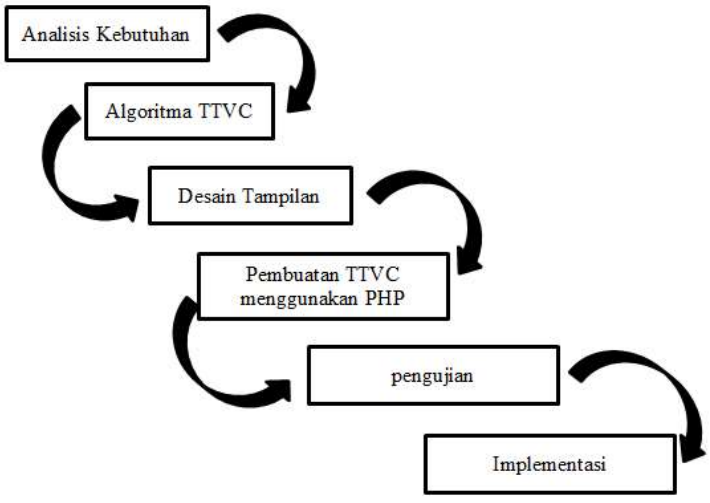
BAB III

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

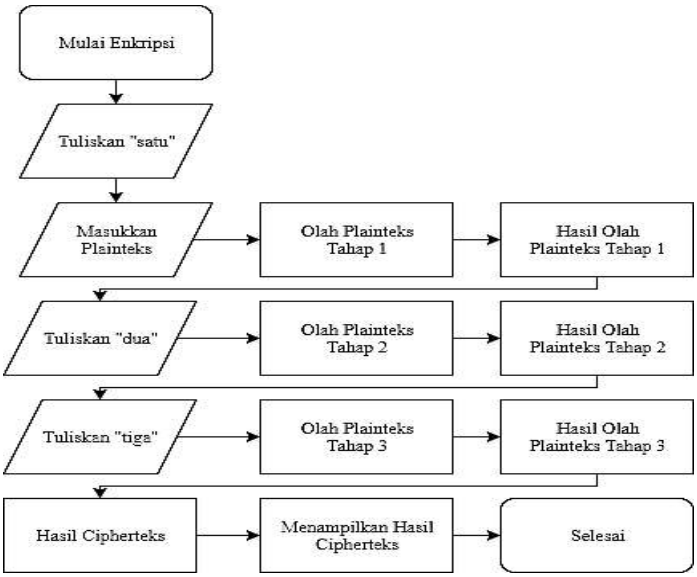
Perancangan dari sistem merupakan tahapan dari pemberian ilustrasi atas sistem yang akan dibuat beserta dengan bentuk perencanaan yang akan dieksekusi saat kegiatan membangun sistemnya (aplikasi enkripsi). Pada sub-bab ini akan dipaparkan terkait algoritma yang akan dipergunakan, pemodelan UML yang akan 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.



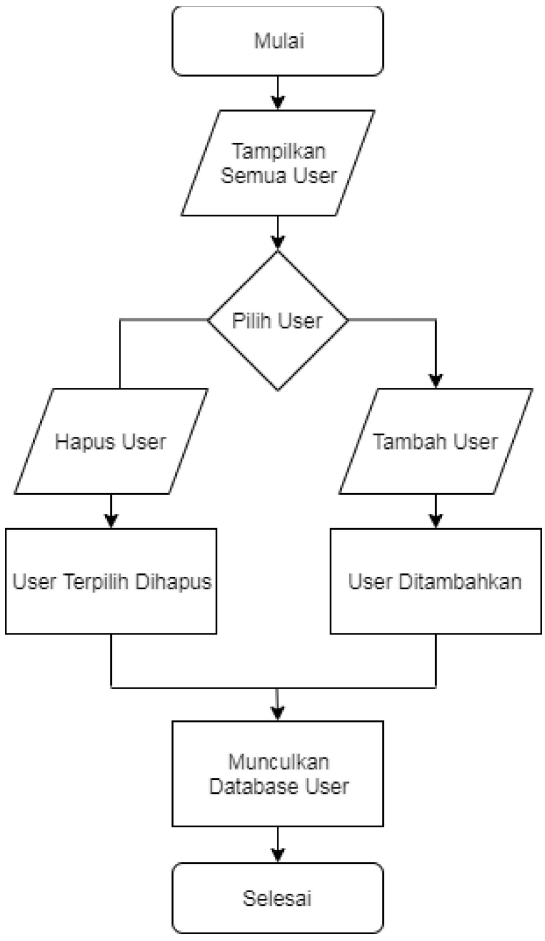
Gambar 3.20 Flowchart algoritma TTVC yang akan diimplementasikan

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.

