

**APLIKASI KRIPTOGRAFI PESAN SINGKAT DENGAN ALGORITMA
RIVEST CHIPER 6 (RC6) DAN BLOWFISH BERBASIS ANDROID**

SKRIPSI



Risky Maulana

1411500049

**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
ATMA LUHUR
PANGKALPINANG
2018**

**APLIKASI KRIPTOGRAFI PESAN SINGKAT DENGAN ALGORITMA
RIVEST CHIPER 6 (RC6) DAN BLOWFISH BERBASIS ANDROID**

SKRIPSI

**Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer**



**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER**

**ATMA LUHUR
PANGKALPINANG**

2018

LEMBAR PERYATAAN

Yang bertanda tangan dibawah ini:

NIM : 1411500049

Nama : Risky Maulana

Judul Skripsi : APLIKASI KRIPTOGRAFI PESAN SINGKAT DENGAN
ALGORITMA *RIVEST CHIPER 6 (RC6)* DAN *BLOWFISH*
BERBASIS ANDROID

Menyatakan bahwa Laporan Tugas Akhir saya adalah hasil karya sendiri dan bukan plagiat. Apabila ternyata ditemukan didalam laporan Tugas Akhir saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

PANGKALPINANG, 27 JULI 2018



Risky Maulana

LEMBAR PENGESAHAN SKRIPSI

APLIKASI KRIPTOGRAFI PESAN SINGKAT DENGAN ALGORITMA
RIVEST CHIPER 6 (RC6) DAN BLOWFISH BERBASIS ANDROID

Yang dipersiapkan dan disusun oleh

Risky Maulana
1411500049

Telah dipertahankan di depan Dewan Penguji
Pada Tanggal 2 Agustus 2018

Susunan Dewan Penguji
Anggota



Benny Wijaya, S.T., M.Kom
NIDN. 0202097902

Dosen Pembimbing



Ari Amir Alkodi, M.Kom
NIDN. 0201038601

Kaprodi/Teknik Informatika



R. Burham Isnanto F., S.Si, M.Kom
NIDN: 0224048003

Ketua



Yohanes Setiawan, M.Kom
NIDN. 0219068501

Skripsi ini telah diterima dan sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 20 Agustus 2018

KETUA STMIK ATMA LUHUR PANGKALPINANG



Dr. Husni Teja Sukmana, S.T., M.Sc
NIP:197710302001121003

KATA PENGANTAR

Puji syukur Alhamdulillah penulis panjatkan kehadiran Allah SWT yang telah melimpahkan segala rahmat dan karunianNya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang Strata Satu (S1) Jurusan Teknik Informatika STMIK Atma Luhur. Penulis menyadari bahwa laporan skripsi ini masih jauh dari sempurna. Karena itu, kritik dan saran akan senantiasa penulis terima dengan senang hati.

Dengan segala keterbatasan, penulis menyadari pula bahwa laporan skripsi ini takkan terwujud tanpa bantuan, pemimbing, dan dorongan berbagai pihak Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Allah SWT yang telah menciptakan dan memberikan kehidupan di dunia.
2. Bapak dan Ibu tercinta atas doa-doanya, dan juga untuk Adik yang telah mendukung dan memberi semangat.
3. Bapak Drs. Djaetun HS yang telah mendirikan Atma Luhur.
4. Bapak Dr. Husni Teja Sukmana, ST., M.Sc selaku ketua STMIK Atma Luhur.
5. Bapak R. Burham Isnanto F., S.Si, M.Kom Selaku Kaprodi Teknik Informatika.
6. Bapak Ari Amir Alkodri, M.Kom selaku pembimbing teori serta pembimbing aplikasi.
7. Sahabatterdekat dan teman seperjuangan penulis yang tidak bisa penulis sebutkan satu persatu yang selalu memberi semangat.

Semoga Tuhan Yang Maha Esa membalas kebaikan dan selalu mencurahkan hidayah serta taufikNya, Amin.

