BAB III

ANALISIS DAN PERANCANGAN

III.1. Analisa Masalah

Kebutuhan manusia akan perangkat informasi dan komunikasi seakan menjadi kebutuhan yang tidak terpisahkan dalam kehidupan. Dengan banyaknya aplikasi saat ini sangat membantu mengurangi aktifitas yang dilakukan banyak orang. Saat ini perkembangan teknologi informasi dan komunikasi dari waktu ke waktu kian meningkat. Didalam dunia teknologi informasi dan komunikasi sangat diperlukan suatu tempat penyimpanan data yang berfungsi menampung data yang penting khususnya pada perangkat *Android Mobile Phone*. Dewasa ini sudah semakin marak pembobolan data baik secara langsung maupun tidak langsung. Untuk itu pentingnya dilakukan pengamanan agar data penting dapat terjamin keamanannya. Perangkat *Android Mobile Phone*merupakan perangkat yang sangat handal karena memiliki kemampuan yang dapat digunakan hampir pada seluruh perangkat lain seperti jam tangan, kulkas, tv, ac, lampu, bahkan pada mobil.

Dalam dunia komputer pengamanan dikenal dengan kriptografi yang berasal dari bahasa Yunani yaitu *cryptos* yang artinya *"secret"* (yang tersembunyi) dan *graphein* yang artinya *"writing"* (tulisan). Jadi kriptografi berarti *"secret writing"* (tulisan rahasia). Kriptografi adalah ilmu dan seni untuk menjaga keamanan pada data sehingga menjamin keamanannya. Salah satu metode yang dipergunakan untuk mengamankan data adalah dengan Algoritma RC4.

Pada desain *menu* di aplikasi untuk keamanan data file ini dapat dijelaskan sebagai berikut :

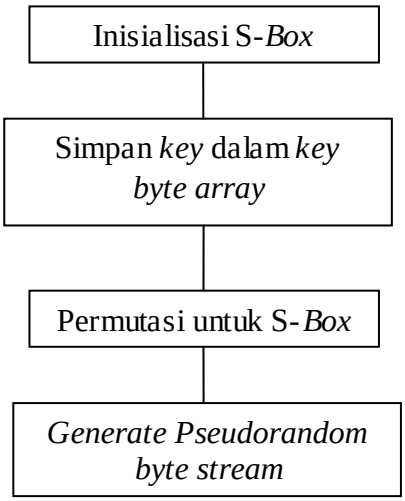
1. *Splash*, yang berfungsi permulaan untuk memuat aplikasi.
2. MenuUtama, merupakan tampilan yang digunakan untuk menginput data, pilihan enkripsi atau dekripsi dan menampilkan isi file.
3. Enkripsi, berfungsi untuk menampilkan hasil dari proses enkripsi.
4. Dekripsi, berfungsi untuk menapilkan hasil dari proses dekripsi.
5. Tentang, merupakan tampilan dari tentang aplikasi.

III.2. Algoritma RC4

Algoritma RC4 merupakan salah satu jenis *stream cipher*, yaitu memproses unit atau input data pada satu saat. Unit atau data pada umumnya sebuah *byte* atau bahkan kadang berupa bit (*byte* dalam hal RC4).

III.2.1. Proses Enkripsi dan Dekripsi Algoritma RC4

Proses enkripsi dan dekripsi RC4 mempunyai proses yang sama sehingga hanya ada satu fungsi yang dijalankan untuk menjalankan kedua proses tersebut. RC4 menggunakan variabel yang panjang kuncinya 1 sampai 256 bit yang digunakan untuk menginialisasikan tabel sepanjang 256 bit. Tabel ini digunakan untuk generasi yang berikut dari *pseudorandom* bit dan kemudian untuk menggenerasikan aliran *pseudorandom* digunakan operasi XOR dengan *plaintext* untuk menghasilkan *ciphertext* Berikut ini akan diberikan sebuah bagan yang menggambarkan rangkaian proses yang dijalankan untuk mengenkripsi atau mendekripsi pada RC4.



Gambar III.1. Proses Enkripsi dan Dekripsi RC4

Untuk lebih jelasnya tahapan-tahapan enkripsi dan dekripsi RC4 adalah sebagai berikut.

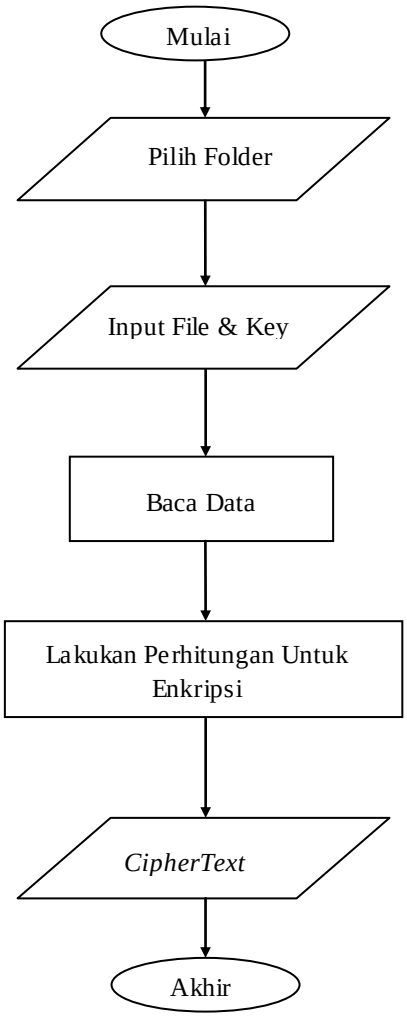
h. Pengguna memasukkan *secret key*
i. Inisialisasi awal S-*Box*berdasarkan indeks
j. Simpan *secret key* yang telah dimasukkan *user* kedalam *array* 256 *byte*
k. Bangkitkan nilai *pseudorandom* berdasarkan nilai *key sequence*
l. Proses permutasi nilai dalam S-*Box* selama 256 kali
m. Bangkitkan nilai *pseudorandom key byte stream* berdasarkan indeks dan nilai S-*Box*
n. Lakukan opersai XOR antara *plaintext/ciphertext* dan *pseudorandom key*.

