

BAB IV

PERANCANGAN PERANGKAT LUNAK

4.1 Metode Perancangan

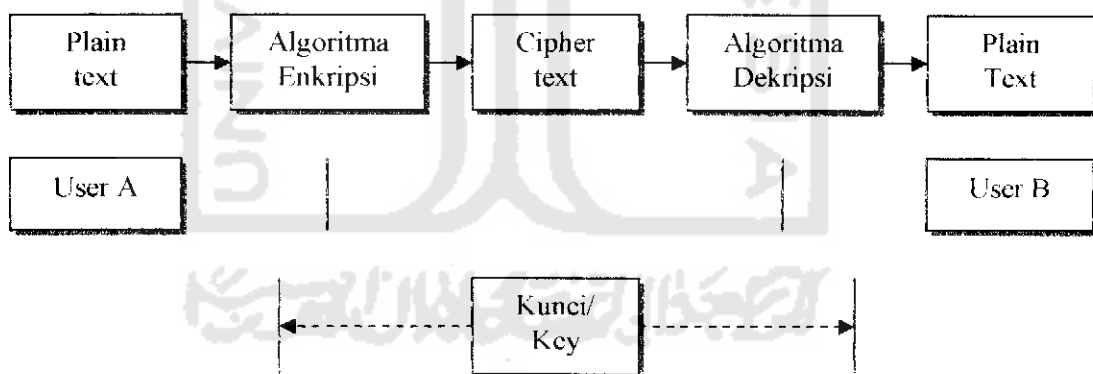
Tahap perancangan sistem dilakukan setelah tahapan analisis kebutuhan selesai dan didefinisikan secara jelas. Dalam tahap ini digambarkan lebih rinci berdasarkan tahapan sebelumnya, sehingga diperoleh algoritma dan detil aliran proses enkripsi dan dekripsi data yang akan dibuat. Adapun tujuan dan maksud dari tahap perancangan sistem adalah :

1. Untuk memenuhi kebutuhan kepada pemakai sistem
2. Untuk memberikan gambaran yang jelas dan rancang bangun yang diinginkan kepada pemrograman komputer.

Hasil dari tahapan perancangan ini harus dapat diterapkan menjadi prosedur dengan alat bantu bahasa pemrograman berorientasi object yaitu Visual Basic 6.0. Metode perancangan yang digunakan yaitu memakai flowchart untuk mengetahui aliran setiap proses yang terjadi dalam proses enkripsi dan dekripsi file menggunakan algoritma RC4.

Diagram alir (*flowchart*) adalah suatu skema yang menggambarkan urutan kegiatan dari suatu program dari awal sampai akhir serta menjadi alat bantu dalam perancangan alir sistem dengan menggunakan simbol-simbol agar mudah dipahami. Dalam diagram alir ini biasanya dibagi menjadi 2 yaitu diagram alir proses dan diagram alir program. [JOG90]. Diagram alir program (*flowchart*) merupakan diagram

Pada aplikasi sistem enkripsi dan dekripsi file dengan menggunakan algoritma RC4 adalah melakukan inialisasi data asli yang akan dienkripsi. Data ini kemudian akan dienkripsi dan didekripsi dengan menggunakan algoritma RC4 dan akan ditampilkan hasilnya, dari data yang telah dienkripsi akan dikembalikan ke data asli dengan proses dekripsi. Proses enkripsi dan dekripsi memerlukan masukkan key yang kemudian key tersebut digunakan untuk menghasilkan variabel enkripsi dengan menggunakan 2 aturan yaitu bagian variabel dan kunci serta jumlah N dari operasi pencampuran. Operasi key dimasukan sebagai kunci untuk proses enkripsi dari data asli (*plaintext*) ke data yang disandikan (*ciphertext*) dan sebaliknya sebagai proses dekripsi atau perubahan data sandi ke data asli, jadi data yang disandikan tidak dapat dikembalikan ke data asli jika kita tidak mempunyai kunci (*key*) pada saat proses enkripsi sebelumnya.