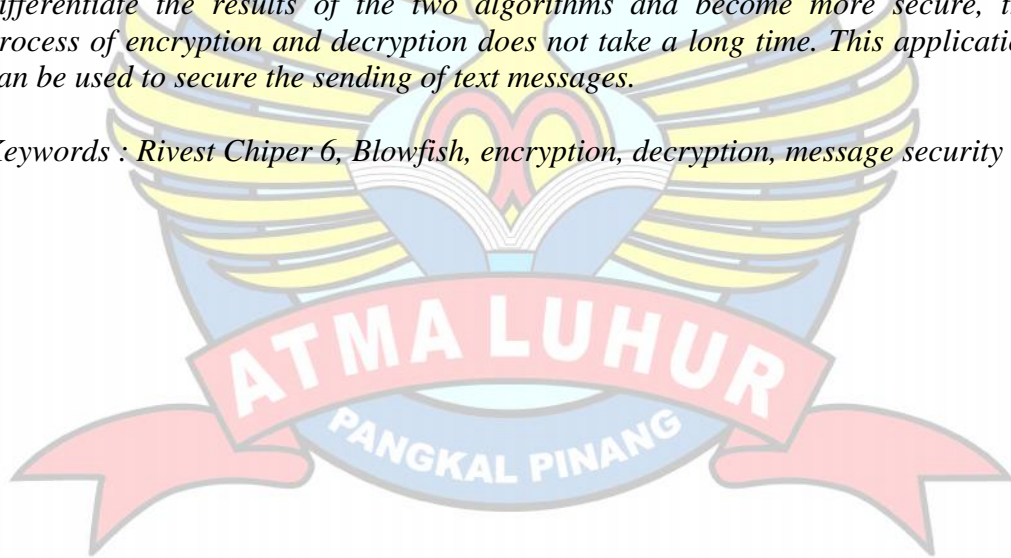
Pangkalpinang, 27 Juli 2018

Risky Maulana

ABSTRACT

Technological development for several years is very rapid, short message technology is still a lot of people who use it, but the security aspect is not guaranteed. People who exchange information are at risk of experiencing theft of information during the shipping process, for this reason it is necessary to have encryption before the message is sent and decryption is done to read so that it is not easily misused by people who do not have authority. With Rivest Chiper 6 and Blowfish cryptographic algorithms this model is one symmetric key algorithm in the form of block cipher that can answer message security, this method is suitable for maintaining message security. This paper will discuss a number of aspects of cryptography and the basic concepts of the Rivest Chiper 6 and Blowfish algorithms. An application designed to implement the Rivest Chiper 6 and Blowfish algorithms. Rivest Chiper 6 and Blowfish algorithms implemented on Android smartphones can encrypt messages before they are sent and decrypt messages when received. By using two encryption options, message security can differentiate the results of the two algorithms and become more secure, the process of encryption and decryption does not take a long time. This application can be used to secure the sending of text messages.

Keywords : Rivest Chiper 6, Blowfish, encryption, decryption, message security



ABSTRAK

Perkembangan teknologi untuk beberapa tahun ini sangat pesat, teknologi pesan singkat masih banyak masyarakat yang menggunakan, tetapi segi keamanan belum terjamin. Orang yang bertukar informasi beresiko mengalami pencurian isi informasi saat proses pengiriman, karena alasan tersebut perlu adanya enkripsi sebelum pesan tersebut dikirim dan dilakukan dekripsi untuk membaca agar tidak mudah disalahgunakan oleh orang yang tidak memiliki kewenangan. Dengan algoritma kriptografi *Rivest Chiper 6* dan *Blowfish* model ini merupakan salah satu algoritma kunci simetris yang berbentuk *block chiper* yang dapat menjawab keamanan pesan, Metode tersebut cocok untuk menjaga keamanan pesan. Pada tulisan ini akan dibahas sejumlah aspek dari kriptografi serta konsep dasar dari algoritma *Rivest Chiper 6* dan *Blowfish*. Sebuah aplikasi dirancang untuk dapat mengimplementasikan algoritma *Rivest Chiper 6* dan *Blowfish*. Algoritma *Rivest Chiper 6* dan *Blowfish* di Implementasikan pada *smartphone* android dapat mengenkripsi pesan sebelum dikirim dan mendekripsi pesan ketika diterima. Dengan menggunakan dua pilihan enkripsi keamanan pesan pengguna bisa membedakan hasil dua algoritma tersebut dan menjadi lebih terjamin, Proses enkripsi dan dekripsi tidak memakan waktu yang lama. Aplikasi ini dapat di manfaatkan untuk mengamankan pengiriman pesan teks.

