BAB III

ANALISIS MASALAH DAN RANCANGAN PROGRAM

III.1. Analisis Masalah

Proses analisa sistem merupakan langkah kedua pada *fase* pengembangan sistem. Analisa sistem dilakukan untuk memahami informasi-informasi yang didapat dan dikeluarkan oleh sistem itu sendiri. Sistem *enkripsi file* belum begitu banyak diketahui oleh seorang operator, seorang operator ingin melakukan pengamanan *file* terhadap dokumennya menggunakan *password* yang ada pada aplikasi atau program yang digunakan. Berkembangnya teknologi informasi secara otomatis akan menambah jumlah data pribadi. Hal ini secara otomatis dapat lupa terhadap pemberian *password* tersebut karena telalu banyak data yang sudah dibuat.

Untuk itu, sistem yang penulis rancang adalah sistem yang melakukan *enkripsi* terhadap data dengan menggunakan metode RC5, agar data penting tersebut tidak dapat dibaca isi *file* aslinya. Dalam tahap pengembangan sistem *enkripsi* ini, analisa sistem merupakan hal yang harus dilakukan sebelum proses perancangan sistem. Pada proses analisa sistem terdapat 3 (tiga) langkah analisa yang harus dilakukan yaitu analisa *input*, analisa proses dan analisa *output*. Adapun analisa sistem yang sedang berjalan sebagai berikut :

III.1.1. *Input*

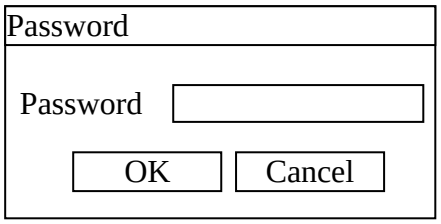
Sistem yang berjalan dalam pemberian *password* dalam sebauh *file* didalam aplikasi tertentu seperti microsoft word.

III.1.2. Analisa Proses

Setelah data pemberian *password* di *input*, maka akan dilakukan analisa proses pengolahan data tersebut. Analisa proses adalah suatu bagian dimana suatu *input* data akan dikelola agar menjadi *output* yang diinginkan. Penginputan data *password* dilakukan oleh seorang operator, kemudian data tersebut diserahkan kebagian tertentu yang berhak menerimanya.

III.1.3 *Output*

Data *output* adalah data hasil pengolahan data pemberian *password* yang telah dilakukan dalam bentuk yang akan ditujukan kepada pihak yang menerima data *file* tersebut. Adapun bentuk–bentuk dari sistem yang berjalan dapat dilihat pada gambar III.1.



Gambar III.1. *Hasil Output Password File*

III.2. Strategi Pemecahan Masalah

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

a. Data yang dibuat didalam sebuah *file* itu sangat penting dan rahasia, apabila dicuri orang *file* tersebut bisa di salah gunakan, daripada itu perlu dibuat *enkripsi file* agar data asli didalam *file* tersebut tidak dapat dibaca oleh orang yang tidak bertanggung jawab.

b. Agar *file* tersebut aman dari kerusakan perangkat keras maka data tersebut harus dipindahkan ke lokasi yang lebih aman misalnya di flashdisk, aplikasi enkripsi *file* ini sudah dirancang tempat pemindahan *file* tersebut.

III.3. 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, apabila *file* tersebut sudah diketahui maka isi *file* aslinya dapat dibaca oleh orang yang tidak bertanggung jawab tersebut.

Maka solusi yang penulis buat untuk mengatasi masalah tersebut adalah membuat suatu sistem *enkripsi* yang berupa *file* untuk merubah isi *file* aslinya dalam bentuk simbol-simbol yang tidak mudah dibaca oleh siapapun.

III.4. RC5ain 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.5. Algoritma 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 ``⊕``.