Gambar 4.1 Rancangan Implementasi Program Secara Umum

Program implementasi algoritma RC4 ini akan dibuat menjadi beberapa fungsi, antara lain:

- Enkripsi dan dekripsi file
- Enkripsi dan dekripsi text

Implementasi program yang dibuat ditujukan untuk studi analisis algoritma RC4, jadi tampilan bersifat program pembelajaran RC4.

4.2 Hasil Perancangan

Dari metode perancangan didapat hasil perancangan sistem yang meliputi program-program sebagai berikut:

1. Proses enkripsi dan dekripsi file
2. Proses enkripsi dan dekripsi text

Rancangan proses-proses implementasi algoritma RC4 ini akan dibahas dibawah ini.

4.2.1 Proses Enkripsi / Dekripsi File

Pada proses ini berfungsi untuk enkripsi dan dekripsi file. Proses ini terdiri dari browse file yang akan dienkripsi, save file hasil enkripsi, browse file enkripsi, save file hasil dekripsi, tombol enkripsi file, tombol dekripsi file, tombol view file, clear file, option hapus file asli dan hapus file enkripsi, tombol file properties, tombol backup file serta informasi file yang terdiri nama file yang akan dienkripsi dan dekripsi, ukuran file dan waktu proses enkripsi dan dekripsi file. Subrutin program enkripsi dan dekripsi file ini:

1. Proses Enkripsi File

Proses ini merupakan proses untuk enkripsi file. Operasi program dimulai dari inisialisasi masukkan program berupa file atau data elektronik kemudian pemberian key / kunci dan setelah proses enkripsi yang akan menyimpan file enkripsi tersebut kedalam file berekstensi *.enc.

2. Proses Dekripsi File

Proses ini adalah proses untuk dekripsi yaitu membuka kembali file yang telah dienkripsi. Operasi program dimulai dari inisialisasi file yang telah terenkripsi yaitu dengan format *.enc kemudian memasukkan key / kunci untuk membuka file enkripsi tersebut dan menyimpannya ke dalam file semula.

3. Informasi waktu proses dan informasi ukuran file

Waktu proses ditampilkan ketika mengenkripsi dan mendekripsi file yang memberikan informasi tentang kecepatan algoritma RC4, serta kapasitas file yang dapat dilihat pada informasi file atau pada tombol file properties.

