BAB III

ANALISIS MASALAH DAN RANCANGAN PROGRAM

III.1. Analisis Masalah

Proses analisa sistem merupakan langkah kedua pada pengembangan sistem. Analisa sistem dilakukan untuk memahami informasi-informasi yang didapat dan dikeluarkan oleh sistem itu sendiri. Saat ini sistem komputer yang terpasang makin mudah diakses, Sistem *time sharing* dan akses jarak jauh menyebabkan masalah keamanan menjadi salah satu kelemahan komunikasi data. Dalam era konektifitas elektronik universal sering terdapat gangguan berupa *hacker*, virus, penipuan elektronik maupun mendengar diam-diam secara elektronik. Oleh karena itu keamanan data benar-benar menjadi permasalahan yang sangat penting, sehingga diperlukan sistem tingkat keamanan yang dapat terjamin dan bisa terhindar dari serangan (*attack*).

Untuk mengamankan data, diperlukan kriptografi dengan metode enkripsi. Enkripsi merupakan salah satu cara yang dilakukan untuk mengamankan data dari hal yang akan menyebabkan aspek-aspek diatas tidak terpenuhi, seperti untuk menjaga keamanan dan integritas data.

Salah satu teknologi metode enkripsi data yang digunakan adalah kriptografi simetris RC-5 (*Rivest Code* 5), sehingga keamanan dan kerahasiaan data dapat terjaga saat melakukan komunikasi dan pertukaran data tidak dapat disadap pihak yang tidak berkepentingan.

III.2. Evaluasi Sistem Yang Berjalan

Sistem pemberian pengamanan data saat ini seperti pemberian *password* pada aplikasi *office* sudah aman tetapi masih dapat di bobol *password* tersebut. Kelemahan dari sistem ini adalah data aslinya tidak berbentuk kode-kode simbol yang tidak dimengerti seseorang jika data tersebut diketahui sandi passwordnya maka data aslinya dapat dibaca dan disalahgunakan orang yang tidak bertanggung jawab, apabila data sudah diketahui dapat merusak tujuan dari surat tersebut.

Maka solusi yang penulis buat untuk mengatasi masalah tersebut adalah membuat suatu sistem *enkripsi* yang berupa data untuk merubah isi data aslinya agar makna dari data aslinya tidak dapat diketahui oleh pihak yang tidak berkepentingan.

III.3. Strategi Pemecahan Masalah

Adapun strategi pemecahan masalah dari sistem *enkripsi* data yang dirancang adalah sebagai berikut :

1. Data yang dibuat didalam sebuah *file* itu sangat penting dan rahasia, apabila data tersebut dicuri orang lain maka data tersebut bisa di salah gunakan, daripada itu perlu dibuat *enkripsi* dalam mengamankan data dengan menggunakan metode RC5.
2. Agar data tersebut aman dari kerusakan perangkat keras maka data tersebut harus dipindahkan ke lokasi yang lebih aman misalnya di *flashdisk*, adapun teknologi yang digunakan dalam mengamankan data ini menggunakan teknologi simetris algoritma 16 Bit.

III.4. Analisa Kebutuhan *Hardware* Dan *Software*

Kebutuhan non fungsional menjabarkan apa-apa saja yang harus dimiliki oleh sistem agar dapat berjalan. Analisis kebutuhan non fungsional bertujuan untuk mengetahui sistem seperti apa yang cocok diterapkan, perangkat keras dan perangkat lunak apa saja yang dibutuhkan serta siapa saja pengguna yang akan menggunakan sistem ini.

1. Aspek Perangkat Keras

Perangkat keras adalah semua bagian fisik komputer dan dibedakan dengan data yang berada di dalamnya atau yang beroperasi di dalamnya, dan dibedakan dengan perangkat lunak yang menyediakan instruksi untuk perangkat keras dalam menyelesaikan tugasnya.

Adapun kebutuhan *hardware* untuk menciptakan aplikasi atau perangkat lunak keamanan data tersebut terdiri dari :

a. *Prosesor Intel Core I3*
b. *Harddisk*
c. *Memory RAM 2 GB*,
d. *Monitor 15* dan *Keyboard dan Mouse*.

2. Aspek Perangkat Lunak (*software*)

Perangkat lunak adalah program yang digunakan untuk menjalankan perangkat keras. Tanpa adanya perangkat lunak ini komponen perangkat keras tidak dapat berfungsi, adapun aplikasi dan *software* yang digunakan dalam pembuatan keamanan data tersebut terdiri dari sistem operasi windows 7, aplikasi visual studio 2010.

III.5. Penerapan Metode RC5

Algoritma enkripsi RC5 didesain oleh Profesor Ronald Rivest dan pertama kali dipublikasikan pada Desember 1994. Sejak publikasinya RC5 telah menarik perhatian banyak peneliti dalam bidang kriptografi dalam rangka menguji tingkat keamanan yang ditawarkan oleh algoritma RC5 (*RSA Laboratory Technical Report TR-602*).

Parameter-parameter yang digunakan dalam RC-5 adalah sebagai berikut :

1. Jumlah putaran ini disimbolkan dengan *r* yang merupakan parameter untuk rotasi dengan nilai 0, 1, 2, …… 255.
2. Jumlah *word* dalam bit disimbolkan dengan *w*. Nilai bit yang di *support* adalah 16 bit, 32 bit, dan 64 bit.
3. Kata kunci (*key word*) Variable ini disimbolkan dengan *b* dengan range 0, 1, 2, …. 255. *Key word* ini dikembangkan menjadi *array S* yang digunakan sebagai *key* pada proses untuk enkripsi dan dekripsi.

