BAB III

ANALISIS DAN DESAIN SISTEM

III.1. Analisa Masalah

Kebutuhan manusia akan perangkat informasi dan komunikasi seakan menjadi kebutuhan yang tidak terpisahkan dalam kehidupan. Dengan banyaknya aplikasi pada saat ini sangat membantu mengurangi aktifitas yang dilakukan oleh banyak orang. Saat ini perkembangan teknologi informasi dan komunikasi dari waktu ke waktu kian meningkat. Salah satunya adalah pengiriman SMS dengan *Mobile Phone Andorid*. Pemanfaatan SMS dalam penggunaannya sangat memungkinkan setiap pengguna dalam mengirim atau menerima informasi dengan cepat. SMS merupakan pesan teks yang mempunyai ukuran yang sudah ditetapkan, dengan batasan 160 karakter per SMS. Dengan penggunaan SMS juga tergantung ketentuan dari operator yang digunakan dengan biaya yang telah ditetapkan oleh masing-masing operator. Pengamanan juga menjadi aspek penting yang perlu diperhatikan dalam penggunaan SMS. Pada masa dewasa ini, masih seringnya beberapa pihak yang tidak bertanggung jawab yang melakukan pembobolan SMS. Untuk itu pentingnya penerapan pengamanan pada SMS sehingga menjamin keaslian SMS yang dikirim maupun yang diterima.Salah satu dukungan yang ada pada perangkat seluler, pengguna dapat menggunakan pesan *SMS* atau dalam bahasa Indonesia adalah pesan singkat.

Dalam dunia komputer pengamanan dikenal dengan Kriptografi yang berasal dari bahasa Yunani yaitu *cryptós* yang artinya "*secret*" (yang tersembunyi)

dan gráphein yang artinya "*writting*" (tulisan). Jadi, kriptografi berarti "*secret writting*" (tulisan rahasia). kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan sehingga memungkinkan kemanan yang dikirim. Salah satu metode kriptografi dalam pengamanan SMS adalah *Blowfish.* Penggunaan algoritma blowfish sangat memungkinkan *Blowfish* melakukan enkripsi data pada *microprocessors* 32-*bit* dengan *rate* 26 *clock cycles* per *byte* serta memiliki tingkat keamanan yang bervariasi, panjang kunci yang digunakan oleh *Blowfish* dapat bervariasi dan bisa sampai sepanjang 448 *bit.*

Pada desain *menu* pada aplikasi untuk keamanan sms dapat dijelaskan sebagai berikut.

1. *Splash*, yang berfungsi permulaan untuk mengload aplikasi.
2. *Menu Sms*, merupakan tampilan yang digunakan untuk memilih layanan aplikasi.
3. *New Sms*, merupakan menu yang berfungsi untuk membuat pesan baru.
4. *Read Sms*, merupakan menu yang berfungsi untuk membaca sms yang diterima oleh aplikasi.

III.2. Spesifikasi Perangkat

Dalam perancangan aplikasi untuk perangkat *mobile android* ini penulis menggunakan beberapa perangkat agar aplikasi berjalan dengan baik dan sesuai dengan yang diharapkan, yaitu sebagai berikut :

1. Perangkat Keras (*Hardware*)
    a. Komputer yang setara *Core i3*.
    b. *Smartphone Android* dengan OS 4.1 atau diatasnya.

c. *Mouse, keyboard*, dan *Monitor.*

2. Perangkat Lunak (*Software*)
   a. *Operating System*, OS yang digunakan dalam perancangan dan tes untuk adalah *Windows* 7 dan OS *Android* pada perangkat *mobile*.
   b. JDK *Java 1.7*, sebagai bahasa program dan *compiler Java*.
   c. *Eclipse,* sebagai *editor source code Java.*

III.2.1. Teknik Pemecahan Masalah

Teknik pemecahan masalah tentang perancangan aplikasi keamanan sms yang dibuat memiliki beberapa poin yaitu sebagai berikut:

1. Pada langkah awal analisa terhadap perancangan yang akan dibangun terutama tentang keamanan sms yang menggunakan perangkat *mobile phone android.*
2. Dalam perancangan aplikasi dalam persiapan adalah menentukan perangkat yang dibutuhkan dalam membangun aplikasi seperti perangkat keras maupun perangkat lunak.
3. Selanjutnya dilakukan perancangan sistem yang nantinya akan di implementasikan pada aplikasi yang akan dibangun.
4. Proses uji coba yang akan dilakukan terhadap *input*an, proses ataupun *output* aplikasi, apakah sudah sesuai dengan perancangan yang telah direncanakan sebelumnya.

III.2.2. Analisa Proses Penyelesaian

Algoritma Blowfish diciptakan oleh seorang Cryptanalyst bernama Bruce Schneier, Presiden perusahaan Counterpane Internet Security, Inc (Perusahaan konsultan tentang kriptografi dan keamanan komputer) dan dipublikasikan tahun 1994. Dibuat untuk digunakan pada komputer yang mempunyai microposesor besar (32-bit keatas dengan cache data yang besar). Blowfish merupakan algoritma yang tidak dipatenkan dan licensefree, dan tersedia secara gratis untuk berbagai macam kegunaan (Syafari, 2007). Pada saat Blowfish dirancang, diharapkan mempunyai kriteria perancangan sebagai berikut (Schneier, 1996) :