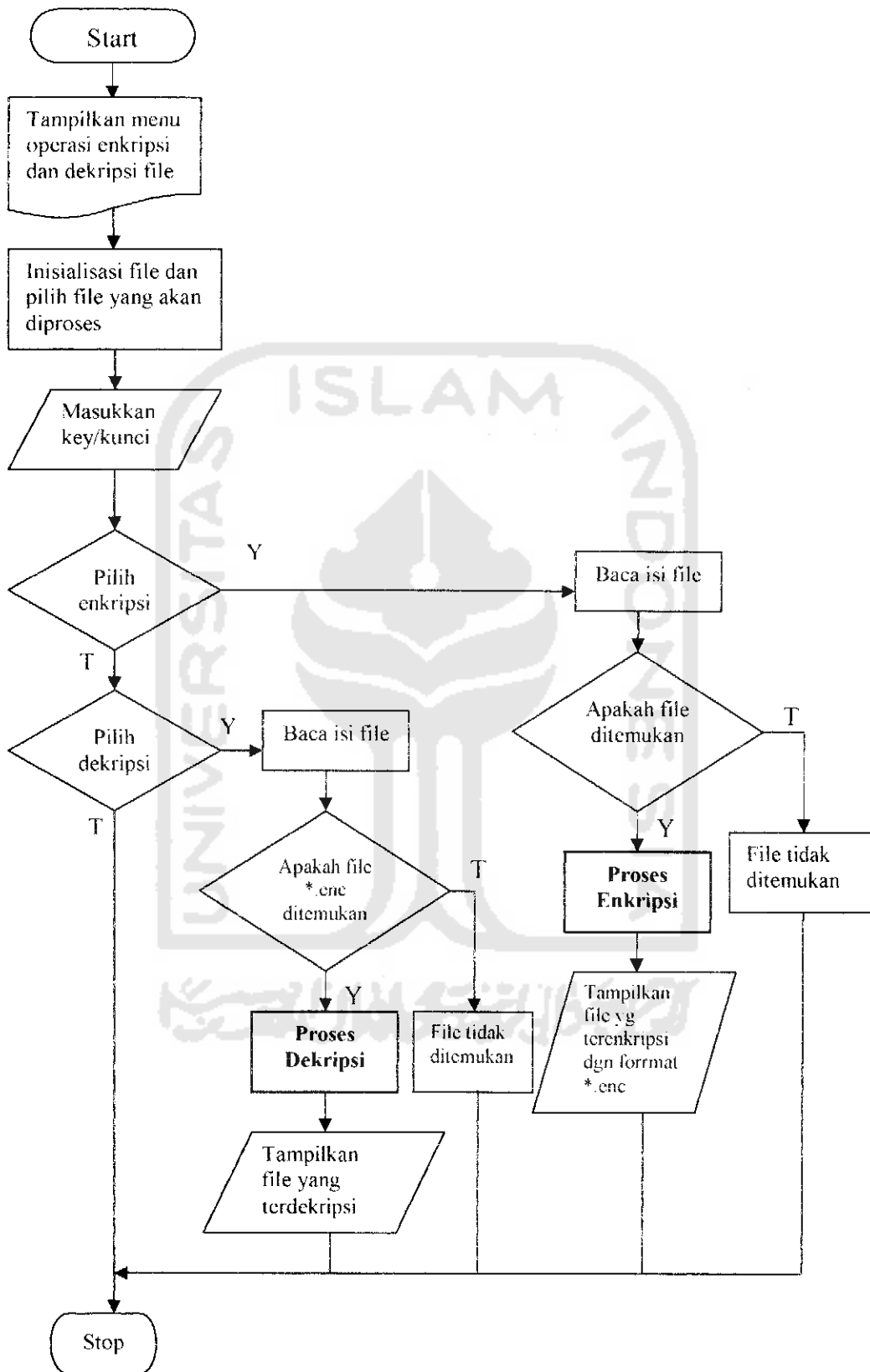
4. View File

Tombol view file yaitu untuk melihat file yang akan dienkripsi dan setelah file terenkripsi.

5. Backup File

Backup file berfungsi untuk membackup file yang akan dienkripsi.

Flowchart dari program enkripsi dan dekripsi file dapat dilihat pada gambar 4.2 dari gambar tersebut kita dapat melihat alur kerja program enkripsi file.



Gambar 4.2 Flowchart untuk enkripsi dan dekripsi file

4.2.2 Proses Enkripsi / Dekripsi Text

Proses ini berfungsi untuk enkripsi dan dekripsi text. Proses ini terdiri dari, tombol enkripsi, tombol dekripsi, tombol browser file text, tombol clear text, dan layar memo untuk mengisi karakter yang akan dienkripsi dan dekripsi. Dalam proses ini terdapat subrutin yaitu:

1. Proses Enkripsi Text

Proses ini merupakan program untuk enkripsi text. Operasi program dimulai dari inialisasi masukkan text pada memo plaintext kemudian pemberian key/kunci dan setelah proses enkripsi akan menampilkan karakter yang telah teracak dengan karakter lain baik berupa simbol atau karakter lain di memo encrypttext sehingga tidak dapat diartikan atau dipahami.

