

## BAB III

### ANALISIS DAN DESAIN SISTEM

#### III.1. Analisis Masalah

SMS memungkinkan pengguna *handphone* untuk mengirim pesan singkat kepada pengguna *handphone* yang lain dengan cepat dan hanya menggunakan biaya yang sedikit. SMS memiliki banyak celah yang memungkinkan para pencuri untuk mengambilnya. Kelebihan dari SMS ini adalah ketika tujuan sedang sibuk, pesan tetap dapat dikirimkan dengan menyimpan pesan tersebut pada SMSC (*Short Message Service Center*) dan akan mengirimkan ketika tujuan sudah tidak sibuk. Namun kelebihan ini juga yang menjadikannya kelemahan, dengan tersimpannya pesan pada SMSC, maka penyerang dapat mendapatkan pesan dengan melakukan penyusupan pada SMSC tersebut.

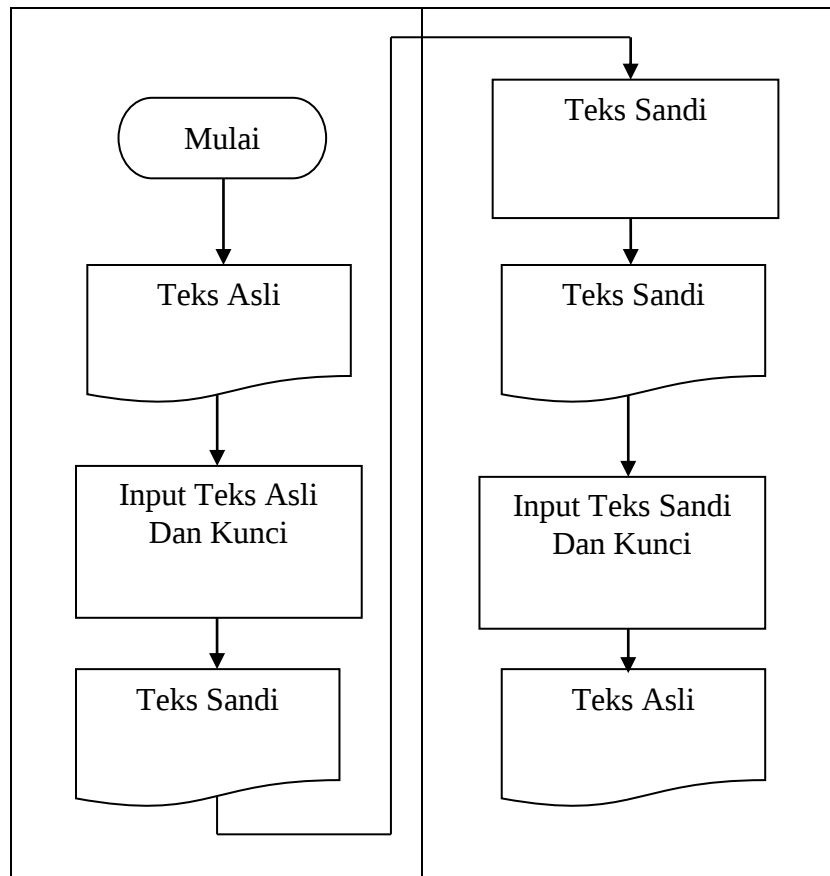
##### III.1.1. Input

*Input* data pada rancang bangun aplikasi kriptografi SMS menggunakan metode *one time pad* berbasis *android* adalah berupa teks SMS.

##### III.1.2. Proses

Berdasarkan sistem yang sedang berjalan, tahapan-tahapan proses penyandian SMS dengan metode *one time pad* dapat dilihat pada gambar III.1. berikut:

|          |          |
|----------|----------|
| Enkripsi | Dekripsi |
|----------|----------|



**Gambar III.1. Proses Enkripsi Dan Dekripsi Pesan**

### III.1.3. Output

Hasil *output* pada rancang bangun aplikasi kriptografi SMS menggunakan metode *one time pad* berbasis *android* adalah berupa isi teks SMS yang tersandikan.

