi TTVC.

Apabila sudah memasukkan kalimat yang ingin di enkripsi (atau dekripsi), maka pengguna juga diminta untuk memasukkan kunci sebanyak tiga kali (karena TTVC bergeser tiga kali dari *vignere* orisinil), dan proses konversi akan dilakukan. Barulah setelah itu sistem baru bisa memulai tugasnya untuk melakukan olah teks dengan substitusi algoritma *vignere.* Proses pengolahan akan diulang sebanyak tiga kali (karena tiga kali transposisi), dan barulah hasil *cipherteks* bisa diapatkan. Hasil enkripsi *cipherteks* akan dimunculkan kepada pengguna dan disitulah proses sistem akan selesai. Keseluruhan dari proses enkripsi-dekripsi menganut sistem yang sangat identik, sehingga dapat dipahami dengan ilustrasi diatas.

Selanjutnya dari sudut pandang sistem yang ada pada administrator, akan ditemui fitur tambahan yang tidak ditemui pada pengguna biasa, yaitu akses untuk melakukan penambahan dan penghapusan dari pengguna yang dapat melakukan akses pada aplikasi kriptografi. Dalam hal ini, administrator memiliki akses yang berkaitan pada sistem dan database yang ada. Untuk lebih jelas, perhatikan gambar 3.21 berikut ini.



Gambar 3.21 Flowchart Sistem Pada Administrator

Sumber: Data olahan peneliti (2019)

Dapat dilihat pada gambar diatas, sistem akan berinteraksi dengan database ketika administrator melakukan penambahan ataupun pengurangan dari pengguna

yang dapat mengakses program. Apabila terdapat pengguna yang sudah terdaftar dan ingin dihilangkan keberadaannya dari sistem, maka administrator akan menmerintahkan perintah hapus, dan otomatis pengguna tersebut tidak lagi mendapatkan akses menggunakan program (karena informasi login dan kunci pengenal kriptografinya sudah tidak ada). Begitu juga sebaliknya, jika ada seseorang yang belum memiliki akun dari login program, maka administrator dapat mendaftarkan seseorang tersebut dan mendapatkan informasi login sekaligus kunci pengenal dari pengguna tersebut.

Bentuk kode program adalah sebagai berikut :

```
# = = = = = = #
Encryption program start;
show "Login Page"{
waiting for "ID" and "password" input};
while input {
"ID" and "password" registered at database.db
then show "Main Page"
else show "silahkan hubungi admin"};
# = = = = = = #
while show "Main Page" , wait interaction {
if "Encryption html" is clicked then show "Encryption Page"
else if "Decryption.html" is clicked then show "Decryption page"
else if "user.data.db.html" is clicked then show "database page"
else if "password.html" is clicked then show "change password page"
```

else if "exit.html" is clicked then activate "terminate program"

else show "dashbord page"};

= = = = = =

Pada saat program dibuka pertama kali maka baris pertama pada program akan langsung diaktifkan. Selanjutnya program akan menunggu inputan yang akan dimasukkan oleh pengguna, apabila benar terdaftar maka program akan memunculkan halaman utama. Sebaliknya jika tidak terdatar maka silahkan menghubungi admin.

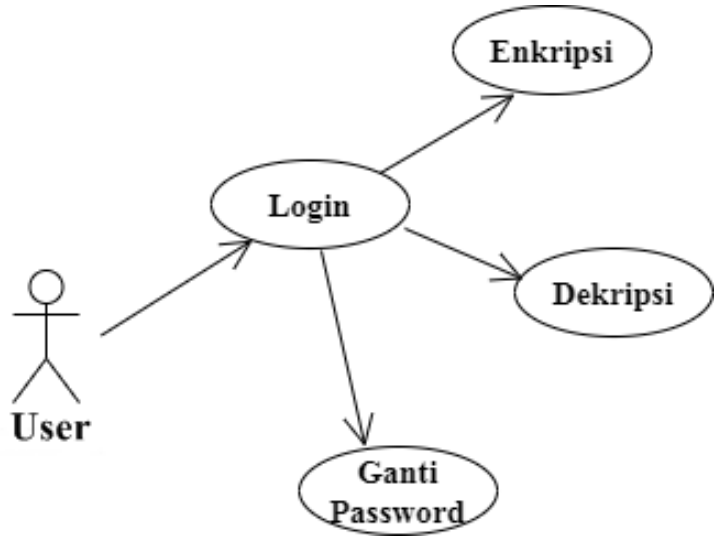
Saat memunculkan halaman menunggu interaksi selanjutnya, jika ingin melakukan enkripsi maka harus diklik tombol enkripsi lalu masukkan teks yang akan dienkripsi. Atau jika ingin melakukan dekripsi maka klik tombol dekripsi lalu akan muncul perintah untuk memasukkan teks yang sebelumnya di enkripsi. Apabila menekan tombol data member maka akan muncul penambahan data member, penghapusan data member, serta mereset *password*. Selanjutnya apabila mengklik tombol *password* maka akan muncul interaksi untuk merubah *password*. Jika mengklik tombol keluar maka akan mengarahkan pengguna untuk keluar dari program.