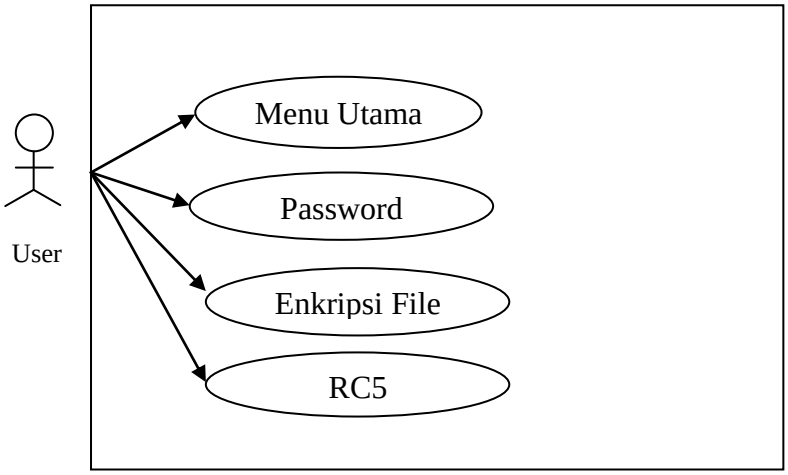
3. Melakukan rotasi kekiri (*shift left*) sepanjang *y* terhadap *x word* yang ditandai dengan *x*<<< *y*. *y* merupakan interpretasi *modulo w* atau jumlah kata *w* dibagi 2. Dengan *lg[w]* ditentukan jumlah putaran yang dilakukan.
4. Tahap akhir dilakukan penggabungan untuk mendapatkan data yang telah 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 ``⊕``.
4. Tahap akhir dilakukan pengurangan terhadap masing-masing register dengan key *word* yang ditunjukan dengan tanda ``-``, untuk mendapatkan *plaintext.*

III.6. *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.3.



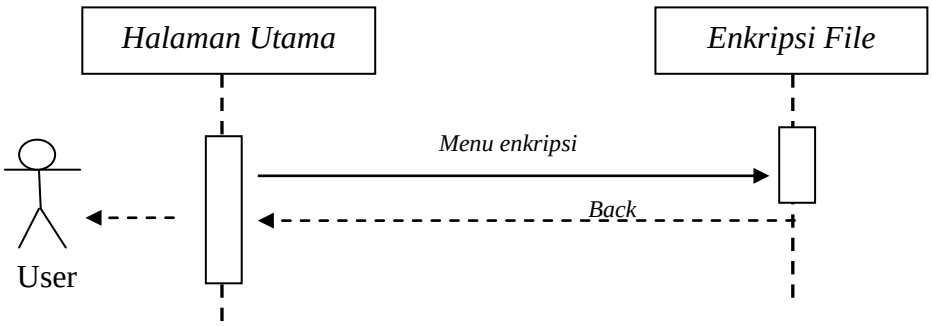
Gambar III.3. ***Use Case Diagram Enkripsi File***

III.7. *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 file* dan *RC5kripsi file*.

1. *Sequence Enkripsi File*

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

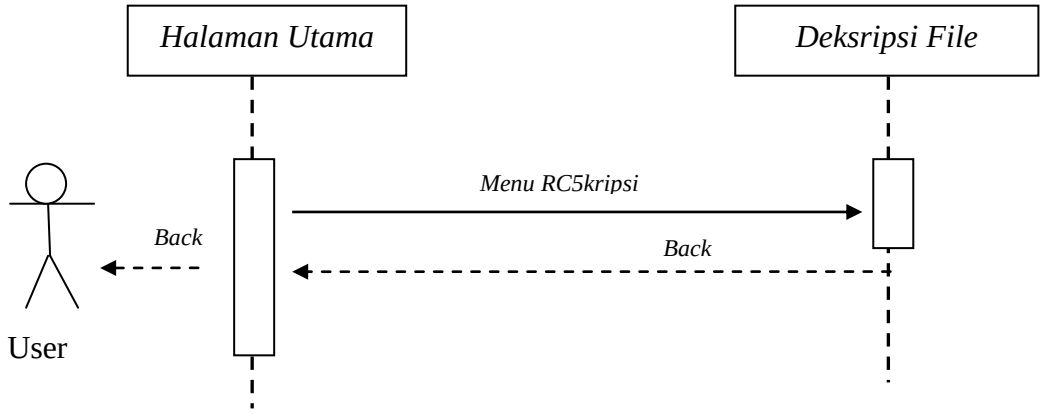


Gambar III.4. ***Sequence Diagram Enkripsi File***

Dari gambar III.4 menunjukkan bahwa seorang *user* jika ingin melakukan *enkripsi* sebuah *file* harus terlebih dahulu masuk kedalam tampilan menu utama, selanjutnya masuk kedalam menu *enkripsi file*.

