BAB III

ANALISA MASALAH DAN RANCANGAN PROGRAM

III.1. Analisa Masalah

Pada bab tiga ini akan dilakukan analisa terhadap landasan dan teori yang telah dijelaskan pada bab sebelumnya. Analisa yang dilakukan bertujuan untuk menentukan solusi dari permasalah untuk melakukan implementasi algoritma RC6 untuk enkripsi SMS pada telepon seluler. Hasil pada bab ini akan membantu dalam penyelesaian implementasi aplikasi dan penulisan bab empat.

Dalam pembahasan kriptografi yang sedang di bahas yaitu mengenai mengamankan isi dari sebuah pesan singkat pada *platform* android dengan menggunakan algoritma kriptografi RC6. Berikut dibawah ini analisa rancangan dari permasalahan yang sedang di bahas :

a. Kuranganya keamanan pada saat pengiriman pesan singkat melalui SMS.

b. Memanfaatkan layanan SMS untuk mengirim pesan atau informasi yang bersifat rahasia.

Masalah utama dari tugas akhir ini adalah melakukan implementasi algoritma RC6 untuk melakukan enkripsi SMS pada *smartphone*. Pada subbab berikut ini akan dibahas analisis dari faktor-faktor penting yang perlu dilakukan dalam implemetasi algoritma RC6 untuk melakukan enkripsi dan deskripsi SMS pada *smartphone*.

III.2. Teknik Pemecahan Masalah

Teknik pemecahan masalah yang diambil penulis terdapat beberapa langkah untuk menghasilkan perangcangan pengamanan SMS yang baik. Adapun langkah-langkah tersebut adalah sebagai berikut:

1. Hal pertama yang harus dilakukan adalah menganalisa tentang aplikasi SMS, metode yang digunakan dan cara kerja aplikasi tersebut.
2. Menentukan perangkat-perangkat apa saja yang dibutukan dalam melakukan perancangan aplikasi tersebut, baik perangkat keras maupun perangkat lunak.
3. Membuat desain sistem atau gambaran yang akan diterapkan pada aplikasi perancangan pengamanan SMS tersebut.
4. Mencoba dan menguji aplikasi tersebut dengan hasil yang diharapkan.

III.3. Penerapan Algoritma RC6 dalam enkripsi dan dekripsi SMS

Algoritma RC6 merupakan algoritma sederhana, fungsi yang digunakan merupakan fungsi yang sederhana dan hanya mengandalkan prinsip *iterated chipper* untuk keamanan. Tampilan hasil enkripsi yang diterima harus diperhatikan, hal ini dikarenakan pada data hasil enkripsi, setiap karakternya akan memiliki panjang karakter 8 bit, sedangkan sebagian telepon seluler hanya dapat menampilkan karakter dengan panjang 7 bit. Dengan demikian dalam penerapan algoritma RC6 pada SMS karakter-karakter yang akan dienkripsi diubah kedalam nilai ASCII, dimana nilai karakter dalam table ASCII ditambah table karakter special adalah 0 sampai dengan 255, artinya satu karakter ASCII akan diwakili oleh 8 bit, dimana 28 = 256. Sehingga, dalam 1 blok *plainteks* (32 bit) akan menyimpan 4 karakter dan setiap kali iterasi, maka akan diambil 16 karakter dari plaintext.

Apabila panjang plaintext atau panjang kunci kurang dari 16 karakter, maka akan

dilakukan *padding*, yaitu dengan menambah bit “0” (nol) di akhir teks, sehingga panjang teks mencukupi 16 karakter. Layar pada sebagian besar telepon selular hanya dapat menampilkan karakter dengan panjang 7 bit dan pesan yang telah terenkripsi akan berbentuk *binary*, sehingga layar tidak akan menampilkan dengan semestinya. Oleh karena itu, pada aplikasi yang akan dibangun, untuk menampilkan pesan yang telah terenkripsi, ditambah informasi karakter yang terdapat pesan tersebut dengan format heksadesimal agar dapat ditampilkan dilayar dan informasinya lebih terbaca.

Algoritma RC6 yang akan digunakan dalam aplikasi Secure SMS yang akan dibangun dengan w sebesar 32 bit, r sebesar 20 kali putaran dan panjang kunci beragam lebih dari 1 karakter (8 bit). Langkah-lanhkah algoritma RC6 dalam Aplikasi SMS Secure ini akan dikelompokan kedalam beberapa bagian, yaitu :

1. Pembangkit Subkunci

   Kunci dari pengguna ini akan dimasukan oleh pengguna pada saat akan melakukan proses enkripsi dan dekripsi. Kunci ini memiliki tipe data string.

2. Baca Masukan untuk proses enkripsi

   Yang dilakukan pada tahapan ini adalah membaca teks yang menjadi masukan pada proses enkripsi,yaitu field dari aplikasi SMS Secure. pada proses enkripsi pesan, fieldnya adalah isi pesan

3. Enkripsi meliputi whitening awal, iterasi, dan whitening akhir.

4. Baca masukan untuk proses dekripsi

   Yang dilakukan pada tahapan ini adalah membaca teks yang menjadi masukan pada proses dekripsi, yaitu record dari hasil pesan yang telah dienkripsi pada pengirim dan menjadi field pesan pada penerima.

