BAB III
ANALISIS DAN PERANCANGAN

III.1. Analisis Masalah

Permasalahan yang terjadi pada saat melakukan penelitian yaitu masih lemahnya sistem keamanan data terutama dalam pengamanan pesan *chat* dan berkembangnya tindakan penyalahgunaan informasi sehingga diperlukan pengembangan teknik keamanan yang dapat memberikan proteksi lebih baik agar kerahasiaan pesan terjaga maka implementasi teknik kriptografi simetrik sangat cocok untuk memenuhi kebutuhan keamanan pesan *chat*, seperti algoritma pertukaran kunci *Diffie-Hellman* pada algoritma *data encryption standard* (*des*).

Strategi dalam melakukan pemecahan masalah yang sedang dianalisa oleh penulis mengenai perancangan Aplikasi Penyandian Pesan chat Menggunakan Metode Diffie-Hellman adalah sebagai berikut :

1. Merancang sebuah aplikasi enkripsi dan deskripsi pesan *chat* dengan memanfaatkan kriptografi pertukaran kunci *Diffie-Hellman* pada algoritma *data encryption standard* (*des*) yang dapat menjaga kerahasiaan pesan text pada aplikasi chat.
2. Mengimplementasikan algoritma pertukaran kunci *Diffie-Hellman* pada algoritma *data encryption standard* (*des*). dalam pembuatan aplikasi pengamanan pesan chat berbasis android.

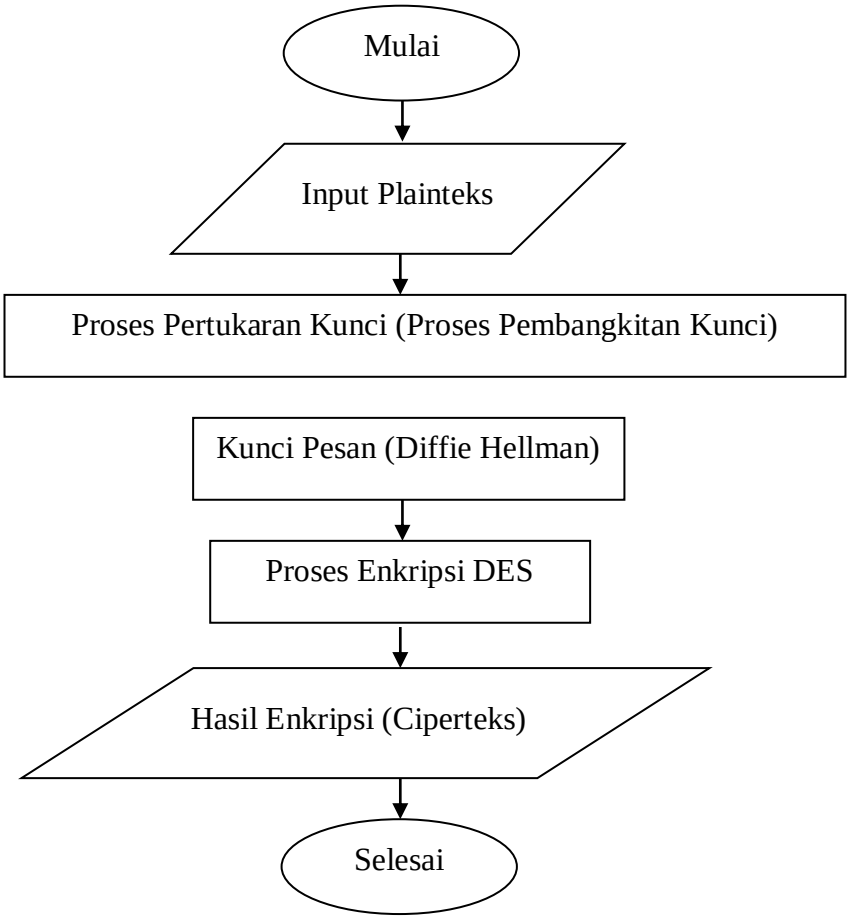
III.1.1. Analisis *Input*

Analisa input digunakan untuk melakukan analisis data pada aplikasi. Data yang digunakan pada analisa input adalah *text chat* sebelum dilakukan enkripsi. Misalnya *text* yang dimasukkan oleh user pada aplikasi *chatting*, data text ini kemudian akan diamankan menggunakan algoritma.

III.1.2. Analisis Proses

1. Analisis Proses Enkripsi *Text*

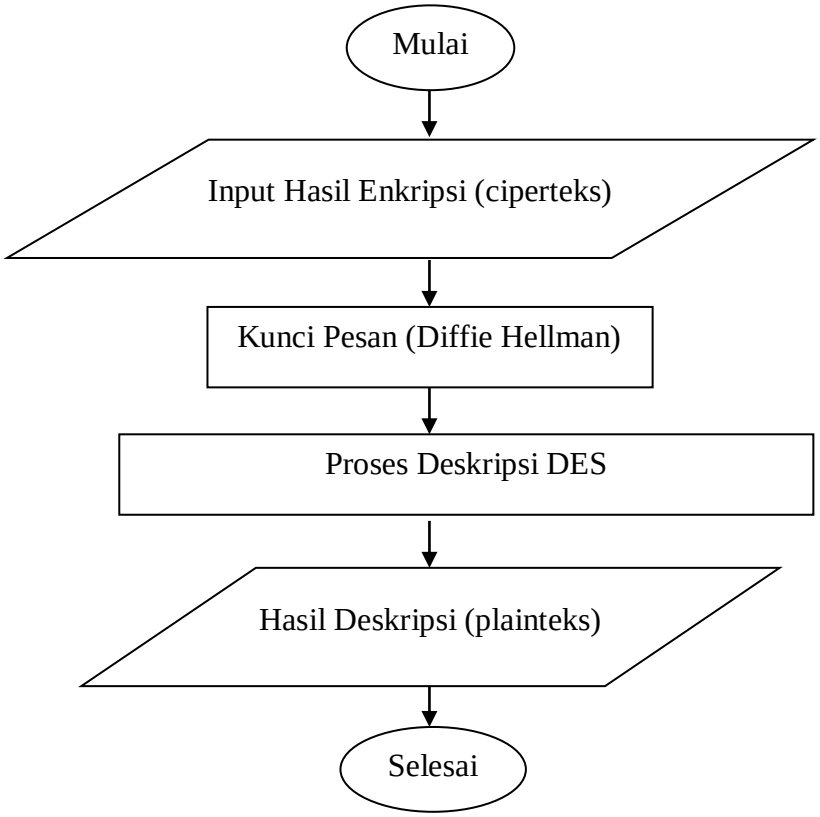
Analisa proses digunakan untuk mengentahui prosedur yang digunakan dalam melakukan pengolahan enkripsi *text*.



Gambar III.1. FOD Proses Enkripsi *Chat Text*

2. Analisis Proses Dekripsi *Text*

Analisa proses digunakan untuk mengentahui prosedur yang digunakan dalam melakukan pengolahan dekripsi *text*.