2. *Sequence RC5kripsi File*

RC5 skripsi file digunakan untuk mengubah data *file* yang sudah terenkripsi kemudian dirubah ke data aslinya. untuk lebih jelasnya dapat dilihat pada Gambar III.5.



Gambar III.5. *Sequence Diagram RC5 skripsi File*

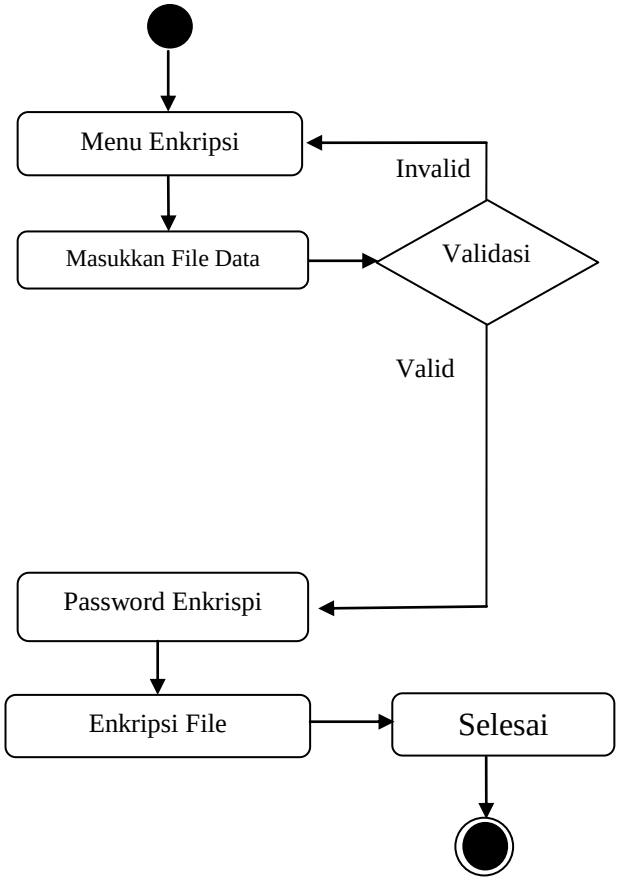
Dari gambar III.5 menunjukkan bahwa seorang *user* melakukan perubahan data *enkripsi* menjadi *RC5kripsi* ke data asli dengan melakukan masuk terlebih dahulu kedalam menu utama kemudian masuk kedalam menu *RC5kripsi file*.

III.8. *Activity* Diagram

Activity diagram merupakan *activity* yang terdiri dari proses *enkripsi file* dan *RC5kripsi file*. *Activity* diagram ini ditunjukkan untuk penggambaran dasar aliran daripada *enkripsi* dan *RC5kripsi file* tersebut.

1. *Activity Diagram Enkripsi File*

Activity diagram *enkripsi file* merupakan *activity* diagram untuk proses *enkripsi file*. *Activity* diagram *enkripsi file* dapat dilihat pada gambar III.6.