5. Dekripsi merupakan kebalikan dari proses enkripsi.

(Rionald Ricardo Mangundap, Wiwin Agus Kristiana ; 2015)

III.3.1. Studi Kasus Perhitungan Manual Algoritma RC6

Pada perhitungan manual algoritma RC6 ini diberikan kunci sebesar 16 byte dan plainteks sebesar 128 bit (16 byte). Kunci dan plainteks yang menjadi contoh masing-masing sebagai berikut :

Kunci : muhammadamin1994

Plainteks : teknik informasi

Langkah pertama adalah membagi plainteks kedalam 4 blok yaitu A, B,C, D, yang masing-masing blok yang terdiri dari 32 bit (4 karakter)

A	B	C	D
Tekn	ik i	nfor	masi

Ubah tiap karakter dalam masing-masing blok kedalam nilai ASCII, selanjutnya ubah nilai ASCII tersebut menjadi bilangan biner masing-masing sepanjang 18 bit, sehingga pada masing-masing blok akan dihasilkan bilangan biner sepanjang 32 bit.

<u>Blok A</u>

Plainteks	t	e	k	n
ASCII	116	101	107	110
Biner	01110100	01100101	01101011	01101110

<u>Blok B</u>

Plainteks	i	k		i

ASCII	105	107	160	105
Biner	01101001	01101011	00100000	01101001
Blok C				
Plainteks	n	f	o	r
ASCII	110	102	111	114
Biner	0110110	01100110	01101111	01110010
Blok D				
Plainteks	m	a	s	i
ASCII	109	97	115	105
Biner	01101101	01100001	01110011	01101001

Kemudian bilangan biner digabungkan kembali, dengan aturan byte pertama plainteks diletakkan pada lest significan bit blok A. Dan byte terakhir plainteks diletakkan pada most significan bit blok D

Blok A : 01101110011010110110010101110100

Dalam desimal = 1.852.532.084

Blok B : 01101001001000000110101101101001

Dalam desimal = 1.763.732.329

Blok C : 01110010011011110110011001101110

Dalam desimal = 1.919.903.342

Blok D : 01101001011100110110000101101101

Dalam desimal = 1.769.169.26

Setelah didapat nilai pada masing-masing blok, maka dilanjutkan dengan langkah-langkah berikut (Perhitungan manual pembangkit sub kunci dapat dilihat pada Lampiran A) :

1. Whitening Awal

Whitening awal, dengan menjumlahkan B dengan sub kunci S(0), dan D dengan sub kunci S(1). Penjunlahan dilakukan dalam modulo 232

B = B + S(0)

D = D + S(1)

B = 1.763.732.329 + 4.033.202.597 mod 2^32

= 5.796.934.926 mod 4.294.967.296

= 1.501.967.630

D = 1.769.169.261 + 1.623.197.347 mod 2^32

= 3.392.366.608 mod 4.294.967.296

= 3.392.366.608

2. Iterasi

Iterasi dilakukan sebanyak 20 kali. Setiap iterasi mengikuti aturan sebagai berikut :

t ← ROTL ((X[1]*(2*X[1]+1)), 5)

u ← ROTL ((X[3]*(2*X[3]+1)), 5)

X[0] ← (ROTL ((X[0] XOR t), u)) + S[2*i]

X[2] ← (ROTL ((X[2] XOR u), t)) + S[2*i + 1]

Temp ← X[0]

X[0] ← X[1]

X[1] ← X[2]

X[2] ← X[3]

X[3] ← Temp

Nilai t dan u didapat dari blok B dan D diproses dengan fungsi f(x) = x(2x+1), kemudian dilanjutkan dengan menggeser nilai t dan u ke kiri sejauh 5 bit.

t = (B * (2*B+1))

= (1.501.967.630 * (2 * 1.501.967.630 + 1)) mod 2^32

= (1.501.967.630 * 3.003.935.261) mod 4.294.967.296

= 4.511.813.524.637.601.430 mod 4.294.967.296

= 4.241.739.414

t : (dalam biner) = 11111100110100111100111010010110

t : (digeser 5 bit) = 10011010011110011101001011011111

t : (dalam desimal) = 2.591.675.103

Nilai 5 bit terakhir dari t yaitu 11111, atau dalam desimal sebesar 31, akan dipergunakan sebagai nilai penggeser blok C pada proses berikutnya, sejauh 31 bit

u = (D * (2 * D + 1) mod 2^32

= (3.392.366.608 * (2 * 3.392.366.608 + 1)) mod 2^32

= (3.392.366.608 * (6.784.733.216 + 1)) mod 2^32

= (3.392.366.608 * 6.784.733.217) mod 2^32

= 4.569.558.335.829.666.320 mod 4.294.967.296 = 2.341.300.752

u : (dalam biner) = 10001011100011010110101000010000

u : (digeser 5 bit) = 01110001101011010100001000010001

u : (dalam desimal) = 1.907.180.049

Nilai 5 bit terakhir dari u yaitu 10001, atau dalam desimal sebesar 17, akan dipergunakan sebagai pergeseran blok A pada proses berikutnya, sejauh 17 bit.

Maka didapatkan nilai-nilai sebagai berikut :

t = 2.591.675.103

u = 1.907.180.049

penggeser t = 31

penggeser u = 16

Langkah selanjutnya adalah memproses blok A dan C dengan nilai-nilai yang telah dihasilkan.