1. Cepat, Blowfish melakukan enkripsi data pada microprocessors 32-bit dengan rate 26 clock cycles per byte.
2. Compact (ringan), Blowfish dapat dijalankan pada memori kurang dari 5K.
3. Sederhana, Blowfish hanya menggunakan operasi-operasi sederhana: penambahan, XOR, dan lookup tabel pada operan 32-bit.
4. Memiliki tingkat keamanan yang bervariasi, panjang kunci yang digunakan oleh Blowfish dapat bervariasi dan bisa sampai sepanjang 448 bit. Dalam penerapannya sering kali algortima ini menjadi tidak optimal. Karena strategi implementasi yang tidak tepat. Algoritma Blowfish akan lebih optimal jika digunakan untuk aplikasi yang tidak sering berganti kunci, seperti jaringan komunikasi atau enkripsi file otomatis. Selain itu, karena algoritma ini membutuhkan memori yang besar, maka algoritma ini tidak dapat diterapkan untuk aplikasi yang memiliki memori kecil seperti smart card. Panjang kunci

yang digunakan, juga mempengaruhi keamanan penerapan algoritma ini. Algoritma Blowfish terdiri atas dua bagian, yaitu ekspansi kunci dan enkripsi.

III.2.3. Ekspansi kunci (Key-expansion)

Berfungsi merubah kunci (minimum 32-bit, maksimum 448-bit) menjadi beberapa array subkunci (subkey) dengan total 4168 byte (18x32-bit untuk P-array dan 4x256x32-bit untuk S-box sehingga totalnya 33344 bit atau 4168 byte). Kunci disimpan dalam K-array:

K1, K2, ... Kj 1 _ j _ 14

Kunci-kunci ini yang dibangkitkan (generate) dengan menggunakan subkunci yang harus dihitung terlebih dahulu sebelum enkripsi atau dekripsi data. Sub-sub kunci yang digunakan terdiri dari :

P-array yang terdiri dari 18 buah 32-bit subkunci,

P1, P2, ..., P18

S-box yang terdiri dari 4 buah 32-bit, masing-masing memiliki 256 entri :

S1,0, S1,1, ..., S1,255

S2,0, S2,1, ..., S2,255

S3,0, S3,1, ..., S3,255

S4,0, S4,1, ..., S4,255

Langkah-langkah perhitungan atau pembangkitan subkunci tersebut adalah sebagai berikut:

1. Inisialisasi P-array yang pertama dan juga empat S-box, berututan, dengan string yang telah pasti.

String tersebut terdiri dari digit-digit heksadesimal dari phi, tidak termasuk angka tiga di awal.

Contoh :

P1= 0x243f6a88

P2= 0x85a308d3

P3= 0x13198a2e

P4= 0x03707344

dan seterusnya sampai S-box yang terakhir (daftar heksadesimal digit dari phi untuk P-array dan Sbox.

2. XOR-kan P1 dengan 32-bit awal kunci, XOR-kan P2 dengan 32-bit berikutnya dari kunci, dan seterusnya untuk semua bit kunci. Ulangi siklus seluruh bit kunci secara berurutan sampai seluruh P-array ter-XOR-kan dengan bit-bit kunci. Atau jika disimbolkan : P1 = P1 _ K1, P2 = P2 _K2, P3 = P3 _ K3, . . . P14 = P14_ K14, P15 = P15 _ K1, . . . P18 = P18 _ K4. Keterangan : _ adalah simbol untuk XOR.
3. Enkripsikan string yang seluruhnya nol (all-zero string) dengan algoritma Blowfish, menggunakan subkunci yang telah dideskripsikan pada langkah 1 dan 2.
4. Gantikan P1 dan P2 dengan keluaran dari langkah 3.
5. Enkripsikan keluaran langkah 3 menggunakan algoritma Blowfish dengan subkunci yang telah dimodifikasi.
6. Gantikan P3 dan P4 dengan keluaran dari langkah 5.

7. Lanjutkan langkah-langkah di atas, gantikan seluruh elemen P-array dan kemudian keempat S-box secara berurutan, dengan hasil keluaran algoritma Blowfish yang terus-menerus berubah.

Total keseluruhan, terdapat 521 iterasi untuk menghasilkan subkunci subkunci dan membutuhkan memori sebesar 4KB.

III.2.4. Enkripsi Data

Terdiri dari iterasi fungsi sederhana (Feistel Network) sebanyak 16 kali putaran (iterasi), masukannya adalah 64-bit elemen data X. Setiap putaran terdiri dari permutasi kunci-dependent dan substitusi kunci- dan datadependent. Semua operasi adalah penambahan (addition) dan XOR pada variabel 32-bit. Operasi tambahan lainnya hanyalah empat penelusuran tabel array berindeks untuk setiap putaran. Langkahnya adalah seperti berikut :

1. Bagi X menjadi dua bagian yang masing-masing terdiri dari 32-bit: XL, XR.
2. Lakukan langkah berikut :

   For i = 1 to 16:

