



**ANALISA DAN IMPLEMENTASI TINY ENCRYPTION  
ALGORITMA (TEA) UNTUK KEAMANAN SMS PADA  
PERANGKAT MOBILE PHONE ANDROID**

Disusun dan Diajukan untuk Memenuhi Persyaratan Ujian Akhir Men peroleh  
Gelar Sarjana Komputer pada Fakultas Sains dan Teknologi  
Universitas Pembangunan Panca Budi  
Medan

---

**SKRIPSI**

---

**OLEH**

**NAMA : ASNI MAISYARAH HARAHAP**  
**NPM : 1514370607**  
**PROGRAM STUDI : SISTEM KOMPUTER**

**FAKULTAS SAINS DAN TEKNOLOGI  
UNIVERSITAS PEMBANGUNAN PANCA BUDI  
MEDAN  
2019**

**LEMBAR PENGESAHAN**

**ANALISA DAN IMPLEMENTASI TINY ENCRYPTION  
ALGORITMA (TEA) UNTUK KEAMANAN SMS PADA  
PERANGKAT MOBILE PHONE ANDROID**

**Disusun Oleh:**

**NAMA : ASNI MAISYARAH HARAHAP  
NPM : 1514370607  
PROGRAM STUDI : SISTEM KOMPUTER**

**Skripsi Telah Disetujui oleh Dosen Pembimbing Skripsi  
Pada tanggal 7 November 2019**

**Dosen Pembimbing I**



**Sukerman, S.Kom., M.Kom**

**Dosen Pembimbing II**



**Akhyar Lubis, S.Kom, M.Kom**

**Mengetahui,**

**Dekan Fakultas Sains Dan Teknologi**



**Sri Shindi Indira, ST., M.Sc**

**Ketua Program Studi Sistem Komputer**



**Eko Hariyanto, S.Kom., M.Kom**

## SURAT PERNYATAAN

Saya yang bertanda tangan di bawah ini :

Nama : Asni Maisyarah Harahap  
NPM : 1514370607  
Prodi : Sistem Komputer  
Konsentrasi : Keamanan Jaringan Komputer  
Judul Skripsi : Analisa Perancangan Sistem Informasi Stok Alat Tulis Kantor (Atk) Pada Unit Pelaksanaan Teknis Pusat Perkuliahan Laboratorium Ilmu Dasar Dan Umum Universitas Sumatera Utara

Dengan ini menyatakan bahwa :

1. Tugas Akhir/Skripsi saya bukan hasil Plagiat
2. Saya tidak akan menuntut perbaikan nilai indeks Prestasi Kumulatif (IPK) setelah ujian Sidang Meja Hijau
3. Skripsi saya dapat dipublikasikan oleh pihak lembaga, dan saya tidak akan menuntut akibat publikasi tersebut

Demikian pernyataan ini saya perbuat dengan sebenar-benarnya, terima kasih

Medan,

Yang membuat pernyataan



Asni Maisyarah Harahap

1514370607

## SURAT PERNYATAAN

Yang Bertanda Tangan Dibawah Ini :

**nama** : ASNI MAISYARAH HARAHAHAP  
**NPM** : 1514370607  
**tempat/Tgl. Lahir** : Medan / 21 September 1997  
**alamat** : Dusun VI Jl. Banten Baru  
**HP** : 082304550974  
**nama Orang Tua** : ASSALUDDIN HARAHAHAP/DARA HASNITA  
**jurusan** : SAINS & TEKNOLOGI  
**program Studi** : Sistem Komputer  
**judul** : Analisa dan Implementasi Tiny Encryption Algoritma (TEA) untuk Keamanan SMS pada Perangkat Mobile Phone Android

Saya dengan surat ini menyatakan dengan sebenar - benarnya bahwa data yang tertera diatas adalah sudah benar sesuai dengan ijazah pada pendidikan terakhir yang saya jalani. Maka dengan ini saya tidak akan melakukan tuntutan kepada UNPAB. Apabila ada kesalahan data pada ijazah saya.

Selanjutnya surat pernyataan ini saya buat dengan sebenar - benarnya, tanpa ada paksaan dari pihak manapun dan saya dalam keadaan sadar. Jika terjadi kesalahan, Maka saya bersedia bertanggung jawab atas kelalaian saya.



21 November 2019  
membuat Pernyataan  
ASNI MAISYARAH HARAHAHAP  
1514370607



Telah Diperiksa oleh LPMU  
dengan Plagiarisme...47.7%

Medan, 25 OKTOBER 2019

FM-BPAA-2012-041

Hal : Permohonan Meja Hijau



Medan, 25 Oktober 2019  
Kepada Yth : Bapak/Ibu Dekan  
Fakultas SAINS & TEKNOLOGI  
UNPAB Medan  
Di  
Tempat

Telah di terima  
berkas persyaratan  
dapat di proses  
Medan, 01 / 11 / 2019

Ka. BPAA  
TEGUH WARYONO, SE., MM.