Untuk memahami cara kerja RC-5, dapat dimulai dengan melihat konsep dasar bagaimana RC-5 ini bekerja. RC-5 Menggunakan operasi dasar untuk proses enkripsi sebagai berikut :

1. Data yang akan dienkripsi dikembangkan menjadi 2 bagian bagian kiri dan bagian kanan dan dilakukan penjumlahan dengan *key word* yang yang telah diekspansi sebelumnya. Penjumlahan ditunjukan dengan tanda ``+``, dan disimpan di dua register A dan register B.
2. Kemudian dilakukan operasi EX-OR, yang ditandai dengan tanda ``⊕``.

3. Melakukan rotasi kekiri (*shift left*) sepanjang *y* terhadap *x word* yang ditandai dengan *x<<< y*. *y* merupakan interpretasi *modulo w* atau jumlah kata *w* dibagi 2. Dengan *lg[w]* ditentukan jumlah putaran yang dilakukan.
4. Tahap akhir dilakukan penggabungan untuk mendapatkan data yang telah dienkripsi.

Proses dekripsi dilakukan dengan konsep dasar sebagai berikut :

1. Data yang telah dienkripsi dikembangkan kembali menjadi 2 bagian dan disimpan di dua register A dan register B.
2. Kemudian dilakukan rotasi ke kanan sejumlah *r*.
3. Selanjutnya dilakukan operasi EX-OR yang ditandai dengan ``⊕``.

Tahap akhir dilakukan pengurangan terhadap masing-masing register dengan key *word* yang ditunjukan dengan tanda ``-``, untuk mendapatkan *plaintext.*

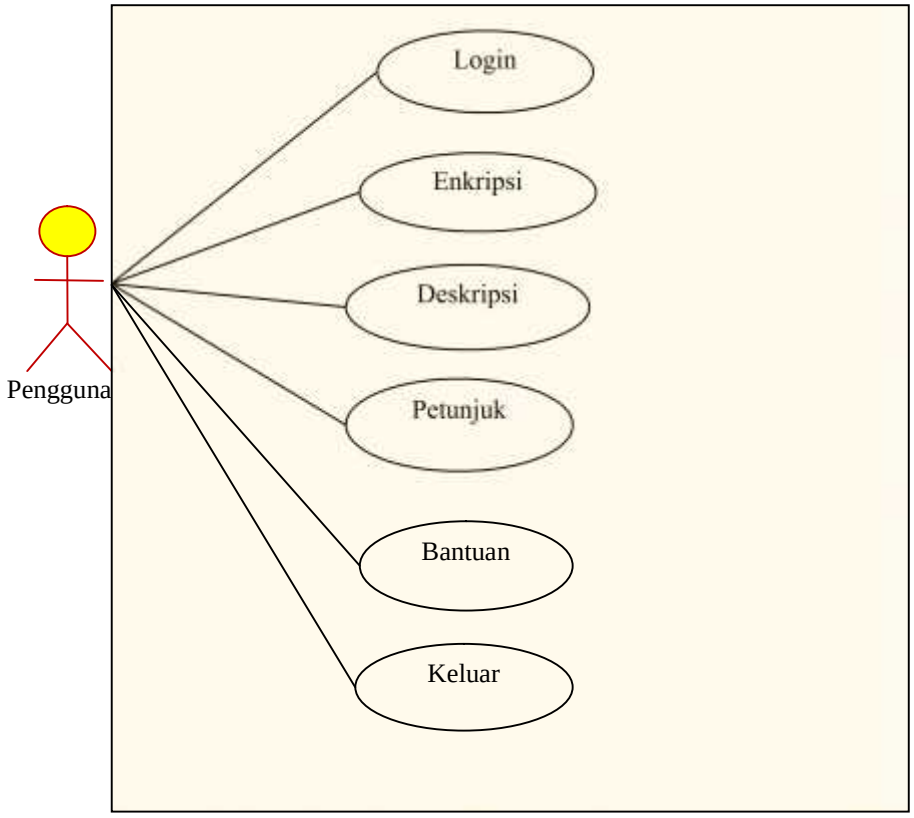
III.6. Desain Sistem

Setelah tahapan analisis sistem, maka selanjutnya dibuat suatu rancangan sistem. Perancangan sistem adalah tahapan yang berguna untuk memperbaiki efisiensi kerja suatu sistem yang telah ada. Pada perancangan sistem ini terdiri dari tahap perancangan yaitu :

1. Perancangan *Use Case Diagram*
2. Perancangan *Sequence Diagram*
3. Perancangan *Activity Diagram*
4. Perancangan *Output* dan *Input*

III.6.1. *Use Case Diagram*

Use case menjelaskan urutan kegiatan yang dilakukan aktor dan sistem untuk mencapai suatu tujuan tertentu. Sebuah *Use Case* mempresentasikan sebuah interaksi antara aktor dengan sistem dan menggambarkan fungsionalitas yang diharapkan dari sebuah sistem *enkripsi file*. Diagram *Use Case* tersebut dapat dilihat pada gambar III.1.