### III.2. Penerapan Metode

Pada rancang bangun aplikasi kriptografi SMS menggunakan metode *one time pad* berbasis *android* dibutuhkan sebuah perhitungan yang sesuai dengan metode yang digunakan.

Adapun rumus dan perhitungan metode yang digunakan adalah sebagai berikut:

Contoh Algoritma enkripsi *One Time Pad cipher*:

$$C = P \text{ XOR } K$$

Contoh Proses Enkripsi  $P \text{ XOR } K$ :

*Plaintext* : xyz

Kunci : 9

Solusi:

*Biner Plaintext*:

$x = 01111000$ ,  $y = 01111001$ ,  $z = 01111010$

*Biner Key*: 9 = 00111001

$C1 = 01111000 \text{ XOR } 00111001$

$= 01000001 = A$

$C2 = 01111001 \text{ XOR } 00111001$

$= 01000000 = @$

$C3 = 01111010 \text{ XOR } 00111001$

$= 01000011 = C$

Hasil dari proses enkripsinya xyz XOR 9 adalah = A@C

Contoh Algoritma dekripsi *One Time Pad cipher*:

$P = C \text{ XOR } K$

Contoh Proses Dekripsi  $C \text{ XOR } K$ :

*Ciphertext* : A@C

Kunci : 9

Solusi:

*Biner Ciphertext*:

$A = 01000001$ ,  $@ = 01000000$ ,  $C = 01000011$

*Biner Key*: 9 = 00111001

P1 = 01000001 XOR 00111001

= 01111000

= x

P2 = 01000000 XOR 00111001

= 01111001

= y

P3 = 01000011 XOR 00111001

= 01111010

= z

Hasil dari proses dekripsinya A@C XOR 9 adalah = xyz

### III.3. Desain Sistem

#### III.3.1. Desain Sistem Secara Global

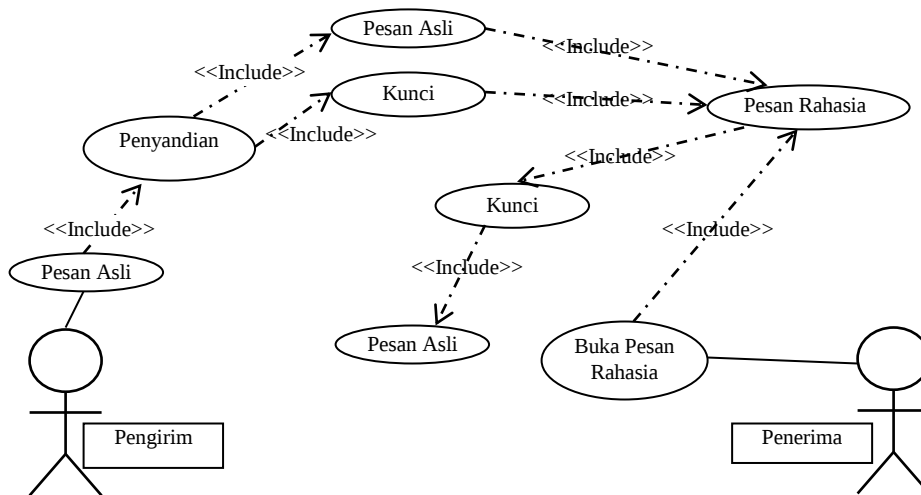
Desain sistem atau perancangan sistem adalah proses pengembangan spesifikasi baru berdasarkan hasil rekomendasi analisis sistem. Dalam tahap perancangan, diharuskan merancang spesifikasi yang dibutuhkan.

Bentuk rancangan sistem yang penulis buat menggunakan beberapa bentuk diagram dari *UML (Unified Modeling Language)* yaitu *Use Case Diagram*, *Class Diagram* dan *Activity Diagram*.