A = (ROTL ((A XOR t), u)) + S[2*i]

A : 1.852.532.084, dalam biner = 01101110011010110110010101110100

t : 2.591.675.103, dalam biner = 10011010011110011101001011011111

A : (hasil xor) = 11110100000100101011011110101011

A : (digeser 31bit) = 11111010000010010101101111010101

A : (dalam desimal) = 4.194.917.333

Niai A dijumlahkan dengan sub kunci S(2), dalam modulo 2^32 :

A = 4.194.917.333 + 1.929.374.348 mod 2^32 = 6.124.291.681 mod 4.294.967.296

= 1.829.324.385

C = (ROTL((C XOR u), t)) + S[2*i+1]

C : 1.919.903.342, dalam biner = 01110010011011110110011001101110

u : 1.907.180.049, dalam biner = 01110001101011010100001000010001

C : (hasil xor) = 00000011110000100010010001111111

C : (digeser 16bit) = 00100100011111110000001111000010

C : (dalam desimal) = 612.303.810

Nilai C dijumlahkan dengan sub kunci S(3), dalam modulo 2^32

C = 612.303.810 + 4.270.616.488 mod 2^32

= 4.882.920.298 mod 4.294.967.296

= 587.953.002

Maka didapat nilai masing-masing blok adalah :

A : 1.829.324.385

B : 1.501.967.630

C : 587.953.002

D : 3.392.366.608

Langkah berikutnya adalah mempertukarkan nilai blok dengan aturan (A, B, C, D) ← (B, C, D, A), sehingga pada iterasi pertama, didapat nilai pada masing-masing blok sebagai berikut :

A : 1.501.967.630

B : 587.953.002

C : 3.392.366.608

D : 1.829.324.385

Nilai masing-masing blok akan dilanjutkan pada iterasi berikutnya sebanyak 20 kali.

III.4. Analisa Dan Kebutuhan Perangkat Keras

Berikut ini adalah spesifikasi perangkat keras minimum yang digunakan dalam pembangunan aplikasi dapat dilihat pada tabel III.1.

Tabel III.1. Spesifikasi Perangkat Keras Smartphone

Smartphone		
No.	**Spesifikasi**	
1	Dimensi Layar	3,5 inches
2	Resolusi	480 x 800 pixels

3	Memori	4GB
4	RAM	512 MB
5	CPU	1GHz

III.5. Analisa Dan Kebutuhan Perangkat Lunak

Analisis perangkat lunak terdiri dari spesifikasi minimum perangkat yang dibutuhkan **.** Berikut ini adalah spesifikasi pernagkat lunak yang digunakan dalam membangun dan mengimplementasikan aplikasi :

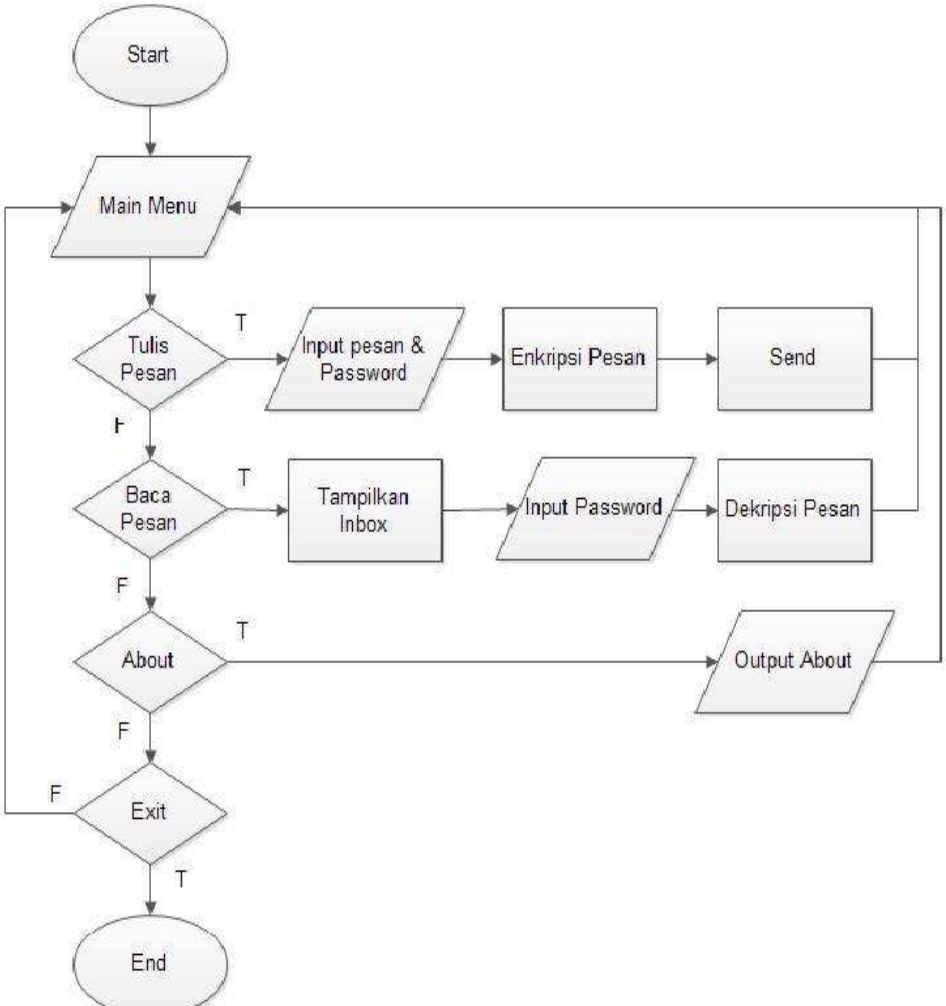
Tabel III.2. Spesifikasi perangkat Lunak

Computer	
No.	**Perangkat Lunak**
1	Sistem Operasi Windows 7 32bit
2	Aplikasi Eclipse ADT
3	JDK versi 1.7 dan Android SDK Windows