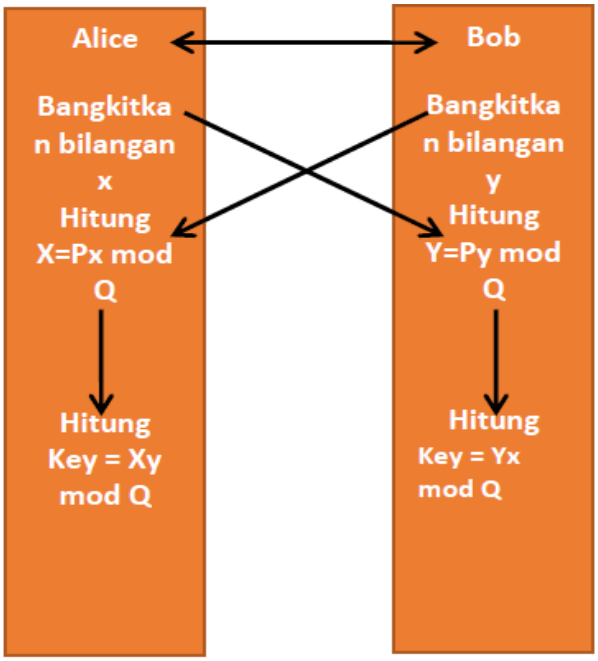
Gambar III.2. FOD Proses Dekripsi *Chat Text*

III.1.3. Analisis *Output*

Analisa output digunakan untuk melihat hasil akhir dari pengolahan data input dan analisa output. Analisa output yang dihasilkan oleh pengolahan data input adalah data dekripsi dari text yang akan dikirmkan, contohnya adalah kata "Hallo" setelah di enkripsikan maka yang keluar adalah "01001000 01000001 01001100 01001111" yang dibentuk sebagai kata kunci dekripsi.

III.2. Pembangkitan Kunci Dengan Menggunakan Metode Diffie Hellman

Algoritma pertukaran kunci Diffie- Hellman (protokol Diffie-Hellman) berguna untuk mempertukarkan kunci rahasia pada komunikasi menggunakan kriptografi simetris..



Gambar III.3. Skema Algoritma Diffie Hellman

Kekuatan algoritma ini adalah pada sulitnya melakukan perhitungan logaritma diskrit. Langkah-langkahnya adalah sebagai berikut,

1. Misalkan Alice dan Bob adalah pihak-pihak yang berkomunikasi. Mula-mula Alice dan Bob menyepakati 2 buah bilangan yang besar (sebaiknya prima) P dan Q, sedemikian sehingga P < Q. Nilai P dan Q tidak perlu rahasia, bahkan Alice dan Bob dapat membicarakannya melalui saluran yang tidak aman sekalipun.

2. Alice membangkitkan bilangan bulat acak x yang besar dan mengirim hasil perhitungan berikut kepada Bob :

$X = Px \bmod Q.$

3. Bob membangkitkan bilangan bulat acak y yang besar dan mengirim hasil perhitungan, berikut kepada Alice:

$Y = P\,y \bmod Q.$

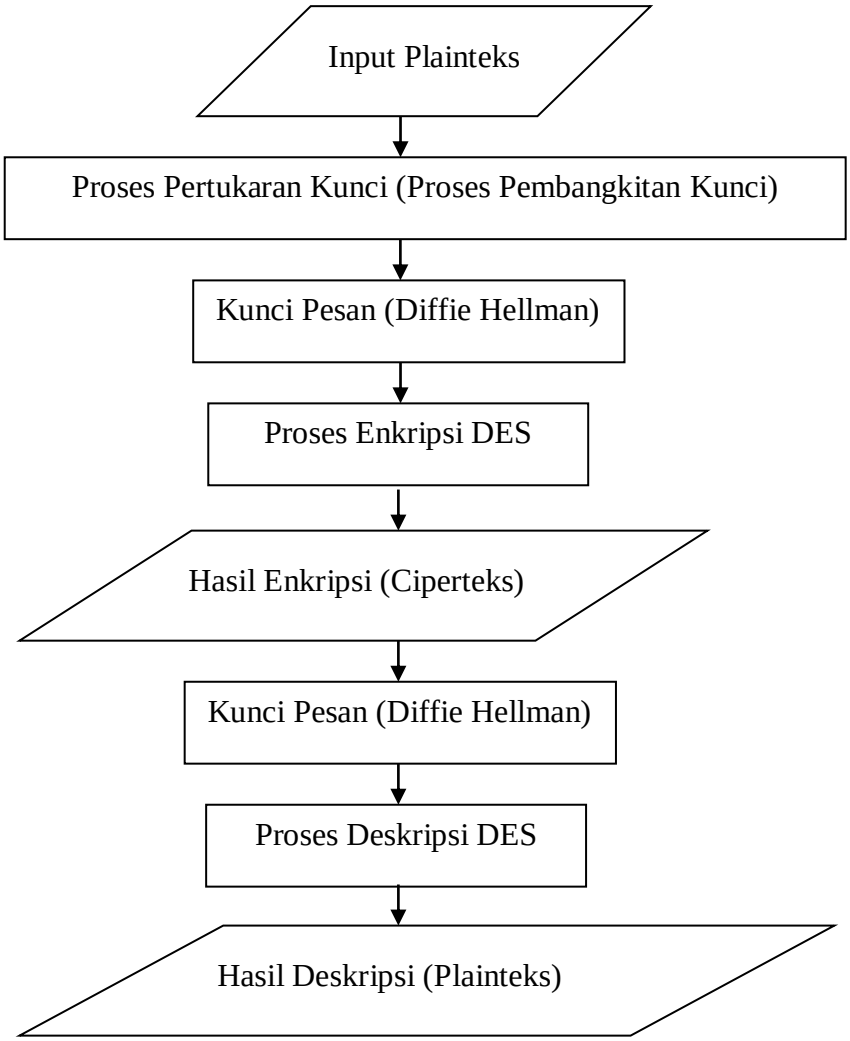
4. Alice menghitung $K = Y\,x \bmod Q.$

5. Bob menghitung $K' = X\,y \bmod Q.$

Jika perhitungan dilakukan dengan benar maka K = K'. Dengan demikian Alice dan Bob telah memiliki sebuah kunci yang sama tanpa diketahui pihak lain. Dan apabila pihak ketiga ingin menyadap informasi percakapan antara Alice dan Bob ia tidak akan menemukan nilai K karena hanya memiliki informasi tentang X, Y, p, q namun tidak memiliki informasi tentang x dan y. Dan untuk mengetauinya ia perlu melakukan perhitungan logaritma diskrit yang sangat sulit untuk dikerjakan.

III.2.1. Implementasi Metode Pertukaran Kunci Diffie Hellman Pada Algoritma Data Encryption Standard (DES)

Implementasi metode diffie hellman pada algoritma DES dapat dilihat dari gambar III.4 Berikut :



Gambar III.4. Implementasi Diffie Hellman Pada Algoritma DES

III.3. Perancangan

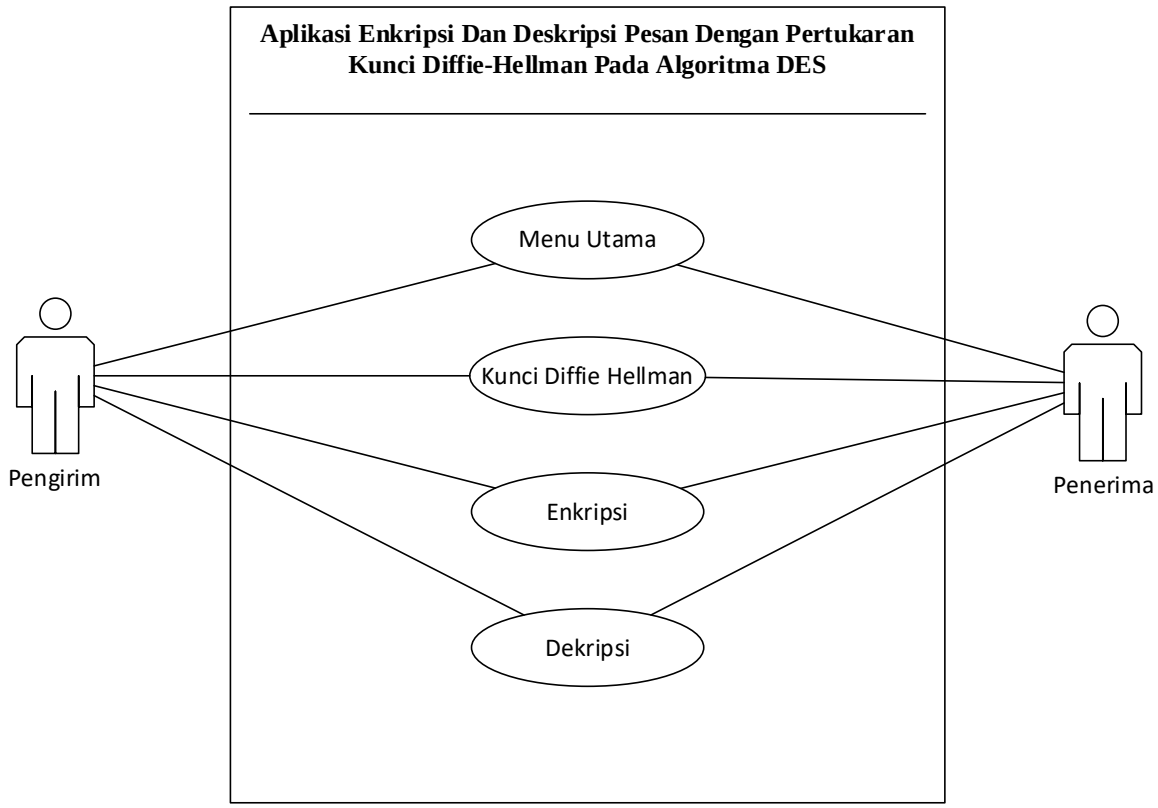
Desain sistem pada penelitian ini dibagi menjadi dua desain, yaitu desain sistem secara global untuk penggambaran model sistem secara garis besar dan desain sistem secara detail untuk membantu dalam pembuatan sistem.