   XL = XL _ Pi

   XR = F(XL) _ XR

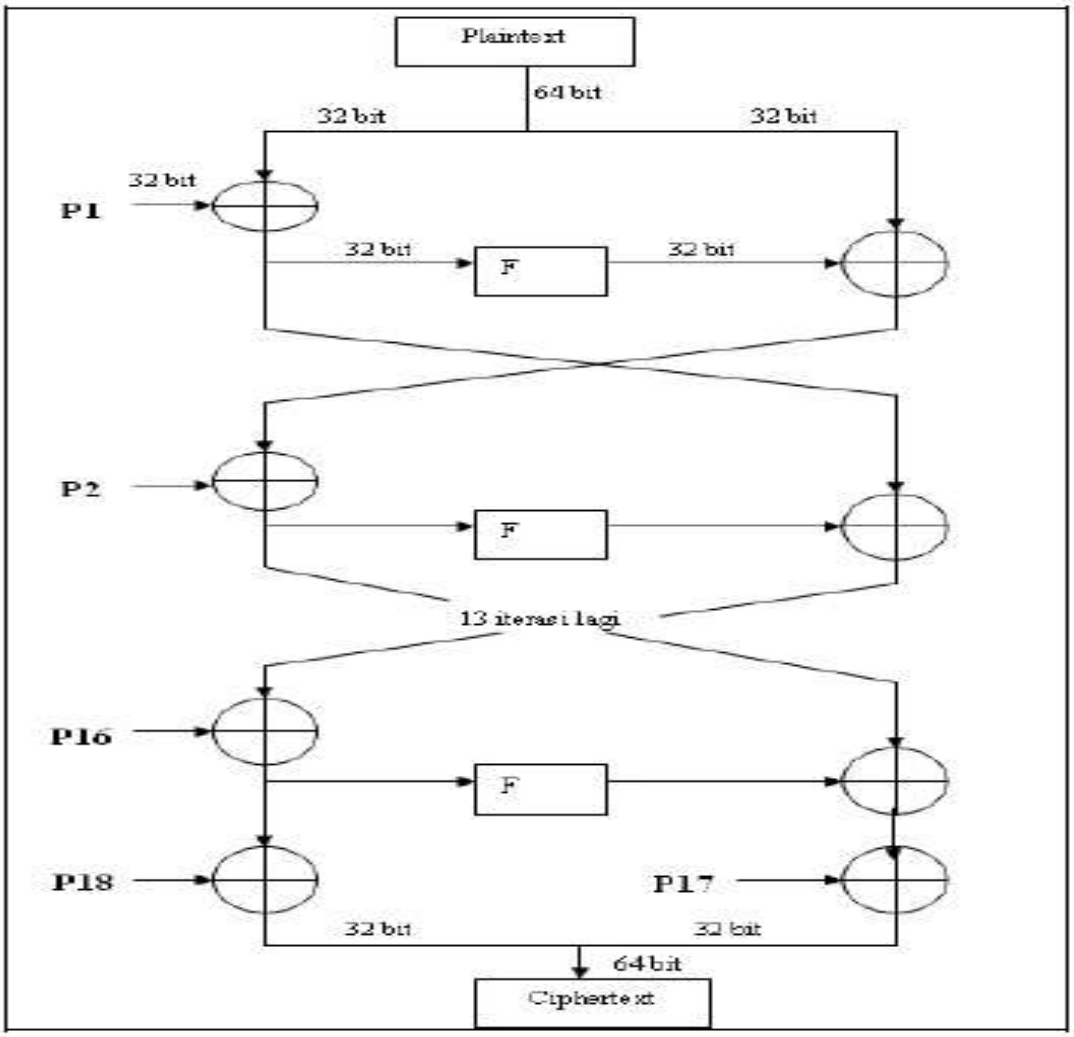
   Tukar XL dan XR
3. Setelah iterasi ke-16, tukar XL dan XR lagi untuk melakukan membatalkan pertukaran terakhir.
4. Lalu lakukan :

   XR = XR _ P17

   XL = XL _ P18

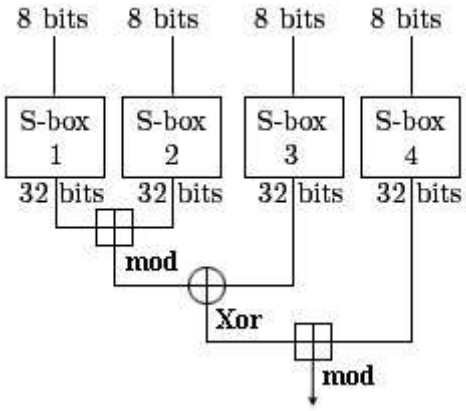
5. Terakhir, gabungkan kembali XL dan XR untuk mendapatkan cipherteks.

Untuk lebih jelasnya, gambaran tahapan pada jaringan feistel yang digunakan Blowfish adalah seperti pada Gambar III.1.



Gambar III.1. *Blok Diagram* Algoritma Enkripsi *Blowfish*

Pada langkah kedua, telah dituliskan mengenai penggunaan fungsi F. Fungsi F adalah: bagi XL menjadi empat bagian 8-bit: a,b,c dan d. F(XL) = ((S1,a + S2,b mod 232) XOR S3,c) + S4,d mod 2. Agar dapat lebih memahami fungsi F, tahapannya dapat dilihat pada Gambar III.2 berikut ini :



Gambar III.2. Fungsi F dalam Blowfish

Dekripsi sama persis dengan enkripsi, kecuali bahwa P1, P2,…, P18 digunakan pada urutan yang berbalik (*reverse*). Algoritmanya dapat dinyatakan sebagai berikut :

