

**PENERAPAN KRIPTOGRAFI ALGORITMA AES (*ADVANCED
ENCRYPTION STANDARD*) SERTA KOMPRESI ALGORITMA
HUFFMAN PADA APLIKASI *MESSAGE***

SKRIPSI



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

**PENERAPAN KRIPTOGRAFI ALGORITMA AES
(*ADVANCED ENCRYPTION STANDARD*) SERTA KOMPRESI
ALGORITMA *HUFFMAN* PADA APLIKASI *MESSAGE***

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 PERNYATAAN

LEMBAR PERNYATAAN



Yang bertanda tangan di bawah ini:

NIM : 1511500167

Nama : Eli Patima

Judul Skripsi : PENERAPAN KRIPTOGRAFI ALGORITMA AES
(*ADVANCED ENCRYPTION STANDARD*) SERTA KOMPRESI
ALGORITMA *HUFFMAN* PADA APLIKASI *MESSAGE*

Menyatakan bahwa Laporan Tugas Akhir saya adalah **HASIL KARYA SENDIRI, TIDAK MEMBAYAR PIHAK LAIN UNTUK MEMBUATKAN 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



Eli Patima

LEMBAR PENGESAHAN SKRIPSI

LEMBAR PENGESAHAN SKRIPSI

PENERAPAN KRİPTOGRAFI ALGORITMA AES SERTA KOMPRESI ALGORITMA HUFFMAN PADA APLIKASI MESSAGE


Yang dipersiapkan dan disusun oleh :

ELI PATIMA
1511500167

Telah dipertahankan di depan Dewan Penguji
Pada Tanggal 10 Agustus 2018

**Susunan Dewan Penguji
Anggota**

Dosen Pembimbing

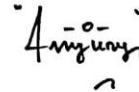


R. Burham Isnanto F., S.Si, M.Kom
NIDN. 0224048003

Laurentinus, M.Kom
NIDN. 0201079201

Kaprodi Teknik Informatika

Ketua



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

Dwi Yuny Sylfania, M.Kom
NIDN. 0207069301

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 kehadiran Tuhan YME yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan skripsi yang merupakan salah satu persyaratan untuk menyelesaikan jenjang strata satu (S1) pada Program Studi 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, bimbingan, dan dorongan dari 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. Ayah dan Ibu tercinta yang telah mendukung penulis baik spirit maupun materi.
3. Kakak – kakakku tercinta yang telah memberikan bantuan baik spirit maupun materi untuk terus menyelesaikan skripsi ini.
4. Bapak Drs. Djaetun Hs yang telah mendirikan Atma Luhur.
5. Bapak Dr. Husni Teja Sukmana, S.T., M.sc, selaku Ketua STMIK Atma Luhur.
6. Bapak R. Burham Isnanto Farid, S.Si., M. Kom Selaku Kaprodi Teknik Informatika.
7. Bapak Laurentinus, M. Kom selaku dosen pembimbing, yang telah memberikan masukan yang sangat berarti dan membimbing penulis sehingga skripsi ini dapat terselesaikan.
8. Teman – teman seperjuangan yang telah membagi ilmu serta memberi warna dalam persahabatan dan kebersamaan yang telah terjalin selama kuliah di STMIK Atma Luhur Pangkalpinang
9. Saudara dan sahabat-sahabatku terutama Kawan-kawan Angkatan 2014 yang telah memberikan dukungan moral untuk terus meyelesaikan skripsi ini.