III.3.1. Desain Sistem

Desain sistem secara global menggunakan bahasa pemodelan UML yang terdiri dari *Usecase Diagram*, *Acitvity Diagram* dan *Sequence Diagram*.

III.3.1.1. *Usecase* Diagram

Dalam penyusunan suatu program diperlukan suatu model data yang berbentuk diagram yang dapat menjelaskan suatu alur proses sistem yang akan di bangun. Dalam penulisan skripsi ini penulis menggunakan metode UML yang dalam metode itu penulis menerapkan diagram *Use Case*. Maka digambarlah suatu bentuk diagram *Use Case* yang dapat dilihat pada gambar dibawah ini



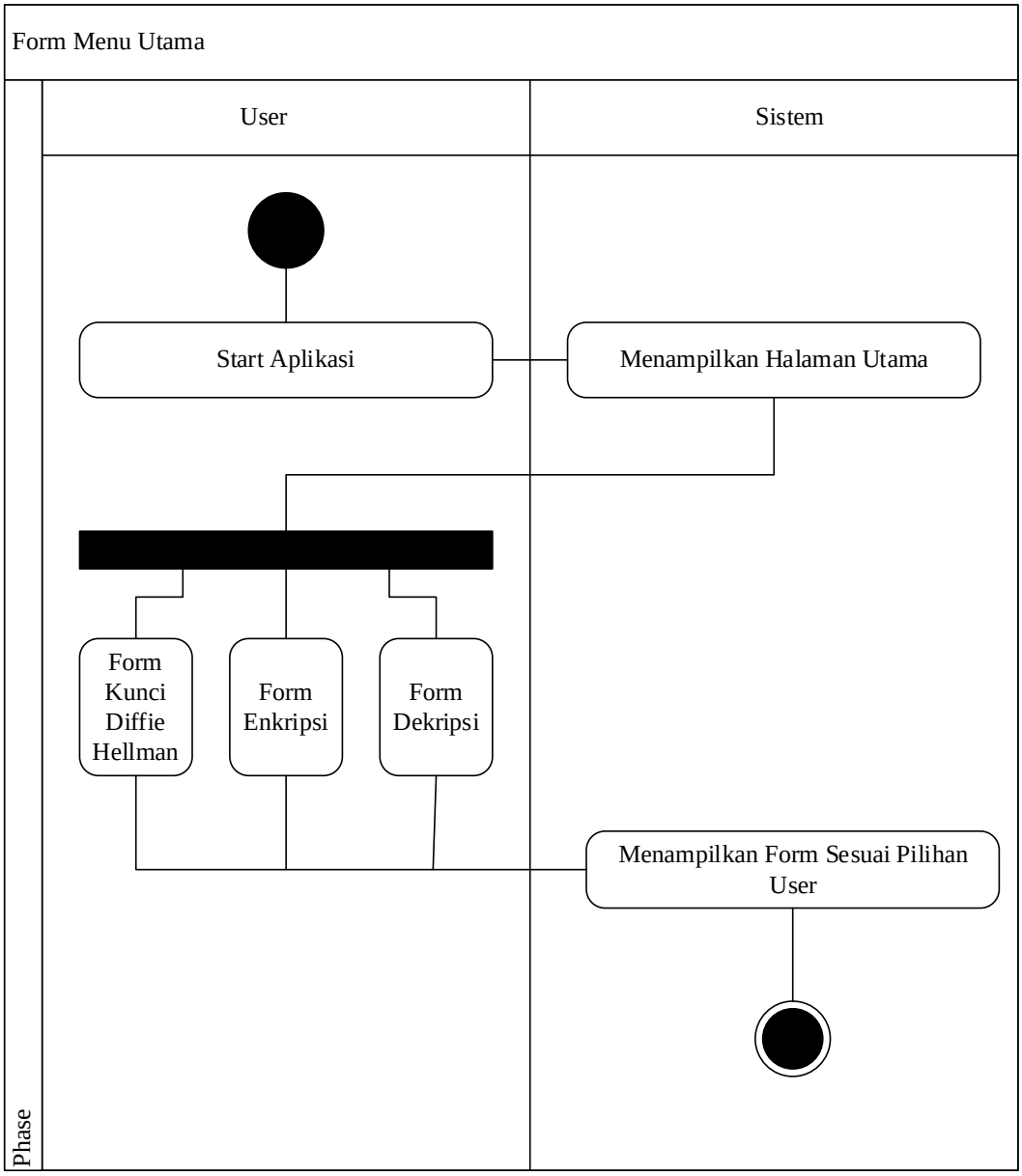
Gambar III.5. *Use Case* Diagram Aplikasi Enkripsi Dan Deskripsi Pesan Dengan Pertukaran Kunci Diffie-Hellman Pada Algoritma DES

III.3.1.2. *Activity* Diagram

Bisnis proses yang telah digambarkan pada *use case diagram* dijabarkan dengan *activity diagram* :