III.6. *Flowchart*

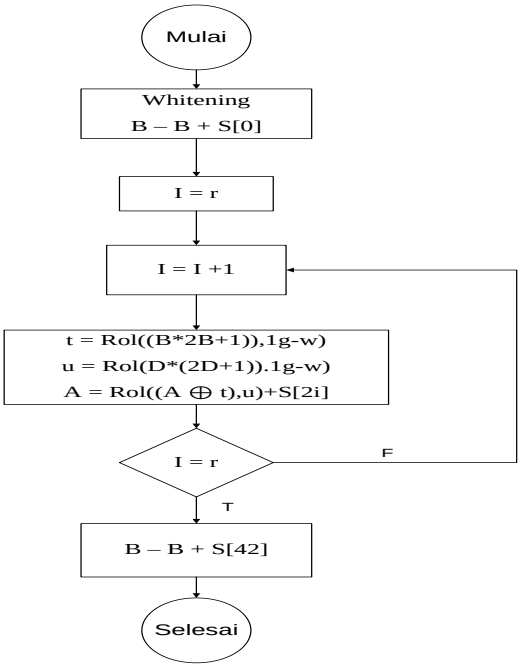
Flowchart atau diagram alur adalah sekumpulan simbol-simbol atau skema yang menunjukkan atau menggambarkan rangkaian kegiatan-kegiatan program dari mulai hingga akhir. Adapun *Flowchart* dari aplikasi enkripsi dengan menggunakan algoritma RC6 yang diterapkan untuk enkripsi SMS adalah pada gambar dibawah ini :

1. *Flowchart* SMS RC6



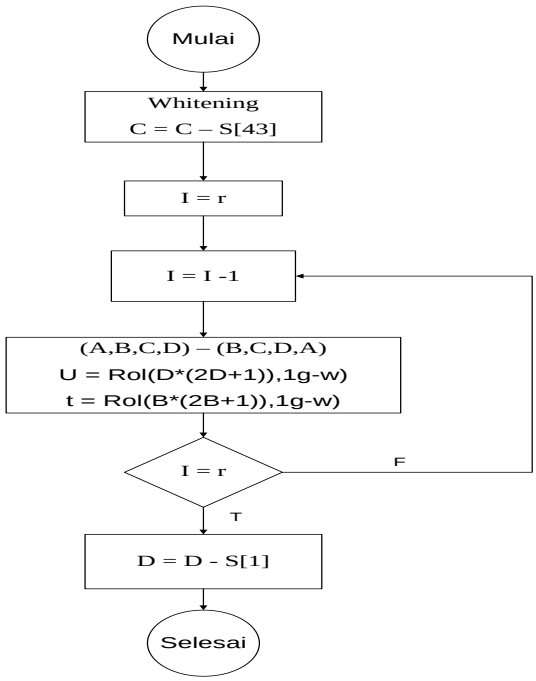
Gambar III.3. *Flowchart* SMS RC6

2. *Flowchart* Proses Enkripsi SMS RC6



Gambar III.4. *Flowchart* Proses Enkripsi SMS RC6

3. *Flowchart* Proses Deskripsi SMS RC6



Gambar III.5. *Flowchart* Proses Deskripsi SMS RC6

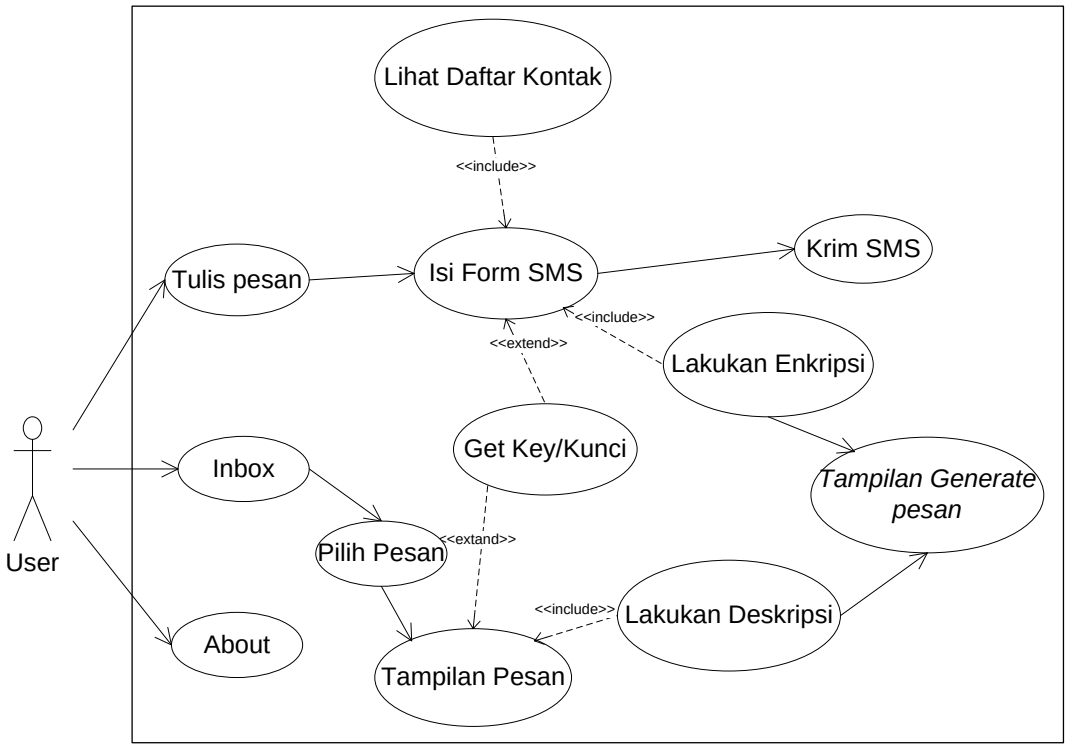
III.7. Perancangan Sistem

III.7.1. *UML Modeling*

Sebelum melangkah kedalam tahap perancangan aplikasi lebih lanjut, maka dilakukan perancangan pemodelan visual dari aplikasi yang akan dibangun dengan menggunakan pemodelan UML (*Unified Modelling Language*), adapun pemodelan konsep perancangannya adalah sebagai berikut :