Dengan hormat, saya yang bertanda tangan di bawah ini :

Nama : ASNI MAISYARAH HARAHAP  
Tempat/Tgl. Lahir : Medan / 21 September 1997  
Nama Orang Tua : ASSALUDDIN HARAHAP  
N. P. M : 1514370607  
Fakultas : SAINS & TEKNOLOGI  
Program Studi : Sistem Komputer  
No. HP : 082304550974  
Alamat : Dusun VI Jl. Banten Baru

Datang bermohon kepada Bapak/Ibu untuk dapat diterima mengikuti Ujian Meja Hijau dengan judul Analisa dan Implementasi Tiny Encryption Algoritma (TEA) Untuk Keamanan SMS Pada Perangkat Mobile Phone Android, Selanjutnya saya menyatakan :

1. Melampirkan KKM yang telah disahkan oleh Ka. Prodi dan Dekan
2. Tidak akan menuntut ujian perbaikan nilai mata kuliah untuk perbaikan indek prestasi (IP), dan mohon diterbitkan ijazahnya setelah lulus ujian meja hijau.
3. Telah tercap keterangan bebas pustaka
4. Terlampir surat keterangan bebas laboratorium
5. Terlampir pas photo untuk ijazah ukuran 4x6 = 5 lembar dan 3x4 = 5 lembar Hitam Putih
6. Terlampir foto copy STTB SLTA dilegalisir 1 (satu) lembar dan bagi mahasiswa yang lanjutan D3 ke S1 lampirkan ijazah dan transkripnya sebanyak 1 lembar.
7. Terlampir pelunasan kwintasi pembayaran uang kuliah berjalan dan wisuda sebanyak 1 lembar
8. Skripsi sudah dijilid lux 2 exemplar (1 untuk perpustakaan, 1 untuk mahasiswa) dan jilid kertas jeruk 5 exemplar untuk penguji (bentuk dan warna penjiilidan diserahkan berdasarkan ketentuan fakultas yang berlaku) dan lembar persetujuan sudah di tandatangani dosen pembimbing, prodi dan dekan
9. Soft Copy Skripsi disimpan di CD sebanyak 2 disc (Sesuai dengan Judul Skripsinya)
10. Terlampir surat keterangan BKKOL (pada saat pengambilan ijazah)
11. Setelah menyelesaikan persyaratan point-point diatas berkas di masukan kedalam MAP
12. Bersedia melunaskan biaya-biaya yang dibebankan untuk memproses pelaksanaan ujian dimaksud, dengan rincian sbb :

1. [102] Ujian Meja Hijau	: Rp.	100,000
2. [170] Administrasi Wisuda	: Rp.	1,500,000
3. [202] Bebas Pustaka	: Rp.	100,000
4. [221] Bebas LAB	: Rp.	5,000
<b>Total Biaya</b>	<b>: Rp.</b>	<b>1,605,000</b>
		1.705.000

My 4/11/19  
Dtz

Ukuran Toga :

M

Mengetahui dan disetujui oleh :  
Indi Indira, S.T., M.Sc.  
Dekan Fakultas SAINS & TEKNOLOGI

Hormat saya

ASNI MAISYARAH HARAHAP  
1514370607

1. Surat permohonan ini sah dan berlaku bila ;
  - a. Telah dicap Bukti Pelunasan dari UPT Perpustakaan UNPAB Medan.
  - b. Melampirkan Bukti Pembayaran Uang Kuliah aktif semester berjalan
2. Dibuat Rangkap 3 (tiga), untuk - Fakultas - untuk BPAA (asli) - Mhs.ybs.



# Plagiarism Detector v. 1092 - Originality Report:

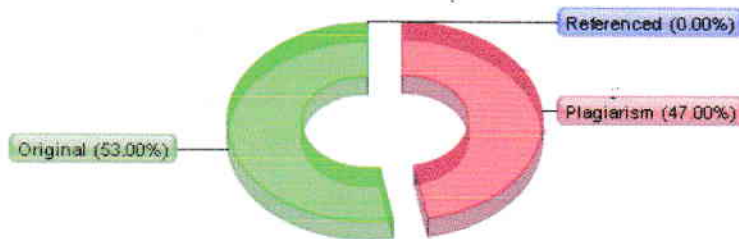
Analyzed document: 19/09/2019 09:22:31

## "ASNI MAISYARAH ARAHAP\_1514370607\_SISTEM KOMPUTER.doc"

Licensed to: Universitas Pembangunan Panca Budi\_License4



Relation chart:



Distribution graph:

Comparison Preset: Rewrite. Detected language: Indonesian

### Top sources of plagiarism:

- 24 wrds: 1536 <https://docplayer.info/55886909-Bab-iii-analisis-dan-desain-sistem.html>
- 17 wrds: 1033 <https://docplayer.info/74561574-Bab-iii-analisis-dan-perancangan.html>
- 12 wrds: 878 <http://repository.usu.ac.id/bitstream/handle/123456789/57394/Chapter%20II.pdf?sequence=4&a...>

other Sources:]