1. *Activity Diagram* Menu Utama

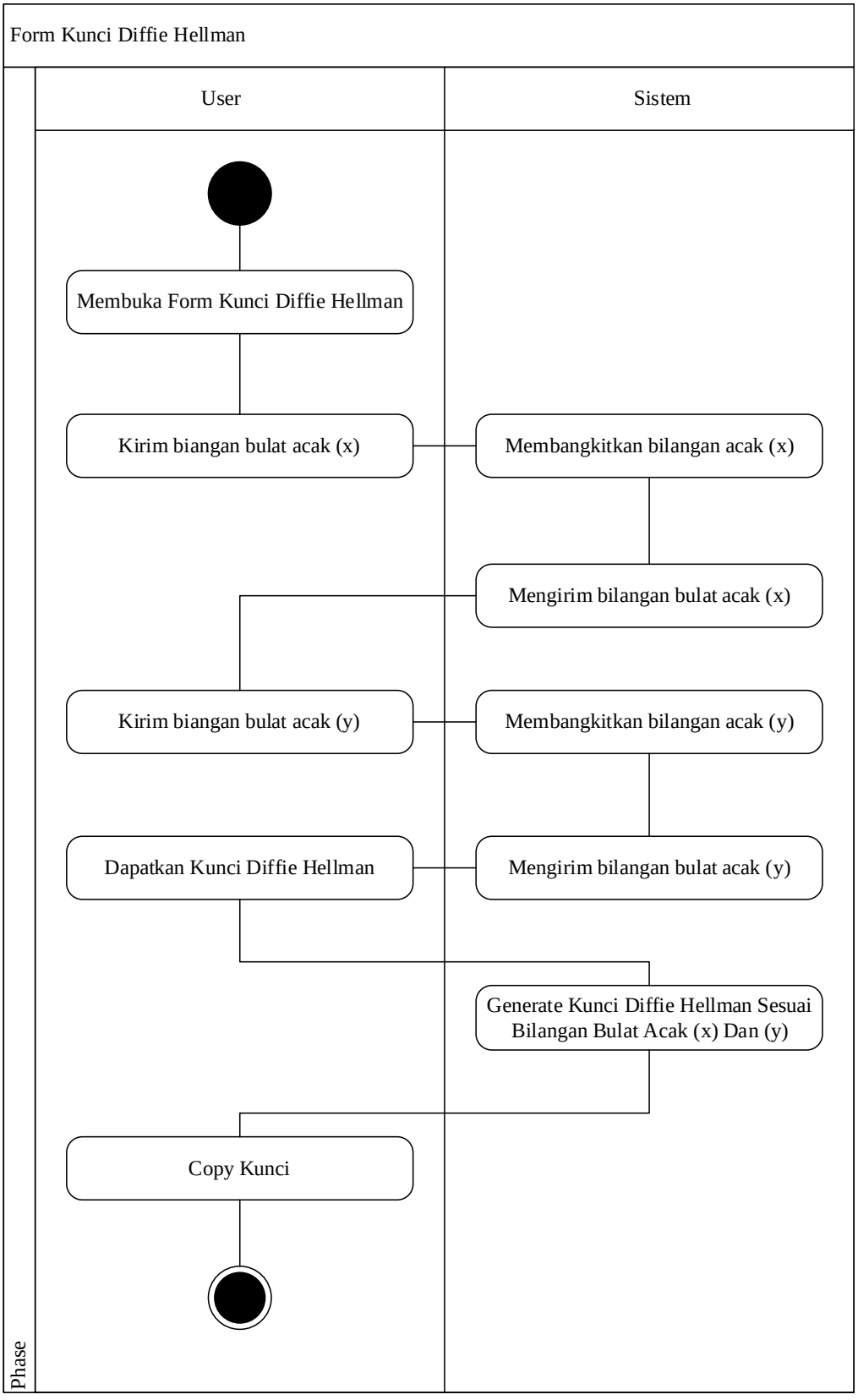
Aktivitas yang dilakukan oleh pengguna pada form menu utama dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar III.6 berikut :



Gambar III.6. *Activity Diagram* Form Pertukaran Kunci

2. *Activity Diagram* Kunci Diffie Hellman

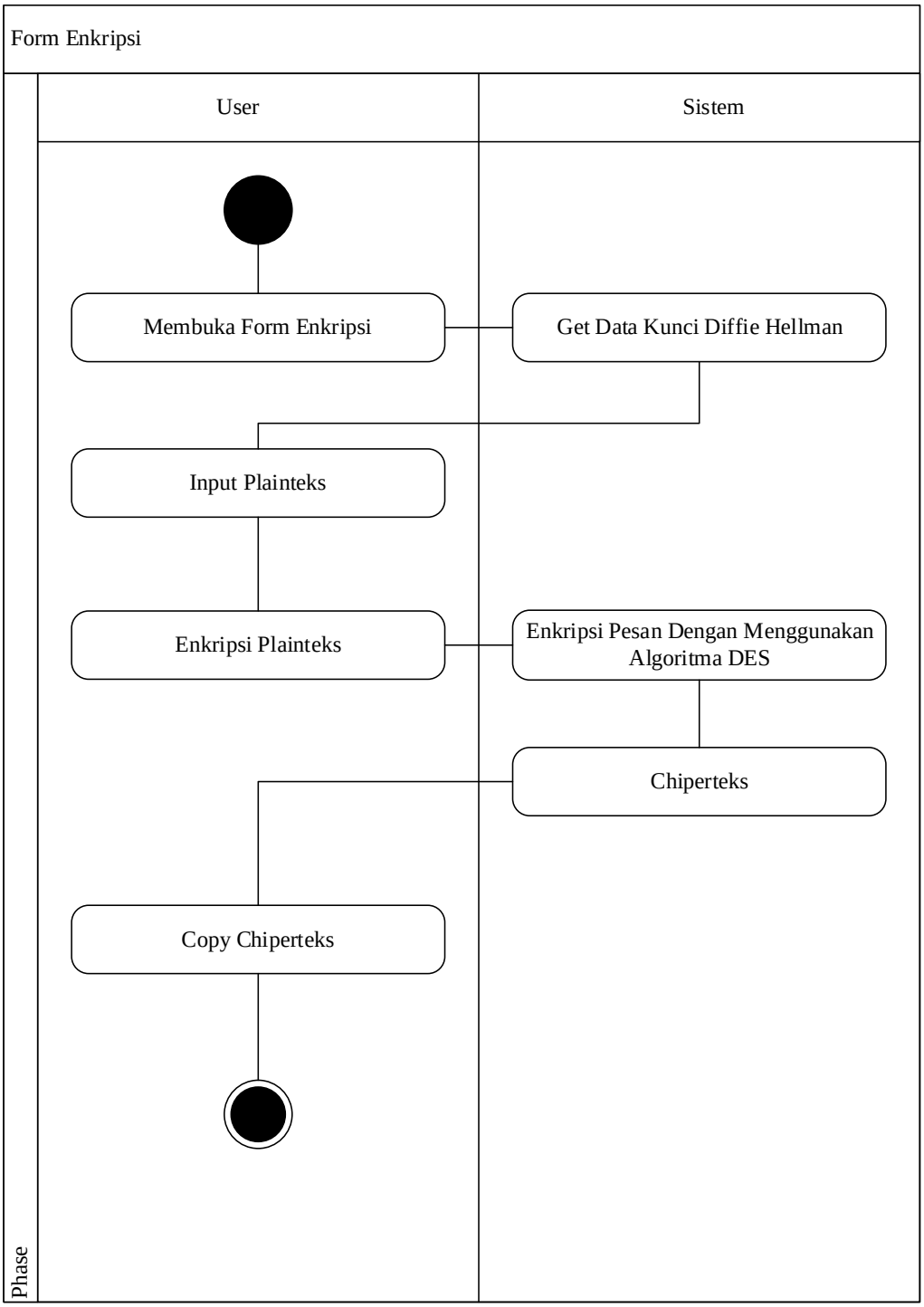
Aktivitas yang dilakukan oleh pengguna pada form kunci diffie hellman dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar III.7 berikut :