Gambar III.1. Diagram Use Case

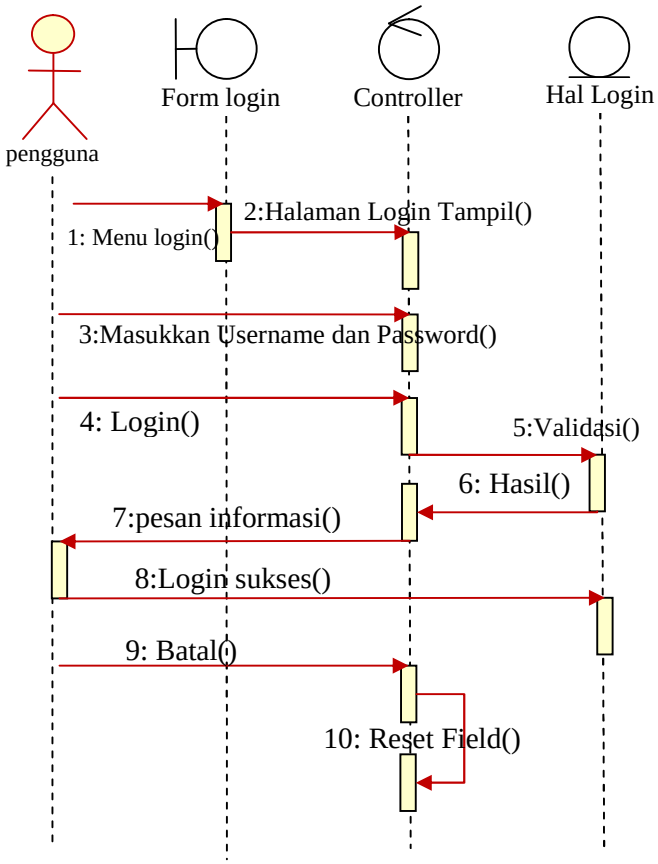
III.6.2. *Sequence* Diagram

Sequence diagram menunjukkan bagaimana operasi yang dilakukan secara detail. *Sequence* diagram menjelaskan interaksi obyek yang disusun dalam suatu urutan waktu. Urutan waktu yang dimaksud adalah urutan kejadian yang

dilakukan oleh seorang *actor* dalam menjalankan sistem, adapun *sequence* yang dilakukan terdiri dari *enkripsi* data dan *dekripsi* data.

1. *Sequence* Login

Login digunakan untuk masuk ke form login yang berisi nama username dan password, untuk lebih jelasnya dapat dilihat pada gambar III.2.

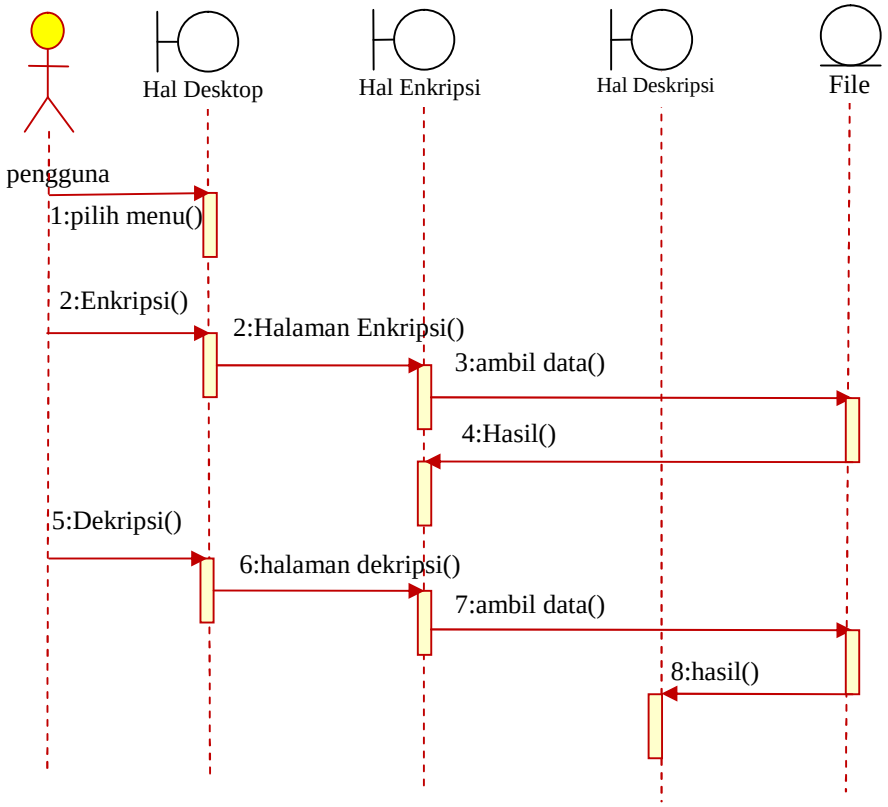


Gambar III.2. *Sequence* Diagram Login

Dari gambar III.2 menunjukkan bahwa seorang pengguna jika ingin masuk ke halaman desktop harus terlebih dahulu memasukkan nama pengguna dan password dengan benar, selanjutnya masuk kedalam menu desktop.

2. *Sequence* Desktop

Desktop digunakan sebagai pusat semua menu yang terdapat di aplikasi, untuk lebih jelasnya dapat dilihat pada gambar III.3.