### Processed resources details:

67 - Ok / 154 - Failed

other Sources:]

### Important notes:

Wikipedia:



[not detected]

Google Books:



[not detected]

Ghostwriting services:



[not detected]

Anti-cheating:



[not detected]



# UNIVERSITAS PEMBANGUNAN PANCA BUDI FAKULTAS SAINS & TEKNOLOGI

Jl. Jend. Gatot Subroto Km 4,5 Medan Fax. 061-8458077 PO.BOX : 1099 MEDAN

PROGRAM STUDI TEKNIK ELEKTRO	(TERAKREDITASI)
PROGRAM STUDI ARSITEKTUR	(TERAKREDITASI)
PROGRAM STUDI SISTEM KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI TEKNIK KOMPUTER	(TERAKREDITASI)
PROGRAM STUDI AGROTEKNOLOGI	(TERAKREDITASI)
PROGRAM STUDI PETERNAKAN	(TERAKREDITASI)

## PERMOHONAN JUDUL TESIS / SKRIPSI / TUGAS AKHIR\*

Yang bertanda tangan di bawah ini :

Nama Lengkap : ASNI MAISYARAH HARAHAP  
 Tempat/Tgl. Lahir : medan / 21 September 1997  
 Nomor Pokok Mahasiswa : 1514370607  
 Program Studi : Sistem Komputer  
 Konsentrasi : Keamanan Jaringan Komputer  
 Jumlah Kredit yang telah dicapai : 138 SKS, IPK 3.44  
 Nomor Hp : 082304550974  
 Yang ini mengajukan judul sesuai bidang ilmu sebagai berikut :

### Judul

Analisa dan Implementasi Tiny Encryption Algorithm (TEA) Untuk Keamanan SMS Pada Perangkat Mobile Phone Android

Diisi Oleh Dosen Jika Ada Perubahan Judul



Yang Tidak Perlu

(Rektor)  
 ( Ir. Bhakti Alamsyah, M.T., Ph.D. )

11 Desember  
 Medan, ~~10 Desember~~ 2019

Pemohon,  
 ( Asni Maisyarah Harahap )

Tanggal : .....  
 Disahkan oleh  
 Dekan  
 ( Sri Shindi Indra, S.Kom., M.Sc. )

Tanggal : .....  
 Disetujui oleh :  
 Dosen Pembimbing I :  
 ( Suherman, S.Kom., M.Kom )

Tanggal : .....  
 Disetujui oleh:  
 Ka. Prodi Sistem Komputer  
 ( Eko Hariyanto, S.Kom., M.Kom )

Tanggal : .....  
 Disetujui oleh:  
 Dosen Pembimbing II:  
 ( Akhyar Lubis, S.Kom., M.Kom )

No. Dokumen: FM-UPBM-18-02

Revisi: 0

Tgl. Eff: 22 Oktober 2018





**UNIVERSITAS PEMBANGUNAN PANCA BUDI**  
**FAKULTAS SAINS & TEKNOLOGI**

Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571  
 website : www.pancabudi.ac.id email: unpub@pancabudi.ac.id  
 Medan - Indonesia

Universitas : Universitas Pembangunan Panca Budi  
 Fakultas : SAINS & TEKNOLOGI  
 Dosen Pembimbing I : Suherman, S.kom., M.kom  
 Dosen Pembimbing II : Akhyar Lubis, S.kom., M.kom  
 Nama Mahasiswa : ASNI MAISYARAH HARAHAP  
 Jurusan/Program Studi : Sistem Komputer  
 Nomor Pokok Mahasiswa : 1514370607  
 Tingkat Pendidikan : S1  
 Tugas Akhir/Skripsi : Analisa dan Implementasi Tiny Encryption Algorithm (TEA) Untuk Keamanan sms Pada Perangkat Mobile Phone Android

ANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
2/10/19	perbaikan di latar belakang	<i>[Signature]</i>	
12/10/19	Ac Bab 7 Lanjut Bab II & III	<i>[Signature]</i>	
12/10/19	Acc seminar proposal	<i>[Signature]</i>	
13/10/19	Ac Bab II, III Lanjut Bab II,	<i>[Signature]</i>	
13/10/19	perbaikan di format penulisan, lihat panduan penulisan penomoran judul, gambar & tabel Lanjut Acc Bab II,	<i>[Signature]</i>	
17/10/19	Acc Bab II Lanjut Bab II Lengkapi keseluruhan	<i>[Signature]</i>	

Medan, 04 Februari 2019  
 Diketahui/Disetujui oleh :  
 Dekan,



Sri Shindi Indira, S.T., M.Sc.