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

Pangkalpinang, 27 Juli 2018

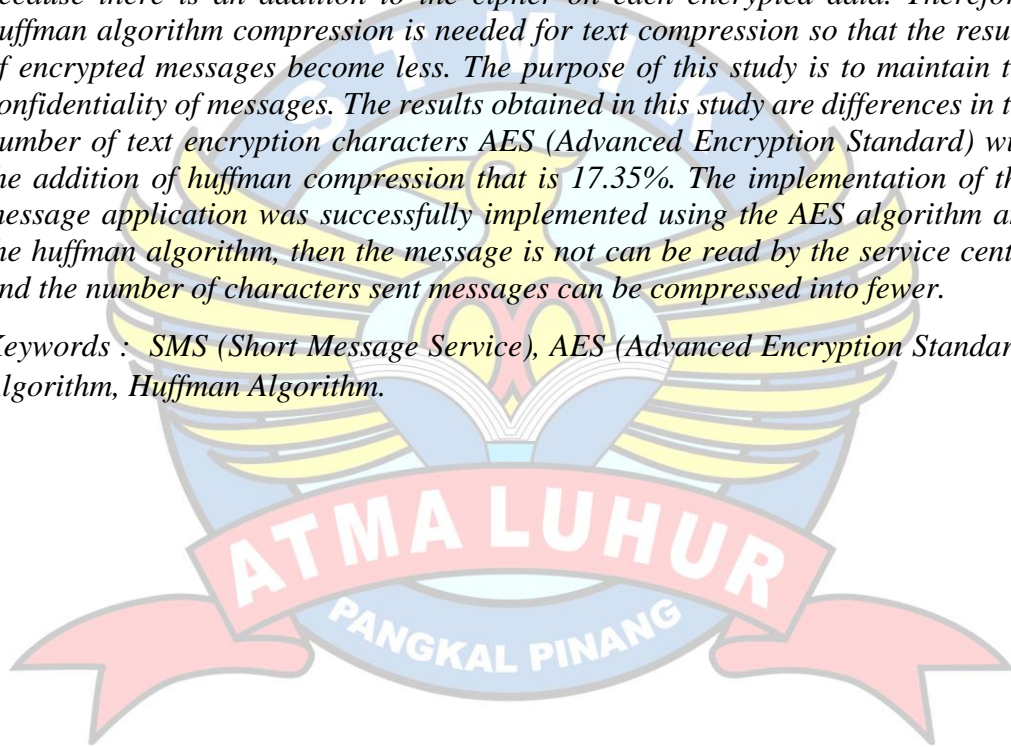


Penulis

ABSTRACT

The development of information technology that increasingly rapidly give a very big influence on telecommunications, especially mobile phones. One feature of cellular telephones is SMS (Short Message Service), but this facility in the form of SMS (Short Message Service) has a vulnerability in the form of information leakage, therefore an encryption application is proposed using OOP (Object Oriented Programming) method with Waterfall's model and (Unified Modeling Language) as tools. To the maintain of the confidentiality a message, its required AES (Advanced Encryption Standard) cryptography. Cryptography AES (Advanced Encryption Standard) had functions to encode messages into the form of ciphertext. But the results of the characters from encryption will usually has more than before because there is an addition to the cipher on each encrypted data. Therefore, huffman algorithm compression is needed for text compression so that the results of encrypted messages become less. The purpose of this study is to maintain the confidentiality of messages. The results obtained in this study are differences in the number of text encryption characters AES (Advanced Encryption Standard) with the addition of huffman compression that is 17.35%. The implementation of this message application was successfully implemented using the AES algorithm and the huffman algorithm, then the message is not can be read by the service center and the number of characters sent messages can be compressed into fewer.

Keywords : SMS (Short Message Service), AES (Advanced Encryption Standard) Algorithm, Huffman Algorithm.