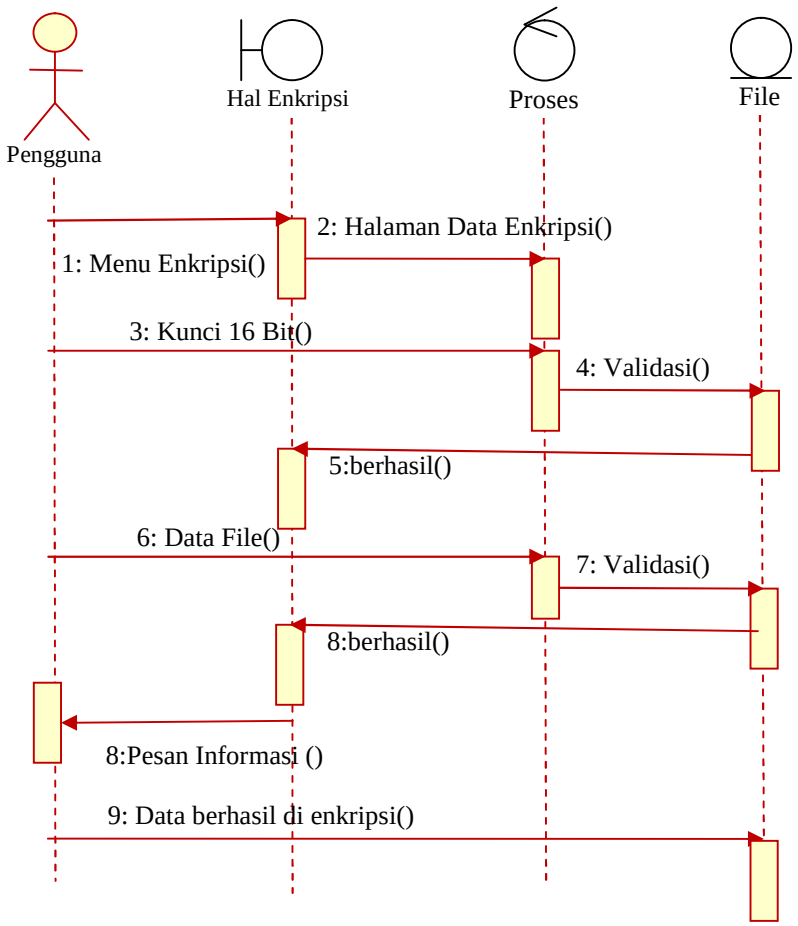


Gambar III.3. *Sequence* Diagram Desktop

Dari gambar III.3 menunjukkan bahwa seorang pengguna dapat melakukan eksekusi dari masing-masing menu yang sudah ditentukan yaitu menu enkripsi untuk mengambil data dalam bentuk *file*, kemudian menu dekripsi untuk mengambil data yang telah di enkripsi.

3. *Sequence* Enkripsi Data

Enkripsi data digunakan untuk mengubah data asli ke data enkripsi dengan metode RC5, untuk lebih jelasnya dapat dilihat pada gambar III.4.

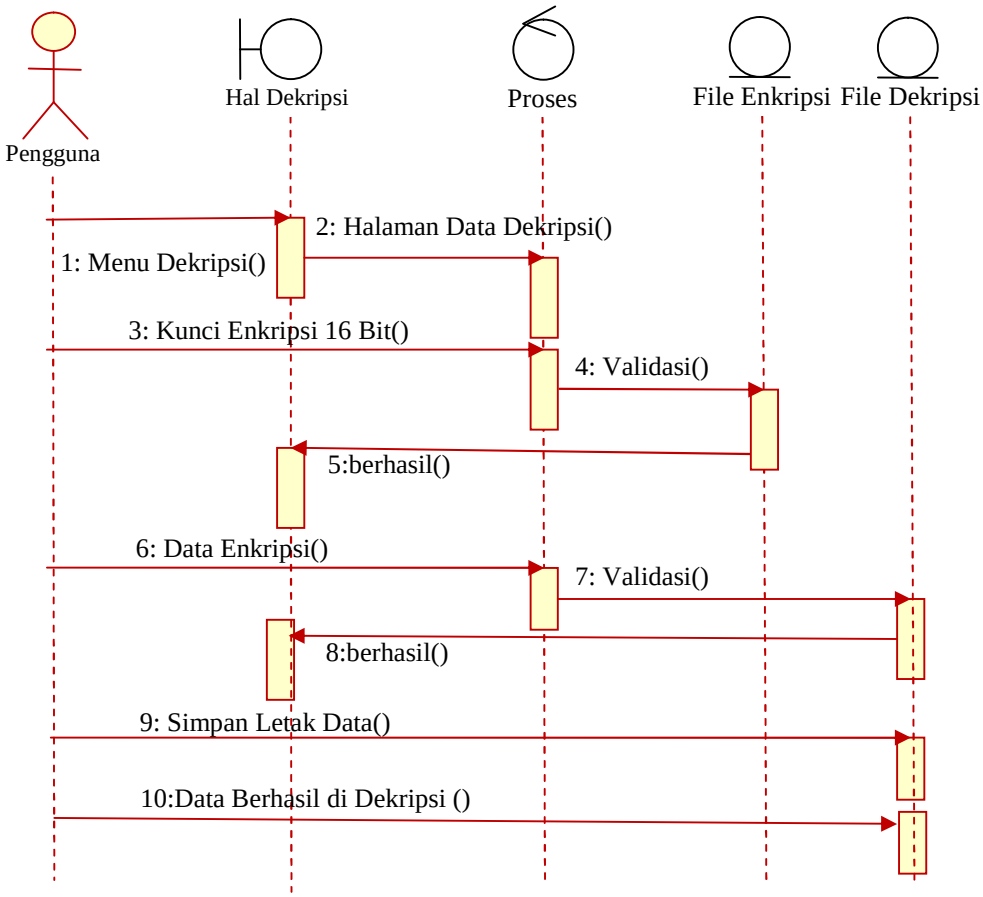


Gambar III.4. *Sequence* Diagram Enkripsi Data

Dari gambar III.4 menunjukkan bahwa seorang pengguna jika ingin melakukan *enkripsi* sebuah data harus terlebih dahulu memasukan kunci dengan panjang 16 *Bit*, mengambil data yang berbentuk *file*, dan melakukan proses enkripsi

4. *Sequence* Dekripsi Data

Dekripsi data digunakan untuk mengubah data enkripsi kemudian data tersebut di ubah ke data yang asli dengan menggunakan tombol dekripsi. untuk lebih jelasnya dapat dilihat pada gambar III.5.