##### III.3.1.1. Use Case Diagram

Perancangan dimulai dari identifikasi aktor dan bagaimana hubungan antara aktor dan *Use Case* didalam sistem. Perancangan *Use Case Diagram* dapat dilihat pada gambar III.2. berikut:

|                                                                                                     |
|-----------------------------------------------------------------------------------------------------|
| <b>Rancang Bangun Aplikasi Kriptografi SMS Menggunakan Metode<br/>One Time Pad Berbasis Android</b> |
|                                                                                                     |



**Gambar III.2. Use Case Rancang Bangun Aplikasi Kriptografi SMS Menggunakan Metode One Time Pad Berbasis Android**

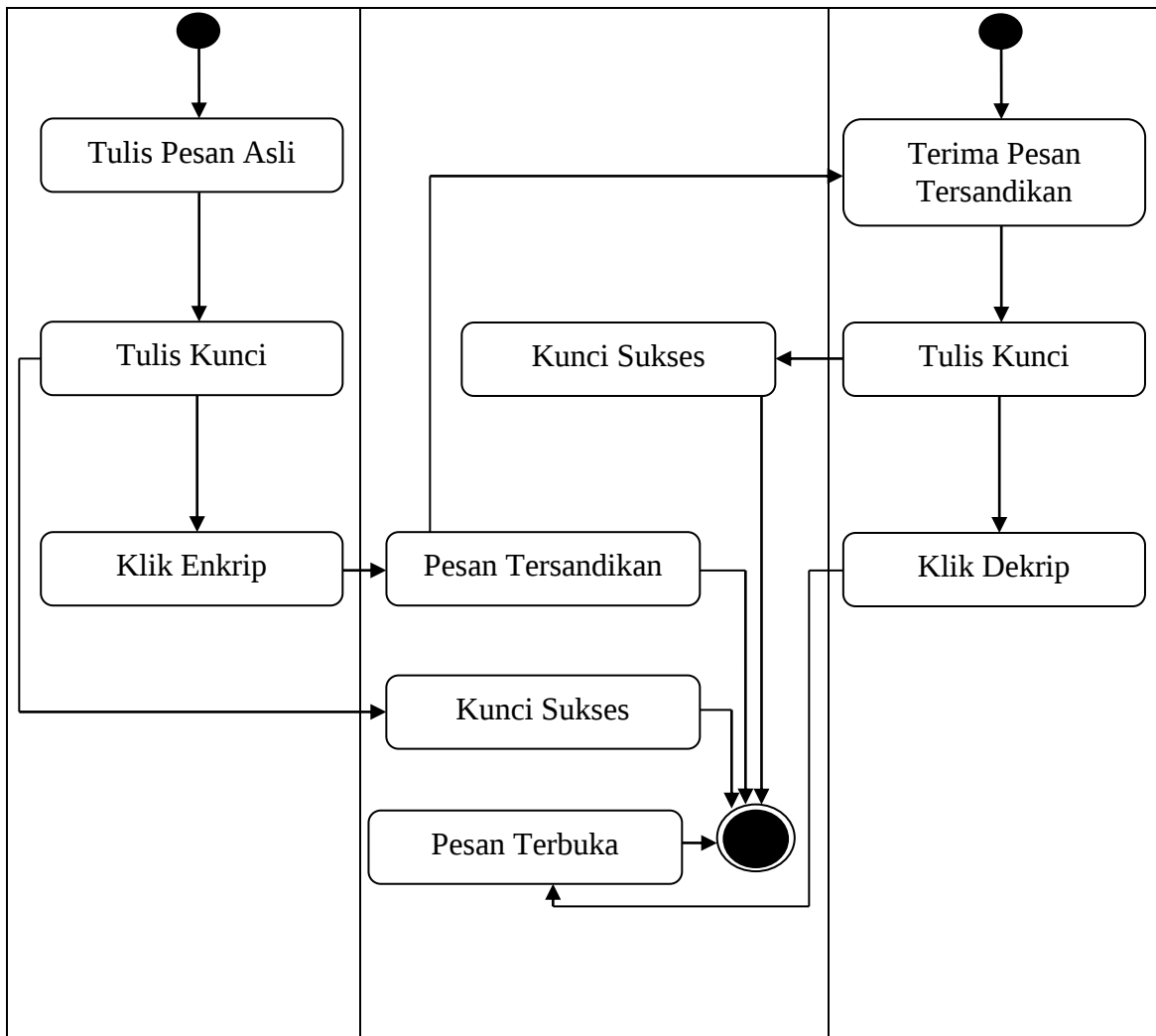