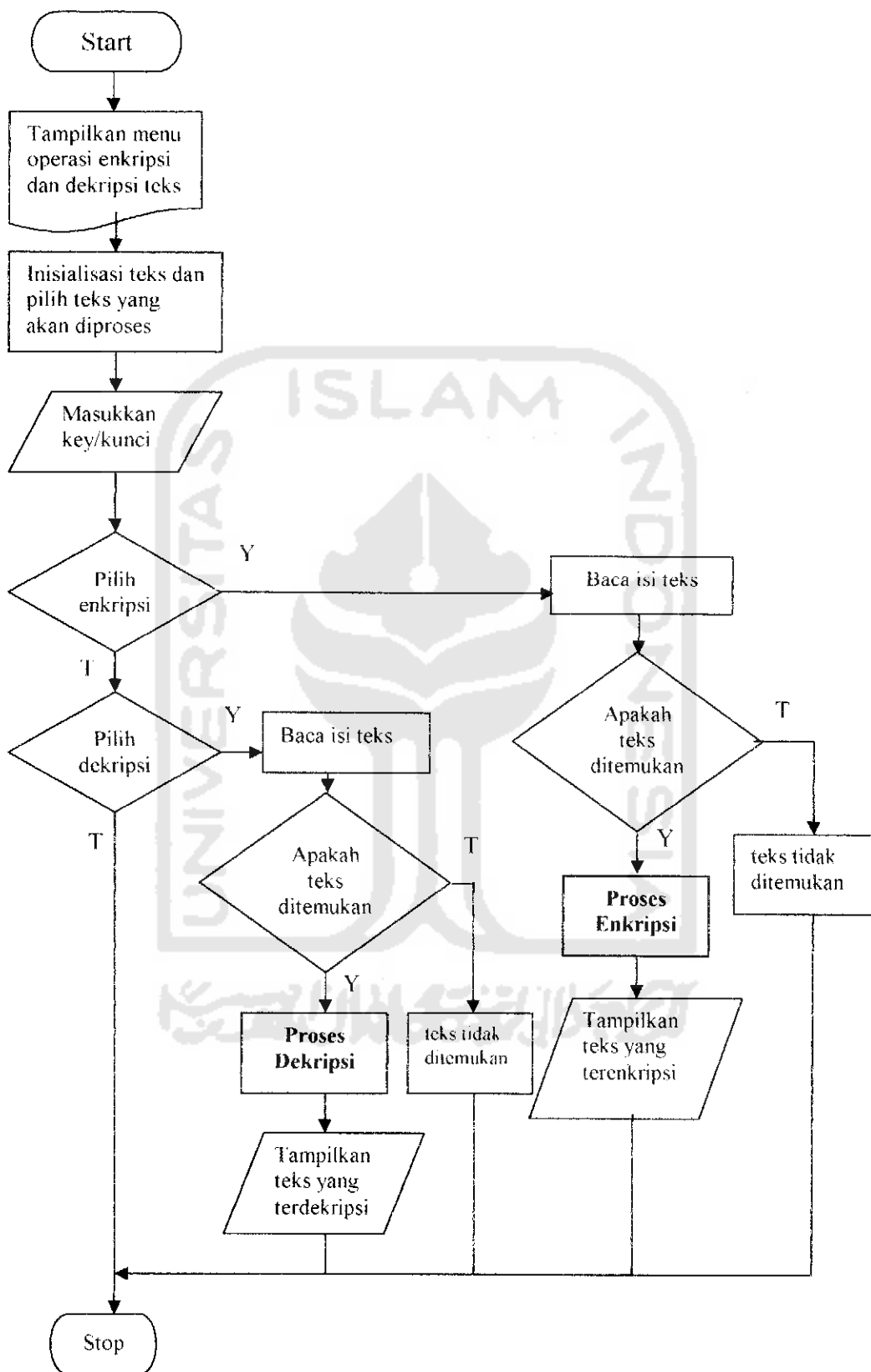
2. Proses Dekripsi Text

Proses ini adalah program untuk proses dekripsi yaitu mengembalikan data text yang tersandi menjadi data semula / asli sehingga dapat dipahami atau terbaca . Operasi program dimulai dari inialisasi text yang telah terenkripsi kemudian memasukkan key/kunci untuk proses dekripsi text dan menampilkannya ke memo decrypttext.