Gambar III.5. *Sequence Diagram Dekripsi Data*

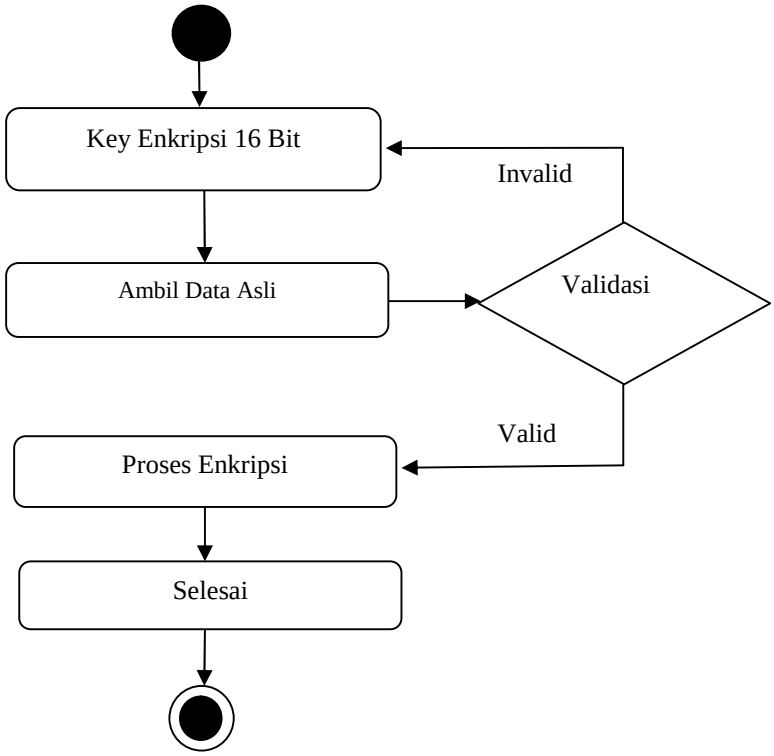
Dari gambar III.5 menunjukkan bahwa seorang pengguna melakukan perubahan data yang dienkripsi menjadi data yang semuala atau data asli dengan proses dekripsi.

III.7. Activity Diagram

Activity diagram ini akan menjelaskan setiap kegiatan yang akan dilakakukan pengguna pada sistem nantinya. Dengan menggambarkan setiap aktivitas dari sistem diharapkan sistem yang akan dibangun lebih mudah dipahami.

1. *Activity Diagram Enkripsi* data

Activity diagram untuk proses *enkripsi* data. *Activity* diagram *enkripsi* data dapat dilihat pada gambar III.6.

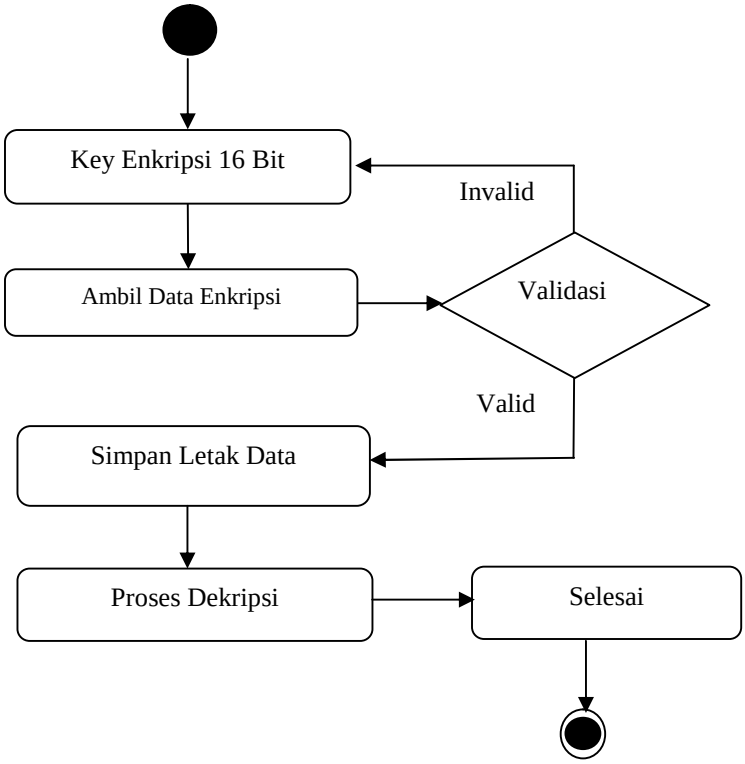


Gambar III.6. *Activity Diagram Enkripsi* Data

Pada gambar III.6 menjelaskan bahwa pengguna menginputkan kunci panjang 16 *Bit*, lalu memasukan data *file* yang ingin di enkripsikan, jika semuanya sudah diinputkan maka proses *enkripsi* selesai dilakukan, jika salah satu belum di inputkan maka kembali diminta untuk menginputkan keseluruhan.

2. *Activity Diagram Dekripsi* Data

Activity diagram merupakan *activity* diagram untuk proses *dekripsi* data. *Activity* diagram tersebut ditunjukkan pada gambar III.7.



Gambar III.7. ***Activity Diagram RC5 Deskripsi File***

Pada gambar III.7 menjelaskan bahwa pengguna menginputkan sebuah *file* yang telah di enkripsikan kemudian memberikan kunci enkripsinya, jika semuanya sudah diinputkan maka proses dekripsi dapat dilakukan, jika salah satu belum di inputkan maka kembali diminta untuk menginputkan keseluruhan.