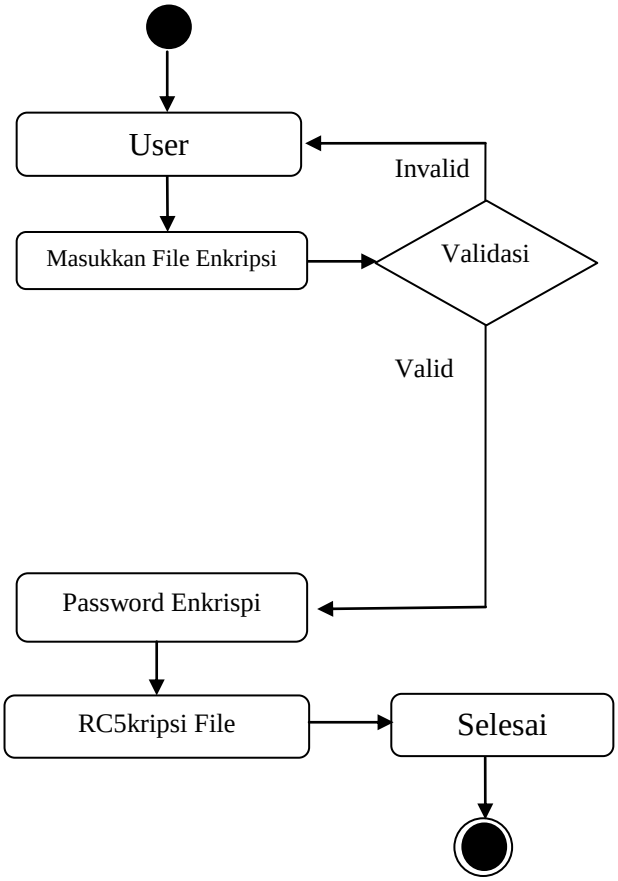


Gambar III.6. ***Activity Diagram Enkripsi File***

Pada gambar III.6 menjelaskan bahwa pengguna menginputkan sebuah *file* yang ingin di enkripsikan kemudian memberikan *password*, jika semuanya sudah diinputkan maka proses *enkripsi* selesai dilakukan, jika salah satu belum di inputkan maka kembali diminta untuk menginputkan keseluruhan.

2. *Activity Diagram RC5kripsi File*

Activity diagram merupakan *activity* diagram untuk proses *RC5kripsi file*. *Activity* diagram tersebut ditunjukkan pada gambar III.7. diberikut ini:



Gambar III.7. *Activity Diagram RC5kripsi File*

Pada gambar III.7 menjelaskan bahwa pengguna menginputkan sebuah file yang telah di enkripsikan kemudian memberikan *password* enkripsinya, jika semuanya sudah diinputkan maka proses RC5kripsi dapat dilakukan, jika salah satu belum di inputkan maka kembali diminta untuk menginputkan keseluruhan.

III.9. RC5 Sistem Detail

Perancangan terinci yang disebut juga RC5 teknis sistem secara fisik (*phisycal system RC5ign*) atau disebut juga RC5 internal (*internal RC5ign*), yaitu perancangan bentuk fisik atau bagan arsitektur sistem yang diusulkan. Dalam

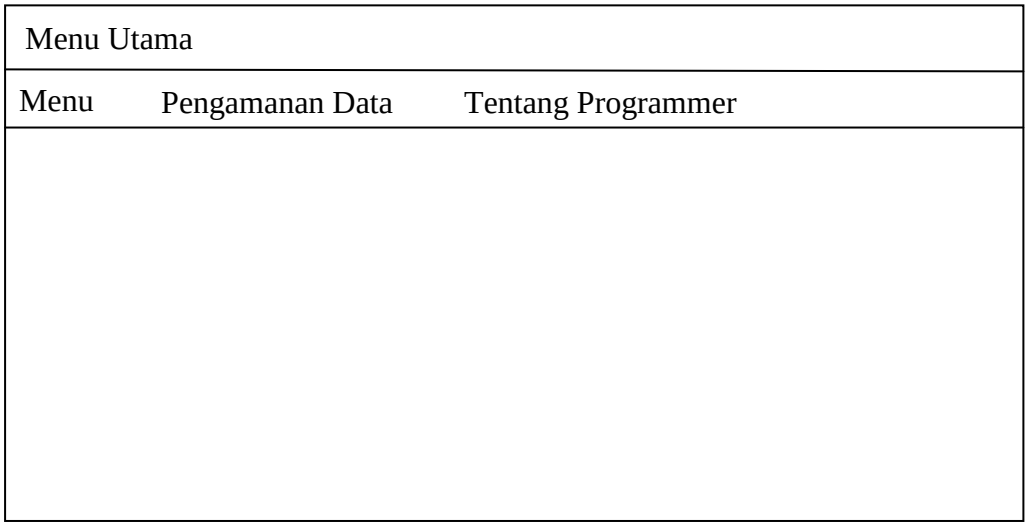
merancang suatu sistem perlu diketahui hal yang akan menunjang sistem, agar dapat mempermudah pengolahan data nantinya. Pengolahan data ini diharapakan dapat mempermudah dalam hal penyajian, pelayanan dan pembuatan berbagai laporan data yang dibutuhkan. Berdasarkan hal tersebut diatas, penulis akan menguraikan lebih detail rancangan sistem yang diusulkan.