ABSTRAK

Perkembangan teknologi informasi yang semakin pesat memberikan pengaruh yang sangat besar terhadap telekomunikasi khususnya telepon seluler. Salah satu fitur telepon seluler adalah SMS (*Short Message Service*), akan tetapi fasilitas berupa SMS (*Short Message Service*) ini memiliki kerentanan berupa kebocoran informasi, maka dari itu diusulkan aplikasi enkripsi menggunakan metode OOP (*Object Oriented Programming*) dengan model *Waterfall* dan *tools* UML (*Unified Modeling Language*). Untuk menjaga kerahasiaan dari sebuah pesan maka dibutuhkan kriptografi algoritma AES (*Advanced Encryption Standard*). Kriptografi AES (*Advanced Encryption Standard*) berfungsi untuk menyandikan pesan kedalam bentuk ciphertext. Namun hasil karakter dari enkripsi biasanya akan semakin banyak dibandingkan sebelum dienkripsi, hal tersebut karena ada penambahan chipper pada setiap data yang dienkripsi. Oleh karena itu kompresi algoritma *huffman* dibutuhkan untuk kompresi teks sehingga hasil pesan yang dienkripsi menjadi lebih sedikit. Tujuan dari penelitian ini adalah untuk menjaga kerahasiaan pesan. Hasil yang didapat dalam penelitian ini yaitu perbedaan jumlah karakter *text* enkripsi AES (*Advanced Encryption Standard*) dengan penambahan kompresi *huffman* yaitu 17,35%. Implementasi pada aplikasi pesan ini berhasil diterapkan dengan menggunakan algoritma AES (*Advanced Encryption Standard*) dan algoritma *huffman* sehingga pesan tidak bisa dibaca oleh pihak layanan *center* dan jumlah karakter pesan yang dikirimkan bisa dikompresi menjadi lebih sedikit.

Kata Kunci : SMS (*Short Message Service*), Algoritma AES (*Advanced Encryption Standard*), Algoritma *Huffman*.



DAFTAR ISI

Halaman

LEMBAR PERNYATAAN	i
LEMBAR PENGESAHAN SKRIPSI	ii
KATA PENGANTAR	iii
ABSTRACT	v
ABSTRAKSI	vi
DAFTAR ISI	vii
DAFTAR GAMBAR	x
DAFTAR TABEL	xii
DAFTAR SIMBOL	xiii
BAB I PENDAHULUAN	
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah	3
1.4 Tujuan dan Manfaat Penelitian.....	3
1.4.1 Tujuan.....	3
1.4.2 Manfaat.....	3
1.5 Sistematika Penulisan	3
BAB II LANDASAN TEORI	
2.1 Model Waterfall.....	6
2.2 Metode OOP (Object Oriented Programming).....	7
2.2 <i>UML (Unified Modelling Language)</i>	7
2.4 Teori Pendukung.....	11
2.4.1 Aplikasi Mobile.....	11
2.4.2 <i>Java</i>	11
2.4.3 <i>Android</i>	12
2.4.3.1 <i>Arsitektur Android</i>	12
2.4.3.2 <i>Android SDK</i>	13
2.4.3.3 <i>ADT Plugin For Eclipse</i>	14
2.4.3.4 <i>Java Development Kit (JDK)</i>	14
2.4.4 <i>Kriptografi</i>	15

2.4.4.2 Tujuan Kriptografi	15
2.4.4.3 Jenis – Jenis Kriptografi.....	15
2.4.4.4 Enkripsi Simetris.....	16
2.4.4.5 Kunci Enkripsi Dengan Fungsi Hash.....	18
2.4.4.6 Daftar Istilah System Security	19
2.4.4.7 Kode ASCII.....	20
2.4.4.8 Algoritma AES.....	22
2.4.5 Kompresi.....	24
2.4.5.1 Model Kompres Data	25
2.4.5.2 Algoritma Huffman.....	26
2.4.6 Blackbox Testing	29
2.5 Penelitian Terdahulu	29
 BAB III METODOLOGI PENELITIAN	
3.1 Model Pengembangan Perangkat Lunak	32
3.2 Metodologi Pengembangan Perangkat Lunak.....	34
3.3 Alat Bantu Pengembangan Sistem.....	34
3.4 Algoritma AES (Advanced Encryption Standard).....	35
3.5 Algoritma Huffman.....	39
 BAB IV HASIL DAN PEMBAHASAN	
4.1 Analisa Masalah.....	41
4.1.1 Analisis Sistem Berjalan.....	41
4.1.2 Analisis Kebutuhan.....	42
4.2 Perancangan.....	44
4.2.1 Identifikasi Sistem Usulan.....	45
4.2.2 Deployment Diagram.....	47
4.2.3 Rancangan Layar Aplikasi.....	47
4.2.4 Sequence Diagram.....	51
4.2.5 Penerapan Algoritma	53
4.2.5.1 Algoritma AES (Advanced Encryption Standard).....	53
4.2.5.2 Huffman	54
4.2.6 Arsitektur Sistem	57