III.8. Rancangan Program

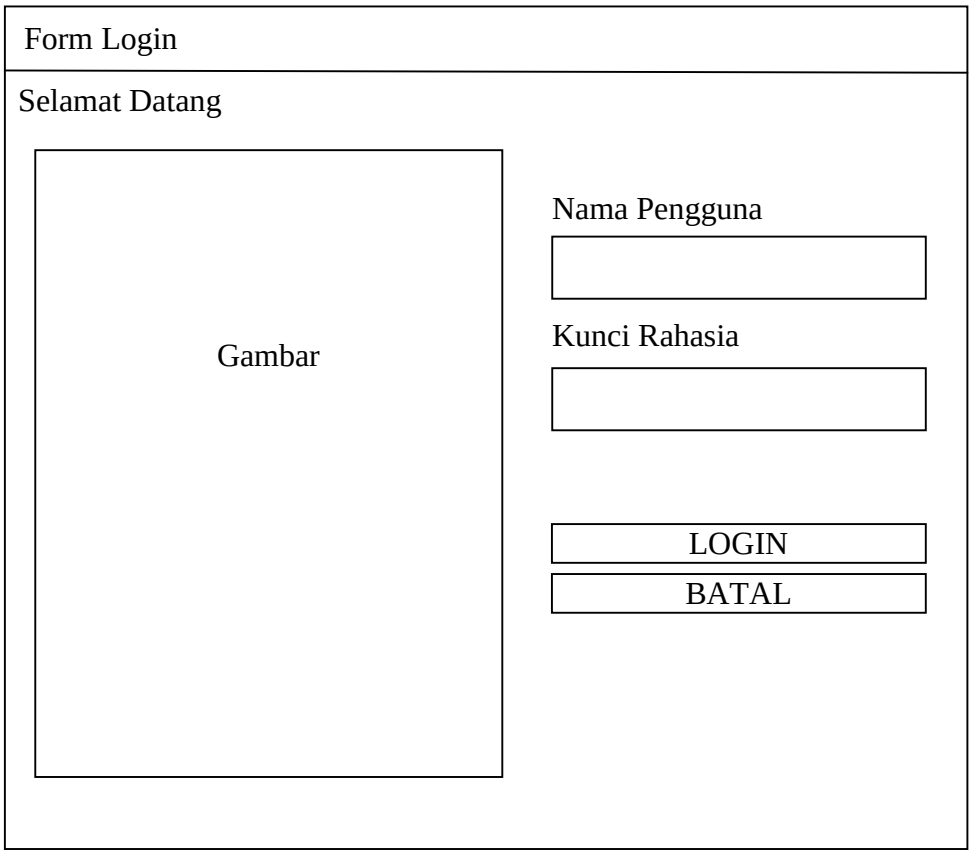
Dalam merancang suatu sistem perlu diketahui hal yang akan menunjang sistem, agar dapat mempermudah pengolahan data nantinya. Pengolahan data ini diharapakan dapat mempermudah dalam hal penyajian, pelayanan dan pembuatan berbagai laporan data yang dibutuhkan.

III.8.1. Rancangan *Output*

Rancangan *output* sistem global sebagaimana telah dijelaskan di atas tidak dapat menggambarkan secara keseluruhan proses yang terjadi dalam sistem, sehingga dibutuhkan disain sistem secara detail yang dapat menjelaskan alur proses yang terjadi di dalam sistem tersebut. Adapun rancangan sistem secara detail yang diusulkan akan dijelaskan satu persatu berikut ini.

1. Rancangan *Form Login*

Dalam perancangan login ini digunakan untuk masuk kedalam menu desktop, untuk lebih jelasnya dapat dilihat pada gambar III.8.