UNIVERSITAS PEMBANGUNAN PANCA BUDI  
FAKULTAS SAINS & TEKNOLOGI

Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571  
website : www.pancabudi.ac.id email: unpab@pancabudi.ac.id  
Medan - Indonesia

Universitas : Universitas Pembangunan Panca Budi  
 Fakultas : SAINS & TEKNOLOGI  
 Dosen Pembimbing I : Suherman, S.Kom., M.Kom  
 Dosen Pembimbing II : Akhyar Lubis, S.Kom., M.Kom  
 Nama Mahasiswa : ASNI MAISYARAH HARAHAP  
 Jurusan/Program Studi : Sistem Komputer  
 Nomor Pokok Mahasiswa : 1514370607  
 Bidang Pendidikan : S1  
 Tugas Akhir/Skripsi : Analisa dan Implementasi Tiny Encryption Algorithm  
 (TEA) Untuk Keamanan SMS Pada Perangkat Mobile  
 Phone Android

WANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
1 Juli 2019	Acc Seminar Hasil		
10/2019	Acc Sidang		
11/2019	perbaiki & lembar Pengesahan		
15/2019	Acc jilid		

Medan, 11 Februari 2019  
Diketahui/Disetujui oleh :  
Dekan,





UNIVERSITAS PEMBANGUNAN PANCA BUDI  
**FAKULTAS SAINS & TEKNOLOGI**

Jl. Jend. Gatot Subroto Km. 4,5 Telp (061) 8455571  
 website : www.pancabudi.ac.id email: unpub@pancabudi.ac.id  
 Medan - Indonesia

Universitas : Universitas Pembangunan Panca Budi  
 Fakultas : SAINS & TEKNOLOGI  
 Pembimbing I : Suherman, S.Kom, M.Kom  
 Pembimbing II : Akhyar Lubis, S.Kom, M.Kom  
 Nama Mahasiswa : ASNI MAISYARAH HARAHAP  
 Jurusan/Program Studi : Sistem Komputer  
 Nomor Pokok Mahasiswa : 1514370607  
 Tingkat Pendidikan : S1  
 Tugas Akhir/Skripsi : Analisa dan Implementasi Tiny Encryption Algorithm (TEA) Untuk Keamanan SMS Pada Perangkat Mobile Phone Android

ANGGAL	PEMBAHASAN MATERI	PARAF	KETERANGAN
2019	Pembelajaran Catah Lalai dan Metode Penelitian - Ace Bab I	[Signature]	
2019	Ace Sempro	[Signature]	
2019	Pembelajaran Acron Sesuai dengan Rencanan	[Signature]	
2019	pelu Acron yang Relevan.	[Signature]	
2019	Analisa Keras Sesuai dengan data.	[Signature]	
2019	Kerangka Sesuai dengan kebutuhan	[Signature]	
2019	Implementasi Keras di dalam Acron dan Koneksi	[Signature]	
2019	Unggah dan Postuler	[Signature]	
2019	Ace Seminar	[Signature]	
2019	Ace Sidang	[Signature]	
	Ace Guide	[Signature]	

Medan, 15 Januari 2019  
 Diketahui/Disetujui oleh :  
 Dekan,



Sri Shindi Indira, S.T., M.Sc.



YAYASAN PROF. DR. H. KADIRUN YAHYA  
UNIVERSITAS PEMBANGUNAN PANCA BUDI  
**LABORATORIUM KOMPUTER**  
Jl. Jend. Gatot Subroto Km 4,5 Sei Sikambing Telp. 061-8455571  
Medan - 20122

**KARTU BEBAS PRAKTIKUM**

Yang bertanda tangan dibawah ini Ka. Laboratorium Komputer dengan ini menerangkan bahwa :

Nama : ASNI MAISYARAH HARAHAP  
N.P.M. : 1514370607  
Tingkat/Semester : Akhir  
Fakultas : SAINS & TEKNOLOGI  
Jurusan/Prodi : Sistem Komputer

Benar dan telah menyelesaikan urusan administrasi di Laboratorium Komputer Universitas Pembangunan Panca Budi Medan.

Medan, 25 Oktober 2019  
a.n/ Ka. Laboratorium



## **ABSTRAK**

*Short Message Service (SMS) adalah suatu fasilitas untuk mengirim dan menerima suatu pesan singkat berupa teks melalui perangkat nirkabel, yaitu perangkat komunikasi telpon selular. Namun pesan yang dikirimkan melalui SMS tidak dapat dijamin integritas dan keamanannya. Hal tersebut dikarenakan pesan yang dikirim akan disimpan di SMSC (Short Message Service Center), yaitu tempat dimana sms disimpan sebelum dikirim ke tujuan. Pesan yang sifatnya plaintext ini dapat disadap oleh siapa saja yang berhasil memiliki akses ke dalam SMSC. Akibatnya informasi penting dapat dilihat oleh orang yang tidak berhak. Hal tersebut sangat dirugikan jika informasi yang di lihat atau disadap adalah informasi yang sifatnya pribadi atau rahasia. Oleh sebab itu maka diperlukan penerapan algoritma enkripsi untuk mencegah penyadapan terhadap pesan SMS. Pada penelitian ini metode yang diterapkan adalah Tiny Encryption Algoritma dan di implementasikan menggunakan bahasa pemrograman Java. JDK Java 1.7 sebagai bahasa program cipherteks menjadi plainteks menggunakan key yang diinputkan oleh penerima kemudian menampilkan pesan asli kepada penerima*