3.2.2 Pemodelan UML

1. Use Case Diagram

Use Case Diagram yang ada dalam sistem yang akan dibangun akan memiliki dua arah bentuk yang terjadi, yaitu dari sisi User dan sisi Administrator. Dalam sisi *user*, akan diisi oleh pemakai yang hanya bisa memanfaatkan konsep kriptografi yang disediakan oleh program yang dibuat. Dan pada sisi

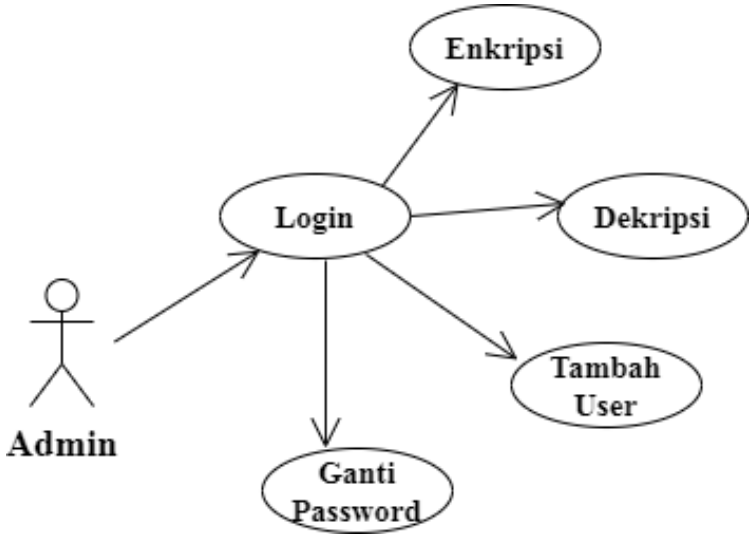
administrator, akan diisi oleh pemakai yang dipercayakan untuk melakukan monitoring dari pemakaian program yang dibuat.



Gambar 3.22 Pemodelan *Use Case* sisi *Client*/*User*

Sumber: Data olahan peneliti (2019)

Dari sisi *User* biasa, jenis operasi yang dapat dilakukan adalah melakukan enkripsi dan dekripsi. Alur yang diperlukan adalah setiap pengguna yang telah terdaftar sebelumnya, diminta untuk login terlebih dahulu (untuk mengetahui kepemilikan dari kunci spesial yang dimilikinya). Apabila telah berhasil masuk, maka sistem akan mulai membawa pengguna tersebut ke menu utama program, dan di menu utama itulah pengguna dapat mulai melakukan konversi *plainteks* menuju *ciphertext* (maupun sebaliknya), sesuai fungsi pembuatan sistem.



Gambar 3.23 Pemodelan *Use Case* sisi Administrator program

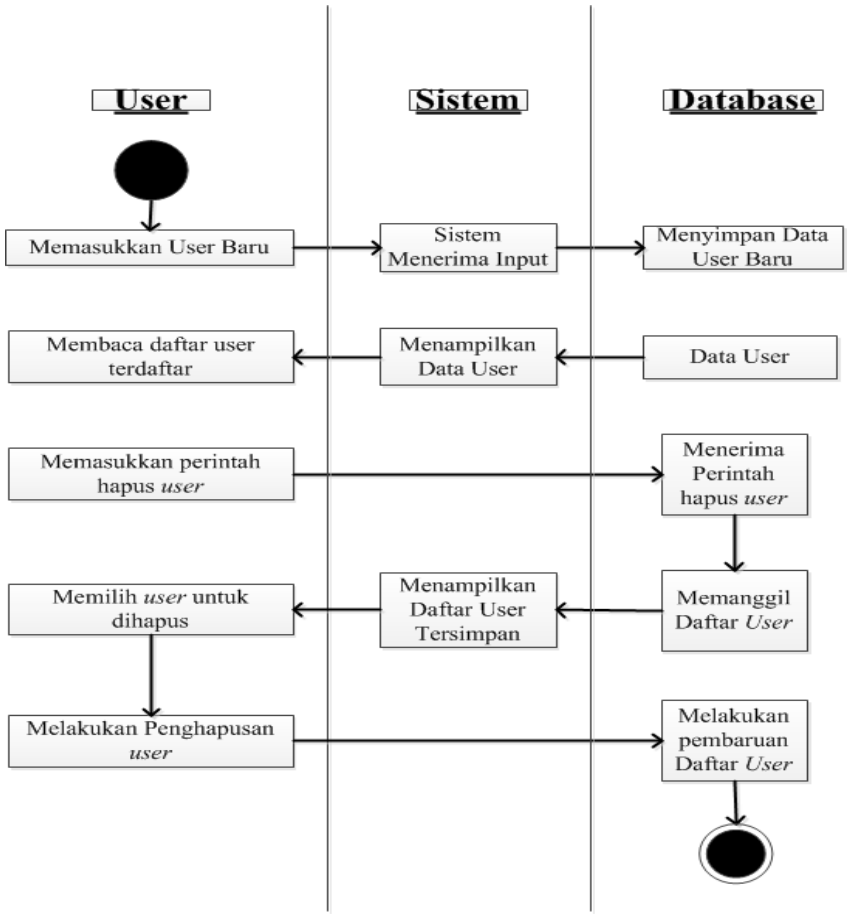
Sumber : Data olahan peneliti (2019)

Selanjutnya dari sisi administrator, ada fitur tambahan yang didapatkan selain dari fungsi enkripsi-dekripsi yang didapatkan pengguna biasa, yaitu melakukan update database program. Aktivitas update database merupakan kegiatan yang dapat dilakukan oleh administrator ketika sudah memasuki sistem dan menambahkan mengurangi jumlah dari pengguna biasa yang dapat melakukan akses terhadap program enkripsi yang dibuat. Hal ini akan membuat sistem lebih tertata rapi database nya dan juga meningkatkan segi keamanan dari program yang telah dibuat (karena database terus dilakukan pembaruan terhadap pengguna yang memiliki hak akses kepada program yang ada).

2. Activity Diagram

Activity diagram yang ada merupakan hasil dari perpanjangan penjelasan sistem *use case* dimana akan membahas lebih dalam dari segi sistem yang berorientasi dari aktivitas yang dapat dan akan dilakukan oleh pengguna program kriptografi ini. *Activity* diagram ini akan memaparkan kegiatan aktivitas antara

pengguna kriptografi, administrator program, sistem program, dan juga database yang ada.