Gambar III.7. *Activity Diagram* Form Diffie Hellman

3. *Activity Diagram* Enkripsi

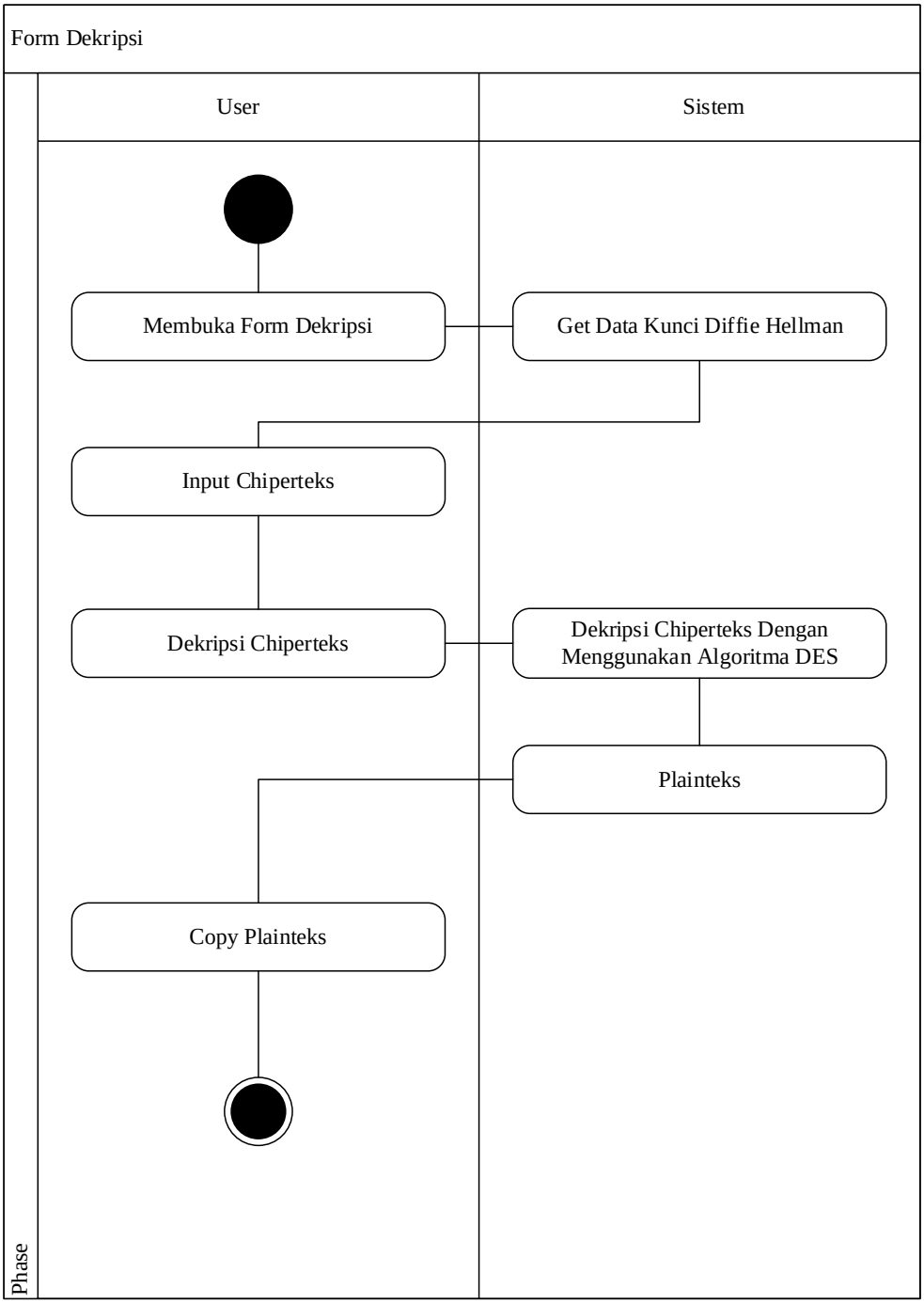
Aktivitas yang dilakukan oleh user pada form Enkripsi dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar III.8 berikut



Gambar III.8. *Activity Diagram* Form Enkripsi

4. *Activity Diagram* Dekripsi

Aktivitas yang dilakukan oleh user pada form Dekripsi dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar III.9 berikut:



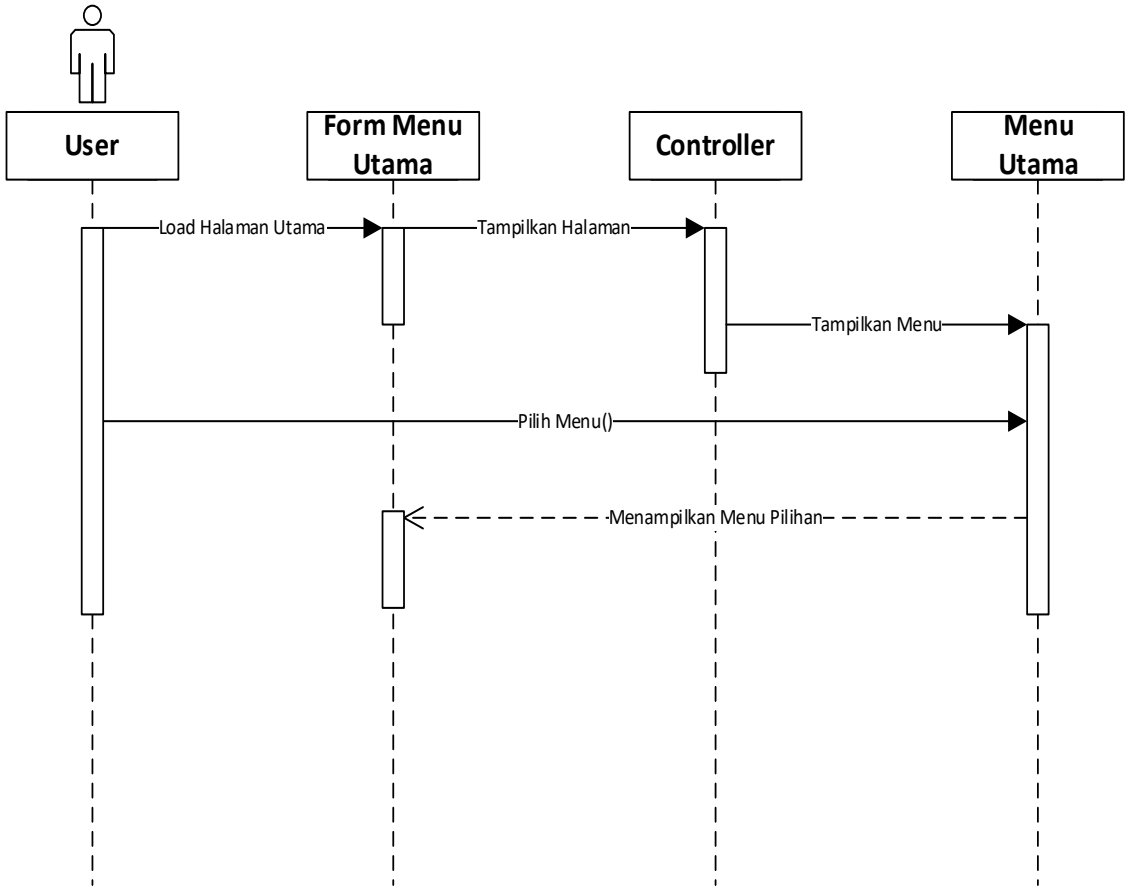
Gambar III.9. *Activity Diagram* Form Enkripsi

III.3.1.3. Sequence Diagram

Sequence Diagram (diagram urutan) adalah suatu diagram yang memperlihatkan atau menampilkan interaksi-interaksi antar objek di dalam sistem yang disusun pada sebuah urutan atau rangkaian waktu. Interaksi antar objek tersebut termasuk pengguna, *display*, dan sebagainya berupa pesan/*message*.