4.3 Implementasi.....	58
4.4 Pengujian	62
4.4.1 Grafik Perbandingan Algoritma AES dan Huffman.....	62
4.4.2 Blackbox Testing	63

BAB V KESIMPULAN DAN SARAN

5.1 Kesimpulan.....	66
5.2 Saran	66

DAFTAR PUSTAKA	67
----------------------	----

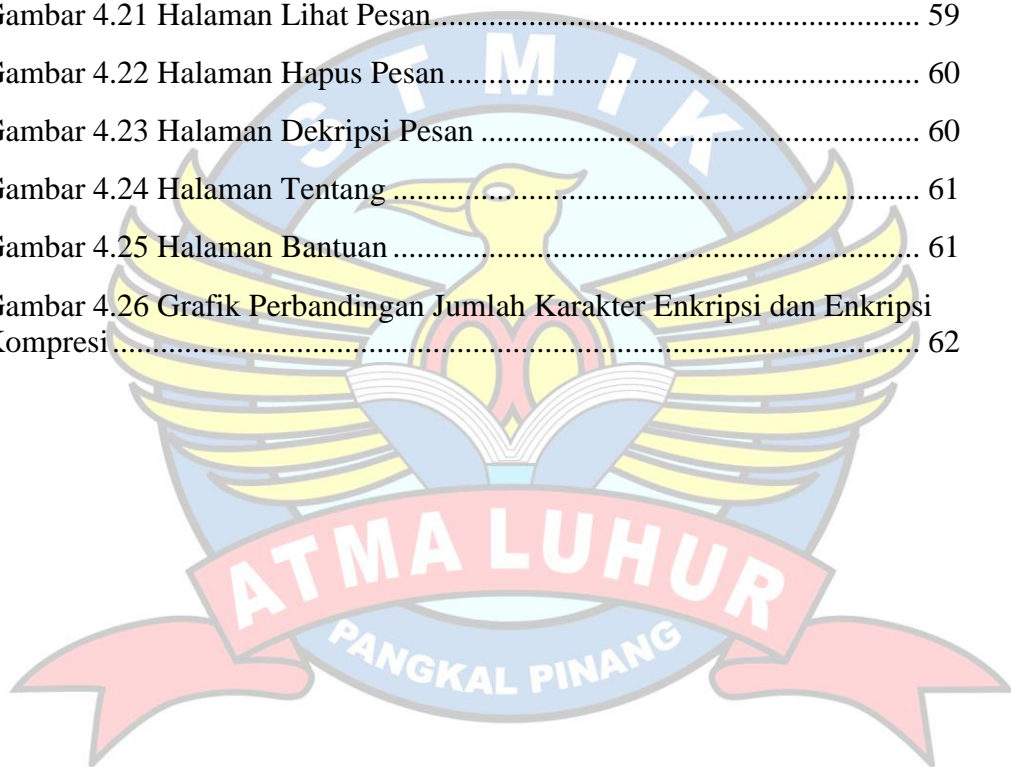
LAMPIRAN	69
----------------	----



DAFTAR GAMBAR

Gambar 2.1 Tahap Model <i>Waterfall</i>	6
Gambar 2.2 Contoh <i>Usecase Diagram</i>	9
Gambar 2.3 Contoh <i>Activity Diagram</i>	9
Gambar 2.4 Contoh <i>Sequence Diagram</i>	10
Gambar 2.5 Contoh <i>Deployment Diagram</i>	11
Gambar 2.6 Arsitektur <i>Android</i>	13
Gambar 2.7 Skema dari <i>Symmetric Chiphers Models</i>	17
Gambar 2.8 Karakter Kontrol ASCII 0 – 127	21
Gambar 2.9 Karakter Kontrol ASCII 128 – 255	21
Gambar 2.10 Proses Enkripsi dan Dekripsi AES.....	23
Gambar 2.11 Proses Round 1-10	24
Gambar 2.12 Pohon <i>Huffman</i> untuk pesan ‘ABACCDA’	29
Gambar 3.1 Model <i>Waterfall</i>	32
Gambar 3.2 <i>S-Box</i>	37
Gambar 3.3 Pohon <i>Huffman</i> “AAAABBBCCCCCD”	40
Gambar 4.1 <i>Activity diagram</i> sistem berjalan.....	42
Gambar 4.2 <i>Usecase diagram</i> sistem usulan	45
Gambar 4.3 <i>Activity diagram</i> Sistem Usulan.....	46
Gambar 4.4 <i>Deployment diagram</i>	47
Gambar 4.5 Rancangan Layar Utama	47
Gambar 4.6 Rancangan Layar Buat Pesan	48
Gambar 4.7 Rancangan Layar <i>List</i> Pesan	48
Gambar 4.8 Rancangan Layar Lihat Pesan	49
Gambar 4.9 Rancangan Layar Dekripsi	49
Gambar 4.10 Rancangan Layar Tentang.....	50
Gambar 4.11 Rancangan Layar Bantuan	50
Gambar 4.12 <i>Sequence Diagram Create Message</i> (buat pesan).....	51

Gambar 4.13 <i>Sequence Diagram</i> Inbox (pesan masuk).....	51
Gambar 4.14 <i>Sequence Diagram</i> Outbox (pesan keluar).....	52
Gambar 4.15 sequence diagram about (tentang).....	52