for i = 1 to 16 do

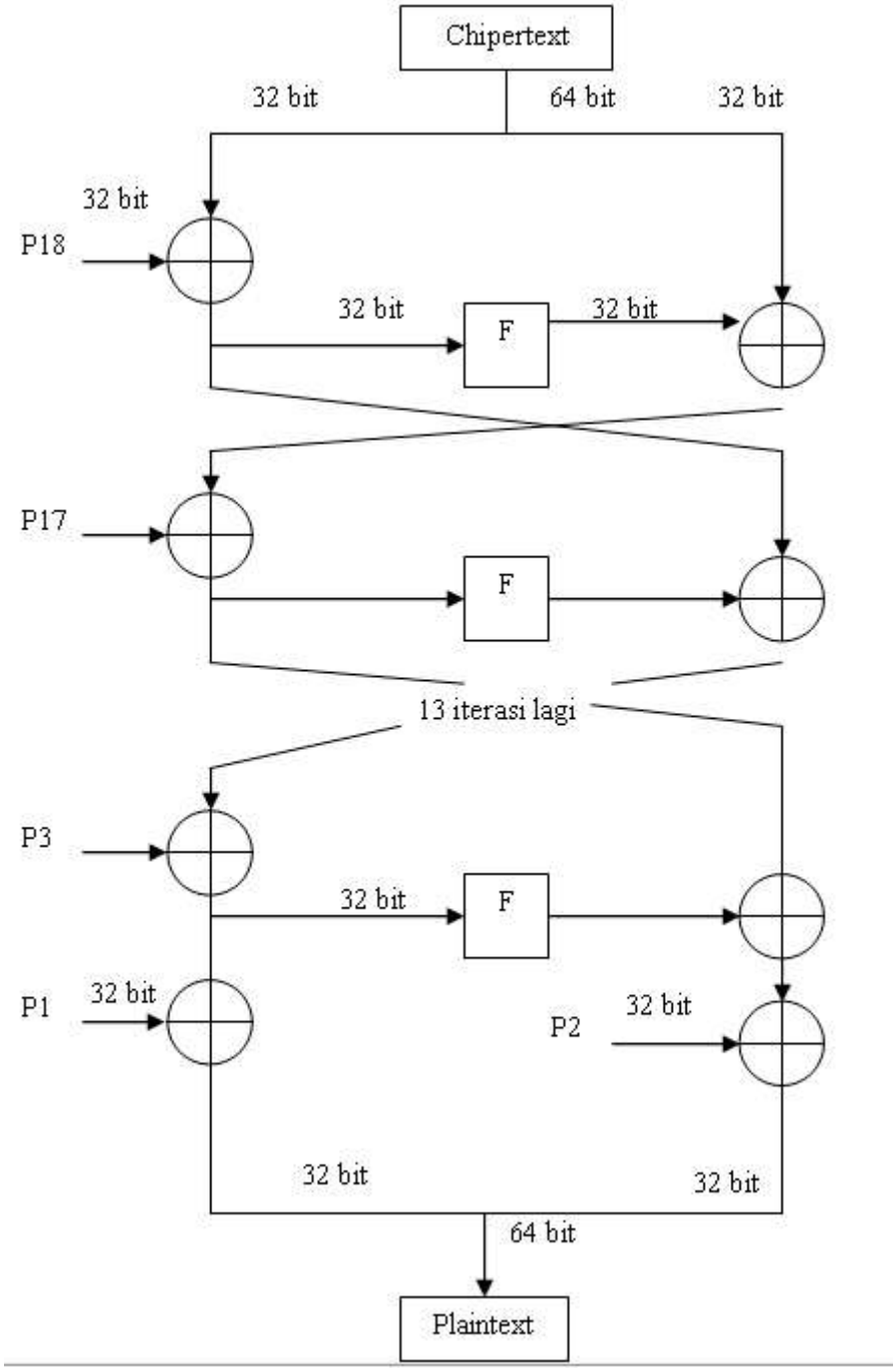
XRi = XLi-1 _ P19-i;

XLi = F[XRi] _ XRi-1;

XL17 = XR16 _ P1;

XR17 = XL16 _ P2;

Blok diagram dekripsi seperti pada Gambar III.3 berikut ini :



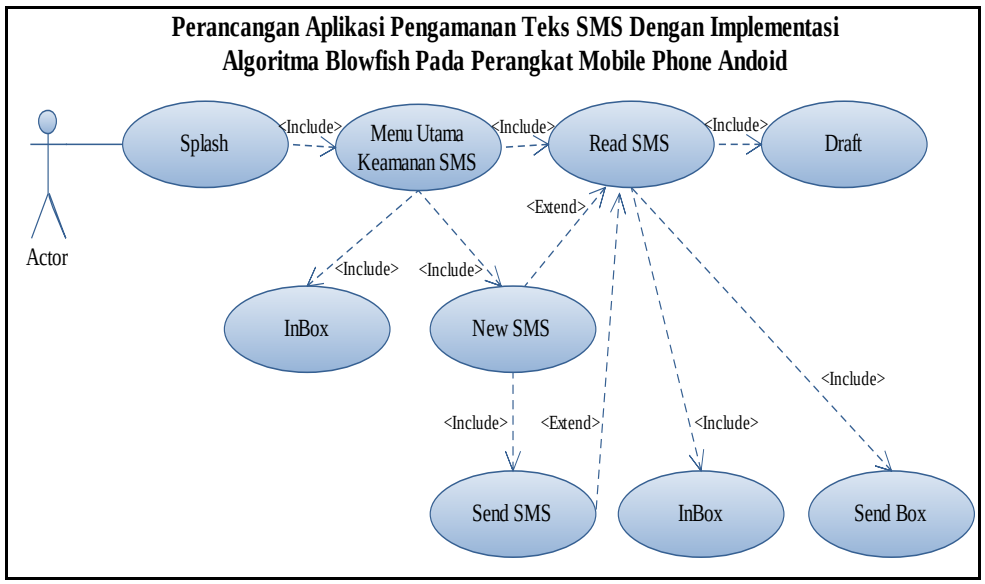
Gambar III.3. Blok Diagram Dekripsi *Blowfish*

III.3. Desain Sistem

Dalam proses perancangan ini akan akan membarikan beberapa penjelasan mengenai beberapa rancangan aplikasi yang akan dikerjakan yang menggunakan perangkat *android* yaitu sebagai berikut:

III.3.1. *Use Case* Diagram

Use case diagram berfungsi untuk menggambarkan kegiatan aktor atau pengguna aplikasi, adapun *use case* diagram aplikasi yang dirancang dapat dilihat pada gambar III.4 berikut.