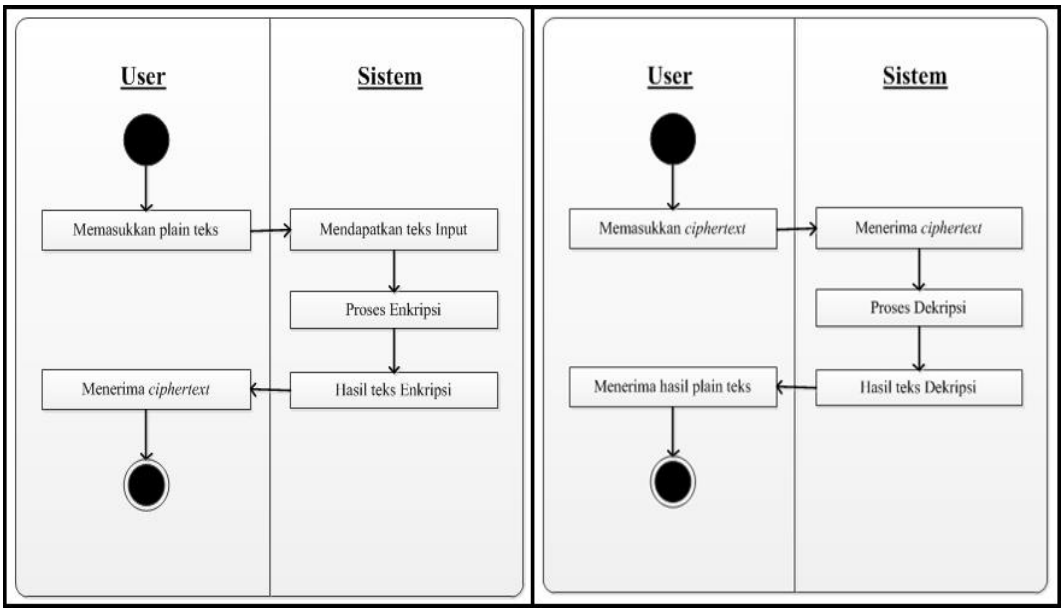


Gambar 3.24 Permodelan Diagram aktivitas dari segi *user* (Admin)

Sumber : Data Penelitian (2019)

Berdasarkan Gambar diatas dapat diketahui bahwa user (admin) berperan penting dalam melakukan penambahan user baru ke sistem kemudian akan menyimpan datanya didatabase. Selanjutnya pada saat user (admin) ingin melakukan penghapusan user yang sebelumnya yang sudah pernah disimpan didatabase, maka akan dilakukan dengan mengakses sistem dan mencari nama user yang akan dihapus kemudian masuk kedatabase user yang akan dihapus. Lalu

menampilkan data user yang sudah tersimpan sebelumnya memanggil data user yang ingin dihapus setelah itu melakukan pembaharuan data user.



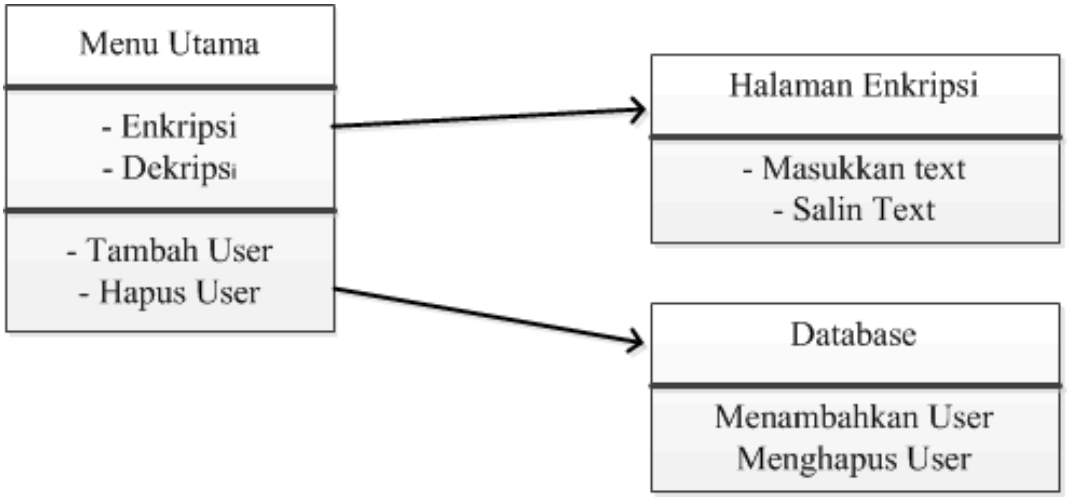
Gambar 3.25 Permodelan Diagram aktivitas dari segi *user* (Pemakai)

Sumber : Data penelitian (2019)

Seperti yang dapat dilihat diatas bahwa interaksi user dengan sistem dapat terjadi jika user ingin memasukan teks yang kemudian akan diinput lalu dilakukan proses enkripsi teks, selanjutnya akan diproses dari sistem yang akan menghasilkan output berupa *ciphertext*. Sebaliknya jika user ingin melakukan perubahan *ciphertext* ke teks yang asli, maka user diharuskan untuk memasukan teks yang masih berupa *ciphertext* lalu input dan dilakukan pen-dekripsi-an teks, dan akan diproses oleh sistem sehingga menghasilkan output berupa *Plaintext.* Hasil dari proses kegiatan ini serupa dengan gambar yang ada pada penjelasan *Use Case* sebelumnya.

3. Class Diagram

Dalam penggambaran model sistem berbentuk kelas dapat diberikan penggambarannya secara sederhana dari sudut pandang sistem yang ditemui oleh pengguna dan database yang mendukung sistem ketika dipergunakan oleh pengguna (User biasa-Admin). Dari segi sistem ketika dibuka akan memberikan tampilan login yang berhubungan dengan database (pengambilan informasi user login), dan ini bekerja pada tahap pembuka sistem.



Gambar 3.26 Pemodelan Diagram Kelas pada Sistem Program Enkripsi

Sumber : Data penelitian (2019)

Dapat dilihat pada gambar 3.26 diatas, setelah melakukan login maka pengguna akan disuguhkan dengan tampilan dari Menu Utama. Menu Utama sendiri memiliki satu tampilan yang Universal (ditemui oleh semua jenis pengguna yang login), yaitu proses melakukan kriptografi (Enkripsi-Dekripsi teks). Hal ini disebut dengan Halaman Enkripsi. Halaman Enkripsi dapat dilakukan aktivitas utama dari tujuan dibuatnya program, yaitu melakukan konversi *Plaintext* dan *Ciphertext* yang diperlukan saat ingin bertukar informasi.