Gambar 4.16 sequence diagram help (bantuan).....	53
Gambar 4.17 Arsitektur Sistem.....	57
Gambar 4.18 Menu Utama Aplikasi	58
Gambar 4.19 Halaman Create Message	58
Gambar 4.20 Halaman Inbox/ Outbox	59
Gambar 4.21 Halaman Lihat Pesan.....	59
Gambar 4.22 Halaman Hapus Pesan.....	60
Gambar 4.23 Halaman Dekripsi Pesan	60
Gambar 4.24 Halaman Tentang	61
Gambar 4.25 Halaman Bantuan	61
Gambar 4.26 Grafik Perbandingan Jumlah Karakter Enkripsi dan Enkripsi Kompresi.....	62



DAFTAR TABEL

Tabel 2.1 Istilah System Security.....	19
Tabel 2.2 Tabel kode ASCII	27
Tabel 2.3 Tabel kekerapan dan kode <i>Huffman</i> untuk string ‘ABACCCA’	28
Tabel 4.1 <i>Presentase</i>	62
Tabel 4.2 Hasil Enkripsi dan Kompresi	63
Tabel 4.3 <i>Blackbox Testing</i>	63



DAFTAR SIMBOL

1. Simbol Activity Diagram



Start Point (Initial Node)

Merupakan simbol untuk memulai *activity diagram*.



End Point (Activity Final Node)

Merupakan simbol untuk mengakhiri *activity diagram*



Transition

Menggambarkan aliran perpindahan kontrol antara *activity*.



Activity

Activity (Aktivitas)

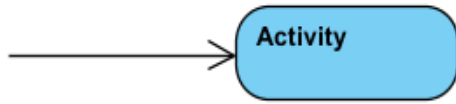
Menggambarkan proses bisnis dan dikenal sebagai *activity state*. *Activity* juga merupakan proses komputasi atau perubahan kondisi yang bisa berupa kata kerja atau ekspresi.



Partition

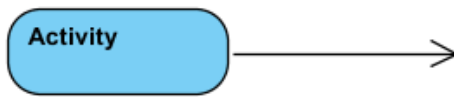
Swimline

Menggambarkan pemisahan atau pengelompokan aktivitas berdasarkan *actor*.



Black Hole Activities

Adanya masukan dan tidak ada keluaran, biasanya digunakan jika dikehendaki ada 1 atau lebih transisi.



Miracle Activities

Tidak ada masukan dan ada keluaran, biasanya dipakai pada waktu *start point* dan dikehendaki ada 1 atau lebih transisi.



Fork (Percabangan)

Mempunyai 1 transisi masuk dan 2 atau lebih transisi keluar.