III.2.2. Enkripsi

Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang lain. Dengan ekkripsi, data kita disandikan

(*Encrypted*) dengan menggunakan sebuah kunci (*key*). Untuk membuka (men-*decrypt*) data tersebut, digunakan kunci yang sama ketika mengenkrip.

Keamanan dari enkripsi tergantung beberapa faktor salah satunya yaitu menjaga kerahasiaan kuncinya bukan algoritmanya. Proses enkripsi dapat diterangkan dengan gambar III.2 berikut ini.



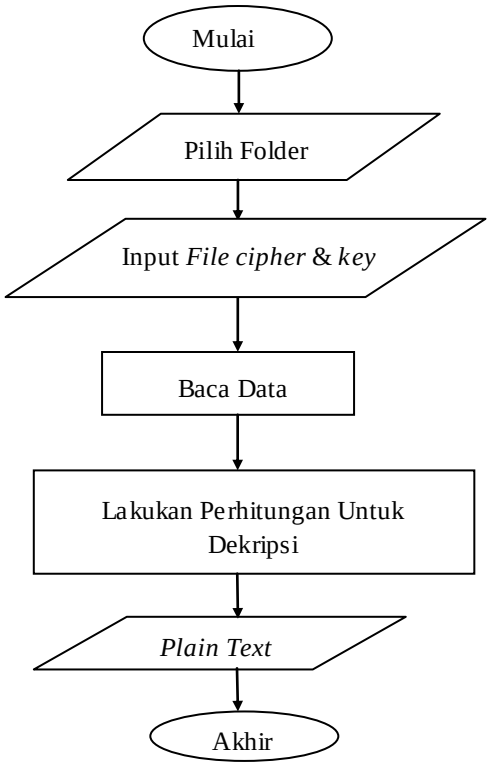
Gambar III.2. *Flowchart* Proses Enkripsi

Keterangan :

1. Pilih Folder Penyimpanan
2. Masukkan *file* dan *key*
3. Baca isi *file*
4. Lakukan perhitungan untuk melakukan enkripsi
5. Outputnya adalah *ciphertext*
6. Selesai

III.2.3. Dekripsi

Dekripsi digunakan untuk mengembalikan data-data atau informasi yang sudah dienkripsi kebentuk awal sehingga dapat dibaca kembali dengan baik. Adapun *Flowchart* dekripsi dapat dilihat pada gambar III.3 berikut.



Gambar III.3. *Flowchart* Proses Dekripsi

Keterangan :

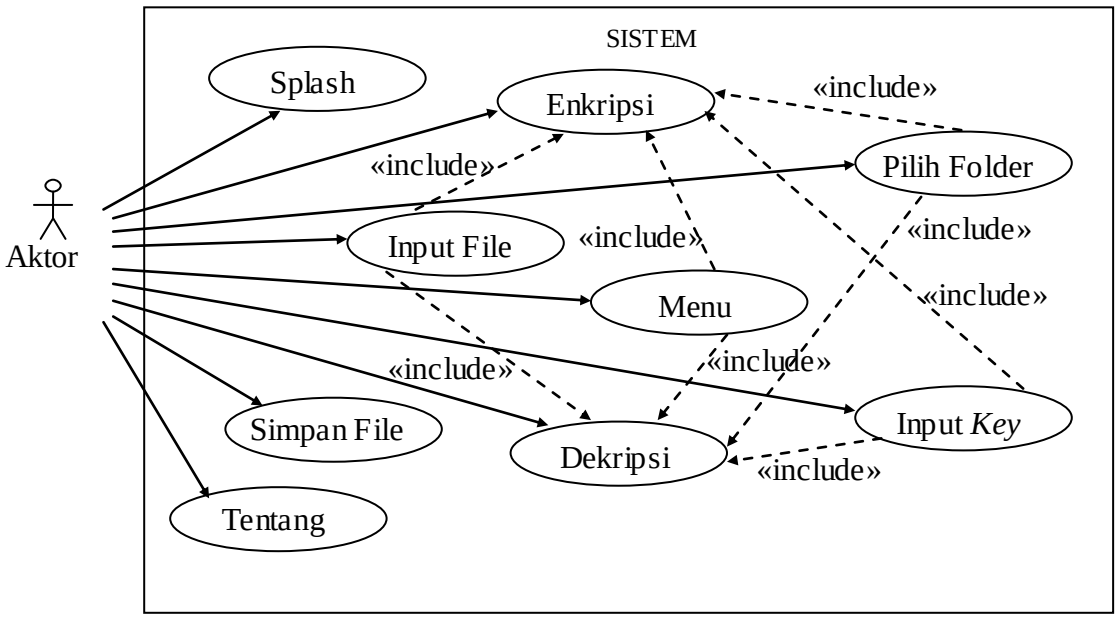
1. Pilih folder penyimpanan
2. Masukkan *file cipher* & *key*
3. Baca isi file
4. Lakukan perhitungan untuk dekripsi
5. Outputnya adalah *plaintext*
6. Selesai.

III.3. UML

Penggambaran UML menggunakan diagram *use-case* yang selanjutnya setiap proses yang terjadi akan diperjelas dengan diagram *activity* lalu diilustrasikan secara detail menggunakan diagram *sequence*.