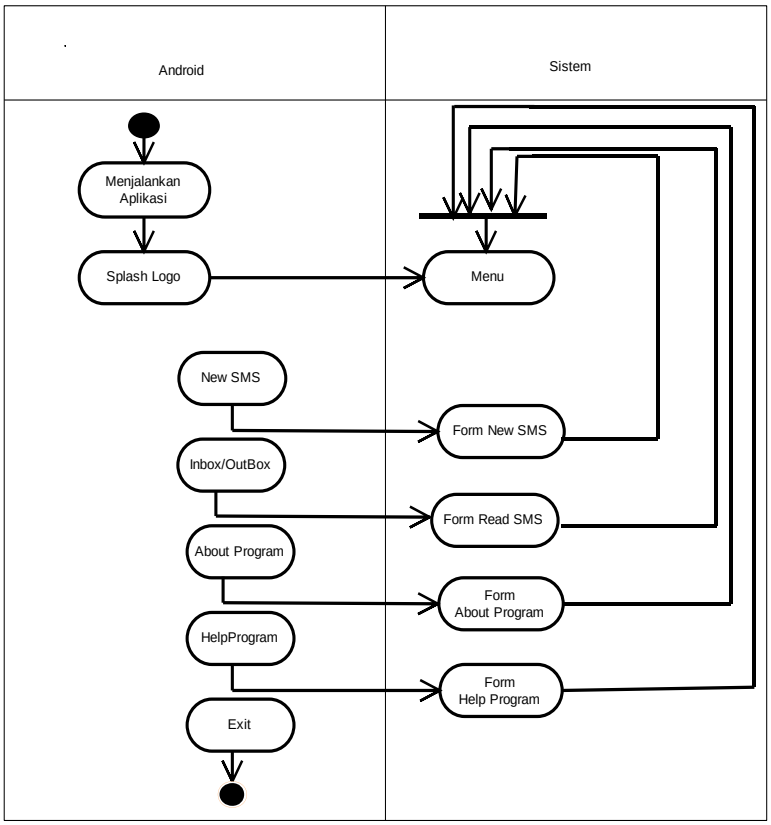
Gambar III.4. *Use Case* Diagram

Dari gambar *use case* diagram diatas, pengguna memulai aplikasi dan memilih menu sms .

III.3.2. *Activity* Diagram

Pada *activity* diagram dibawah ini menggambarkan proses yang berjalan pada aplikasi *android* terdapat beberapa menu yang ditampilkan.Proses yang

berlangsung terjadi setelah pengguna menjalankan aplikasi, yang dapat dilihat pada gambar III.5 berikut.



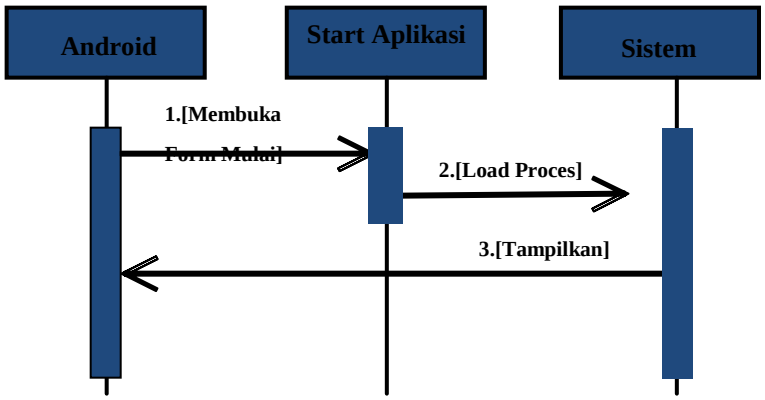
Gambar III.5. *Activity*Diagram*Android*

Dari gambar *Activty* diagram diatas, proses aplikasi merupakan tahapan yang disajikan terhadap cara kerja aplikasi keamanan sms ketika digunakan oleh pengguna.

III.3.3. *Sequence* Diagram

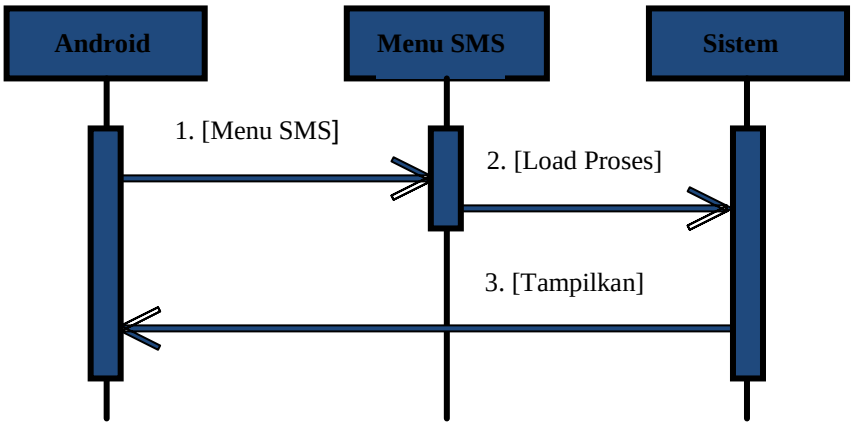
Sequence diagram yang digunakan untuk menggambarkan sistem pada sebuah adegan untuk proses penggunaan aplikasi. Berikut ini adalah *Sequence* diagram yang dirancang

1. *Sequnce* Diagram *Strart* Aplikasi, untuk diagram proses *start* aplikasi dapat dilihat pada gambar III.6 dibawah ini.