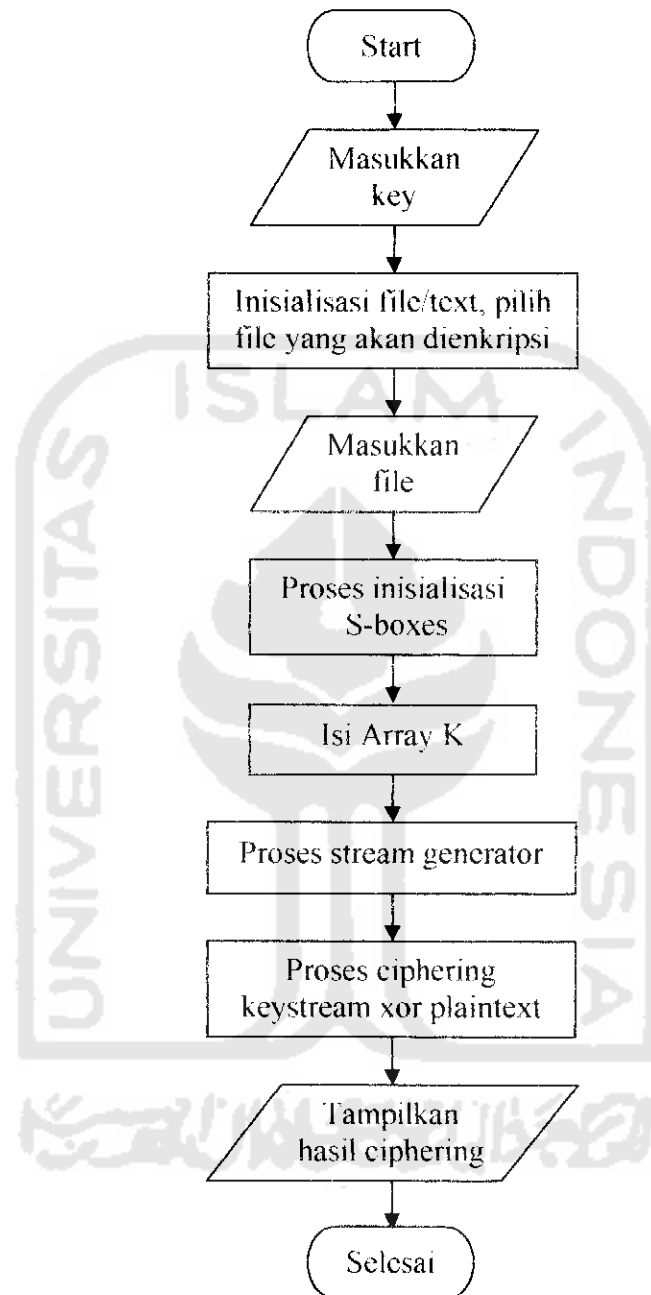
3. Browse File Text

Tombol ini berfungsi untuk mencari file yang akan dienkripsi dengan ekstensi *.text