III.3.1. *Use Case* Diagram

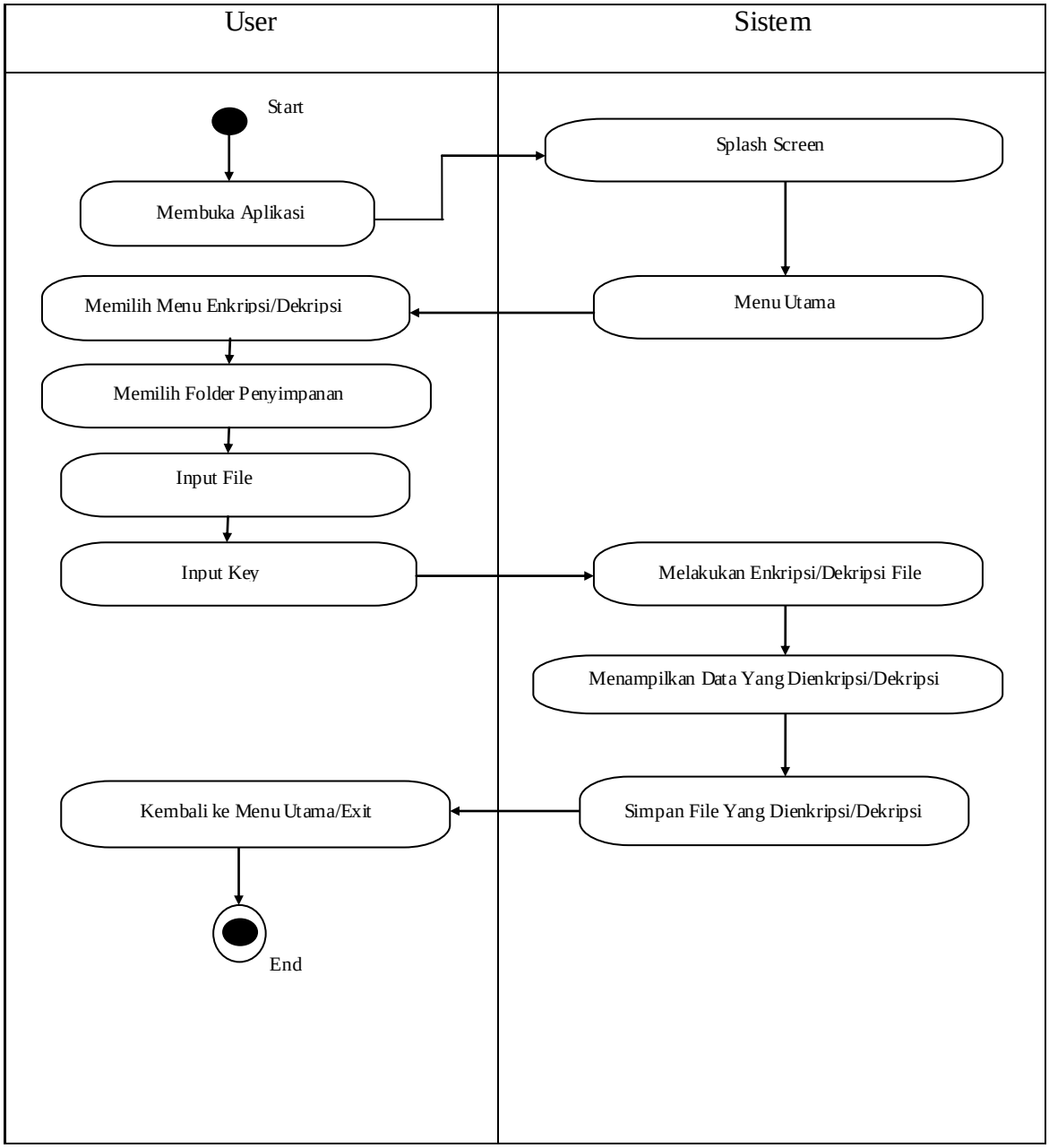
Adapun *use-case* diagram dapat dilihat pada gambar III.4 berikut.



Gambar III.4. *Use Case Diagram* Aplikasi yang Dibangun

III.3.2. *Activity* Diagram

Activity diagram adalah teknik untuk menggambarkan logika prosedural, proses bisnis, dan jalur kerja. Berikut ini akan dijelaskan *activity diagram* pada setiap proses enkripsi dan dekripsi yang terjadi pada aplikasi yang dibangun.