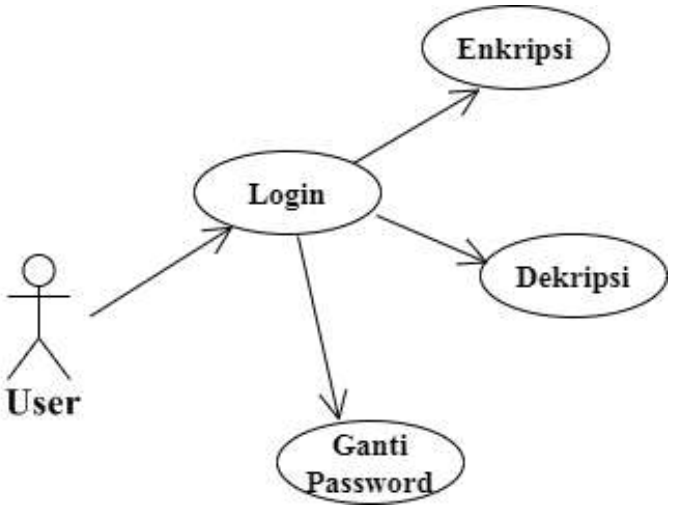
Saat memunculkan halaman menunggu interaksi selanjutnya, jika ingin melakukan enkripsi maka harus diklik tombol enkripsi lalu masukkan teks yang akan dienkripsi. Atau jika ingin melakukan dekripsi maka klik tombol dekripsi lalu akan muncul perintah untuk memasukkan teks yang sebelumnya di enkripsi. Apabila 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

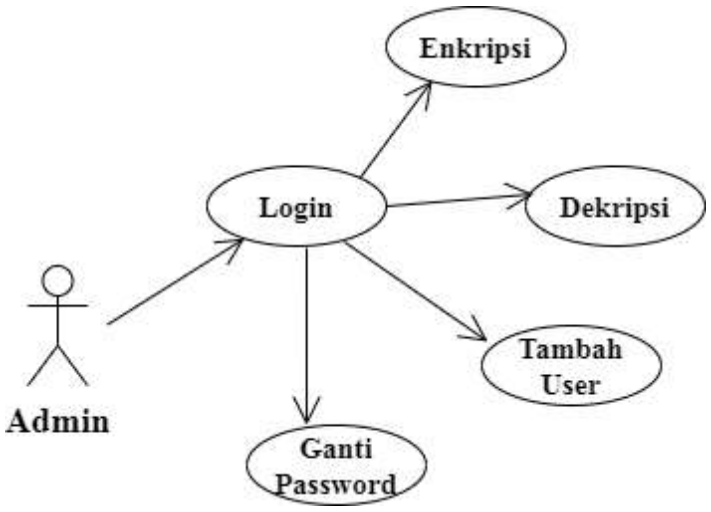
administrator, akan diisi oleh pemakai yang dipercayakan untuk melakukan monitoring dari pemakaian program yang dibuat.