*Kata kunci: Enkripsi, SMS, Tiny Encryption Algorithm (TEA)*



## DAFTAR ISI

	<b>Halaman</b>
<b>KATA PENGANTAR .....</b>	<b>i</b>
<b>DAFTAR ISI.....</b>	<b>iii</b>
<b>DAFTAR GAMBAR .....</b>	<b>v</b>
<b>DAFTAR TABEL.....</b>	<b>vii</b>
<b>DAFTAR LAMPIRAN.....</b>	<b>viii</b>
<b>BAB I. PENDAHULUAN .....</b>	<b>1</b>
1.1 Latar Belakang Masalah.....	1
1.2 Perumusan Masalah .....	3
1.3 Batasan Masalah.....	3
1.4 Tujuan Penelitian .....	3
1.5 Manfaat Penelitian .....	4
<b>BAB II. LANDASAN TEORI.....</b>	<b>5</b>
2.1 Masalah Keamanan .....	5
2.1.1 Aspek-aspek Keamanan .....	5
2.1.2 Serangan Keamanan.....	6
2.2 Kriptografi .....	6
2.2.1 Jenis Algoritma Kriptografi .....	8
2.3 Tujuan Kriptografi.....	10
2.4 Algoritma TEA (Tiny Encryption Algorithm) .....	12
2.5 Short Message Service (SMS).....	13
2.6 Eclipse .....	15
2.7 Android.....	16
2.7.1 Android SDK (Software Development Kit).....	16
2.7.2 AVD (Android Virtual Device).....	17
2.7.3 Bahasa Pemrograman Java .....	18
2.8 Konsep UML (Unified Modelling Language) .....	18
2.8.1 Diagram-diagram UML.....	19
<b>BAB III. ANALISIS DAN DESAIN SISTEM .....</b>	<b>23</b>
3.1 Analisa Kebutuhan Sistem .....	23
3.2 Sistem Yang Sedang Berjalan .....	23
3.3 Algoritma TEA (Tiny Encryption Algorithm).....	25
3.4 Analisis Proses Enkripsi Algoritma TEA.....	28
3.5 Analisis Proses Deskripsi Algoritma TEA.....	34

3.6	Teknik Pemecahan Masalah.....	35
3.7	Spesifikasi Perangkat .....	35
3.8	Desain Sistem Usulan.....	36
3.8.1	Use Case Diagram.....	36
3.8.2	Sequence Diagram.....	37
3.8.3	Activity Diagram.....	39
3.8.4	Class Diagram .....	41
3.9	Desain Interface.....	41
3.9.1	Rancangan Splash .....	42
3.9.2	Rancangan Menu.....	42
3.9.3	Rancangan Pesan Baru .....	44
3.9.4	Rancangan Read SMS .....	44
3.9.5	Rancangan From Profil .....	46
3.9.6	Rancangan From Bantuan .....	47
<b>BAB IV. HASIL DAN UJI COBA.....</b>		<b>48</b>
4.1	Hasil .....	48
4.1.1	Tampilan Menu Splash.....	48
4.1.2	Tampilan Menu Utama.....	49
4.1.3	Tampilan Menu Pesan Baru .....	49
4.1.4	Tampilan Menu Inbox .....	50
4.1.5	Pembahasan.....	52
4.2	Uji Coba Sistem .....	53
4.2.1	Skenario Pengujian.....	53
4.3	Kelebihan dan Kekurangan Sistem yang Dirancang.....	55
4.3.1	Kelebihan Sistem.....	55
4.3.2	Kekurangan Sistem .....	56
<b>BAB V. KESIMPULAN DAN SARAN .....</b>		<b>57</b>
5.1	Kesimpulan.....	57
5.2	Saran.....	57

## DAFTAR PUSTAKA

## LAMPIRAN-LAMPIRAN

# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang Masalah**

Arif Rahman Sujatmika (2015) Dari kemajuan teknologi yang pesat saat ini, mobile phone juga bukan hanya sebagai media untuk berkomunikasi saja, akan tetapi sudah di design dengan fitur aplikasi yang memiliki kelebihan masing – masing. Teknologi informasi dan komunikasi di dunia berkembang setiap waktu, salah satunya adalah teknologi mobile phone. Dengan diluncurkan sistem operasi android pada saat ini, memudahkan kita untuk mengakses informasi melalui gadget mobile kita. Tetapi belum semuanya memanfaatkan kemajuan teknologi ini, bahkan ada yang belum mengenalnya sama sekali karena keterbatasan kemampuan dan pengetahuan tentang perkembangan teknologi.