III.9.1 RC5ain *User Interface*

RC5ain sistem ini berisikan pemilihan menu dan hasil pencarian yang telah dilakukan. Adapun bentuk rancangan output dari sistem *enkripsi file* ini adalah sebagai berikut :

1. Menu Utama

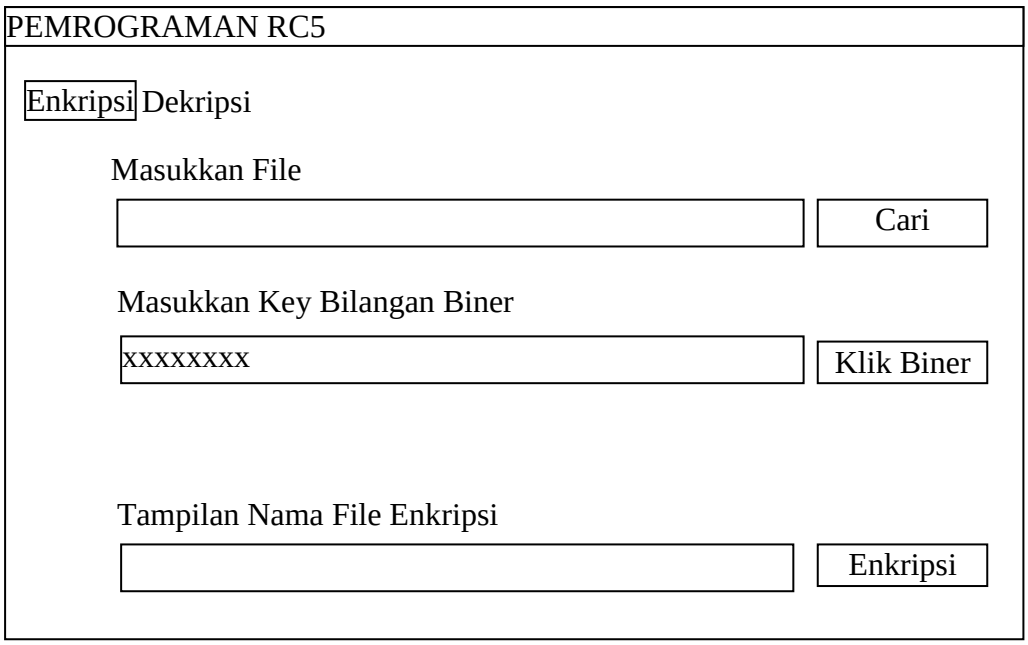
   Setelah selesai melakukan login dengan berhasil, maka menu utama akan tampil dilayar monitor, adapun bentuk daripada menu utama dapat dilihat pada Gambar III.8.



Gambar III.8. Menu Utama

2. *Enkripsi*

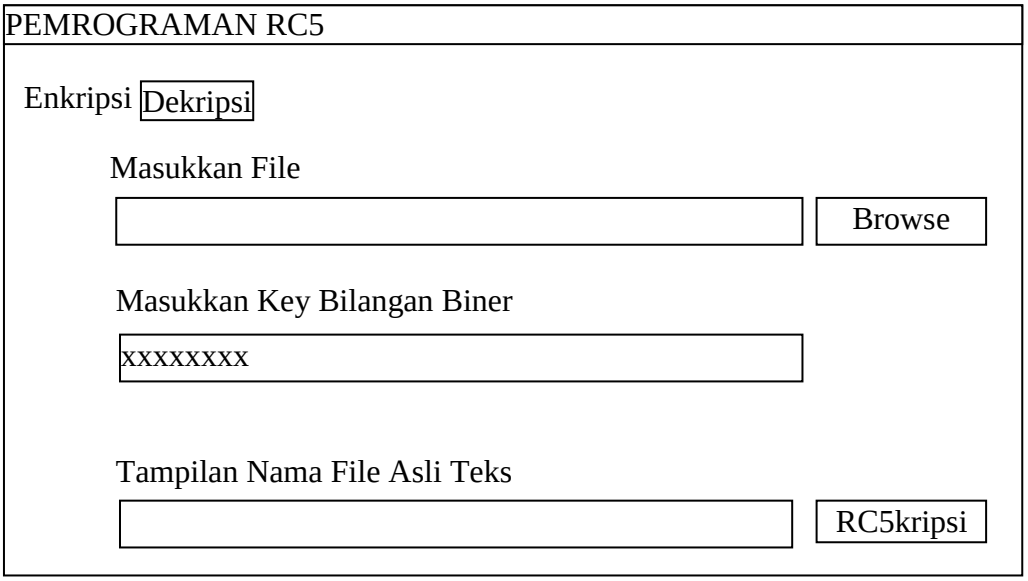
Bentuk form *enkripsi* yang dirancang dapat dilihat pada Gambar III.9.