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

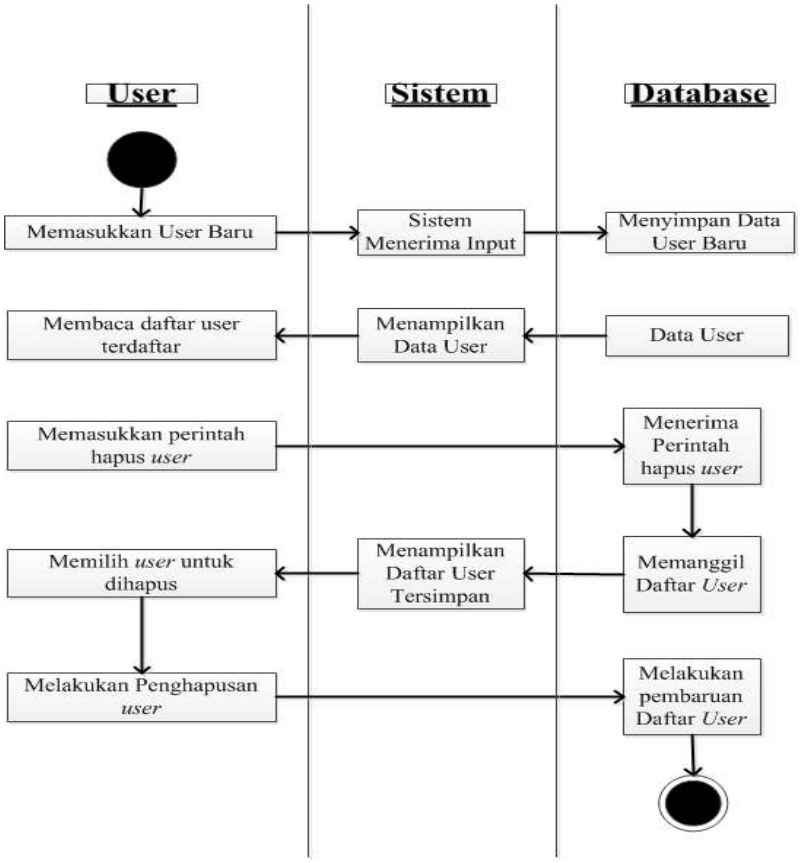
Sumber : Data olahan peneliti (2019)

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.

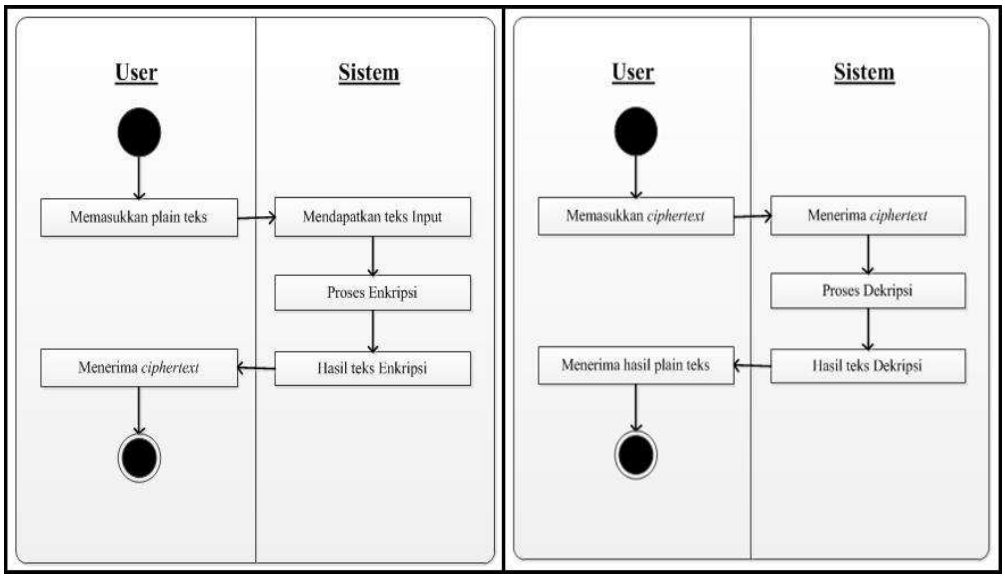


Gambar 3.24 Permodelan Diagram aktivitas dari segi *user* (Admin)

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.