Arif Rahman Sujatmika (2015) SMS adalah sebuah layanan yang dilaksanakan dengan ponsel untuk mengirim maupun menerima pesan-pesan pendek. SMS sekarang ini menjadi salah satu layanan komunikasi yang sangat populer dikalangan masyarakat. Dengan SMS dapat memudahkan dalam komunikasi dengan waktu yang singkat dan biaya yang murah. SMS juga menjadi salah satu fitur utama dalam telepon seluler. Namun dengan fasilitas yang ada, timbul pertanyaan mengenai keamanan data SMS tersebut. Keamanan data SMS sangat di perlukan baik itu tidak di kehendaki dan hanya orang tertentu saja yang bisa membaca SMS tersebut.

Pradana Marlando (2015) Algoritma kriptografi dibagi menjadi dua kelompok besar yaitu algoritma simetris dan algoritma asimetris. Algoritma simetris menggunakan kunci rahasia yang umum dimiliki oleh pengirim maupun penerima sering disebut secret-key cipher system. Algoritma asimetris memiliki dua kunci yang berbeda yaitu kunci publik dan private key yang berbeda untuk proses enkripsi dan dekripsinya

Pradana Marlando (2015) Salah satu teknik kriptografi adalah menggunakan algoritma *Tiny Encryption Algorithm (TEA)*. *Tiny Encryption Algorithm (TEA)* merupakan suatu algoritma sandi yang diciptakan oleh David Wheeler dan Roger Needham dari *Computer Laboratory, Cambridge University, England* pada bulan November 1994. Algoritma ini merupakan algoritma mengenkripsi suatu blok plaintext dengan jumlah bit tertentu dan menghasilkan blok ciphertext yang dirancang untuk penggunaan memory yang seminimal mungkin dengan kecepatan proses yang maksimal. Hal yang paling menonjol dari *TEA* adalah kesederhanaan implementasi, ketiadaan *S-Box* maupun *P-Box* dan kecepatan yang tinggi. Penulis mencoba untuk membangun sebuah aplikasi yang dapat mengamankan pesan teks *SMS* dengan algoritma kriptografi *Tiny Encryption Algorithm (TEA)*. Seperti dengan latar belakang yang dijelaskan sebelumnya penulis berinisiatif mengangkat judul skripsi ini dengan judul **“Analisa dan Implementasi Tiny Encryption Algoritma (TEA) Untuk Keamanan SMS Pada Perangkat Mobile Phone Android”**



## 1.2 Perumusan Masalah

Penelitian dan perancangan untuk pembuatan skripsi ini diperlukan perumusan masalah, yaitu sebagai berikut :

1. Bagaimana cara membuat dan mengimplementasikan keamanan pesan untuk pengiriman dan terima *SMS*?
2. Bagaimana membangun aplikasi untuk pengiriman dan terima pesan teks *SMS* dengan pemrograman *Java* pada perangkat *mobile phone Android* ?

## 1.3 Batasan Masalah

Batasan masalah dibuat agar pembahasan terfokus dalam penulisan skripsi ini, yaitu sebagai berikut :

1. Perancangan sebuah aplikasi yang dapat melakukan pengamanan pesan teks *SMS* pada perangkat *mobile phone Android* dengan *Algoritma Tiny Encryption Algorithm (TEA)*.
2. Bahasa pemrograman yang digunakan adalah *Java*, dengan *editor* pemrograman *Eclipse*, *SDK Java* dan *SDK Android*.

## 1.4 Tujuan Penelitian

Adapun tujuan dari penulisan skripsi ini adalah sebagai berikut:

1. Untuk menerapkan konsep kriptografi dalam proses pengamanan pesan teks *SMS* pada perangkat seluler.
2. Untuk membuat sebuah aplikasi pengamanan pesan teks *SMS* dengan implementasi algoritma *Tiny Encryption Algorithm (TEA)*.

3. Untuk menyediakan perangkat lunak pendukung penyandian pesan teks *SMS* yang dapat mudah digunakan untuk pengamanan pesan teks *SMS*.

### **1.5 Manfaat Penelitian**

Adapun manfaat dari penulisan skripsi ini adalah sebagai berikut:

1. Memberikan kemudahan kepada pengguna untuk pengamanan teks *SMS* dalam proses pengiriman dan terima pesan pada perangkat seluler.
2. Menyajikan aplikasi yang dikhususkan untuk mengamankan pesan teks *SMS*. Dengan kemudahan enkripsi dan dekripsi menggunakan teknik kriptografi.
3. Memahami bagaimana proses algoritma *Tiny Encryption Algorithm* dalam melakukan enkripsi dan deskripsi terhadap pesan teks *SMS*.