III.7.2. *Use Case* Diagram SMS RC6

Hal-hal dapat dilakukan oleh pengguna terhadap sistem dapat dilihat pada diagram *use case* pada gambar dibawah ini :

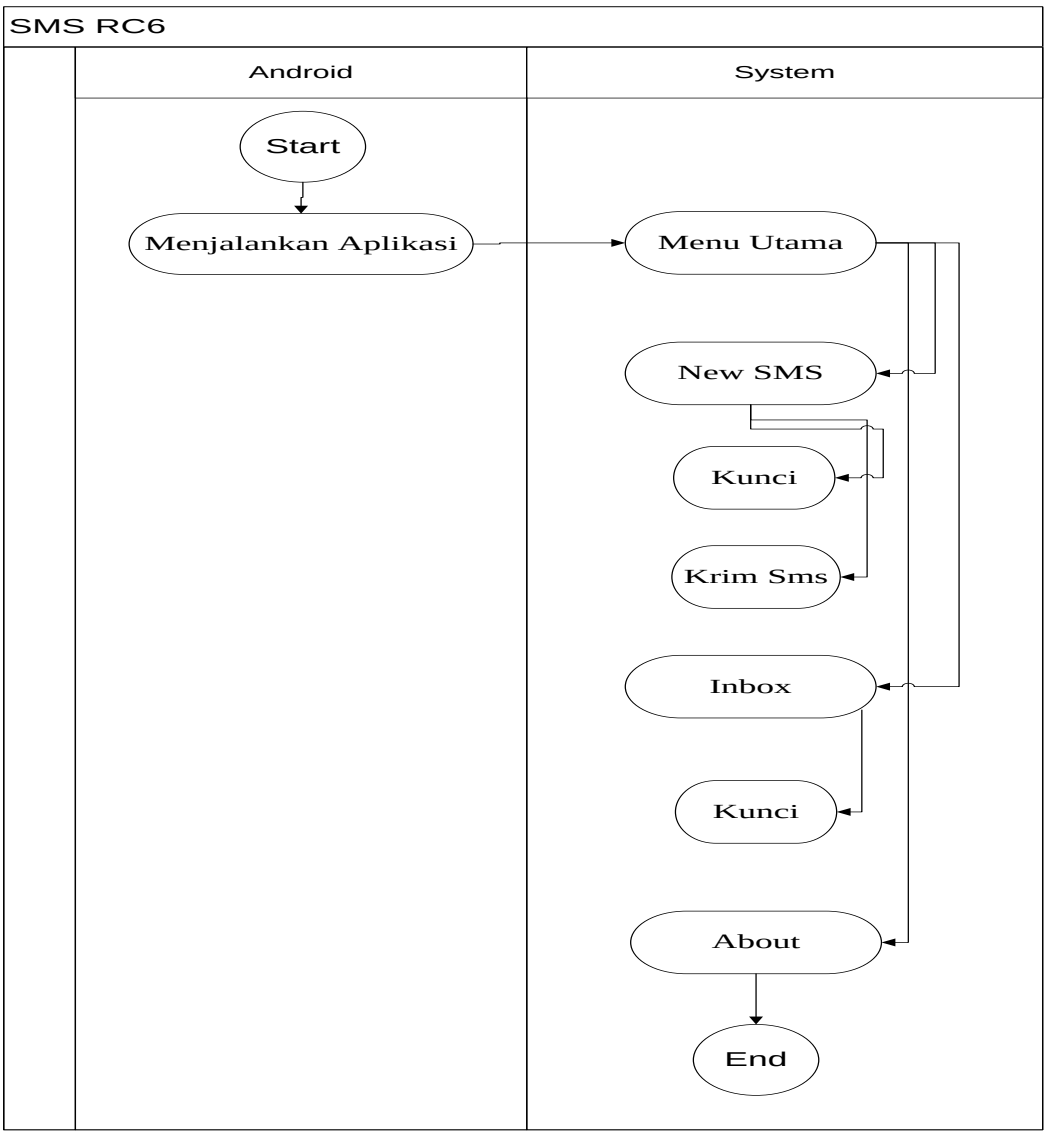


Gambar III.6. Diagram *Use Case* SMS RC6

Gambar III.6. menjelaskan langkah-langkah yang dapat dilakukan oleh user dalam melakukan pengelolaan pesan SMS yang ingin disampaikan. Pada gambar dijelaskan bahawa user Merupakan aktor yang menggunakan aplikasi untuk mengirim pesan singkat yang sudah terenkripsi, dan mendekripsi pesan masuk yang terenkripsi.

III.7.3. *Activity* Diagram SMS RC6

Pada *Activity* diagram menggambarkan berbagai aliran aktivitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir aktivitas berawal. Adapun rancangan diagram aktivitas sms yang dirancang adalah sebagai berikut:



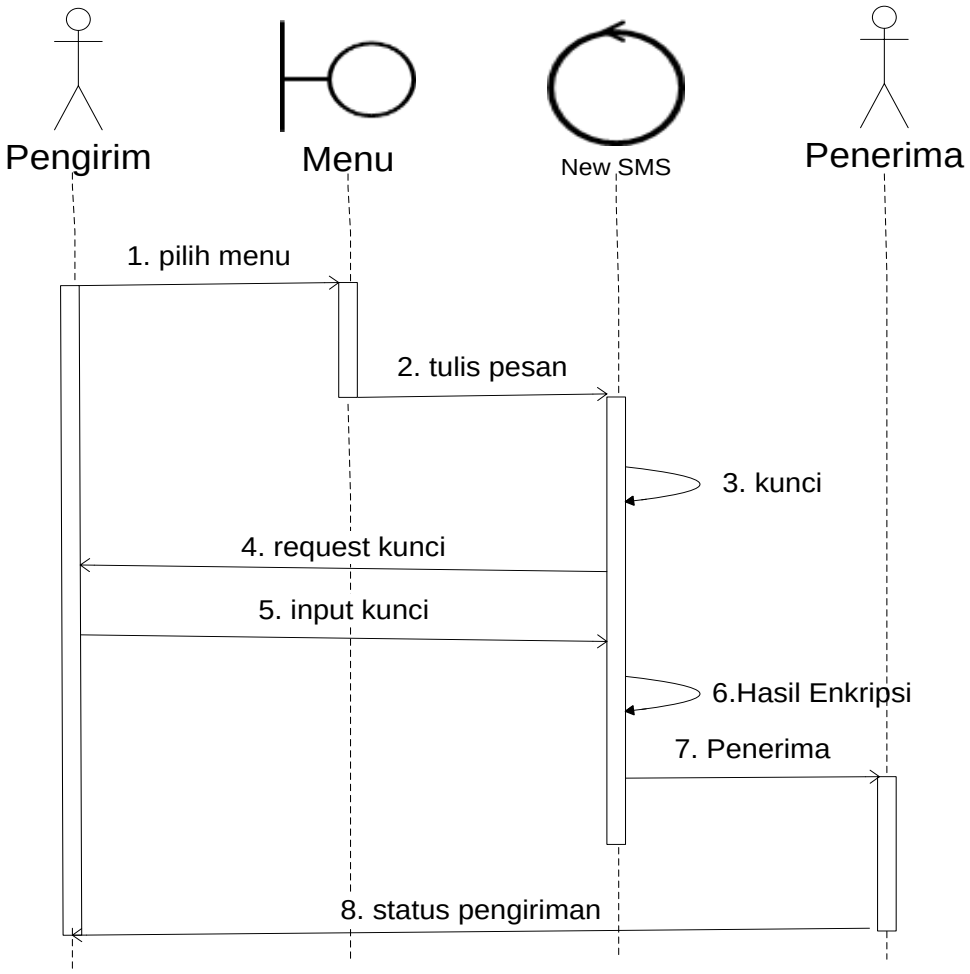
Gambar III.7. *Activity* Diagram SMS RC6

Dari Gambar *Activity Diagram* di atas menjelaskan tentang gambaran *system* aplikasi keamanan SMS pada android saat dijalankan oleh pengguna.

III.7.4. *Sequence* Diagram Enkripsi dan Deskripsi SMS

Pada bagian ini terdiri dari dua bagian yang penting yaitu tulis sms dan baca sms. Berikut ini sequence diagram enkripsi dan deskripsi :

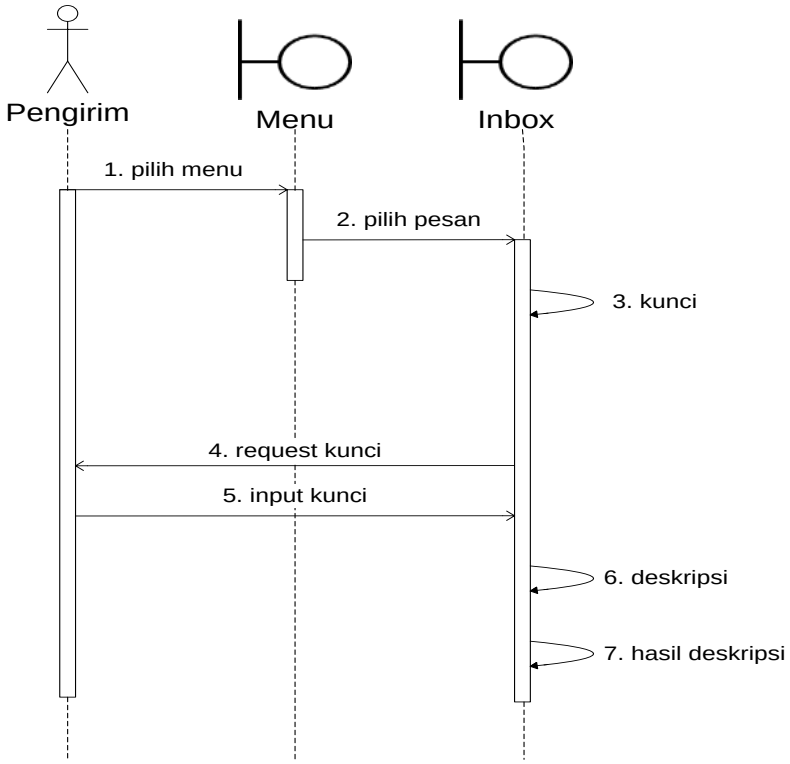
1. Enkripsi



Gambar III.8. *Sequence* Diagram Enkripsi SMS

Dari gambar diatas terlihat pengirim memilih menu tulis pesan. Setelah pesan selesai ditulis, proses selanjutnya adalah user diminta untuk memasuki kunci enkripsi. Setelah pesan selesai dienkripsi maka hasil enkripsi akan tampil pada fungsi tulis sms dan kemudian pesan dapat dikirim dan pengirim mendapatkan pesan enkripsi tersebut.