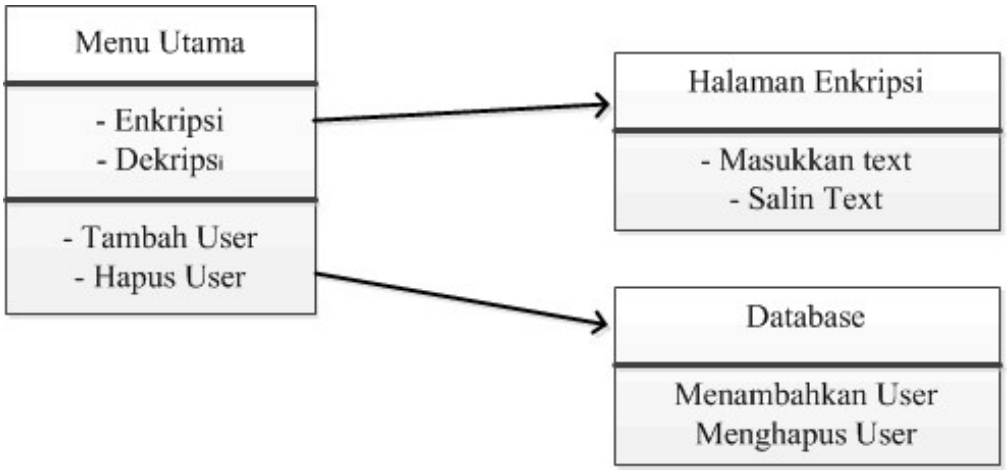
Gambar 3.25 Permodelan Diagram aktivitas dari segi *user* (Pemakai)

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.

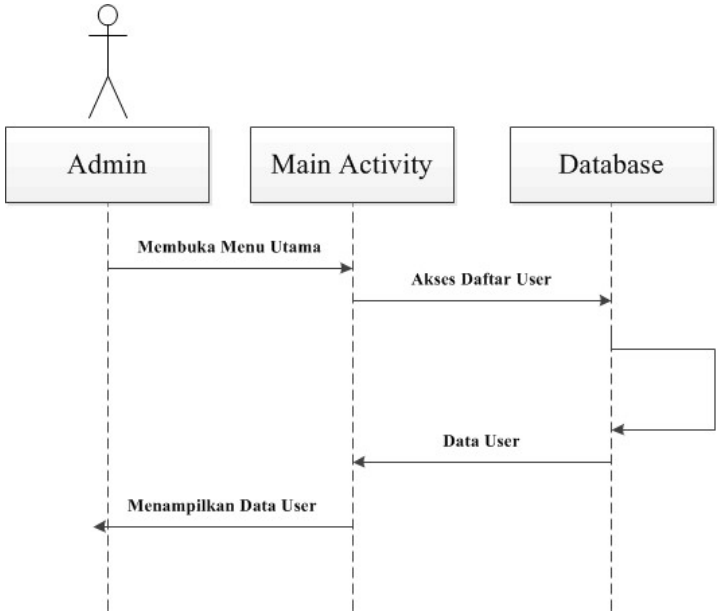
Selanjutnya adalah opsi khusus yang hanya ditemui/dimiliki oleh pengguna jenis Admin, yaitu manajerial pengguna (Menambah-Mengurangi user). Pada fungsi spesial ini, admin bertanggung jawab melakukan pemberian hak akses pada pengguna untuk bisa menggunakan program enkripsi, dan hal ini ditujukan untuk 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.



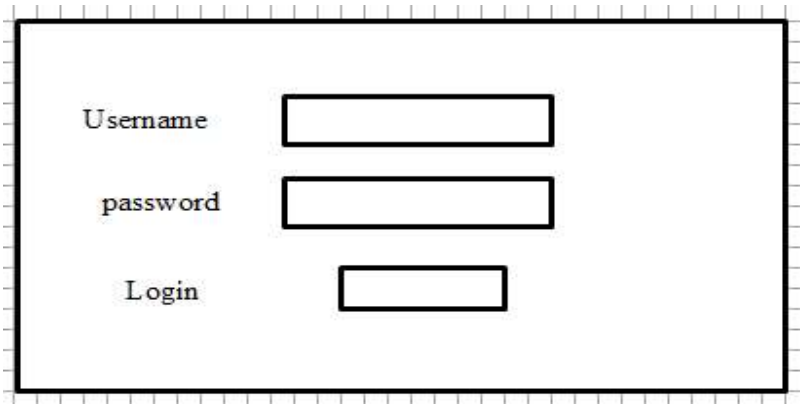
Gambar 3.27 Pemodelan Diagram *Sequence* Program Enkripsi