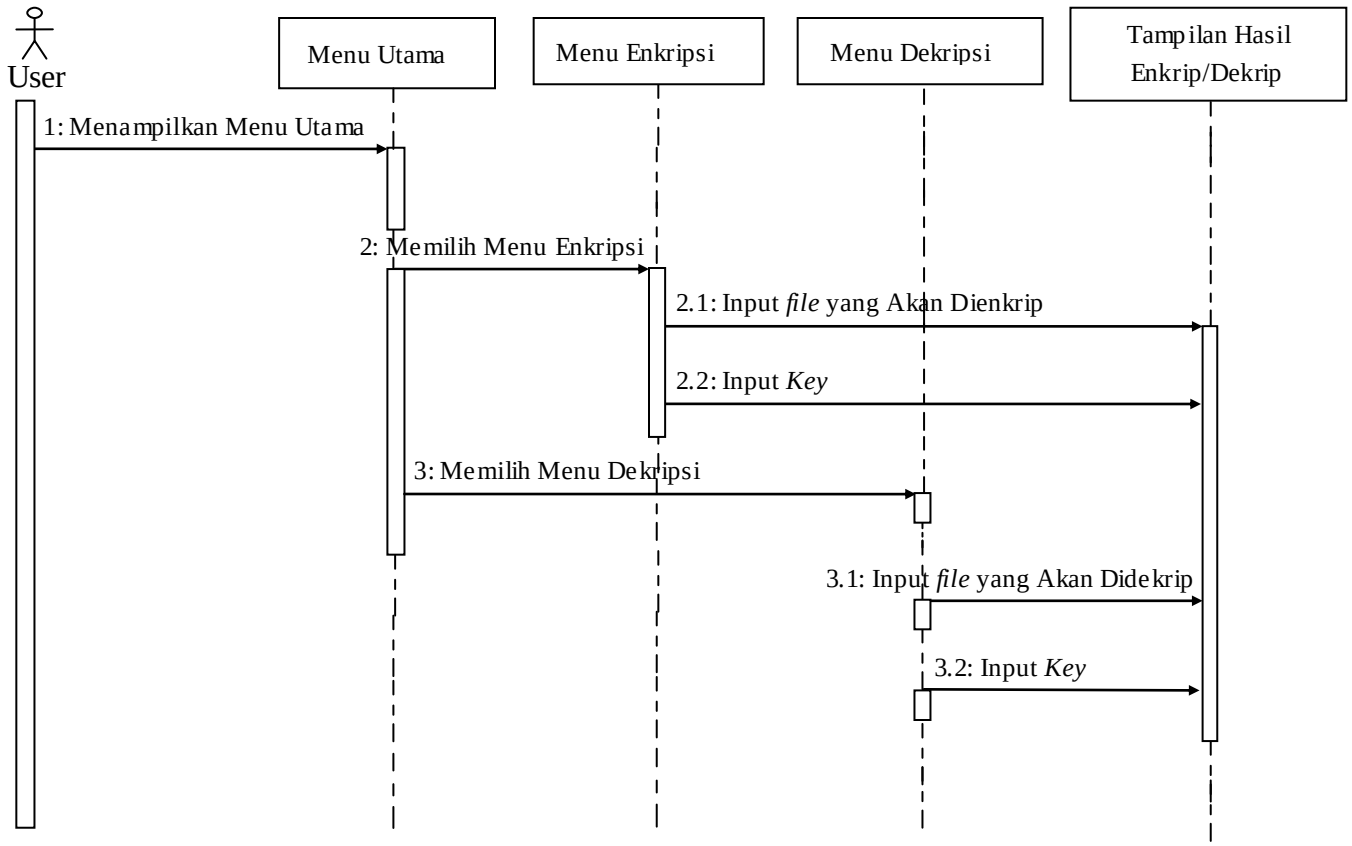


Gambar III.5. *Activity Diagram* Aplikasi yang Dibangun

Pada proses enkripsi, menunjukkan bahwa hal pertama dilakukan adalah memilih folder penyimpanan. Setelah file diinputkan maka isi file akan diambil lalu akan dilakukan proses enkripsi dengan menggunakan algoritma RC4. Kemudian data yang sudah dienkripsi akan disimpan pada direktori yang sudah dipilih di awal, begitu juga halnya pada proses dekripsi.

III.3.3. *Squence* Diagram

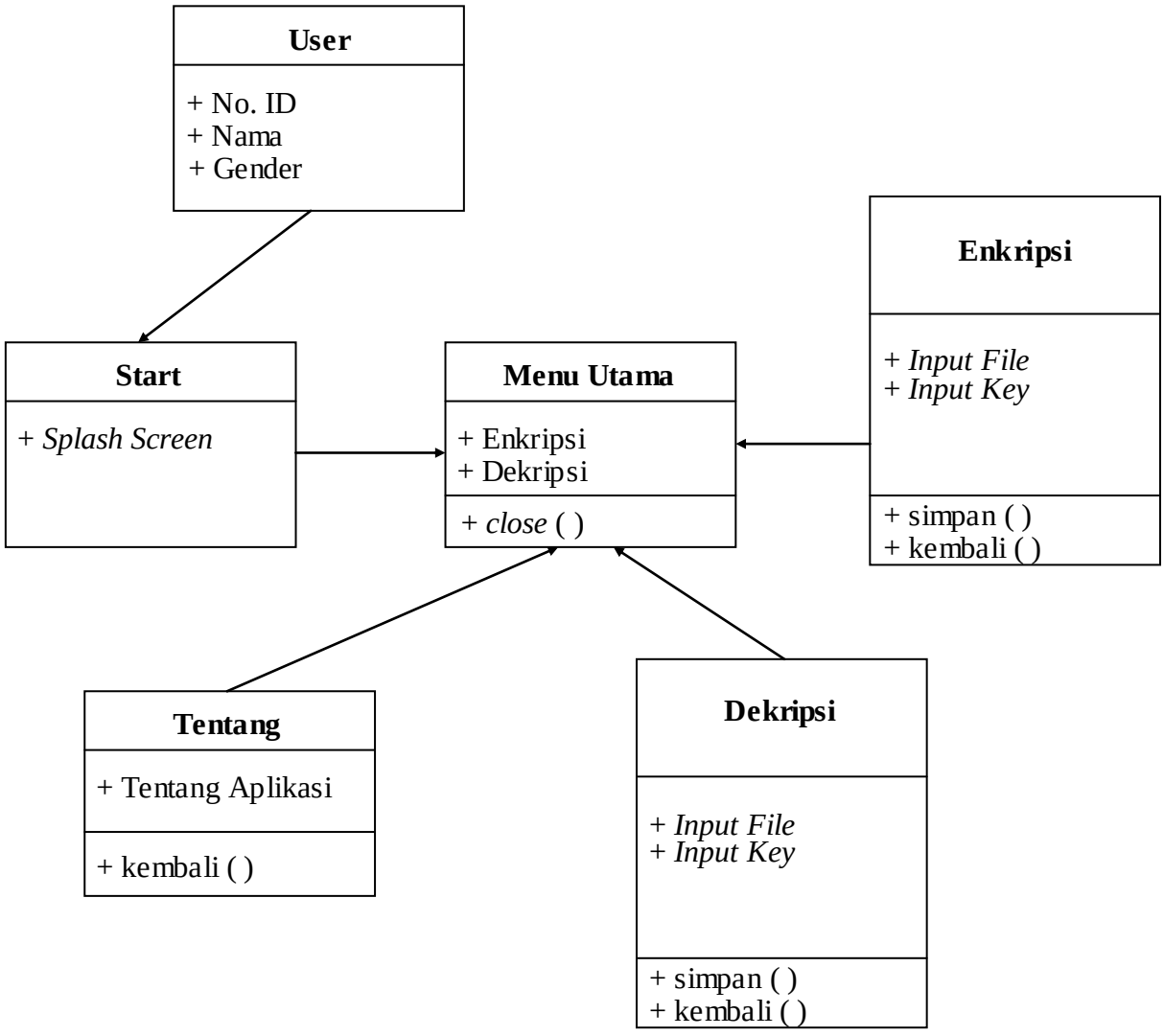
Squence diagram adalah suatu diagram yang menggambarkan interaksi antar objek dan mengindikasikan komunikasi diantara objek-objek tersebut. Berikut sequence diagram aplikasi yang dibangun.