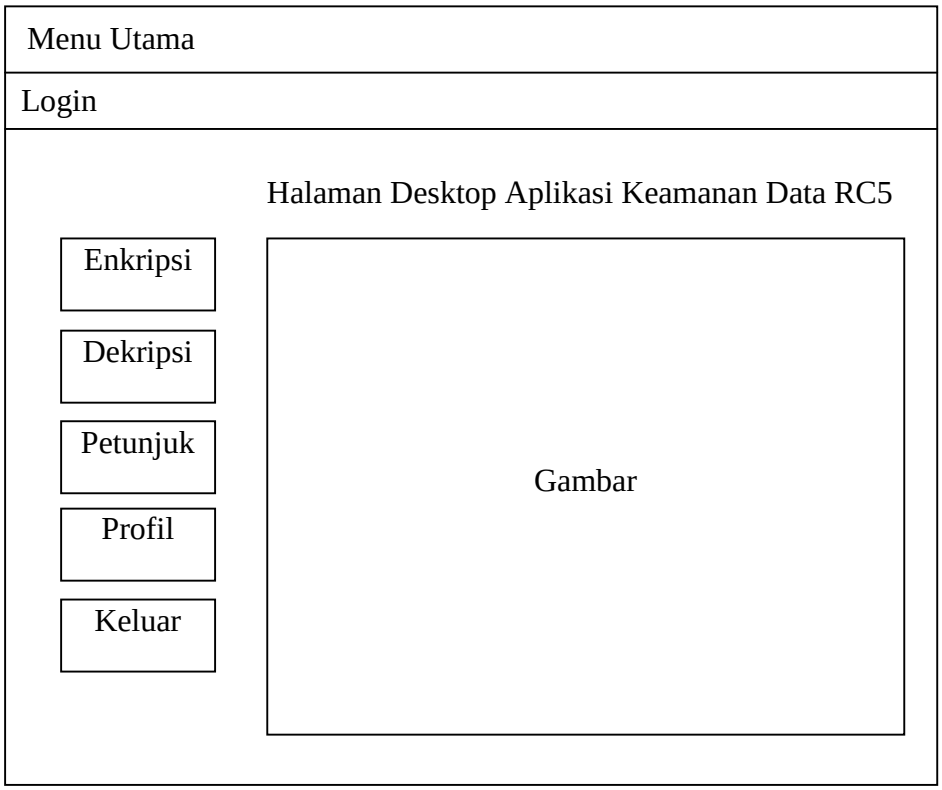


Gambar III.8. Rancangan Form Login

Rancangan login yang terdapat pada gambar III.8 terdiri dari gambar, dua *textbox*, tiga *label* dan dua *button*. Dari masing-masing *tool* tersebut tugasnya berbeda-beda.

2. Rancangan *Form Desktop*

Dalam perancangan menu utama ini digunakan sebagai pusat dari program perancangan keamanan data dari masing-masing menu, untuk lebih jelasnya dapat dilihat pada gambar III.9.



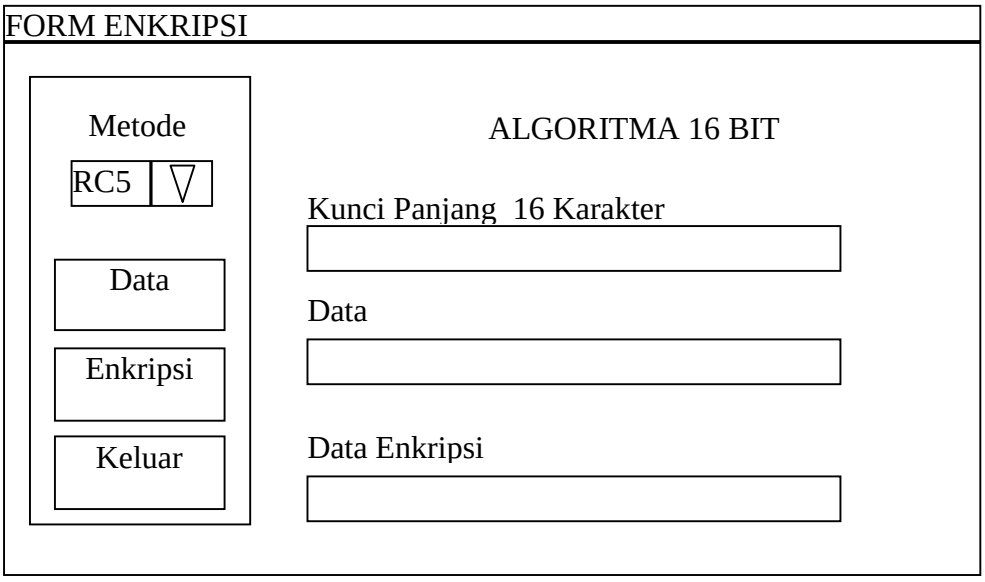
Gambar III.9. Rancangan Form Desktop

Rancangan menu utama atau menu desktop terdiri dari beberapa menu yaitu, menu enkripsi, menu dekripsi, menu petunjuk, menu profil dan menu keluar.

Jika pengguna ingin melakukan enkripsi data klik pada menu enkripsi, jika pengguna ingin mengembalikan ke data asli klik menu dekripsi, Jika pengguna bingung dalam menjalan aplikasi ini, pengguna klik menu petunjuk, jika ingin keluar klik menu keluar.

3. Rancangan *Form Enkripsi*

Dalam perancangan *form enkripsi* ini berfungsi melakukan pengambilan data untuk melakukan keamanan data tersebut, untuk lebih jelasnya dapat dilihat pada gambar III.10.

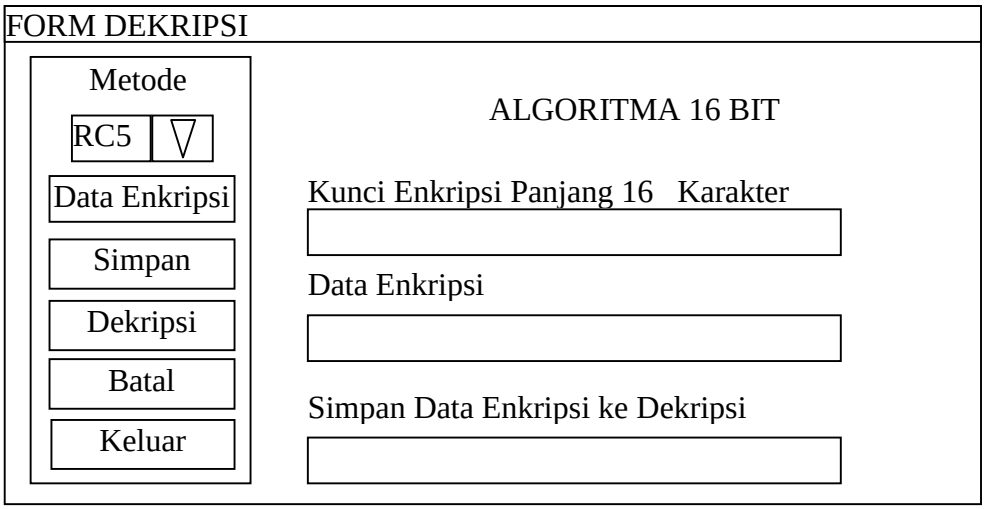


Gambar III.10. Rancangan *Form Enkripsi*

Rancangan form enkripsi yang terdapat pada gambar III.10 terdiri dari tombol data, enkripsi, keluar. Berikutnya pengguna diminta masukkan kunci, data dan terakhir adalah hasil enkripsi.