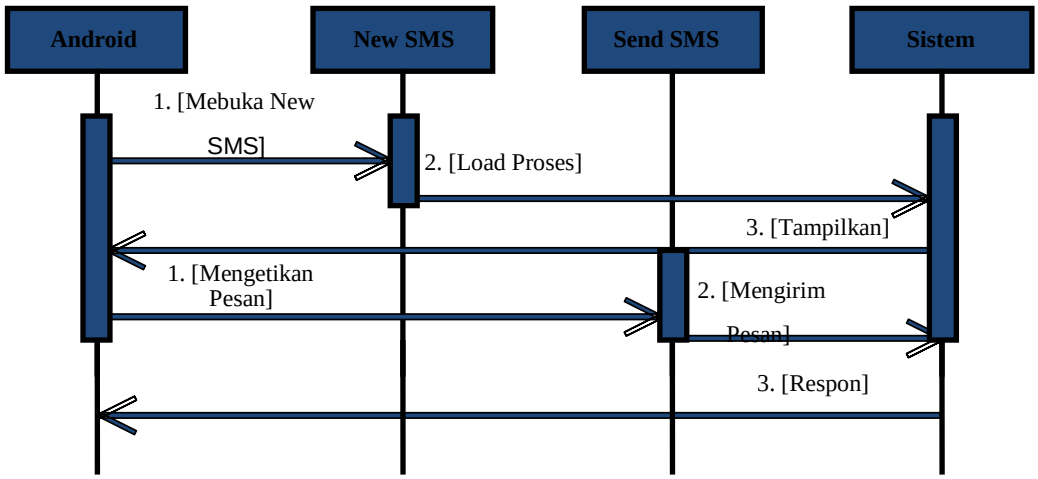
Gambar III.6. *Sequence* Diagram *Start* Aplikasi

2. *Sequnce* Diagram menampilkan *menu sms*, untuk diagram proses menampilkan *menu sms* dapat dilihat pada gambar III.7 dibawah ini.



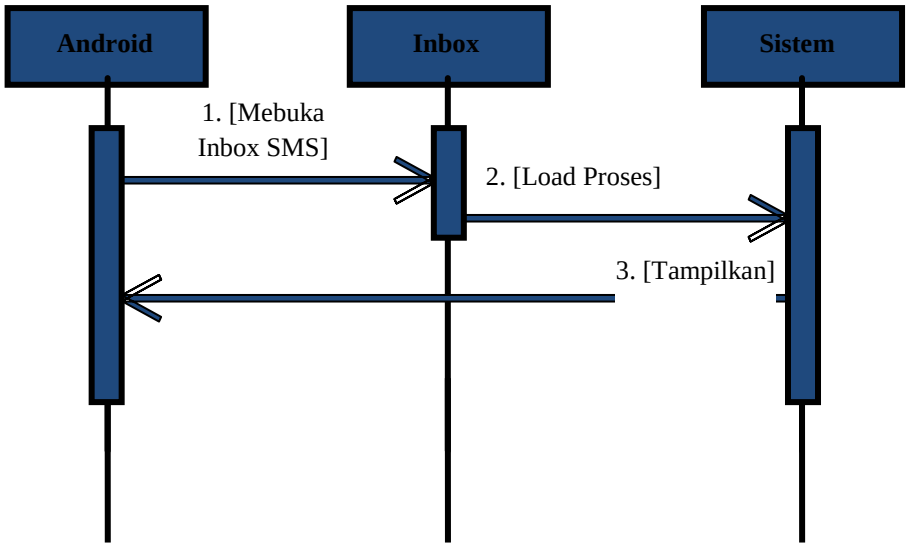
Gambar III.7. *Sequence* Diagram Menampilkan *Menu SMS*

3. *Sequnce* Diagram Mengirim *SMS*, untuk diagram proses Mengirim *SMS* dapat dilihat pada gambar III.8 dibawah ini.



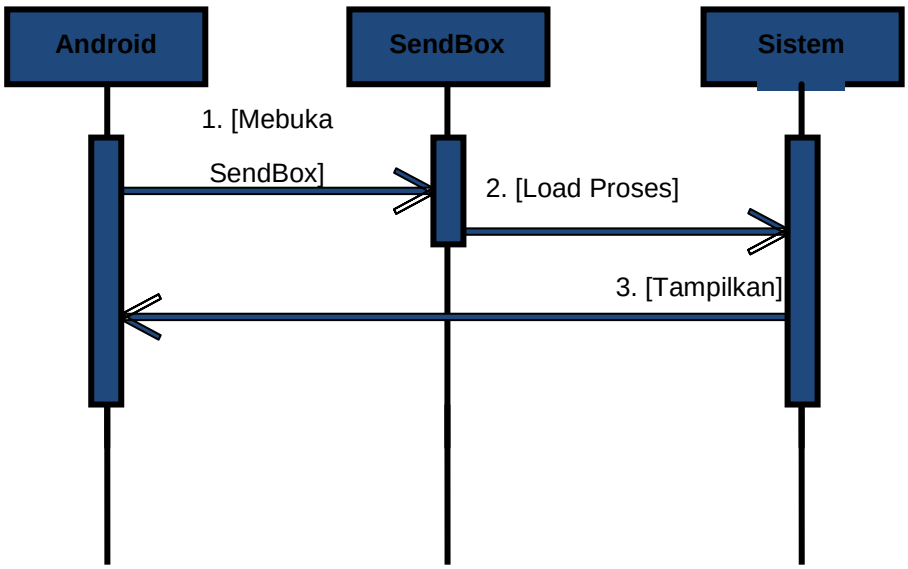
Gambar III.8. *Squence* Diagram Mengirim Pesan

4. *Sequnce* Diagram Pesan Masuk, untuk diagram Pesan Masuk dapat dilihat pada gambar III.9 dibawah ini.