Gambar III.6. *Squence Diagram* Aplikasi yang Dibangun

III.3.4. *Class* Diagram

Class Diagram adalah diagram yang menunjukkan *class-class* yang ada dari sebuah sistem dan hubungannya secara logika. *Class Diagram* menggambarkan hubungan statis dari sebuah sistem. Karena itu *class diagram* merupakan tulang punggung atau kekuatan dasar dari hampir setiap metode berorientasi objek termasuk UML (Henderi, 2008). Berikut ini akan dijelaskan uraian proses yang terjadi pada aplikasi yang dibangun.



Gambar III.7. *Class Diagram* Aplikasi yang Dibangun

III.4. Spesifikasi Perangkat

Dalam perancangan aplikasi untuk perangkat *Android Mobile Phone* ini penulis menggunakan beberapa perangkat agar aplikasi ini dapat berjalan lancar dan sesuai dengan yang diharapkan. Perangkat-perangkat tersebut berupa perangkat keras dan perangkat lunak yang nantinya akan digunakan untuk membangun aplikasi pengamanan data teks menggunakan algoritma RC4, yaitu sebagai berikut :

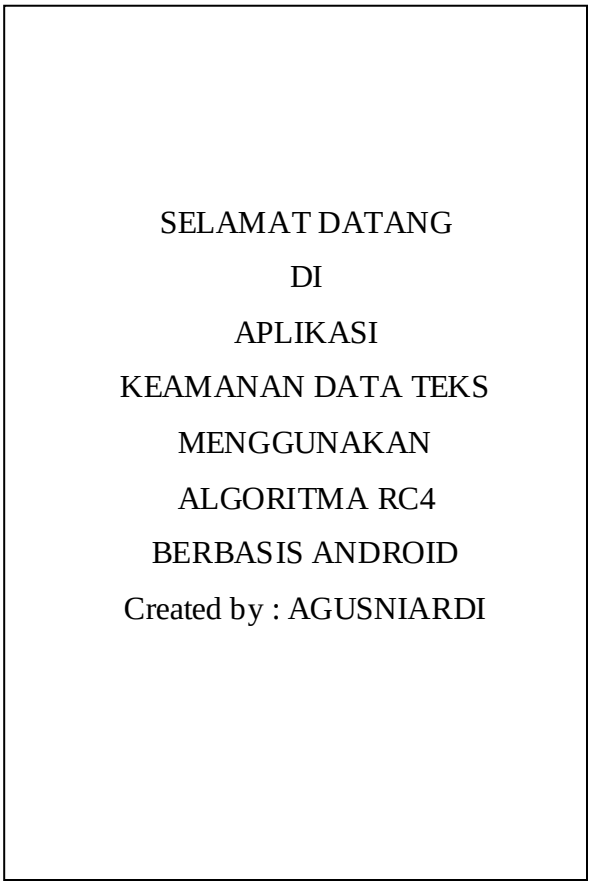
1. Perangkat Keras (*Hardware*)
   a. Komputer yang setara *Core i3*
   b. *Smartphone Android* dengan OS 4.2.1 atau diatasnya
   c. *Mouse*
   d. *Keyboard*
   e. *Monitor*
   f. USB Cable
2. Perangkat Lunak (*Software)*
   a. Operating System, OS yang dipergunakan dalam perancangan adalah *Windows* 8 dan untuk pengujian adalah OS Android pada perangkat *mobile phone Android*.
   b. Eclipse ADT (Android Development Tools), sebagai editor *source code Java*.
   c. JDK *Java 7.0,* sebagai bahasa program.

III.5. Desain Sistem

Dalam proses perancangan ini akan dijelaskan beberapa rancangan aplikasi yang akan dibangun yaitu sebagai berikut :

III.5.1.Rancangan Awal Pembukaan Program

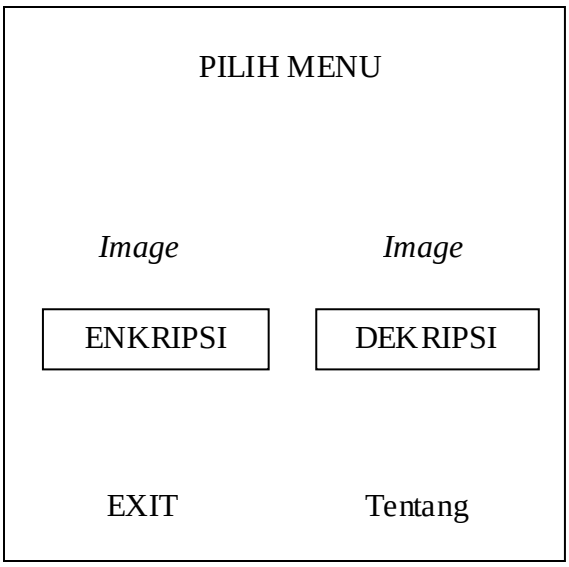
Gambar III.6 ini dibuat untuk menampilkan rancangan awal ketika program pertama kali dibuka.