Kata kunci :*Rivest Chiper 6* (RC6), *Blowfish*, enkripsi, dekripsi, keamanan pesan



DAFTAR ISI

	Halaman
LEMBAR PERNYATAAN	i
LEMBAR PENGESAHAN	ii
KATA PENGANTAR	iii
ABSTRACT	iv
ABSTRAK	v
DAFTAR ISI	vi
DAFTAR GAMBAR	ix
DAFTAR TABEL	xi
DAFTAR SIMBOL	xii
DAFTAR ISTILAH	xvi
 BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	3
1.4 Tujuan dan Manfaat Penelitian	3
1.5 Sistematika Penulisan.....	4
 BAB II LANDASAN TEORI	
2.1 Aplikasi	5
2.2 Kriptografi.....	5
2.3 Android	7
2.3.1 Fitur Perangkat Lunak Android	7
2.3.2 Privasi dan Keamanan Pada Android.....	7
2.3.3 Fitur Perangkat Keras Android.....	7

2.3.4	Arsitektur Android	8
2.3.5	Dasar Pemrograman Android.....	9
2.4	<i>Short Message Service</i> (SMS).....	10
2.5	Algoritma <i>Rivest Chiper 6</i> (RC6).	11
2.5.1	Pembentukan Kunci Internal.....	11
2.5.2	Proses Enkripsi dan Deskripsi.....	13
2.6	Algoritma <i>Blowfish</i>	14
2.7	<i>Unified Modeling Language</i> (UML).....	15
2.8	Model Pengembangan Sistem dengan Metode <i>Waterfall</i>	19
2.9	Java.....	20
2.10	Eclipse.....	21
2.11	<i>Object Oriented Programing</i>	21
2.12	<i>Black Box Testing</i>	22
2.13	Penelitian Terdahulu	23
 BAB III METODOLOGI PENELITIAN 		
3.1	Model Pengembangan Sistem.....	27
3.2	Metode <i>Object Oriented Programming</i>	28
3.3	Tools Pengembangan Sistem	28
3.4	Algoritma <i>Rivest Chiper 6</i> (RC6) dan <i>Blowfish</i>	29
 BAB IV HASIL DAN PEMBAHASAN 		
4.1	Analisis Masalah	30
4.1.1	Analisis Kebutuhan	30
4.1.2	Analisis Sistem Berjalan	33
4.2	Perancangan Sistem	34
4.2.1	Identifikasi Sistem Usulan	34
4.2.2	Rancangan Sistem	35
4.2.3	Rancangan Layar.....	48
4.3	Implementasi	

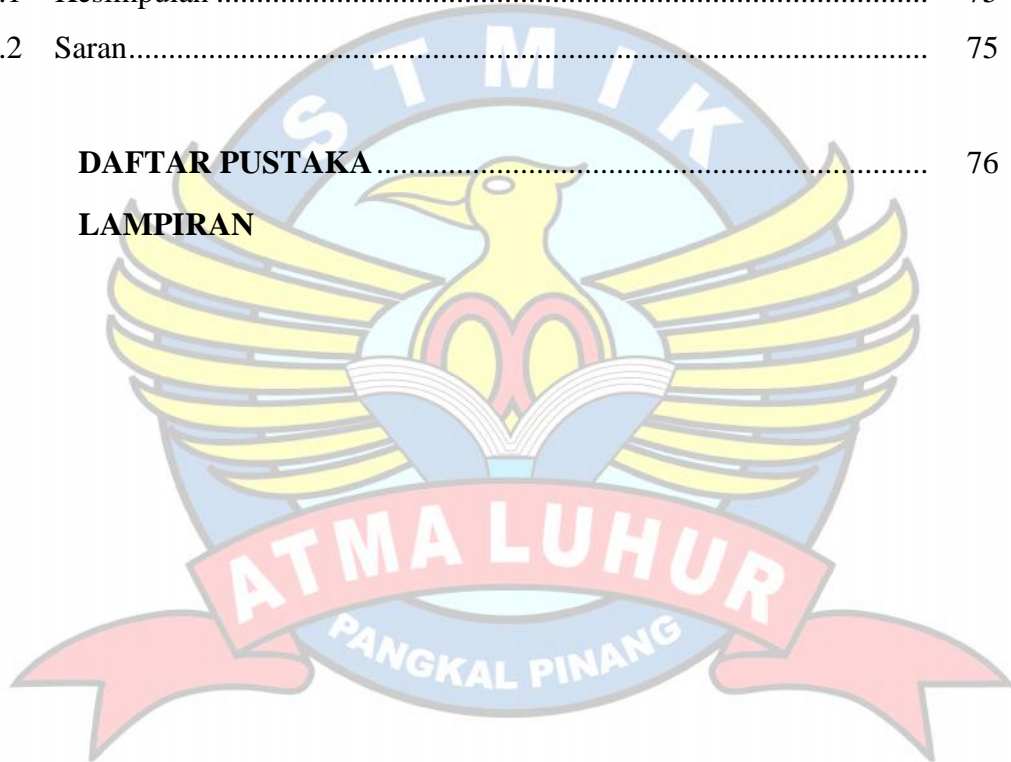
4.3.1 Tampilan Layar	55
4.4 Penerapan Algoritma.....	64
4.4.1 Analisa Peneapan Algoritma RC6	62
4.4.2 Algoritma <i>Blowfish</i>	68
4.4.3 Perbandingan hasil algoritma <i>Rivest Chiper 6 (RC6)</i> dan <i>Blowfish</i> ...	71
4.5 Pengujian.....	73