Join (Penggabungan)

Mempunyai 2 atau lebih transisi masuk dan hanya 1 transisi keluar.

Decision

Merupakan cara untuk menggabungkan ketika ada lebih dari 1 transisi yang masuk atau pilihan untuk mengambil keputusan.

2. Simbol Use Case Diagram



Use case

Gambaran fungsionalitas dari suatu sistem, sehingga pengguna sistem paham dan mengerti mengenai kegunaan sistem yang akan dibangun.



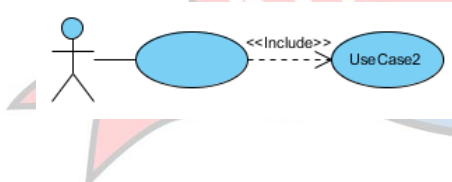
Actor

Sebuah entitas manusia atau mesin yang berinteraksi dengan sistem untuk melakukan pekerjaan-pekerjaan tertentu.



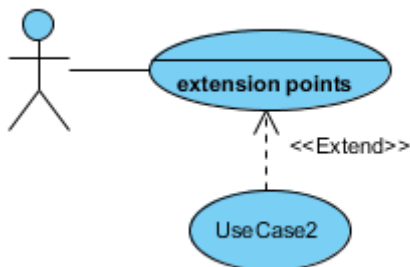
Association

Merupakan abstraksi berupa garis tanpa panah yang menghubungkan antara aktor dan use case.



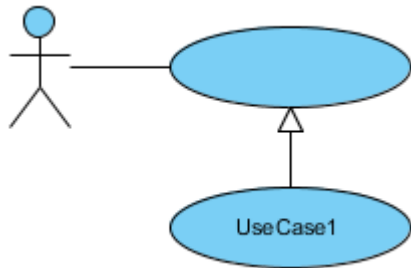
Include

Menunjukkan bahwa suatu use case seluruhnya merupakan fungsionalitas dari use case lainnya.



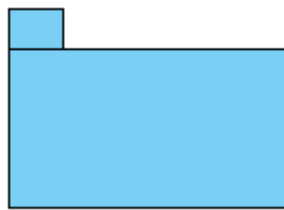
Extend

Menunjukkan suatu use case merupakan tambahan fungsional dari use case lainnya jika suatu kondisi terpenuhi.



Generalization

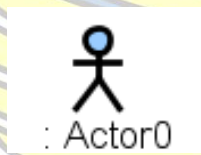
Disebut juga *inheritance* (pewarisan), sebuah elemen dapat merupakan spesialisasi dari elemen lainnya.



Packages

Digambarkan sebagai sebuah direktori yang berisikan model-model elemen. *Packages* digunakan untuk mengorganisasikan sebuah diagram yang besar menjadi beberapa diagram kecil.

3. Simbol Sequence Diagram



Actor

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



Boundary

Menggambarkan interaksi antara satu atau lebih *actor* dengan sistem, memodelkan bagian dari sistem yang bergantung pada pihak lain disekitarnya dan merupakan pembatas sistem dengan dunia luar.



Control

Menggambarkan “perilaku untuk mengatur atau kegiatan mengontrol”, mengkoordinasikan perilaku sistem dan dinamika dari suatu sistem, menangani tugas utama dan mengontrol alur kerja suatu sistem.