Gambar III.8. Halaman Pembuka

III.5.2.Rancangan Menu Utama

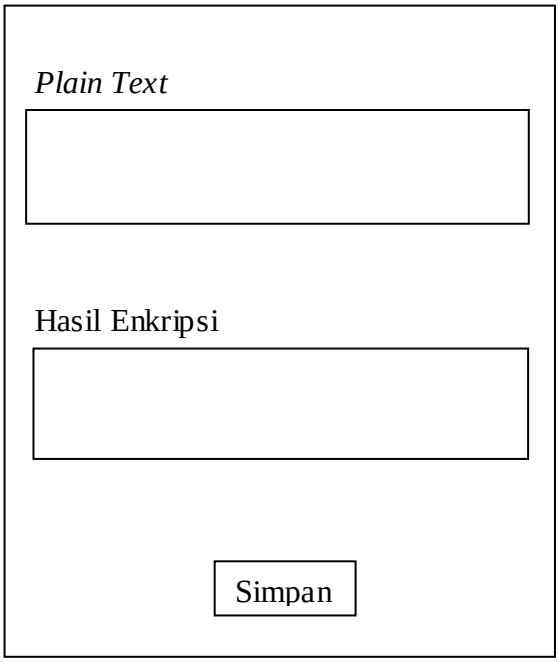
Berikut ini adalah rancangan form menu utama yang dapat lihat pada gambar III.6 dibawah ini.



Gambar III.9. *Form* Menu Utama

III.5.3. Rancangan Form Hasil Enkripsi

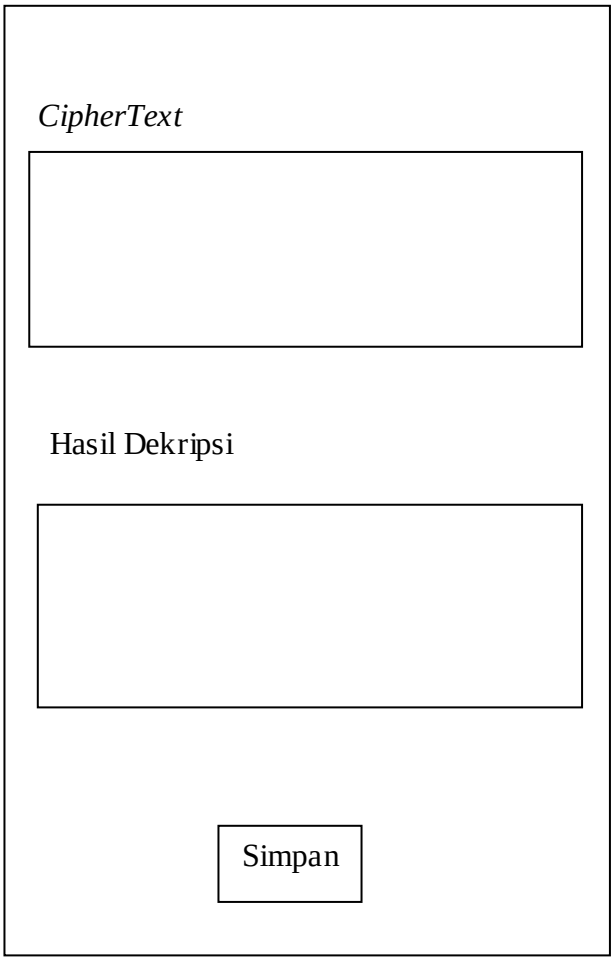
Berikut ini adalah rancangan form hasil enkripsi yang dapat lihat pada gambar III.8 di bawah ini.



Gambar III.10. *Form* Hasil Enkripsi

III.5.4. Rancangan Form Hasil Dekripsi

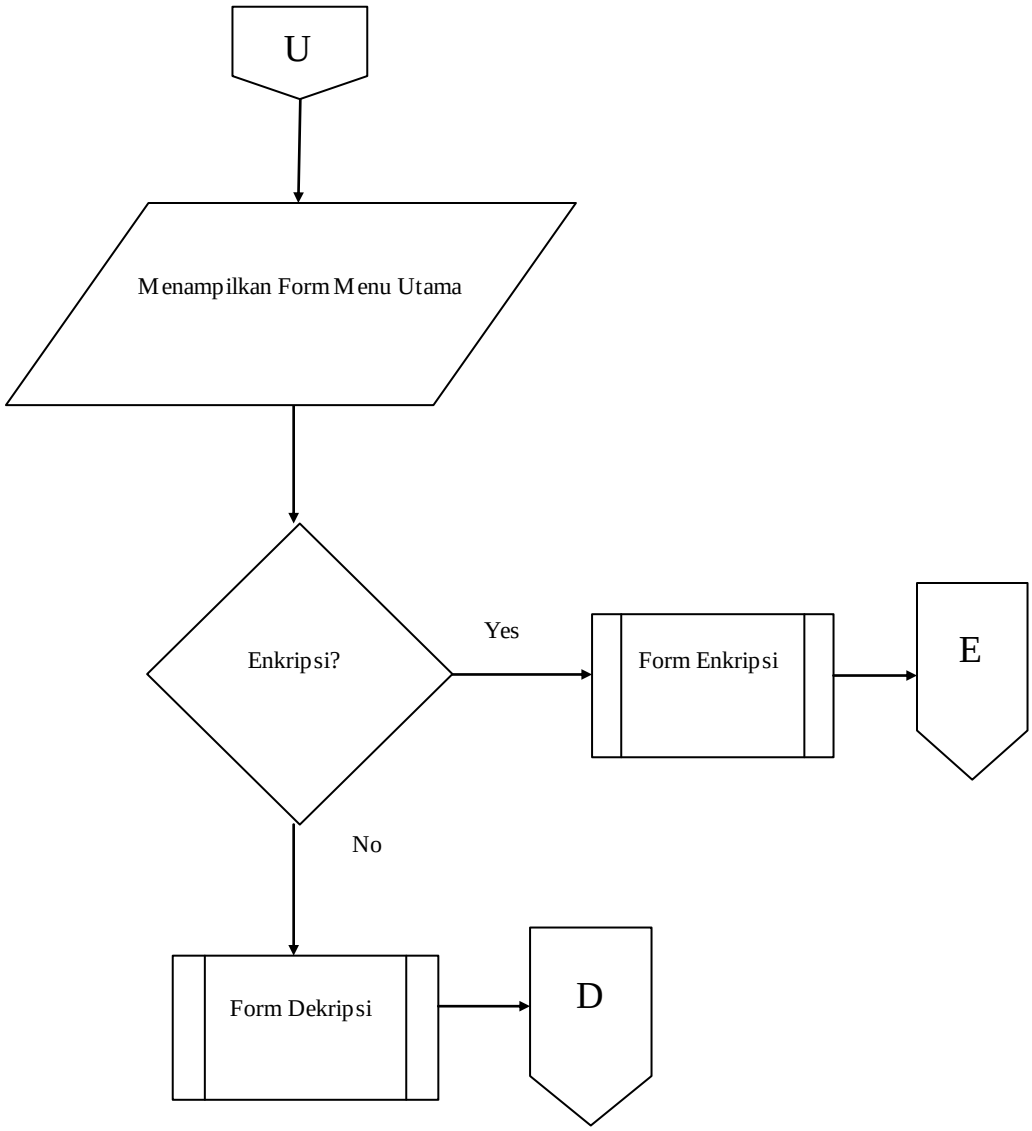
Berikut ini adalah rancangan form hasil dekripsi yang dapat lihat pada gambar III.9 di bawah ini.