Baik pengguna biasa, maupun Admin, nantinya bisa menggunakan fungsi ini, dan belum ada campur tangan database yang terjadi.

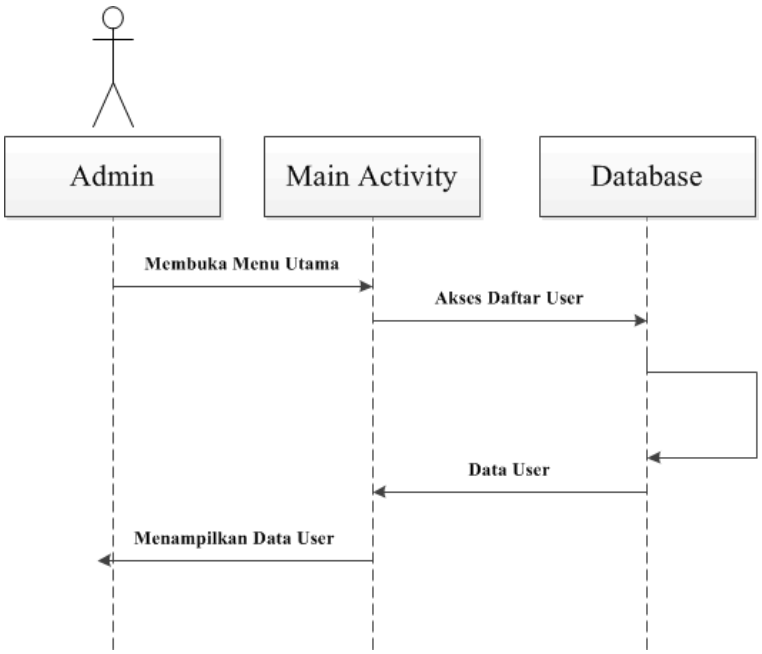
Selanjutnya adalah opsi khusus yang hanya ditemui/dimiliki oleh pengguna jenis Admin, yaitu manajerial pengguna (Menambah-Mengurangi user). Pada fungsi spesial ini, admin bertanggung jawab melakukan pemberian hak akses pada pengguna untuk bisa menggunakan program enkripsi, dan hal ini ditujukan untuk melengkapi segi keamanan dari program yang dibuat. Lebih spesifik pada aspek pelengkap keamanan yang dimaksud adalah admin akan bisa melakukan penambahan pada user yang diperkenankan menggunakan program (karyawan baru, pegawai magang, dsb) agar bisa memanfaatkan program enkripsi ketika mengakses jaringnan yang ada pada lokasi penelitian. Sehingga, keberadaan pengguna yang diterapkan melipatgandakan keamanan yang ditawarkan oleh program enkripsi.

Selanjutnya apabila seorang pengguna dinyatakan tidak lagi absah untuk menggunakan program enkripsi ini, maka admin akan bisa melakukan penghapusan atas pengguna yang sebelumnya terdaftar didalam database program. Hal ini akan mengindikasikan bahwa ada kewaspadaan yang dibangun dari segi admin agar bisa menjaga program enkripsi dari segi integritas, yaitu pemakai program hanyalah pihak yang dipercaya menggunakannya. Sebab apabila seorang pengguna yang telah terdaftar namun tidak aktif lagi sebagai instrumen yang melengkapi bagian di pihak lokasi penelitian (lembaga pendidikan swasta), terdapat ancaman laten berupa penyalahgunaan akun akses dari pengguna yang tidak aktif tadi dan melakukan intersepsi (pencegalan pesan ditengah jalan) atas

pesan terenkripsi, dan dilakukan pendekripsian secara ilegal oleh pihak yang tidak berwenang tersebut, karena memiliki hak akses pengguna yang sudah tidak lagi aktif sebelumnya (pegawai resign, pegawai magang yang selesai, dsb). Oleh karena itu, fitur dari penghapusan pengurangan pengguna yang ada di database dan bisa mengakses program enkripsi akan diawasi dan terus dilakukan pembaruan dari pihak pengguna baru-lamanya, agar program enkripsi yang dibuat dapat memaksimalkan aspek keamanan dari pertukaran informasi yang dilakukan pada lokasi penelitian yang dipilih.

4. Sequence Diagram

Berdasarkan pada gambar yang tercantum (lihat gambar 3.25), dapat dipahami bahwa dari segi program yang dibuat, ada komponen yang saling berinteraksi untuk bisa memenuhi permintaan yang dikeluarkan oleh pengguna (Biasa-Admin) ketika menggunakan program enkripsi yang dibuat. Dari segi pengguna Biasa, program melakukan pelayanan pada pengguna hingga tingkat User (awal) hingga Sistem umum (*Main Activity*- Enkripsi/Dekripsi). Ini adalah fungsi utama yang dimiliki oleh program enkripsi dan batas akhir dari hak akses yang didapatkan oleh pengguna biasa ketika menggunakan program enkripsi ini. Akan tetapi, dari segi pengguna Admin, program akan lebih jauh lagi proses kerjanya karena bisa sampai memasuki/melakukan pengubahan database yang ada pada program (Tambah hapus). Pengguna biasa memang terintegrasi dengan database, tapi ditingkat *read-only* (membaca pengguna yang terdaftar), sedangkan dari pihak pengguna Admin, mampu melakukan *Read-Write* pada database yang dimiliki oleh sistem dari program enkripsi yang dirancang pada penelitian ini.