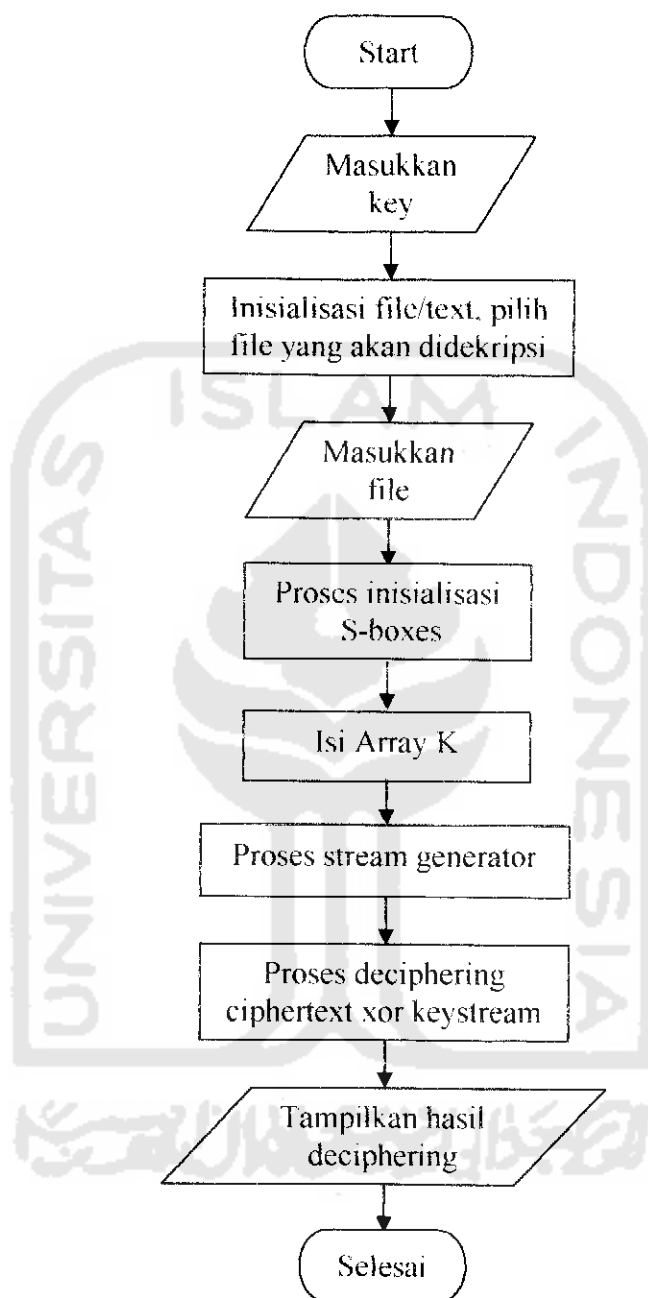
Flowchart dari program enkripsi dan dekripsi text dapat dilihat pada gambar 4.3 dari gambar tersebut kita dapat melihat alur kerja program enkripsi file text.



Gambar 4.3 Flowchart untuk enkripsi dan dekripsi teks



Gambar 4.4 Flowchart Proses Enkripsi Algoritma RC4



Gambar 4.5 Flowchart Proses Dekripsi Algoritma RC4

4.3 Perancangan Antar Muka (*Interface*)

Antar muka (*interface*) dirancang agar pengguna dapat berinteraksi secara baik dengan aplikasi, sehingga tercipta komunikasi yang mudah dipahami. Komunikasi tersebut dapat terdiri dari proses memasukkan data dan menampilkan kepada pengguna untuk tercapainya antarmuka yang diinginkan. Ada beberapa hal perlu diperhatikan, yaitu:

1. Aplikasi harus menyediakan fungsi-fungsi yang akan dikerjakan oleh pengguna.
2. Layar dialog harus dibentuk sedemikian rupa sehingga informasi, instruksi dan bantuan-bantuan selalu ditampilkan pada area yang sudah pasti. Dengan demikian pengguna akan dapat dengan mudah mencari informasi yang diinginkan. Untuk maksud ini, layar dialog dapat dibagi-bagi dalam bentuk jendela sesuai dengan kegunaannya masing-masing.
3. Menggunakan kalimat yang mudah dimengerti untuk dialog.

Pada sistem aplikasi yang dibangun ini terdiri dari beberapa *interface* yaitu:

1. Encrypt file yaitu menu untuk mengenkripsi file

Pada *interface* ini terdapat beberapa tombol yaitu: browse file yang akan dienkrpsi, save enkripsi file, browse file yang akan didekripsi, save dekripsi file, tombol encrypt file yang berfungsi sebagai enkripsi file, tombol decrypt file yang berfungsi sebagai dekripsi file, tombol view file yang berfungsi untuk melihat isi file, tombol file properties yang berfungsi untuk melihat informasi file, tombol backup file, tombol clear file, tombol exit untuk keluar