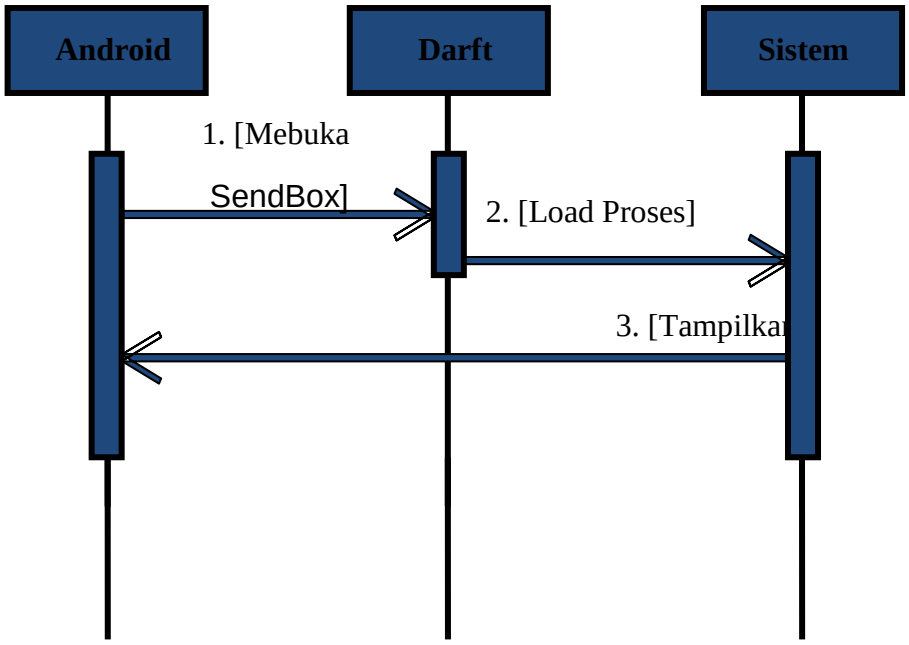
Gambar III.9. *Sequence* Diagram Pesan Masuk

5. *Sequnce* Diagram Pesan Pesan Terkirim , untuk diagram Pesan Terkirim dapat dilihat pada gambar III.10 berikut :



Gambar III.10. *Sequence* Diagram Pesan Terkirim

6. *Sequnce* Diagram Pesan Tersimpan , untuk diagram Pesan Tersimpan dapat dilihat pada gambar III.11 dibawah ini.



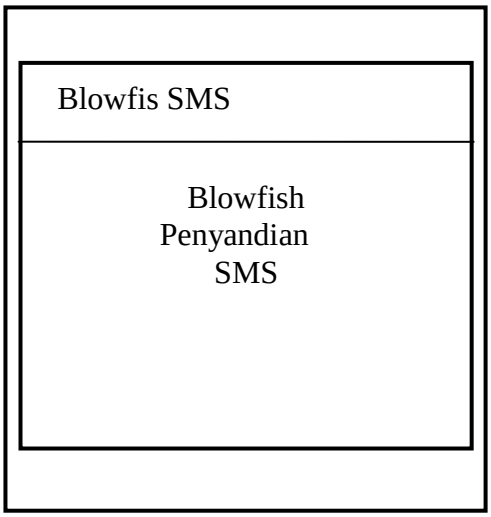
Gambar III.11. *Sequence* Diagram Pesan Tersimpan

III.4. Desain *Interface*

Dalam perancangan aplikasi memiliki beberapa tampilan yang disediakan, rancangan tampilan yang ada pada aplikasi *android* adalah sebagai berikut.

1. Rancangan *Splash*

Rancangan layar *splash* merupakan rancangan awal diamana saat aplikasi dibuka atau dijalankan , adapun rancangan tersebut dapat dilihat pada gambar III.12.



Gambar III.12. Rancangan *Form Splash*

2. Rancangan Menu

Rancangan menu adalah tampilan menu yang ada setelah pengguna masuk ke dalam aplikasi. Untuk lebih jelasnya dapat dilihat pada gambar III.13 berikut.

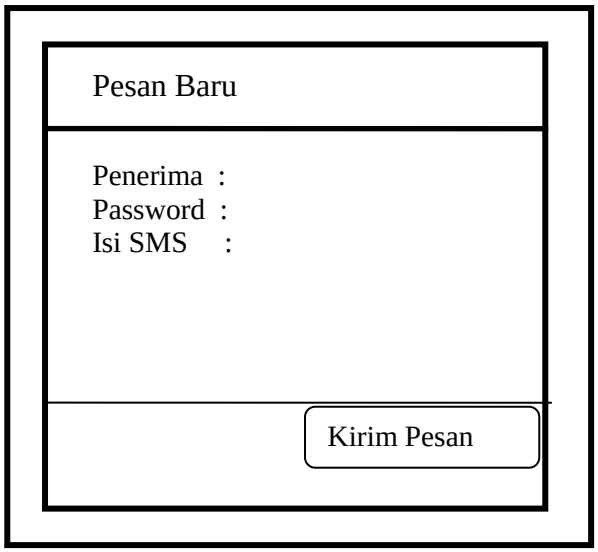
Gambar III.13. Rancangan Menu

Pada gambar diatas terdapat beberapa menu yang dapat dijelaskan antara lain sebagai berikut :