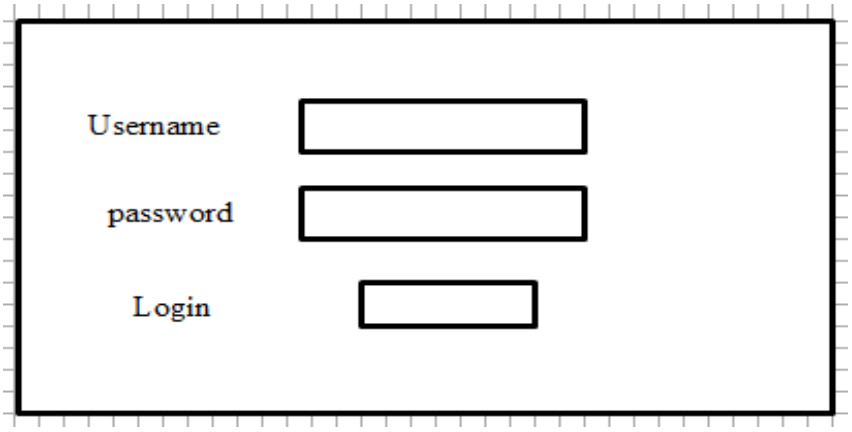
Gambar 3.27 Pemodelan Diagram *Sequence* Program Enkripsi

Sumber : Data Penelitian (2019)

3.2.3 Rancangan Sistem

Pada sebuah perancangan sistem, diperlukan beberapa komponen/instrumen yang dimanfaatkan oleh peneliti untuk bisa mensukseskan perencanaan yang dibuat menjadi sebuah produk/output jadi (dalam penelitian ini berupa program enkripsi). Dan dalam proses pembuatannya, peneliti akan memanfaatkan beberapa komponen ini dan akan dijabarkan secara eksplisit atas komponen tersebut berdasarkan fungsi dan keberadaannya, kemudian dilanjutkan dengan perencanaan yang dilakukan (tahap perancangan) agar dilihat kesinambungan atas komponen yang dipakai terhadap hasil program yang dibuat. Adapun spesifikasi rancangan sistem yang akan dipaparkan ini meliputi atas Perangkat perancangan program dan Integrasi Program pendukung yang dipakai.

1. Form login

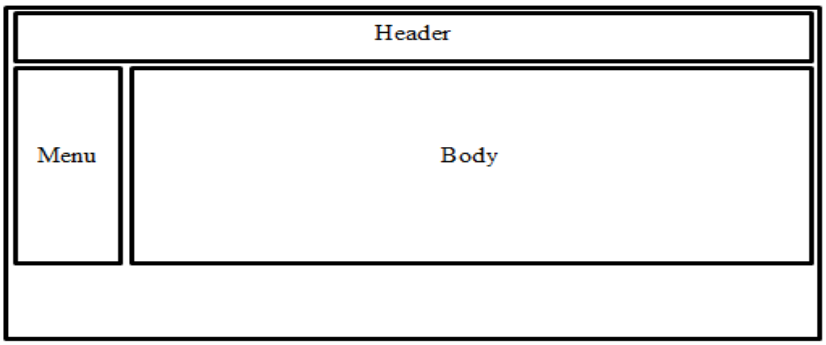


Gambar 3.28 Sketsa login

Sumber : Data Penelitian (2019)

Pada tampilan diatas memiliki komponen yang dapat diinteraksikan dengan pengguna seperti memasukkan user name dan password kemudian mengklik tombol login maka akan menu selanjutnya yaitu dasboard.

2. Form Dasboard

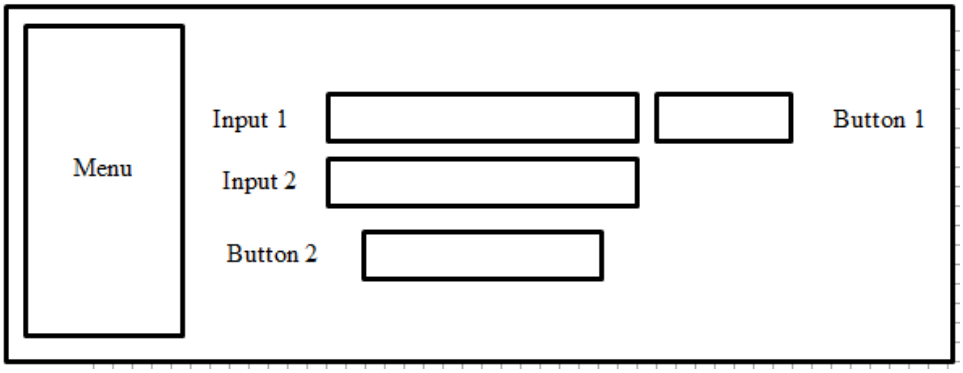


Gambar 3.29 Sketsa dasboard

Sumber : Data Penelitian (2019)

Pada tampilan diatas memiliki komponen yang dapat diinteraksikan dengan pengguna seperti bagian header serta fungsi di bagian menu tidak lupa juga dengan body yang mempunyai informasi bagaimana cara dalam penggunaan.

3. Form Enkripsi

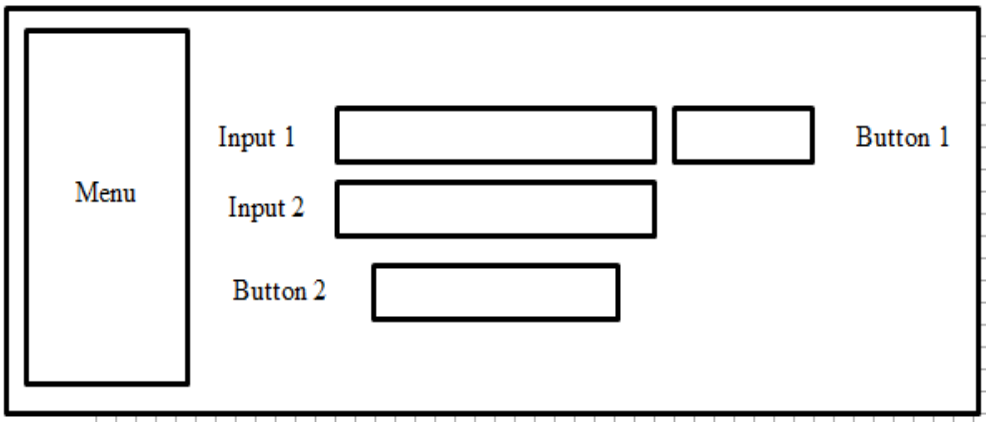


Gambar 3.30 Form enkripsi

Sumber : data penelitian (2019)