1. *Sequence Diagram* Halaman Utama

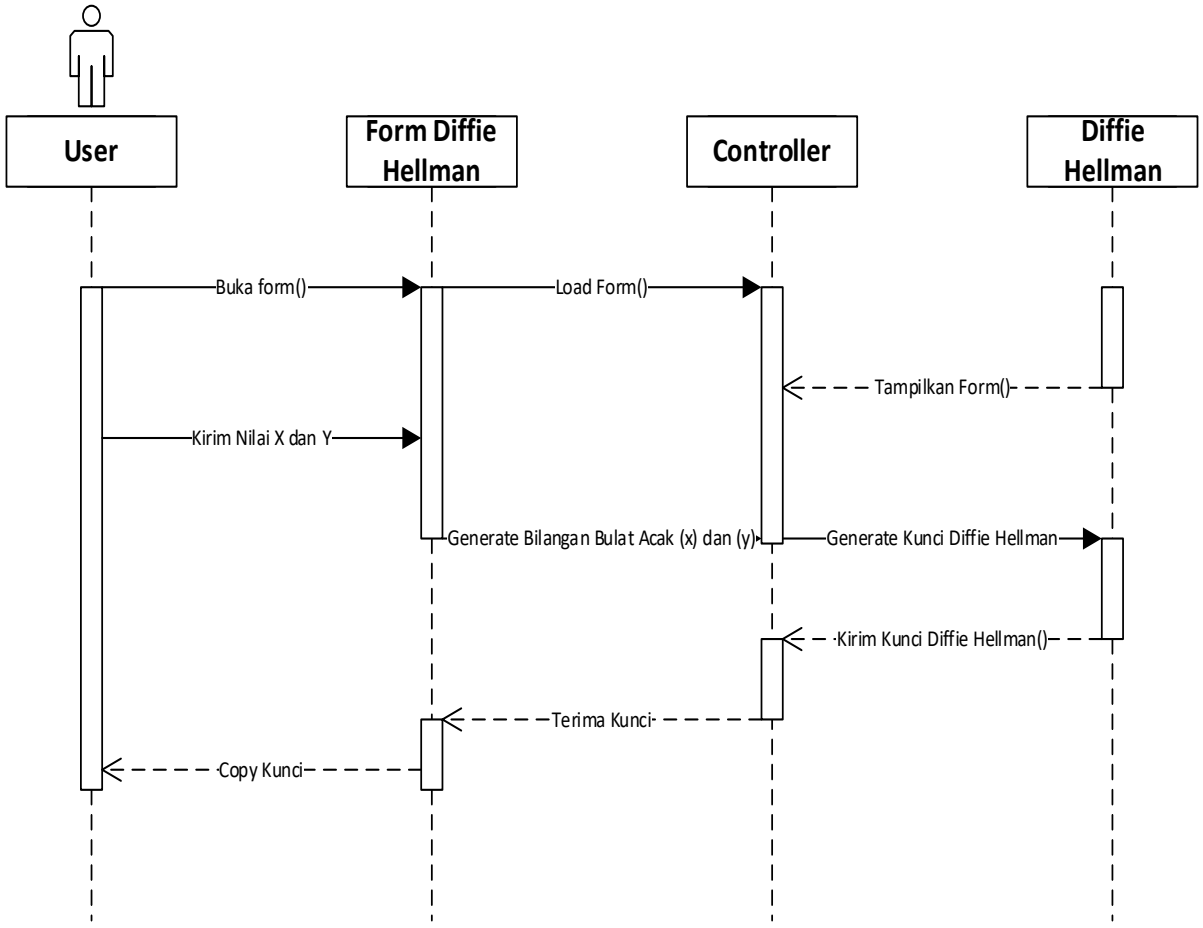
Serangkaian kegiatan sistem yang dilakukan oleh user pada form halaman utama dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar III.10 berikut :



Gambar III.10. *Sequence Diagram* Form Halaman Utama

2. *Sequence Diagram* Form Pertukaran Kunci

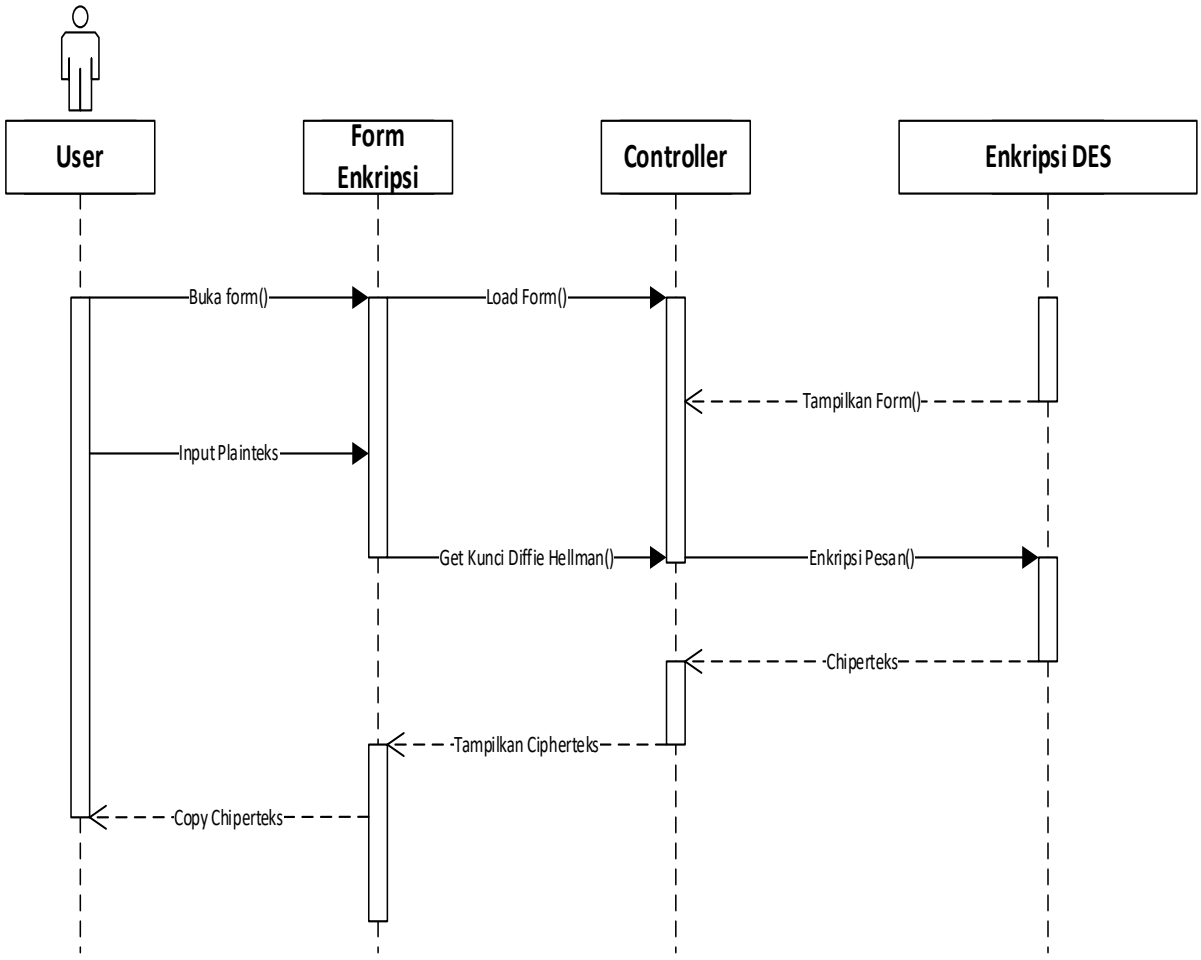
Serangkaian kegiatan sistem yang dilakukan oleh user pada form kunci diffie hellman dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar III.11 berikut :