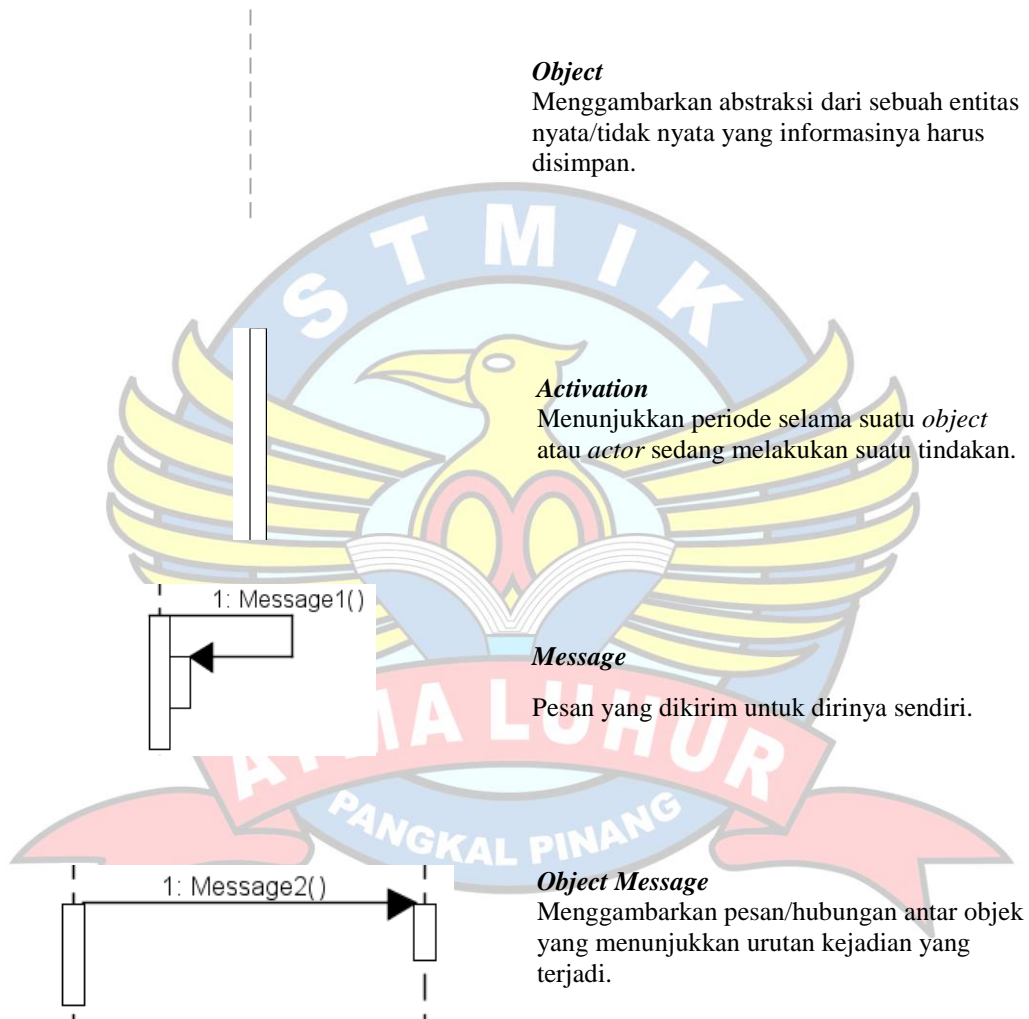


Entity

Menggambarkan informasi yang harus disimpan oleh sistem (struktur data dari sebuah sistem).

Object

Menggambarkan abstraksi dari sebuah entitas nyata/tidak nyata yang informasinya harus disimpan.



Activation

Menunjukkan periode selama suatu *object* atau *actor* sedang melakukan suatu tindakan.

Message

Pesan yang dikirim untuk dirinya sendiri.

Object Message

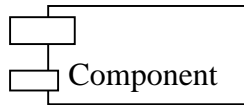
Menggambarkan pesan/hubungan antar objek yang menunjukkan urutan kejadian yang terjadi.



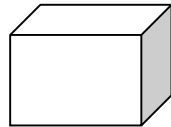
Looping logic

Menggambarkan dengan sebuah *frame* dengan label *loop* dan sebuah kalimat yang mengindikasikan pengulangan dan *interaction operator loop*.

4. Simbol *Deployment Diagram*



Pada deployment diagram, komponen-komponen yang ada diletakkan didalam node untuk memastikan keberadaan posisi mereka.



Node menggambarkan bagian-bagian hardware dalam sebuah sistem. Notasi untuk node digambarkan sebagai sebuah kubus tiga dimensi.



Sebuah association digambarkan sebuah garis yang menghubungkan dua node yang mengindikasikan jalur komunikasi antara lement-element hardware