Pada tampilan diatas memiliki komponen yang dapat diinteraksikan dengan pengguna seperti bagian input 1 untuk memasukan kata kunci serta pada kotak yang ada dibawahnya merupakan teks yang akan di enkripsi. Pada bagian button 1 ialah syarat agar kata kuncinya bekerja dengan seharusnya, sedangkan button 2 akan mengarahkan hasil dari semua proses. serta fungsi di bagian menu merupakan bagian fitur yang ingin dipakai.

4. Form Dekripsi



Gambar 3. 31 Form Dekripsi

data penelitian (2019)

Pada tampilan diatas memiliki komponen yang dapat diinteraksikan dengan pengguna seperti bagian input 1 untuk memasukan kata kunci serta pada kotak yang ada dibawahnya merupakan teks yang akan di enkripsi. Pada bagian button 1 ialah syarat agar kata kuncinya bekerja dengan seharusnya, sedangkan button 2 akan mengarahkan hasil dari semua proses. serta fungsi di bagian menu merupakan bagian fitur yang ingin dipakai.

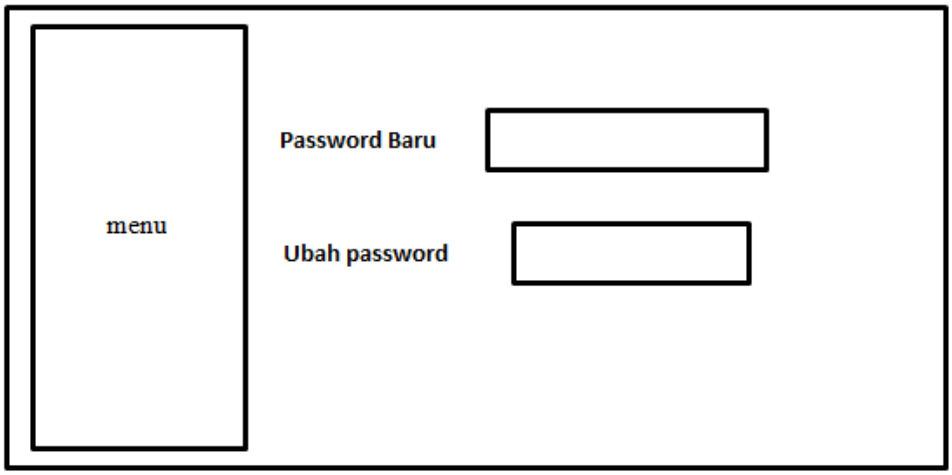
5. Form pengiriman Pesan

Gambar 3.32 tampilan form pengiriman pesan

Sumber : data penelitian (2019)

Pada tampilan diatas memiliki komponen yang dapat diinteraksikan dengan pengguna seperti bagian pada fitur menu pengiriman pesan untuk melakukan pengiriman pesan lewat whatsapp web.

6. Form Ubah Password

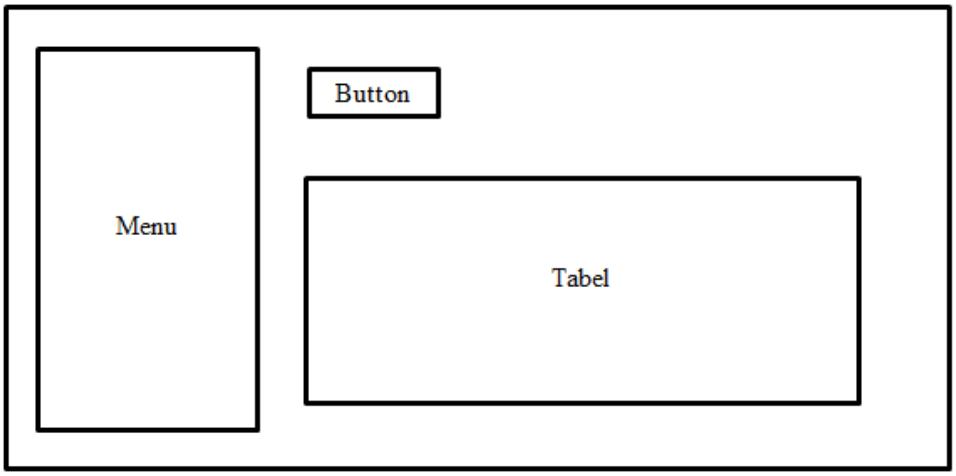


Gambar 3. 33 Form ubah password

Sumber : data penelitian (2019)

Pada tampilan diatas memiliki komponen yang dapat diinteraksikan dengan pengguna seperti bagian pada form menu ubah password untuk melakukan pergantian password.

7. Form Akses Data Member



Gambar 3. 34 Form akses data member

Sumber : data penelitian (2019)

Pada tampilan diatas memiliki komponen yang dapat diinteraksikan dengan pengguna seperti bagian pada form menu akses data member yang didalamnya terdapat tabel yang berisi bagaimana cara menambahkan member baru atau menghapus member lama.

Pada Perancangan Program Enkripsi yang dibangun, memanfaatkan sebuah portable desktop (*Notebook*) yang dimiliki oleh peneliti. Adapun spesifikasi dari *Notebook* yang dipergunakan untuk merancang sistem adalah sebagai berikut.