## **BAB II**

### **TINJAUAN PUSTAKA**

#### **2.1 Masalah Keamanan**

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Salah satu hal penting dalam komunikasi menggunakan komputer dan dalam jaringan komputer untuk menjamin keamanan pesan, data atau pun informasi adalah enkripsi. Enkripsi dapat diartikan sebagai sebuah proses yang dilakukan untuk mengubah pesan asli menjadi pesan yang tersandikan. Sebuah cipher adalah sebuah algoritma untuk menampilkan enkripsi dan kebalikannya dekripsi. Informasi yang asli disebut sebagai plaintext, dan bentuk yang sudah dienkripsi disebut sebagai ciphertext. Pesan ciphertext berisi seluruh informasi dari pesan plaintext, tetapi tidak dalam format yang dapat dibaca oleh manusia ataupun komputer tanpa menggunakan mekanisme yang tepat untuk melakukan dekripsi. (*Andi Riski Alvianto; 2015 : 1*).

##### **2.1.1 Aspek – aspek Keamanan**

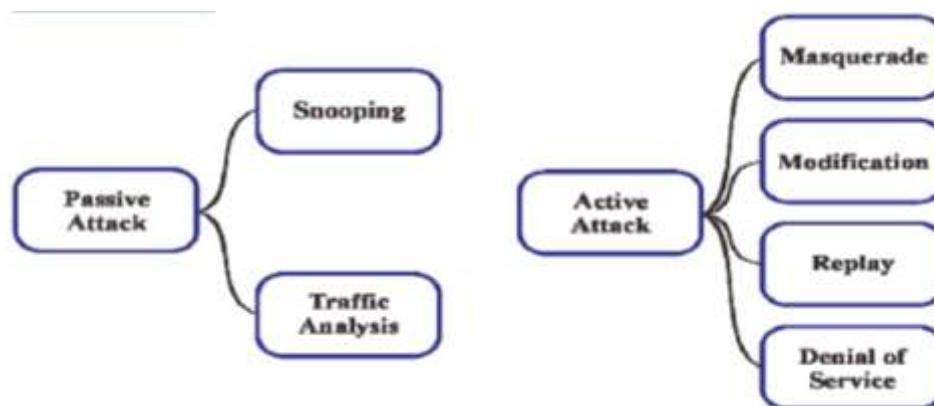
Keamanan data dan informasi memiliki beberapa aspek penting, antara lain :

- a. Authentication
- b. Integrity
- c. Non-repudiation
- d. Authority

- e. Confidentiality
- f. Availability

### 2.1.2 Serangan Keamanan

Secara umum serangan pada sistem keamanan dapat dikategorikan menjadi 2 jenis yaitu serangan pasif (passive attack) dan serangan aktif (active attack) seperti gambar 2.1 dibawah ini :



**Gambar 2.1 Serangan terhadap keamanan**  
 Sumber : (Andi Riski Alvianto; 2015 : 2).

## 2.2 Kriptografi

Kriptography (*Cryptography*) berasal dari bahasa Yunani yaitu dari kata *Crypto* dan *Graphia* yang berarti penulisan rahasia. Kriptography adalah suatu ilmu yang mempelajari penulisan secara rahasia, yang mana pengertian kriptography menurut (Schneier, 1996) adalah ilmu sekaligus seni untuk menjaga keamanan pesan (*message*) Kriptography merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptology*. Kriptography bertujuan menjaga



kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Dalam menjaga kerahasiaan data, kriptography mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. *Ciphertext* inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, *ciphertext* tersebut ditransformasikan kembali ke dalam bentuk *plaintext* agar dapat dikenali. Proses transformasi dari *plaintext* menjadi *ciphertext* disebut proses *Encipherment* atau enkripsi (*encryption*), sedangkan proses mentransformasikan kembali *ciphertext* menjadi *plaintext* disebut proses dekripsi (*decryption*). Untuk mengenkripsi dan mendekripsi data. Kriptography menggunakan suatu algoritma (*cipher*) dan kunci (*key*). *Cipher* adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi data . Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data. Algoritma kriptography modern tidak lagi mengandalkan keamanannya pada kerahasiaan algoritma tetapi kerahasiaan kunci. *Plaintext* yang sama bila disandikan dengan kunci yang berbeda akan menghasilkan *ciphertext* yang berbeda pula. Dengan demikian algoritma kriptography dapat bersifat umum dan boleh diketahui oleh siapa saja, akan tetapi tanpa pengetahuan tentang kunci, data tersandi tetap saja tidak dapat terpecahkan. Sistem kriptography atau *Cryptosystem* adalah sebuah algoritma kriptography ditambah semua kemungkinan *plaintext*, *ciphertext* dan kunci. (Dahlan Abdullah ; 2013 : 153)

### **2.2.1 Jenis Algoritma Kriptografi**

Berdasarkan jenis kunci, algoritma kriptografi dikelompokkan menjadi dua

bagian, yaitu : algoritma simetris (algoritma kunci privat) dan algoritma asimetris (algoritma kunci publik)

### 1. Algoritma Simetris

Algoritma simetris adalah salah satu jenis kunci pada algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Istilah lain untuk kriptografi kunci simetri adalah kriptografi kunci privat (private-key cryptography). Sistem kriptografi kunci-simetri diasumsikan sebagai pengirim dan penerima pesan yang sudah berbagi kunci yang sama sebelum bertukar pesan. Keamanan sistem kriptografi simetri terletak pada kerahasiaan kuncinya.