Gambar III.11. *Sequence Diagram* Form Diffie Hellman

3. *Sequence Diagram Form* Enkripsi

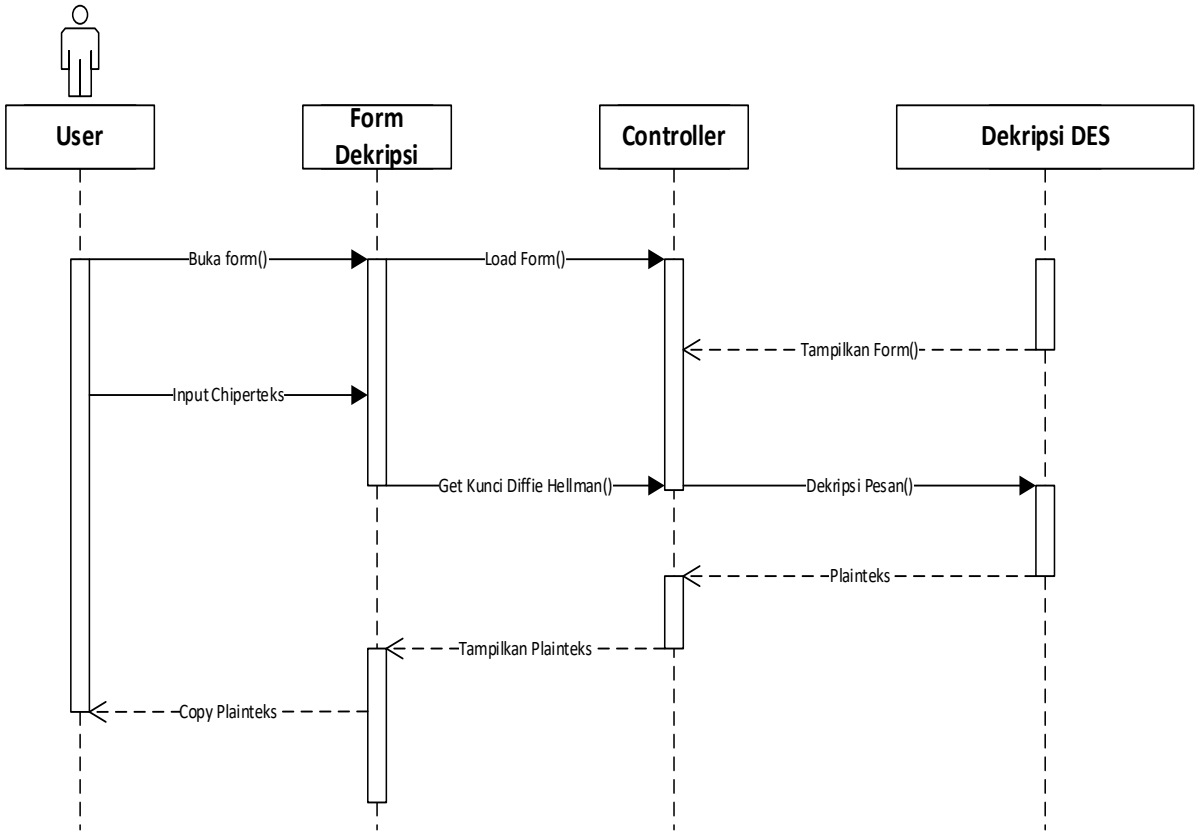
Serangkaian kegiatan sistem yang dilakukan oleh user pada form Enkripsi dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar III.12 berikut :



Gambar III.12. *Sequence Diagram* Form Enkripsi

4. *Sequence Diagram Form* Deskripsi

Serangkaian kegiatan sistem yang dilakukan oleh user pada form Deskripsi dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar III.13 berikut :



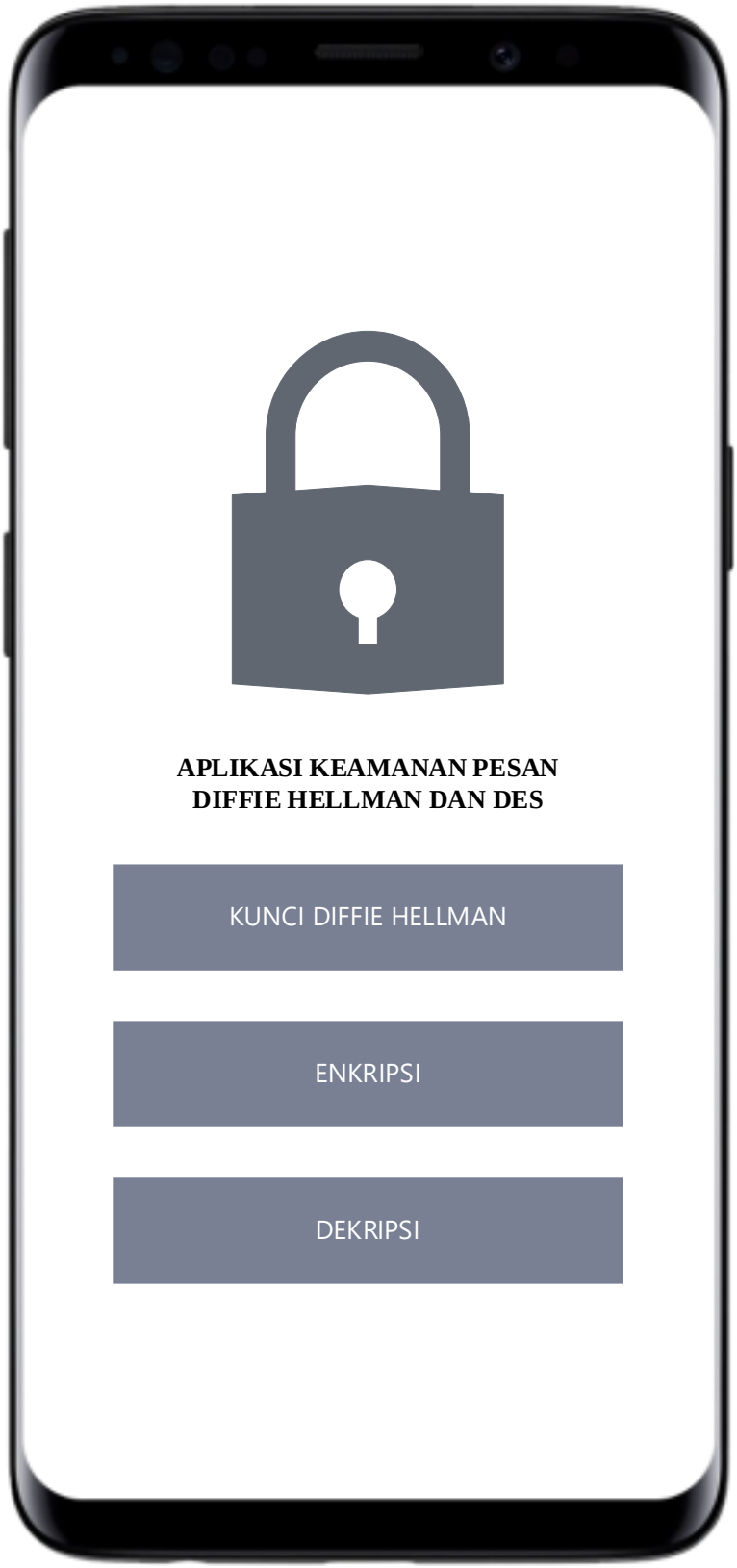
Gambar III.13. *Sequence Diagram* Form Dekripsi

III.3.2. Desain Interface

Tahap perancangan berikutnya yaitu desain tampilan secara detail yang meliputi desain sistem.