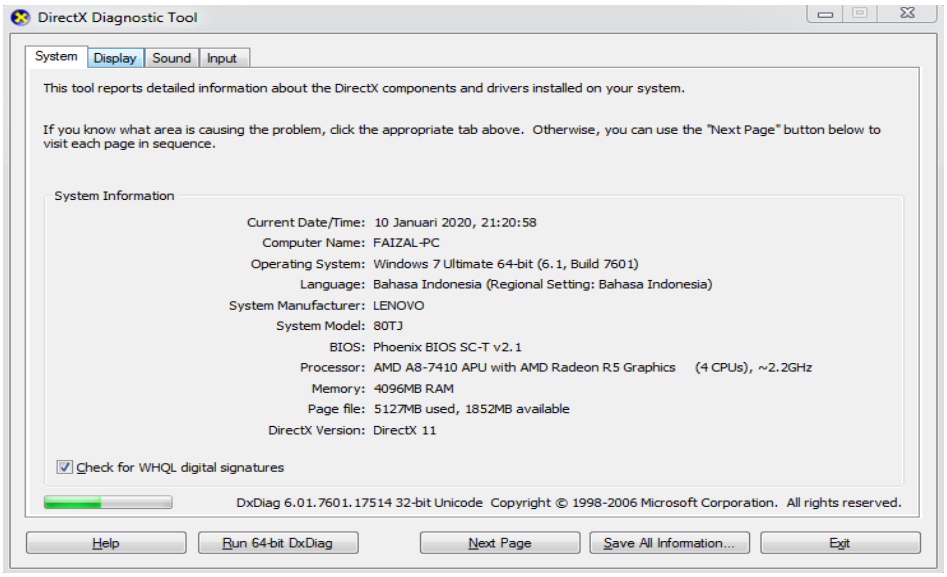
Tabel 3.5 Spesifikasi *Notebook* yang dipakai

No	Spesifikasi	Deskripsi
1	AMD APU A8-7410 quad-core 2,2GHz Turbo 2,5Ghz	Processsor (AMD)
2	AMD Radeon R5 (Intergrated Graphic APU)	VGA (AMD)
3	4GB DDR3L (Single Channel Memory)	RAM
4	Samsung 1TB 5400rpm HDD Drive	Storage
5	TFT LCD (LED backlight) 15,6” (1366 x 768 aspect ratio)	Monitor
6	Windows 7 Ultimate Service Pack 1 (64-bit)	Operating System

Sumber: Data Penelitian (2019)

Dapat dilihat diatas, bahwa spesifikasi dari *Notebook* yang dipakai merupakan sebuah perangkat yang memiliki dapur pacu yang mumpuni untuk melakukan perancangan program *(Quad Core Processo*r). Dan dalam proses perancangan program, kebutuhan kinerja grafis dapat dikatakan cukup minimal dikarenakan program yang dibuat berorientasi pada penerapan algoritma terhadap sebuah program yang bersifat solutif terhadap permasalahan yang ditemui (mengamankan pesan teks dengan kriptografi). Agar lebih leluasa dalam proses perancangan program, kebutuhan dari memori akses yang dimiliki oleh *Notebook* tergolong dalam spesifikasi standar yang dipergunakan pada masanya (4GB Ram), dan

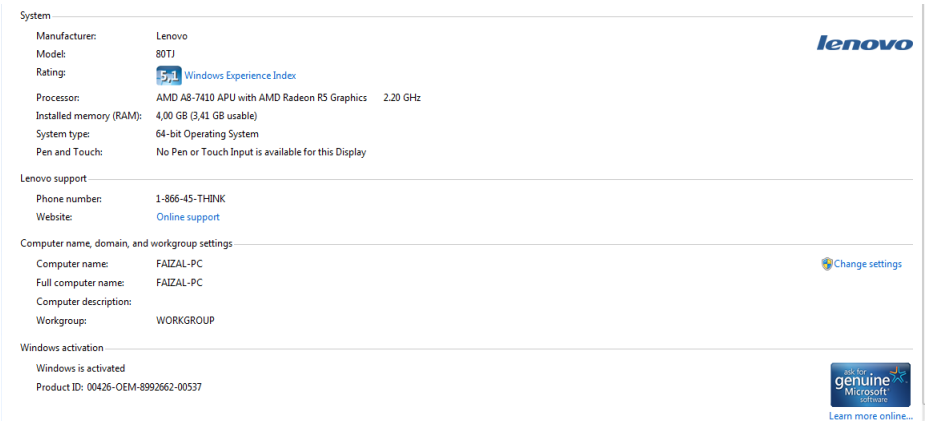
kapasitas yang dimiliki untuk menampung semua komponen pendukung program enkripsi dapat ditampung dengan baik dengan adanya media penyimpanan yang memadai (1TB Storage).



Gambar 3.35 Spesifikasi sistem yang dipergunakan

Sumber: data penelitian (2019)

Dari segi sistem operasi, Notebook menggunakan OS *Windows 7 Ultimate* edisi *service pack* 1 yang sudah memiliki pengembangan segi stabilitas tinggi karena telah mengalami banyak pembaruan sistem terhitung diluncurkan hingga proses perancangan ini dilakukan (2019). Dengan kompatibilitas dan stabilitas yang tinggi atas sistem operasi dan program yang dipergunakan, menjadikan *Notebook* yang digunakan memberikan kenyamanan bagi peneliti sebagai pemrogram sistem enkripsi untuk bisa mengefektifitaskan waktu yang dimiliki dalam mengeksekusi perencanaan realisasi perancangan yang akan dilakukan.

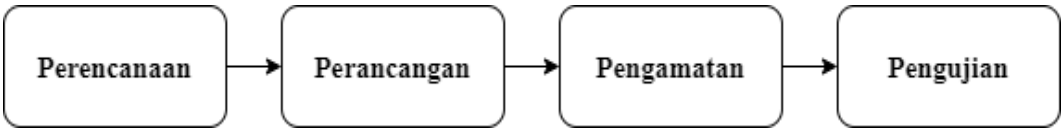


Gambar 3.36 Spesifikasi sistem yang dipergunakan

Sumber: data penelitian (2019)

3.3 Desain Sistem

Desain Sistem dapat juga berisi atas penjabaran atas tahapan dari perancangan sistem yang akan dilakukan pada proses pembuatan program enkripsi dari awal pembuatan program, langkah yang dilakukan dalam perencanaan, pemilihan debug sistem yang ada pada program, dan ditutup dengan pengujian program yang telah dibuat.