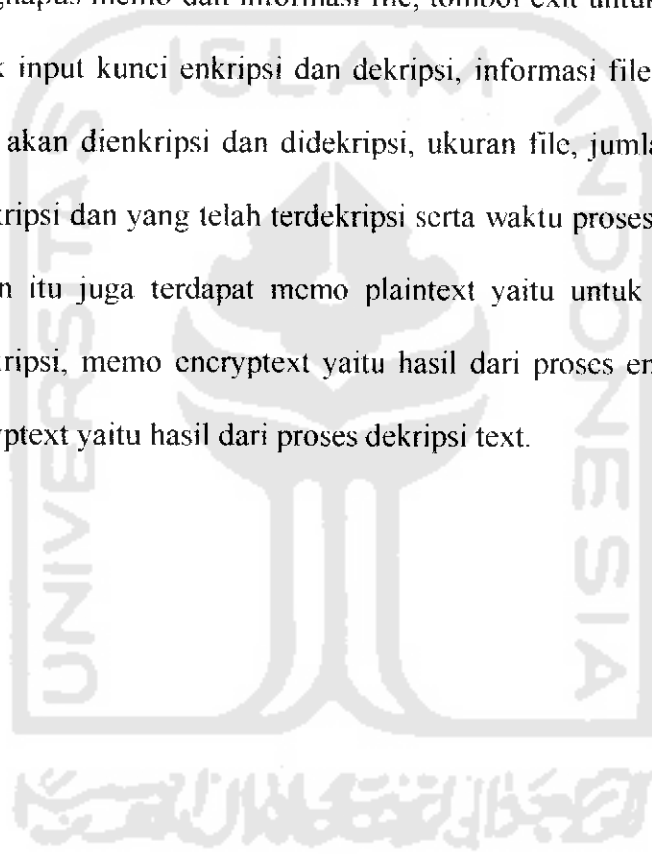
informasi file, tombol backup file, tombol clear file, tombol exit untuk keluar dari form encrypt file, option hapus file original dan hapus file enkripsi, text key untuk memasukkan kunci enkripsi dan informasi file yang terdiri dari kapasitas file original dan kapasitas file enkripsi serta waktu enkripsi dan dekripsi. Berikut gambar rancangan *interface* untuk enkripsi file.

The image shows a software interface for RC4 encryption. The window title is "Kriptografi Algoritma RC4". The main area is titled "Algoritma RC4" and "Encrypt File". It features a menu bar with "Encrypt Files", "Decrypt Files", "Backup Files", "View Files", "File Properties", "Clear", and "Exit". A sidebar on the left contains buttons for "Home", "Encrypt Files", "Encrypt Text", "Algorithm RC4", and "About Program". The main interface includes a "Key" input field, an "Enkripsi Files" section with a "Hapus File Original" checkbox, and a "Dekripsi Files" section with a "Hapus File Enkripsi" checkbox. Both sections have "Pilih" and "Save" file selection fields with "Browse" buttons. At the bottom, an "Informasi Files" section displays "Nama File Original", "Ukuran File Original", and "Waktu Proses Enkripsi".

Gambar 4.6 Perancangan Interface Encrypt Files

2. Encrypt text yaitu menu untuk mengenkripsi text

Pada interface ini terdapat beberapa tombol yaitu : tombol encrypt text yang berfungsi sebagai enkripsi text, tombol decrypt text yang berfungsi sebagai dekripsi text, tombol browse yang berfungsi untuk mencari file text dan menampilkan pada memo plaintext, tombol clear yang berfungsi untuk menghapus memo dan informasi file, tombol exit untuk keluar form, text key untuk input kunci enkripsi dan dekripsi, informasi file yang berisi nama file yang akan dienkripsi dan didekripsi, ukuran file, jumlah karakter yang akan dienkripsi dan yang telah terdekripsi serta waktu proses enkripsi dan dekripsi. Selain itu juga terdapat memo plaintext yaitu untuk input text yang akan dienkripsi, memo encrypttext yaitu hasil dari proses enkripsi text dan memo decrypttext yaitu hasil dari proses dekripsi text.



Kriptografi Algoritma RC4 - x

Algoritma RC4 **Encrypt Text**

Home

Encrypt Files

Encrypt Text

Algorithm RC4

About Program

Encrypt TextDecrypt TextBrowseClearExit

Key :

Plaintext :

Encrypttext :

Decrypttext :

Informasi Files :

Nama Files	:	
Ukuran Files	:	
Character Plaintext	:	
Waktu Proses	:	

Gambar 4.7 Perancangan Interface Encrypt Text