Gambar III.11. *Form* Hasil Dekripsi

III.7. *Flowchart* Menu Utama

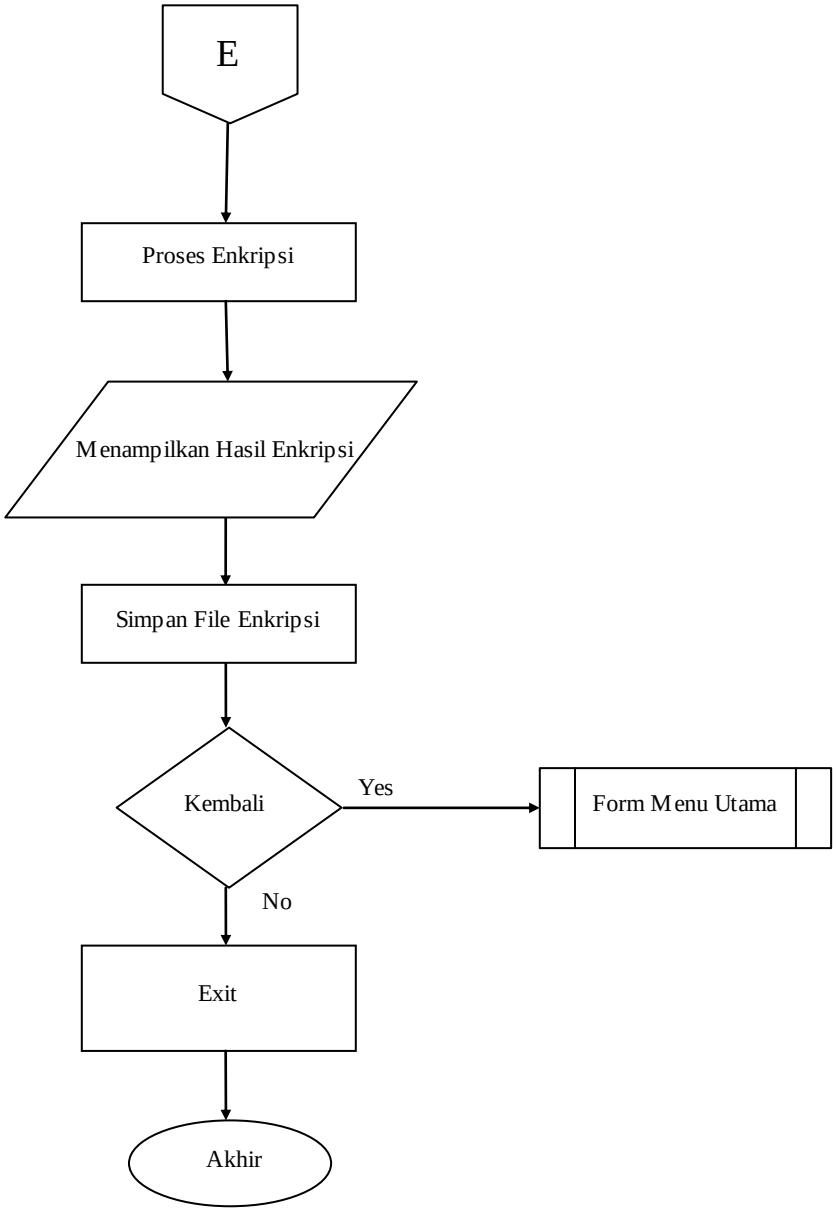
Flowchart ini dibuat untuk menjelaskan proses jalannya menu utama pada program, seperti pada gambar III.10 di bawah ini.