a. Pesan baru, merupakan menu untuk rancangan dalam membuat sms baru yaitu dengan mengetikkan text kata-kata melalui menu pesan baru.
b. Pesan masuk, pada menu ini merupakan menu yang digunakan untuk membuka pesan masuk dan membaca pesan masuk.
c. Pesan keluar, merupakan menu untuk membuka pesan yang telah terkirim.
d. Tentang Aplikasi, merupakan menu untuk menyajikan informasi mengenai *developer* pembuat program.
e. Panduan Aplikasi, merupakan menu untuk menyajikan inforamsi tetang cara penggunaan aplikasi sehingga memudahkan pengguna dalam mengoperasikannya.
f. Tutup, merupakan menu untuk keluar dari aplikasi.

3. Rancangan *New Sms*

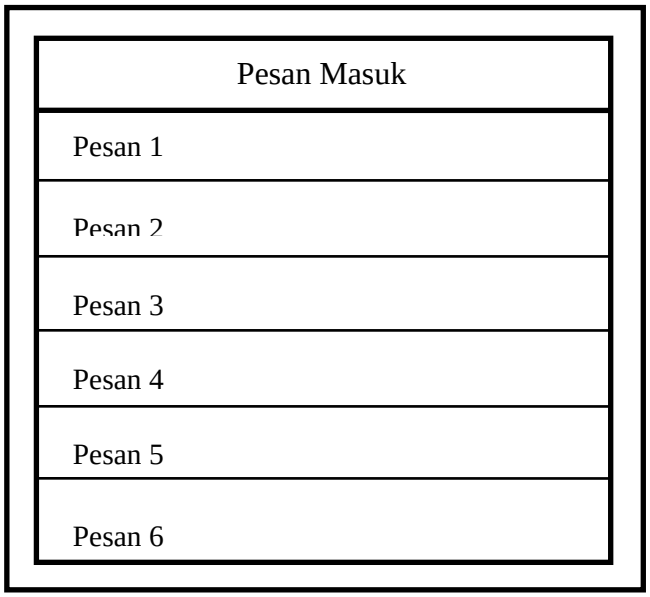
Form ini berfungsi untuk tampilan awal pengguna sebelum masuk ke permainan. Yang dapat dilihat pada gambar III.14. berikut.



Gambar III.14. Rancangan *New Sms*

4. Rancangan *Read Sms*

Form ini berfungsi untuk menampilkan sms pesan masuk, pesan terkirim, dan pesan yang tersimpan di aplikasi keamanan sms. Yang dapat dilihat pada gambar III.15. berikut :



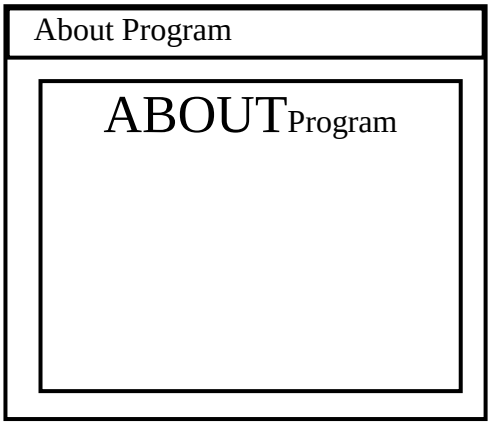
Gambar III.15. Rancangan Papan Permainan

Pada gambar diatas terdapat fitur-fitur ketika pengguna menjalankan aplikasi yang diantaranya adalah sebagai berikut :

a. *Inbox* yang digunakan untuk menampung dan menampilkan pesan masuk.
b. *Sent Box* yang berguna untuk menampung pesan terkirim .
c. Darft, menu yang berguna untuk menampung pesan yang isin disimpan.
d. Item merupakan dafatar urusan pesan yang tertampil di list pesan Pengguna dapat melihat semua pesan yang telah dikirim, membaca pesan yang masuk, melihat daftar pesan yang dikirim kepada yang di tuju, serta menyimpan pesan yang kita anggap penting .

5. Rancangan *Form About*

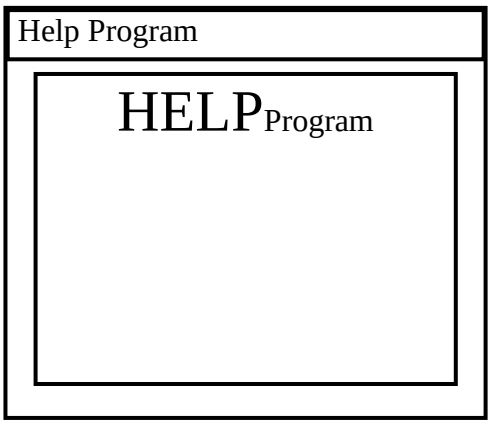
Form ini menampilkan informasi tentang penggunaan aplikasi*keamanan sms*, yang dapat dilihat pada gambar III.16 berikut.



Gambar III.16. Rancangan *Form About Program*

6. Rancangan *Form* tentang Aplikasi

Form ini berfungsi untuk menampilkan informasi tentang cara menggunakan aplikasi keamanan sms ini, dapat dilihat pada gambar III.17 berikut.



Gambar III.17. Rancangan *Form Help*