BAB V PENUTUP

5.1 Kesimpulan	75
5.2 Saran.....	75

DAFTAR PUSTAKA	76
-----------------------------	----

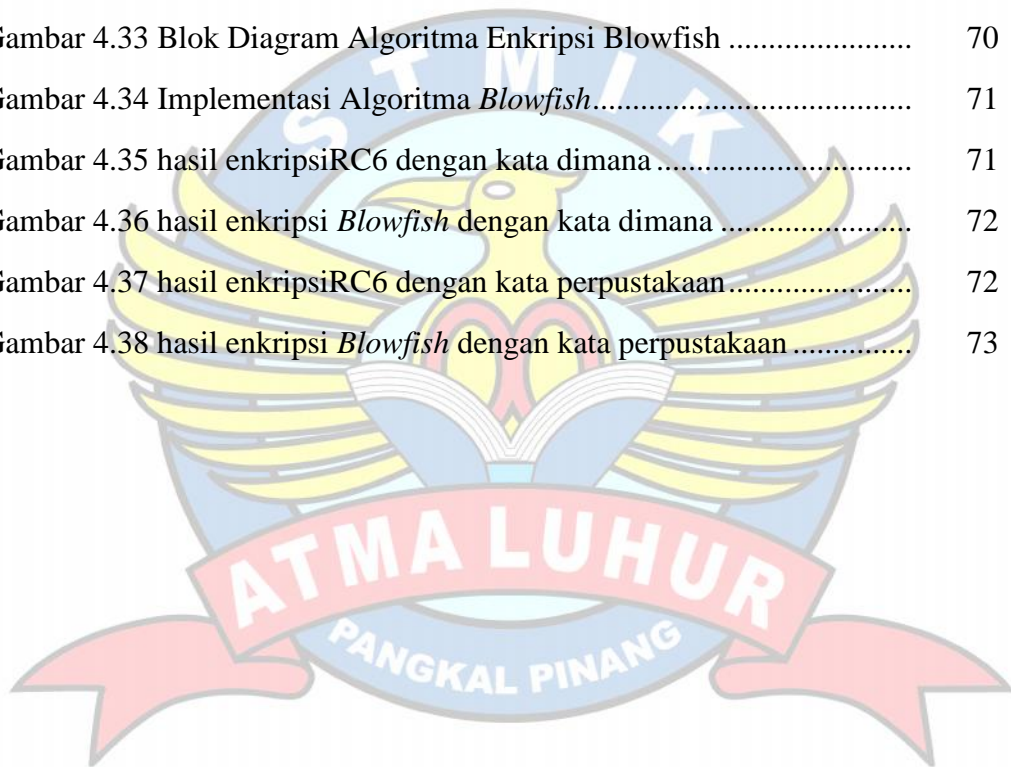
LAMPIRAN



DAFTAR GAMBAR

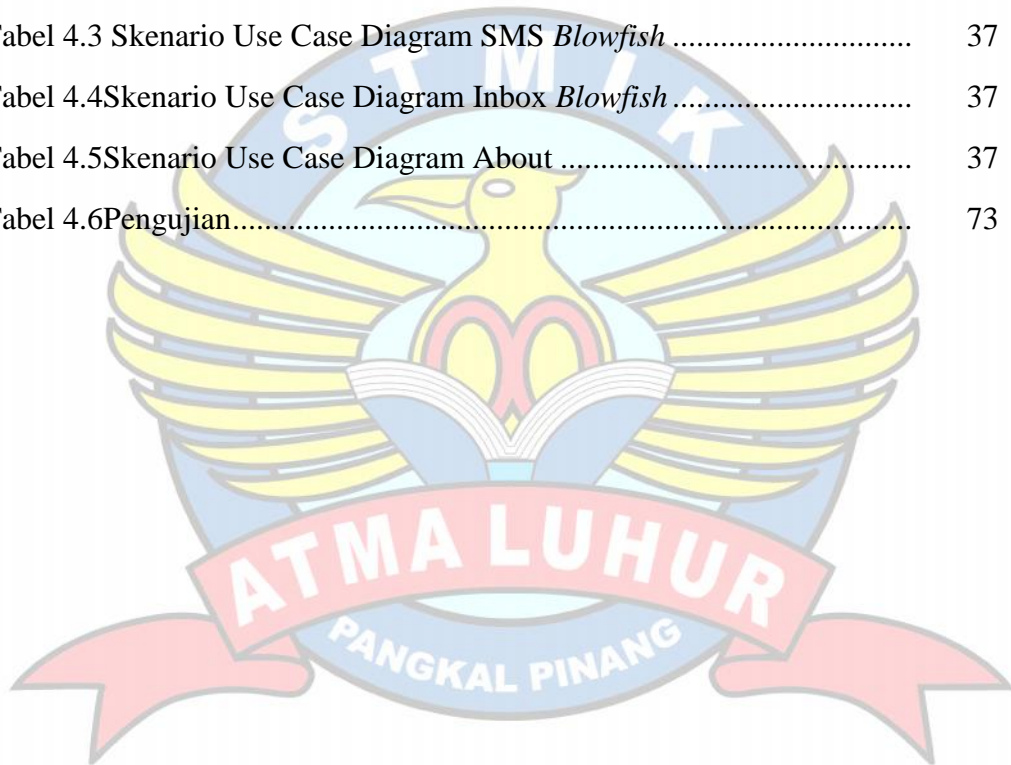
	Halaman
Gambar 2.1 Skema enkripsi dan deskripsi dengan menggunakan kunci ...	6
Gambar 4.1 <i>Activity Diagram</i> Sistem Berjalan Sebelum Aplikasi.....	33
Gambar 4.2 <i>Activity Diagram</i> SMS Kriptografi.....	34
Gambar 4.3 Use case Diagram Aplikasi SMS Kriptografi	35
Gambar 4.4 <i>Activity Diagram</i> SMS RC6	38
Gambar 4.5 <i>Activity Diagram</i> <i>Inbox</i> RC6.....	39
Gambar 4.6 <i>Activity Diagram</i> SMS <i>Blowfish</i>	40
Gambar 4.7 <i>Activity Diagram</i> <i>InboxBlowfish</i>	41
Gambar 4.8 <i>Activity Diagram</i> <i>About</i>	42
Gambar 4.9 <i>Sequence Diagram</i> SMS RC6.....	43
Gambar 4.10 <i>Sequence Diagram</i> <i>Inbox</i> RC6.....	44
Gambar 4.11 <i>Sequence Diagram</i> SMS <i>Blowfish</i>	45
Gambar 4.12 <i>Sequence Diagram</i> <i>Inbox Blowfish</i>	46
Gambar 4.13 <i>Sequence Diagram</i> <i>About</i>	47
Gambar 4.14 Rancangan Layar Menu utama.....	48
Gambar 4.15 Rancangan Layar menu SMS RC6.....	49
Gambar 4.16 Rancangan Layar <i>Inbox</i> RC6	50
Gambar 4.17 Rancangan Layar Baca <i>Inbox</i> RC6	51
Gambar 4.18 Rancangan Layar Menu SMS <i>Blowfish</i>	52
Gambar 4.19 Rancangan Layar <i>Inbox Blowfish</i>	53
Gambar 4.20 Rancangan Layar <i>About</i>	54
Gambar 4.21 Tampilan Layar Menu utama	55
Gambar 4.22 Tampilan Layar SMS RC6.....	56
Gambar 4.23 Tampilan Layar <i>Inbox</i> RC6.....	57
Gambar 4.24 Tampilan Layar menu baca SMS RC6.....	58