1. *Desain* Halaman Utama

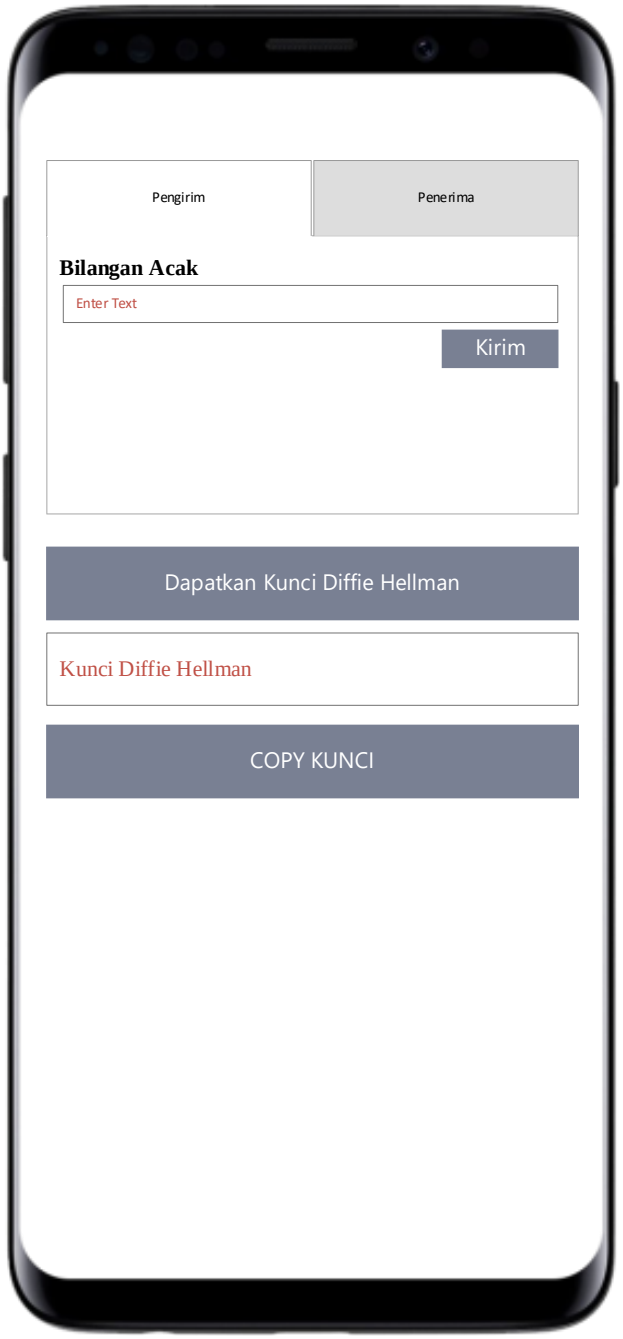
Serangkaian kegiatan sistem yang dilakukan oleh user pada form halaman utama dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar III.14 berikut :



Gambar III.14. *Desain* Form Halaman Utama

2. *Desain* Kunci Diffie Hellman

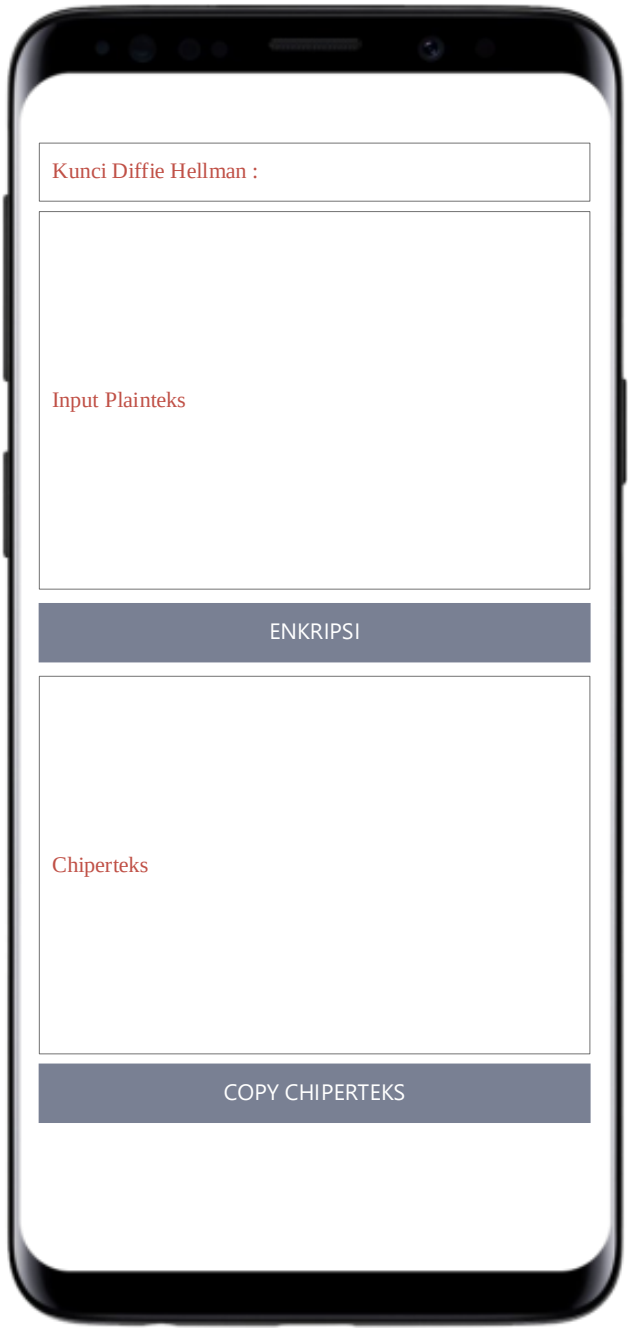
Serangkaian kegiatan sistem yang dilakukan oleh user pada form kunci diffie hellman dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar III.15 berikut :



Gambar III.15. *Desain* Form Kunci Diffie Hellman

3. *Desain* Enkripsi

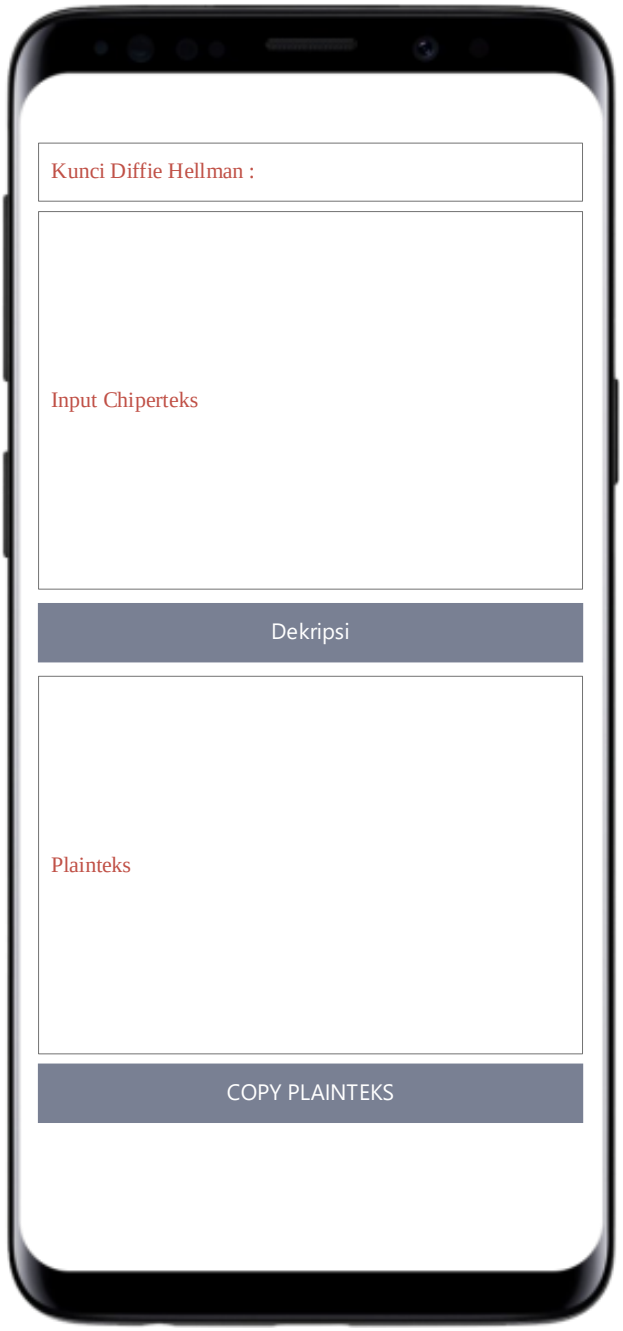
Serangkaian kegiatan sistem yang dilakukan oleh user pada form enkripsi dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar III.16 berikut :



Gambar III.16. *Desain* Form Enkripsi

4. *Desain* Dekripsi

Serangkaian kegiatan sistem yang dilakukan oleh user pada form dekripsi dapat diterangkan dengan langkah-langkah *state* berikut, yang ditunjukkan pada gambar III.17 berikut :



Gambar III.17. *Desain* Form Dekripsi