### III.3.1.2. Sequence Diagram

Rangkaian kegiatan pada setiap terjadi *event* sistem digambarkan pada *sequence* diagram berikut:

#### 1. Sequence Diagram Penyandian

Serangkaian kerja melakukan penyandian dapat terlihat seperti pada gambar III.3. berikut:

|          |        |          |
|----------|--------|----------|
| Pengirim | Sistem | Penerima |
|----------|--------|----------|



**Gambar III.3. Sequence Diagram Penyandian**

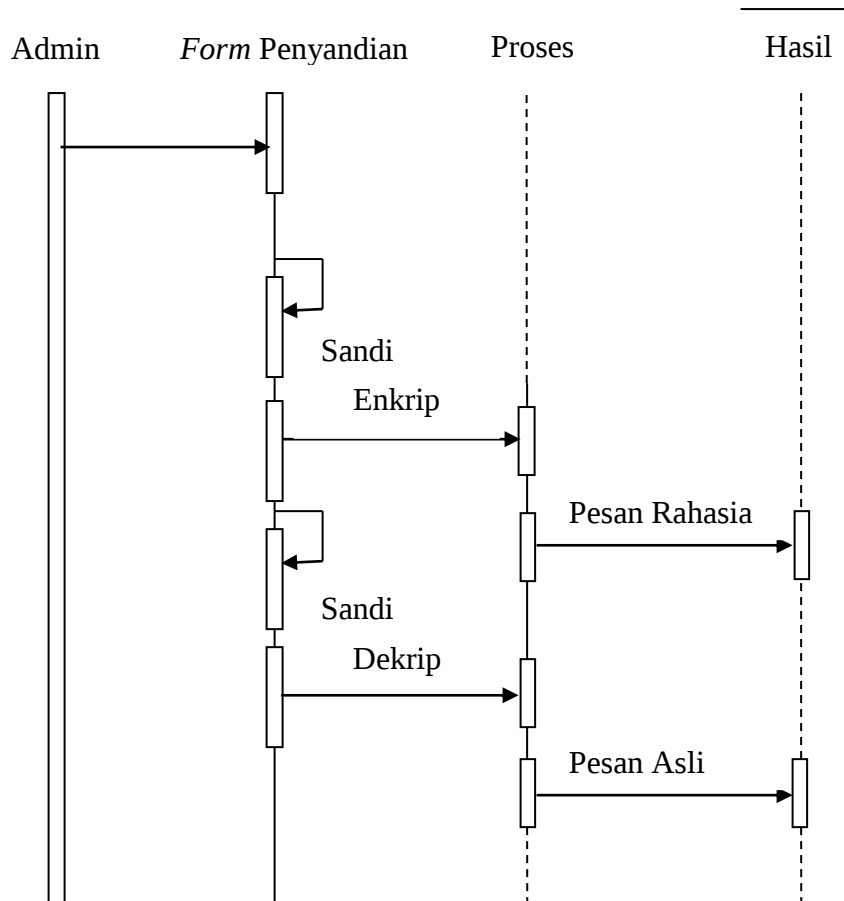
### III.3.1.3. Activity Diagram Penyandian

Pada proses ini kita akan membuat alur dari system yang dirancang yaitu *activity diagram*. Berikut adalah *activity diagram* sistem yang dirancang.