2. Deskripsi

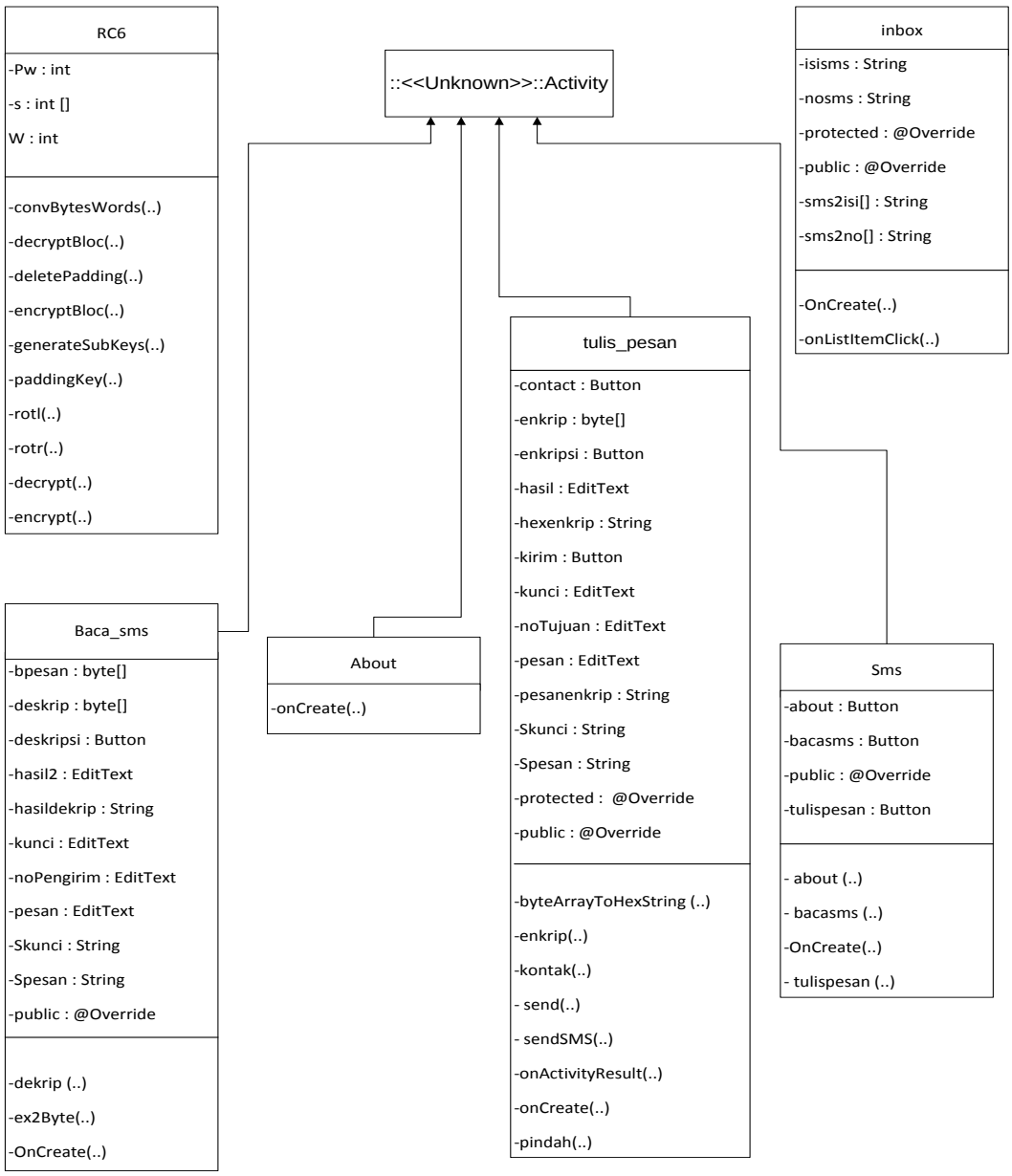


Gambar III.9. *Sequence* Diagram Dekripsi SMS

Dari gambar diatas penerima memilih menu inbox yang berisi pesan, kemudian dari inbox yang berisi pesan, kemudian dari inbox yang berisi pesan dibuka maka sistem minta key/kunci sama dengan key enkripsinya kalau salah password tidak bisa dibuka pesan sms dari sang pengirim.

III.7.5. *Class* Diagram SMS RC6

Pada *Class* diagram perancangan aplikasi ini, dapat dilihat pada gambar III.10 sebagai berikut.



Gambar III.10. *Class* Diagram Enkripsi SMS

Keterangan *Class* Diagram

1. Sms = kelas ini merupakan tampilan utama dari aplikasi SMS RC6, ketika aplikasi dijalankan, maka kelas ini yang pertama dipanggil.
2. Tulis_sms = kelas ini merupakan tampilan untuk melakukan penulisan, enkripsi pesan sms, dan pengiriman pesan sms.

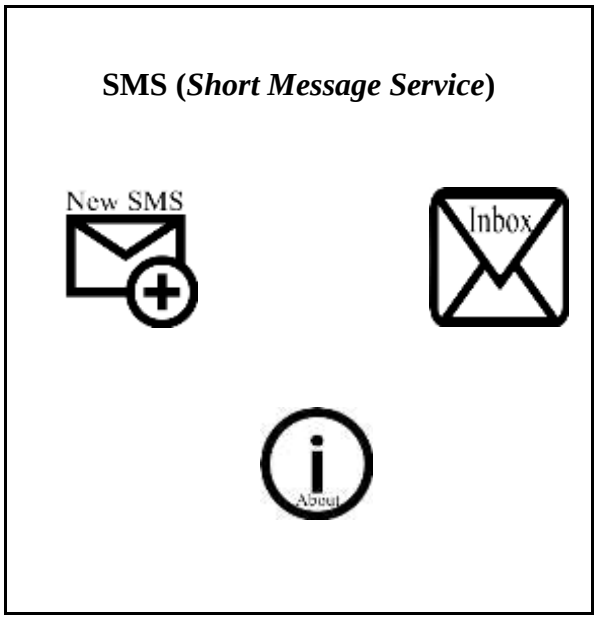
3. Inbox = kelas ini berisi *list-list* dari daftar pesan yang masuk kedalam *smartphone*.
4. Baca_sms = kelas ini merupakan kelas untuk membaca sms yang dipilih didalam kelas inbox, serta mendekripsikan pesan tersebut.
5. About = kelas ini untuk menampilkan perkenalan penulis.
6. RC6 = kelas ini merupakan kelas algoritma enkripsi dan deskripsi RC6, serta kuncinya.