Gambar III.9. RC5 *Form Enkripsi*

3. RC5kripsi

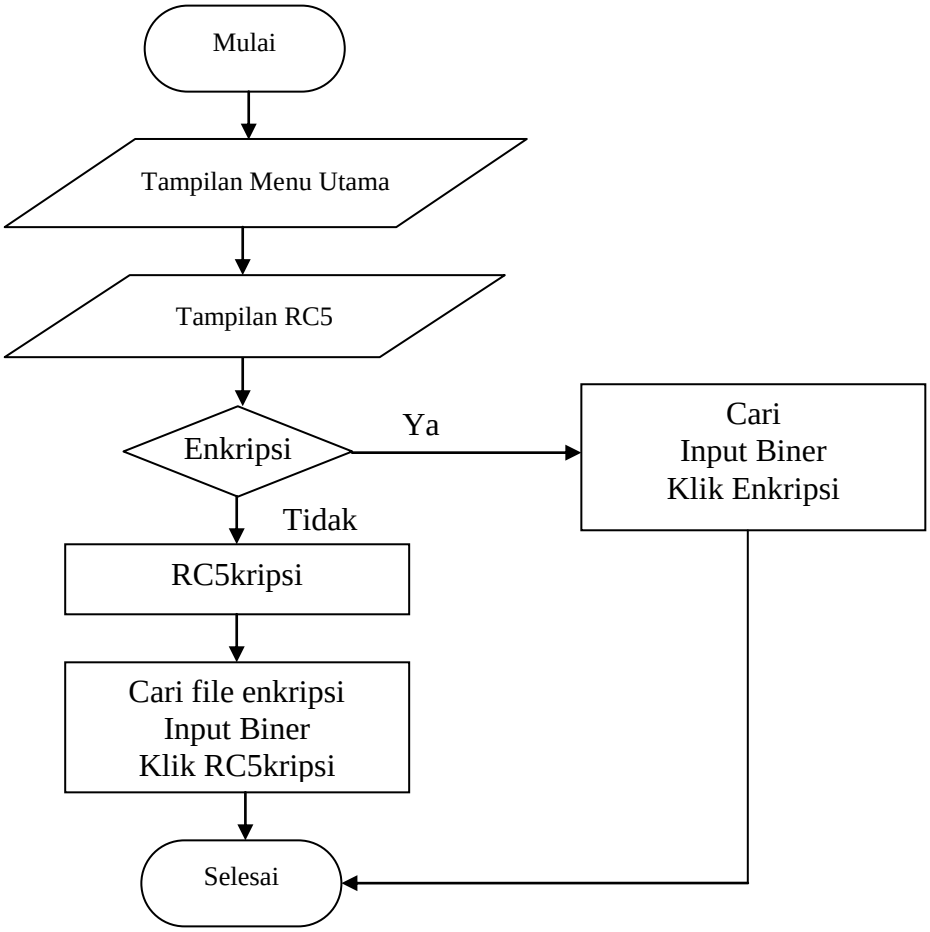
Bentuk daripada *form file RC5kripsi* yang dirancang dapat dilihat pada Gambar III.10.



Gambar III.10. Desain *Form RC5kripsi*

III.10. Logika Program

Algoritma adalah urutan langkah-langkah logis penyelesaian masalah yang disusun secara sistematis. Perancangan algoritma dalam skripsi ini dituangkan ke dalam *flowchart*. Berikut perancangan algoritma-algoritma yang dibahas dalam perancangan sistem, dapat dilihat pada Gambar III.11.



Gambar III.11. Flowchart Algoritma RC5