#### 1. Activity Diagram Penyandian

Aktivitas yang dilakukan untuk melakukan penyandian dapat dilihat seperti pada gambar III.4. berikut:





**Gambar III.4. Activity Diagram Penyandian**

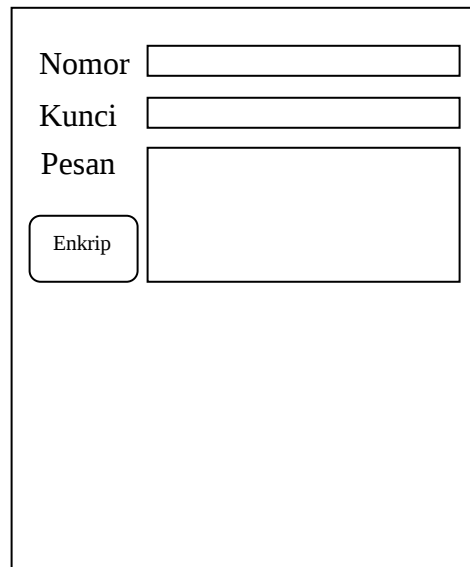
### III.3.2. Desain Sistem secara Detail

Perancangan *User Interface* merupakan masukan yang penulis rancang guna lebih memudahkan dalam *entry* data. *Entry* data yang dirancang akan lebih mudah dan cepat dan meminimalisir kesalahan penulisan dan memudahkan perubahan.

Perancangan tampilan yang dirancang adalah sebagai berikut:

#### 1. Perancangan *Form* Enkripsi SMS

Perancangan *Form* Enkripsi SMS berfungsi untuk menyandikan isi teks SMS. Adapun rancangan *form* Enkripsi SMS dapat dilihat pada gambar III.5. berikut:



The diagram shows a rectangular form with a border. Inside, there are three input fields stacked vertically. The first is labeled 'Nomor' and is a single-line text box. The second is labeled 'Kunci' and is also a single-line text box. The third is labeled 'Pesan' and is a larger multi-line text area. To the left of the 'Pesan' field, there is a rounded rectangular button labeled 'Enkrip'.

**Gambar III.5. Rancangan *Form* Enkripsi SMS**

Penjelasan Gambar:

Kolom nomor : berfungsi untuk menginput nomor telepon tujuan.

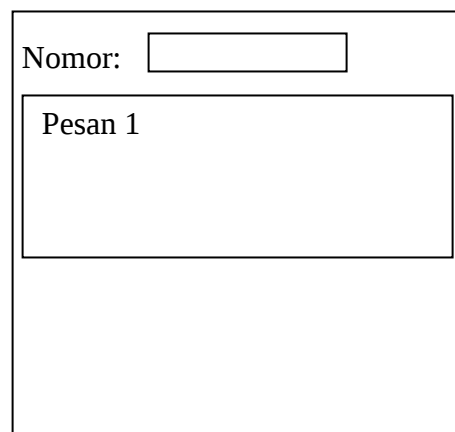
Kolom kunci : berfungsi untuk menginput kunci yang diinginkan.

Kolom pesan : berfungsi untuk menginput pesan yang akan kita kirim.

Tombol enkrip : berfungsi untuk mengenkripsi pesan dan mengirimkannya.

## 2. Perancangan *Form* Dekripsi SMS

Perancangan *Form* Dekrip SMS berfungsi untuk membuka pesan sandi isi teks SMS. Adapun rancangan *form* Dekripsi SMS dapat dilihat pada gambar III.6. berikut:



The diagram shows a rectangular form with a border. Inside, there is a single-line text box labeled 'Nomor:'. Below this, there is a larger rectangular area labeled 'Pesan 1'.



### **Gambar III.7. Rancangan *Form* Kontak**

Penjelasan Gambar:

Berfungsi untuk menampilkan kontak / nomor telepon yang tersimpan pada *handphone* atau kartu.