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

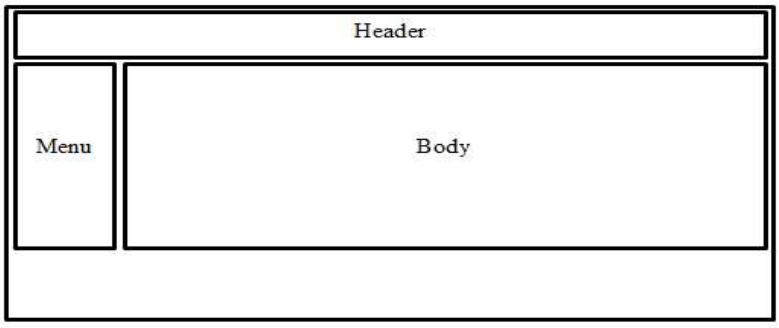


Gambar 3.28 Sketsa login

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

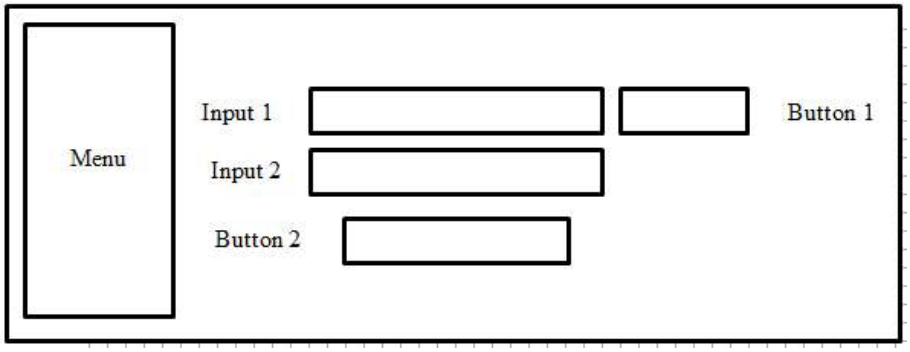


Gambar 3.29 Sketsa dasboard

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

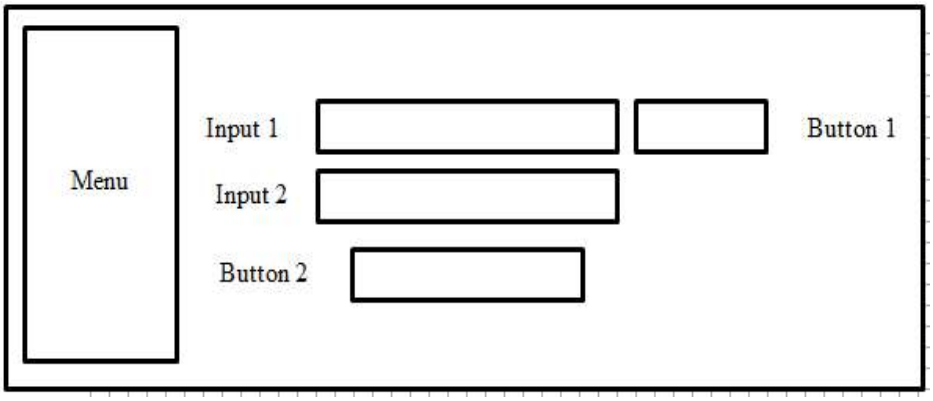


Gambar 3.30 Form enkripsi

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

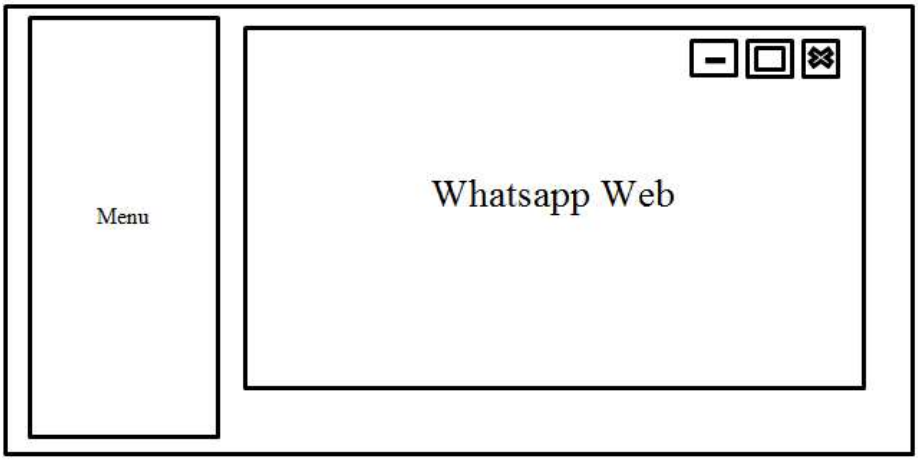