Gambar 4.25 Tampilan Layar SMS <i>Blowfish</i>	59
Gambar 4.26 Tampilan Layar <i>InboxBlowfish</i>	60
Gambar 4.27 Tampilan Layar Menu <i>About</i>	61
Gambar 4.28 Enkripsi RC6	66
Gambar 4.29 Deskripsi RC6	67
Gambar 4.30 Pengujian Memilih SMS	67
Gambar 4.31 Pengujian Memilih SMS	67
Gambar 4.32 Fungsi F	69
Gambar 4.33 Blok Diagram Algoritma Enkripsi Blowfish	70
Gambar 4.34 Implementasi Algoritma <i>Blowfish</i>	71
Gambar 4.35 hasil enkripsiRC6 dengan kata dimana	71
Gambar 4.36 hasil enkripsi <i>Blowfish</i> dengan kata dimana	72
Gambar 4.37 hasil enkripsiRC6 dengan kata perpustakaan	72
Gambar 4.38 hasil enkripsi <i>Blowfish</i> dengan kata perpustakaan	73








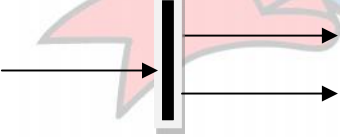
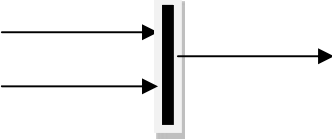
DAFTAR TABEL

	Halaman
Tabel 2.1 <i>Use Case Diagram</i>	15
Tabel 2.2 <i>Activity Diagram</i>	16
Tabel 2.3 <i>Sequence Diagram</i>	18
Tabel 4.1 Skenario Use Case Diagram SMS RC6	36
Tabel 4.2 Skenario Use Case Diagram <i>Inbox</i> RC6	36
Tabel 4.3 Skenario Use Case Diagram SMS <i>Blowfish</i>	37
Tabel 4.4 Skenario Use Case Diagram <i>Inbox Blowfish</i>	37
Tabel 4.5 Skenario Use Case Diagram About	37
Tabel 4.6 Pengujian	73



DAFTAR SIMBOL

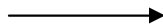
1. Activity Diagram

	<p><i>Start Point</i></p> <p>Menggambarkan awal dari suatu aktivitas yang berjalan pada sistem.</p>
	<p><i>End Point</i></p> <p>Menggambarkan akhir dari suatu aktivitas yang berjalan pada sistem.</p>
	<p><i>Activity State</i></p> <p>Menggambarkan suatu proses / kegiatan bisnis.</p>
	<p><i>Swimlane</i></p> <p>Menggambarkan pembagian / pengelompokkan berdasarkan tugas dan fungsi sendiri.</p>
	<p><i>Decision Points</i></p> <p>Menggambarkan pilihan untuk pengambilan keputusan, true atau false.</p>
	<p><i>Fork</i></p> <p>Menggambarkan aktivitas yang dimulai dengan sebuah aktivitas dan diikuti oleh dua atau lebih aktivitas yang harus dikerjakan.</p>
	<p><i>Join</i></p> <p>Menggambarkan aktivitas yang dimulai dengan dua atau lebih aktivitas yang sudah dilakukan dan menghasilkan sebuah aktivitas.</p>

[...]

Guards

Sebuah kondisi benar sewaktu melewati sebuah transisi, harus konsisten dan tidak overlap.



Transition

Menggambarkan aliran perpindahan control antara state.

2. Use Case Diagram



Actor

Abstraksi dari orang atau sistem yang mengaktifkan fungsi dari use case.



Use Case

Menggambarkan proses sistem dari perpektif pengguna (user).



Relasi/Asosiasi

Menggambarkan hubungan antara actor dengan use case.

<<include>>

----->

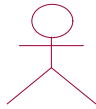
Asosiasi yang termasuk didalam *use case* lain, yang bersifat harus dilakukan bila *use case* lain tersebut dilakukan.

<<extend>>

----->

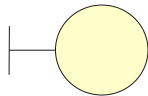
Perluasan dari *use case* lain jika kondisi atau syarat terpenuhi dan tidak harus dilakukan.