III.8. Perancangan *Interface*

Pada perancangan ini, dilengkapi dengan rancangan *user interface*, yang menjadi acuan dalam implementasi dengan menggunakan bahasa pemrograman *java/eclipse.*

1. Rancangan Menu Utama

Tampilan menu merupakan pilihan yang dapat dilakukan pengguna dalam menggunakan aplikasi keamanan SMS tersebut. Rancangannya dapat dilihat pada gambar III.11.



Gambar III.11. *Form* Menu Utama

Dari tampilan rancangan di atas ada beberapa menu pilihan. Berikut penjelasannya:

a) New SMS adalah menu yang digunakan untuk mengirim pesan kepada orang lain.

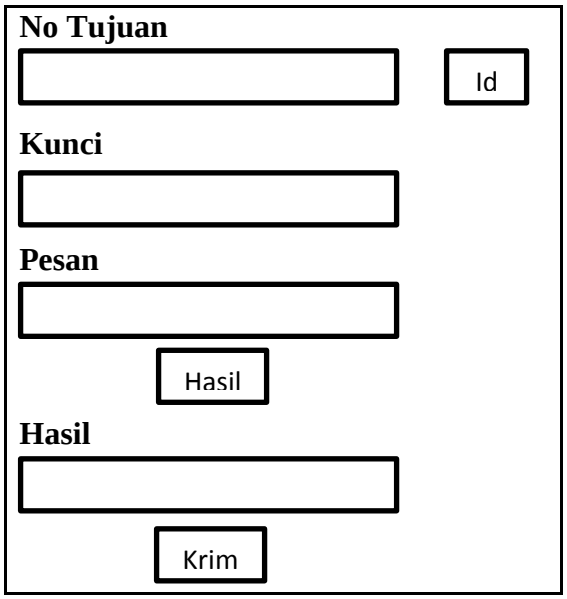
b) Inbox adalah menu yang berfungsi untuk melihat pesan yang telah diterima dari orang lain.

c) About merupakan menu yang digunakan untuk menampilkan perkenalan diri.

2. Rancangan Tulis Pesan / *New* Sms

Tampilan tulis pesan adalah tampilan dimana pesan akan diciptakan atau dibuat dan dikirim ke nomor tujuan. Tampilan buat pesan dapat dilihat pada gambar III.12.

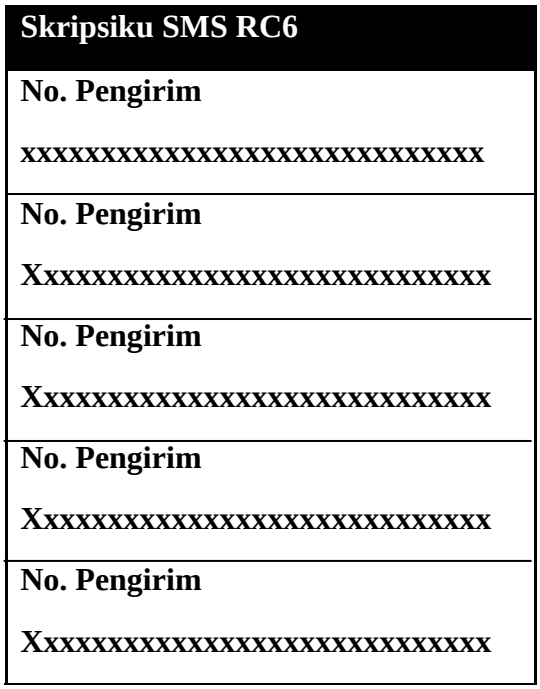
Skripsiku SMS RC6



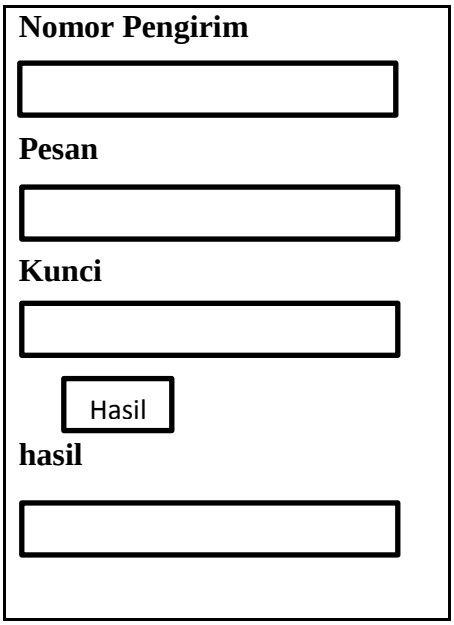
Gambar III.12. *Form New* Sms/Tulis Pesan dienkripsi

3. Rancangan Kotak Masuk

Pada rancangan kotak masuk, lebih sederhana hanya menampilkan nama/nomor, tanggal dan pesan secara berulang-ulang tergantung pesan yang diterima. Berikut tampilan rancangan kotak masuk dan pesan terkirim.



Gambar III.13. Rancangan *Inbox*



Gambar III.14. Rancangan *Inbox*

Deskripsi

4. Rancangan About

Pada rancangan About, lebih sederhana hanya menampilkan keterangan penulis seperti gambar, nama, kelas, jurusan, dan universitas.

Enkripsi dan Deskripsi RC6

M.Amin

1210000187

Teknik Informatika

2016-2017

UPU Potensi Utama

Gambar III.15. *Form About*