Gambar 3. 31 Form Dekripsi

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

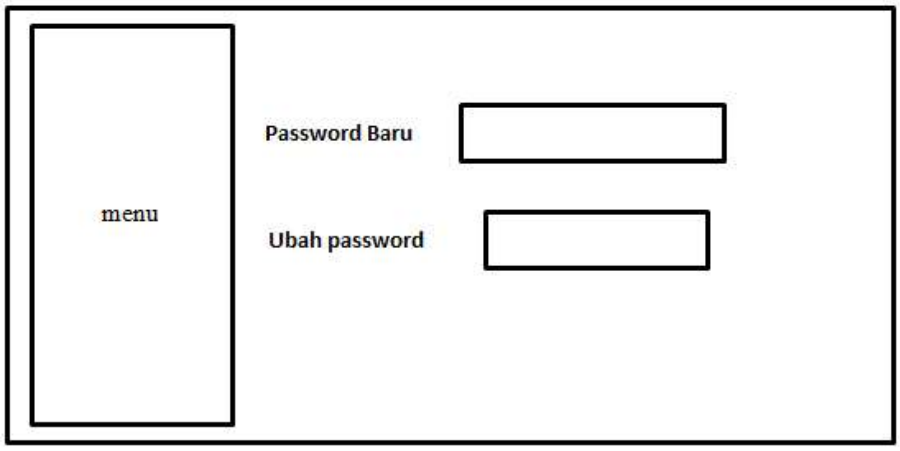


Gambar 3.32 tampilan form pengiriman pesan

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

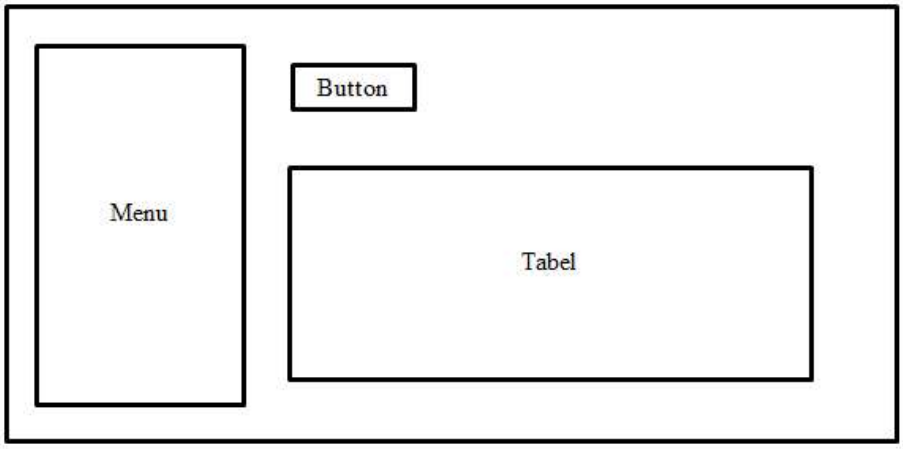


Gambar 3. 33 Form ubah password

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.

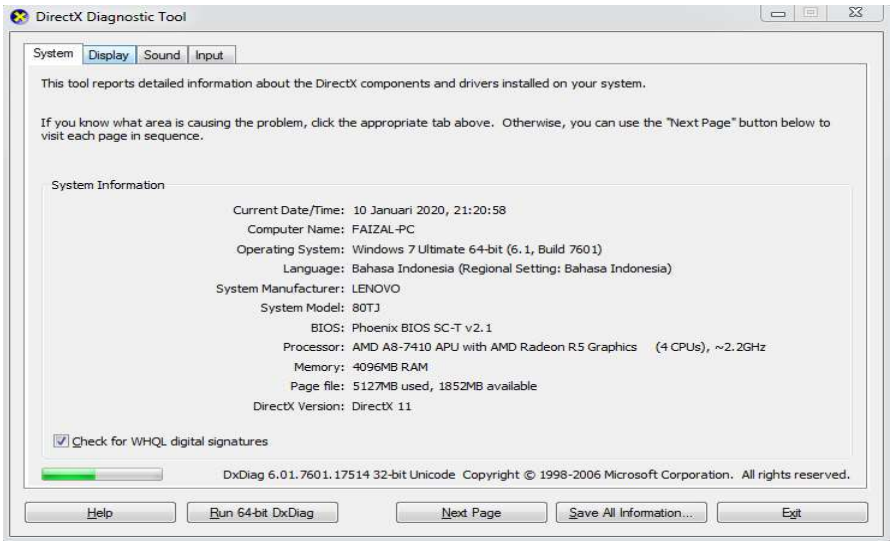
Tabel 3.5 Spesifikasi *Notebook* yang dipakai