Gambar 3.37 Tahapan Perancangan Sistem yang dibangun

Sumber: data penelitian (2019)

Dapat dilihat dari gambar diatas, desain sistem akan dibuat pertama kali akan dirumuskan perencanaannya. Dalam perencanaan, peneliti memilih sebuah siklus pembuatan program yang populer, yaitu metode *waterfall* (air terjun *linie*r). Dalam proses ini, sistem akan dibangun atas beberapa pertimbangan, yaitu analisis kebutuhan program, perancangan program, penerapan atas komponen inti

program (dalam penelitian ini berupa algoritma TTVC), dilanjutkan dengan melakukan pengetesan program (debug berorientasi *blackbox testing*), dan ditutup dengan perawatan hasil program yang dibuat (sentuhan terakhir atas program purwarupa menuju program paripurna).

Selanjutnya setelah merumuskan perencanaan program, maka masuklah tahap perancangan program yang dibuat menggunakan instrumen perangkat yang telah dijabarkan sebelumnya (*Notebook*). Pada proses ini, semua *software* pendukung akan saling diintegrasikan secara silang dan akan mengintegrasi satu sama lain sehingga sebuah program enkripsi yang dibangun dapat berhasil dibuat dan sesuai dengan kebutuhan yang diperlukan. Pada tahapan ini peneliti akan berfokus pada implementasi algoritma TTVC kedalam program yang berbasis web, dan dapat diakses sesuai dengan perencanaan yang dilakukan sebelumnya.

Setelah proses perancangan yang dilakukan selesai, maka masuklah pada proses pengetesan yang memilih metode berbentuk *Blackbox Testing*. *Blackbox Testing* adalah sebuah metode pengetesan atas sistem/program dengan orientasi pengamatan ada pada struktural internal program (coding), desain, dan fungsional yang dimiliki program/sistem, dan dicocokan pada hasil program yang telah dibuat. apabila ditemui perbedaan atas fungsional perencanaan dengan fungsional hasil yang dibangun, maka akan dilakukan revisi atas rancangan tersebut. Dan apabila telah memasuki tahap dimana perencanaan aspek diatas telah identik dengan hasil program/sistem yang dibuat, maka program telah siap untuk diluncurkan.

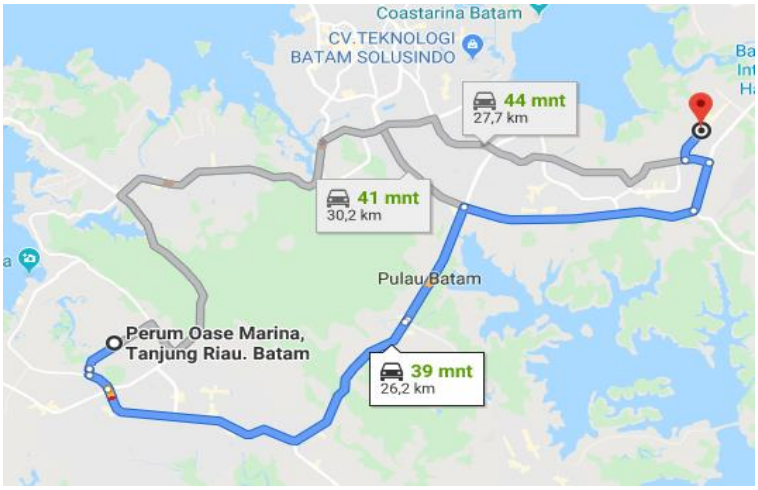
Hasil dari program yang diluncurkan (program enkripsi) pada penelitian ini nantinya akan dilanjutkan dengan tahapan terakhir yaitu pengujian sederhana dari program enkripsi yang dibuat terhadap efektivitas yang dimilikinya. Proses ini bertujuan untuk melakukan demonstrasi dan pengamatan terkait algortma yang dimiliki dalam mengamankan pesan teks pada masa ini. Pengujian akan menggunakan aplikasi penetrasi (*Pentest*) berbasis online, dan hasilnya akan disuguhkan dalam laporan hasil akhir penelitian yang dilakukan.

3.4 Lokasi dan Jadwal Penelitian

Dalam sebuah penelitian yang dilakukan, diperlukan sebuah perencanaan prosesi pelaksanaan penelitian beserta dengan penjelasan terkait lokasi spesifik dilakukannya penelitian. Hal ini dimaksudkan untuk membuat sebuah penelitian lebih dapat terarah pelaksanaannya dan diketahui lokasi yang dipilih.

3.4.1 Lokasi Penelitian

Lokasi penelitian merupakan sebuah tempat berbasis geografis tertentu yang terpilih untuk dijadikan tempat penelitian berlangsung. Adapun lokasi yang dipilih untuk penelitian ini beralamat di Ruko *Hollywood Hill* blok *Jackie Chan* no. 9e-9f.



Gambar 3. 38 Lokasi Penelitian yang dilakukan

Sumber: *maps.google.com*

3.4.2 Jadwal Penelitian

Jadwal penelitian adalah proses rencana dari pelaksanaan sebuah penelitian, dimulai dari awal menempuh pembuatannya hingga selesai dengan rincian dari jadwal yang ditentukan, yaitu:

Tabel 3.6 Jadwal Penelitian

No	Kegiatan	Oktober-19	November-19	Desember-19	Januari-20
1	Pengumpulan Data	2,8,13-19			
2	Pembuatan Skripsi	1-31	1-30	1-20	1-28
3	Bimbingan Penulisan	5,12,19,26	2,9,30	7,14	4,11,18,25
4	Pembuatan Program	1-31			
5	Pengujian Program	24-31			
6	Pengumpulan Skripsi				28

Sumber Tabel: data penelitian (2019)