Gambar III.12. *Flowchart* Menu Utama

III.8. *Flowchart* Enkripsi

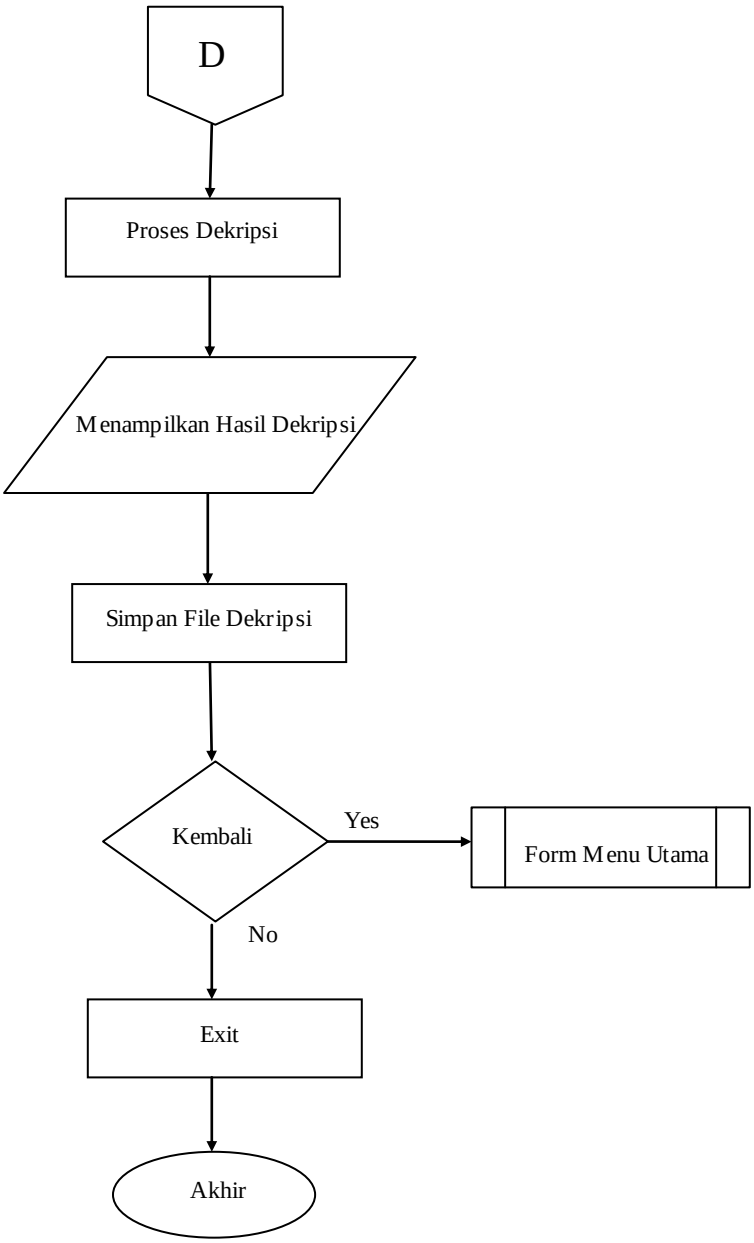
Flowchart ini dibuat untuk menjelaskan proses jalannya enkripsi pada program, seperti pada gambar III.11 di bawah ini.



Gambar III.13. *Flowchart* Enkripsi

III.9. *Flowchart* Dekripsi

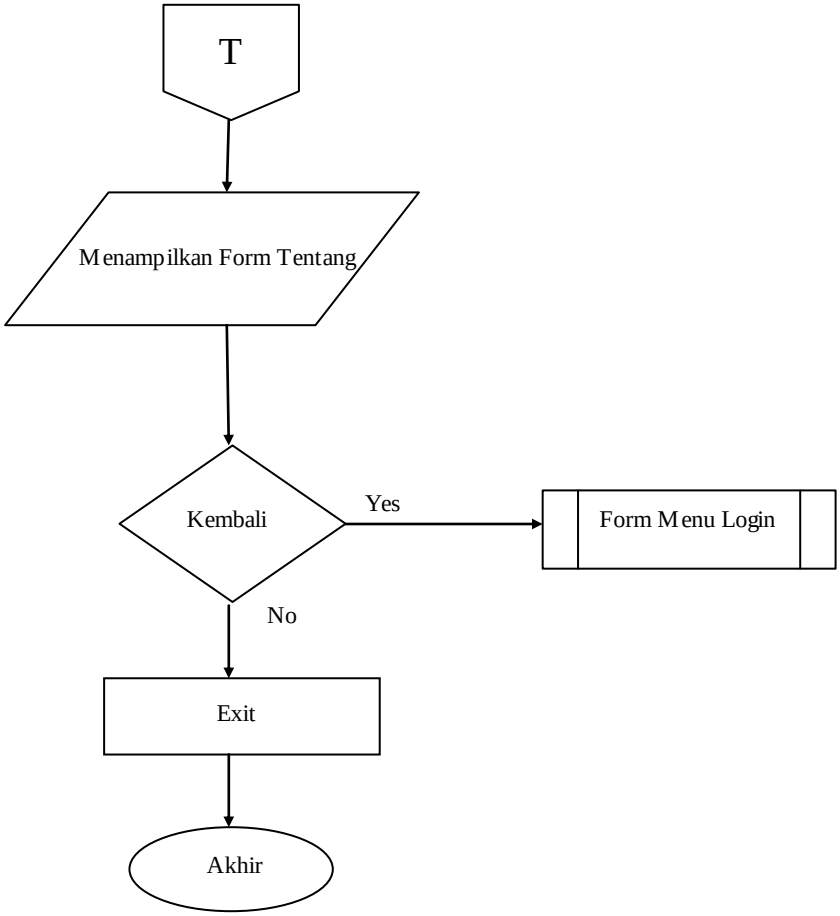
Flowchart ini dibuat untuk menjelaskan proses jalannya dekripsi pada program, seperti pada gambar III.12 di bawah ini.



Gambar III.14. *Flowchart* Dekripsi

III.10. *Flowchart* Tentang

Flowchart ini dibuat untuk menampilkan tentang program, seperti pada gambar III.13 di bawah ini.



Gambar III.15. *Flowchart* Tentang