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

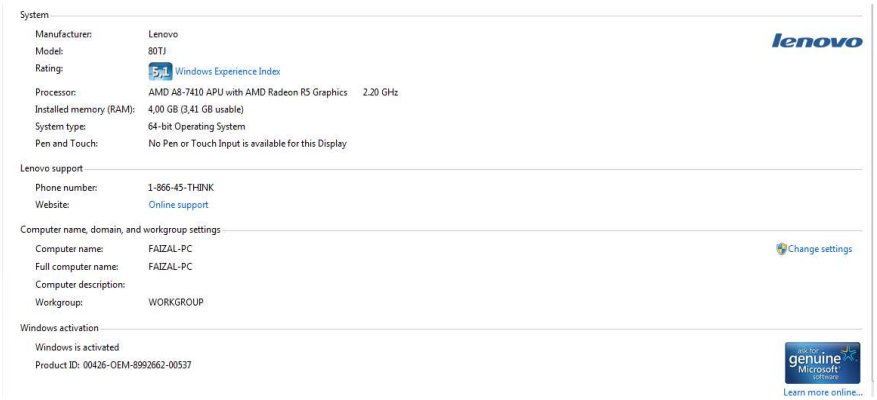
kapasitas yang dimiliki untuk menampung semua komponen pendukung program enkripsi dapat ditampung dengan baik dengan adanya media penyimpanan yang memadai (1TB Storage).



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.

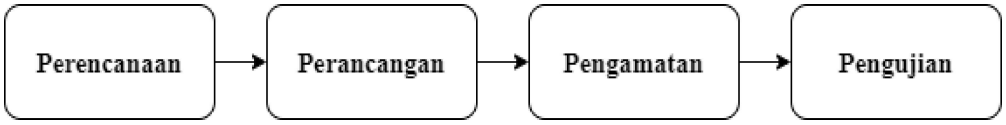


Gambar 3.36 Spesifikasi sistem yang dipergunakan

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.

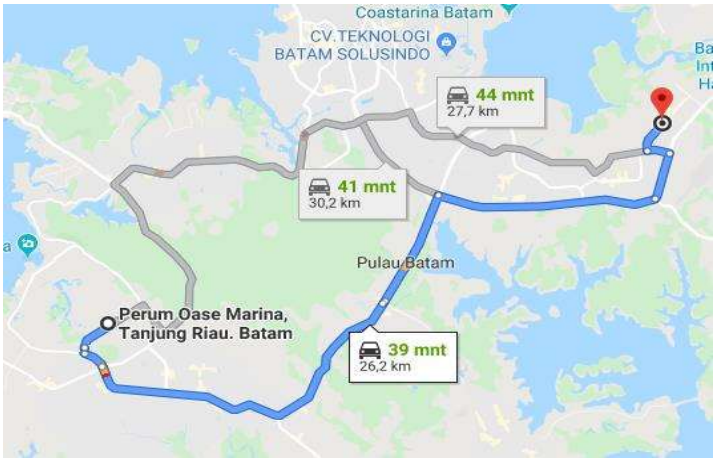
Hasil dari program yang diluncurkan (program enkripsi) pada penelitian ini nantinya akan dilanjutkan dengan tahapan terakhir yaitu pengujian sederhana dari program enkripsi yang dibuat terhadap efektivitas yang dimilikinya. Proses ini bertujuan untuk melakukan demonstrasi dan pengamatan terkait algortma 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)