4. Rancangan *Form Deskripsi*

Bentuk daripada *form deskripsi* yang dirancang dapat dilihat pada gambar III.11.



Gambar III.11. Rancangan *Form Deskripsi*

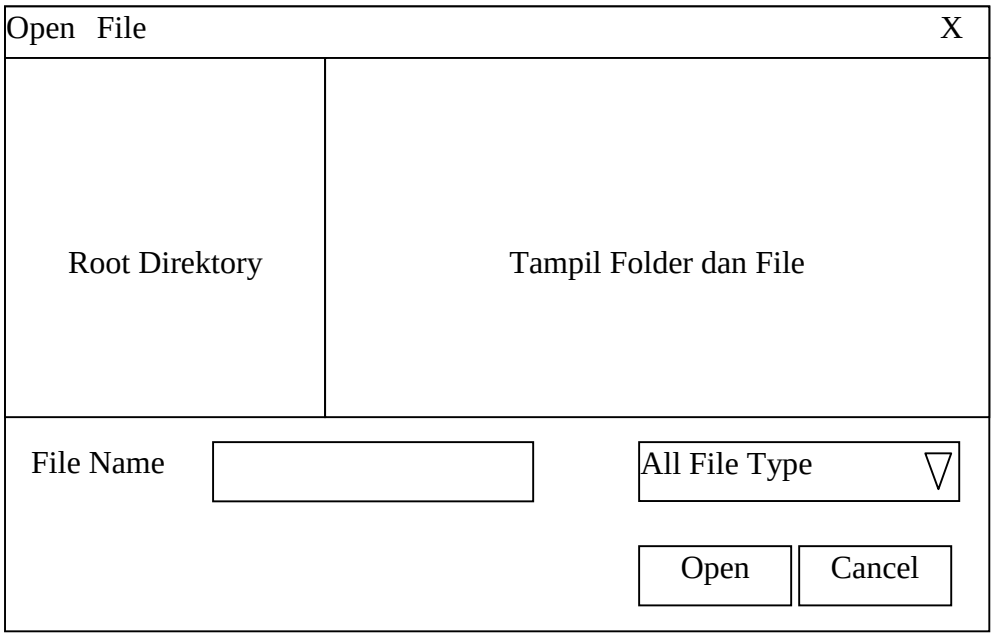
Rancangan form dekripsi yang terdapat pada gambar III.11 terdiri dari tombol data enkripsi, simpan, dekripsi, batal, keluar. Berikutnya pengguna diminta masukkan kunci enkripsi terlebih dahulu, lalu cari data *file* enkripsi, lalu simpan letak *file* dekripsi dan terakhir melakukan dekripsi.

III.8.2. Rancangan *Input*

Sistem ini mempunyai beberapa halaman yang akan menjadi *input*. Dalam perancangannya, sistem yang diusulkan adalah sebagai berikut :

1. **Rancangan *Form Input* data *File***

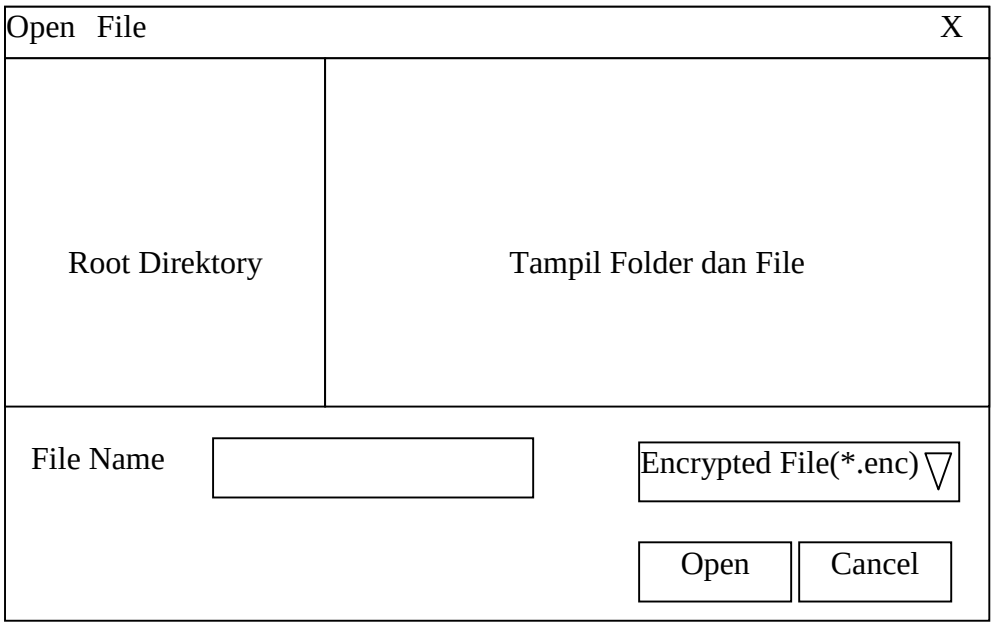
   Rancangan *form input* data enkripsi ini digunakan untuk mengambil data dari sebuah *root direktory* yang terletak didalam sebuah *folder* tertentu. Bentuk daripada *form input* data enkripsi yang dirancang dapat dilihat pada gambar III.12.



Gambar III.12. Rancangan *Form Input File*

2. Rancangan *Form Input* data *Enkripsi*

Bentuk daripada *form input* data enkripsi yang dirancang dapat dilihat pada gambar III.13.



Gambar III.13. Rancangan *Form Input* Data Enkripsi