3. Sequence Diagram



Actor

Menggambarkan seseorang atau sesuatu (seperti perangkat, sistem lain) yang berinteraksi dengan sistem.



Boundary

Sebuah obyek yang menjadi penghubung antara user dengan sistem. Contohnya window, dialogue box atau screen (tampilan layar).



Control

Suatu obyek yang berisi logika aplikasi yang tidak memiliki tanggung jawab kepada entitas.



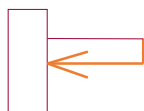
Entity

Menggambarkan suatu objek yang berisi informasi kegiatan yang terkait yang tetap dan disimpan kedalam suatu database.



Object Message

Menggambarkan pengiriman pesan dari sebuah objek ke objek lain.



Recursive

Sebuah obyek yang mempunyai sebuah operation kepada dirinya sendiri.



Return Message

Menggambarkan pesan/hubungan antar objek, yang menunjukkan urutan kejadian yang terjadi.



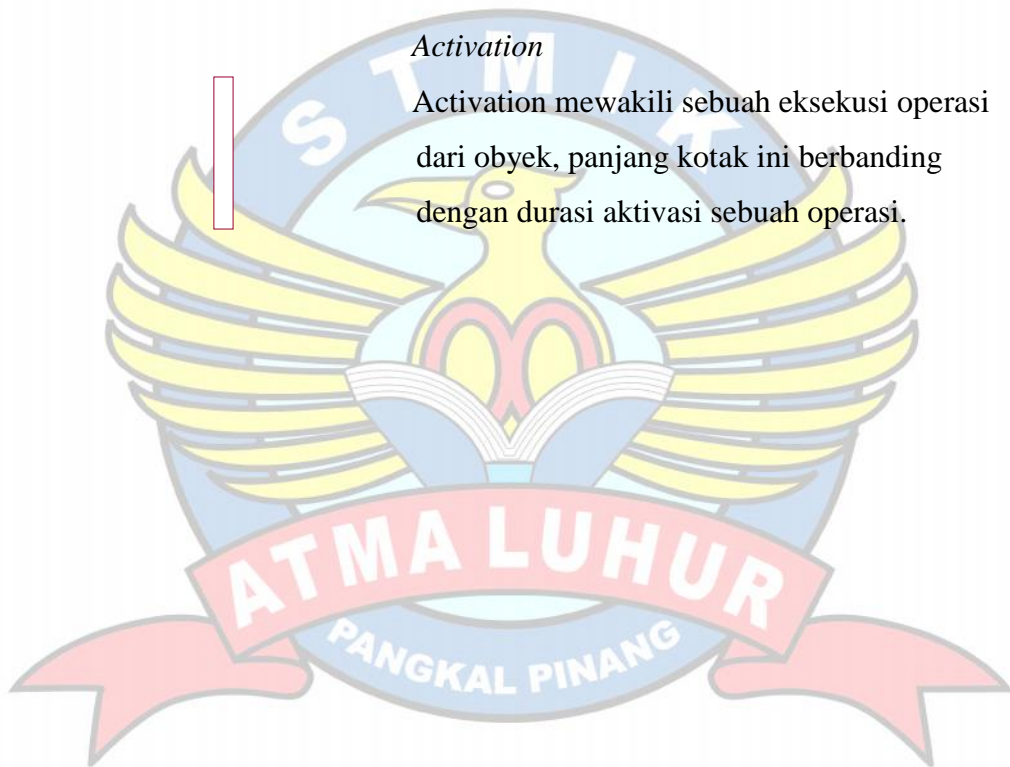
Lifeline

Garis titiktitik yang terhubung dengan obyek, sepanjang lifeline terdapat activation.



Activation

Activation mewakili sebuah eksekusi operasi dari obyek, panjang kotak ini berbanding dengan durasi aktivasi sebuah operasi.



DAFTAR ISTILAH

1. SMSC = *Short Message Service Center*
2. SMS = *Short Message Service*
3. GSM = *Global Systema For Mobile Communication*
4. TDMA = *Time Division Multiple Access*
5. CDMA = *Code Division Multiple Access*
6. AES = *Advanced Encryption Standard*
7. RC6 = *Rivest Chiper 6*
8. UML = *Unified Modeling Language*