Kriptografi simetri adalah jenis kriptografi yang diketahui masuk ke dalam catatan sejarah hingga tahun 1976. Semua algoritma kriptografi klasik termasuk ke dalam sistem kriptografi simetri. Salah satu kelebihan pada algoritma simetris yaitu proses enkripsi dan deskripsinya jauh lebih cepat dibandingkan dengan algoritma asimetris. Sedangkan kelemahannya yaitu pada permasalahan distribusi kunci (key distribution).

Seperti yang telah dibahas sebelumnya, proses enkripsi dan deskripsi pada kriptografi simetri menggunakan kunci yang sama. Sehingga timbul persoalan untuk menjaga kerahasiaan kunci. Contohnya pada saat pengiriman kunci dilakukan melalui media yang tidak aman seperti internet. Jika kunci ini hilang atau sudah diketahui oleh orang yang tidak berhak, maka kriptosistem ini dinyatakan tidak aman lagi. Kelemahan lain adalah masalah efisiensi jumlah kunci. Jika terdapat  $n$  user, maka diperlukan  $n(n-1)/2$  kunci, sehingga untuk

jumlah user yang sangat banyak, sistem ini tidak efisien lagi. (*Anandia Zelvina; 2012 : 57*)

## 2. Algoritma Asimetris

Algoritma asimetris atau dapat disebut juga dengan algoritma kunci public, didesain sebaik mungkin sehingga kunci yang digunakan untuk enkripsi berbeda dengan kunci dekripsinya. Dimana kunci untuk enkripsi tidak rahasia (diumumkan ke publik), sementara kunci dekripsinya bersifat rahasia (hanya diketahui oleh penerima pesan).

Pada kriptografi asimetris, setiap orang yang akan berkomunikasi harus mempunyai sepasang kunci, yaitu kunci privat dan kunci publik. Pengirim pesan akan mengenkripsi pesan menggunakan kunci publik si penerima pesan dan hanya penerima pesan yang dapat mendekripsi pesan tersebut karena hanya ia yang mengetahui kunci privatnya sendiri. Kriptografi kunci-publik dapat dianalogikan seperti kotak surat yang terkunci dan memiliki lubang untuk memasukkan surat. Setiap orang dapat memasukkan surat ke dalam kotak surat tersebut, tetapi hanya pemilik kotak yang dapat membuka kotak dan membaca surat di dalamnya karena ia yang memiliki kunci. Sistem ini memiliki dua keuntungan. Yang pertama yaitu, tidak ada kebutuhan untuk mendistribusikan kunci privat sebagaimana pada sistem kriptografi simetri. Kunci publik dapat dikirim ke penerima pesan melalui saluran yang sama dengan saluran yang digunakan untuk mengirim pesan. Saluran untuk mengirim pesan umumnya tidak aman.

Kedua, jumlah kunci yang digunakan untuk berkomunikasi secara rahasia dengan banyak orang tidak perlu sebanyak jumlah orang tersebut, cukup membuat dua buah kunci, yaitu kunci publik bagi para koresponden untuk mengenkripsi pesan, dan kunci privat untuk mendekripsi pesan. Berbeda dengan kriptografi kunci-simetris yang membuat kunci sebanyak jumlah pihak yang diajak berkorespondensi.

Meski masih terbilang baru (sejak 1976), kriptografi kunci-publik mempunyai kontribusi yang luar biasa dibandingkan dengan sistem kriptografi simetri. Kontribusi yang paling penting adalah tanda-tangan digital pada pesan untuk memberikan aspek keamanan otentikasi, integritas data, dan nirpenyangkalan. Tanda-tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci yang digunakan. Pengirim pesan mengenkripsi pesan (yang sudah diringkas) dengan kunci privatnya, hasil enkripsi inilah yang dinamakan tanda-tangan digital. Tanda-tangan digital dilekatkan (embed) pada pesan asli. Penerima pesan memverifikasi tanda-tangan digital dengan menggunakan kunci publik. (*Anandia Zelvina; 2012 : 58*)

### **2.3 Tujuan Kriptografi**

Tujuan dari kriptografi yang juga merupakan aspek keamanan informasi adalah sebagai berikut :

1. Kerahasiaan (confidentiality) adalah layanan yang digunakan untuk menjaga isi informasi dari semua pihak kecuali pihak yang memiliki otoritas terhadap informasi. Ada beberapa pendekatan untuk menjaga kerahasiaan, dari



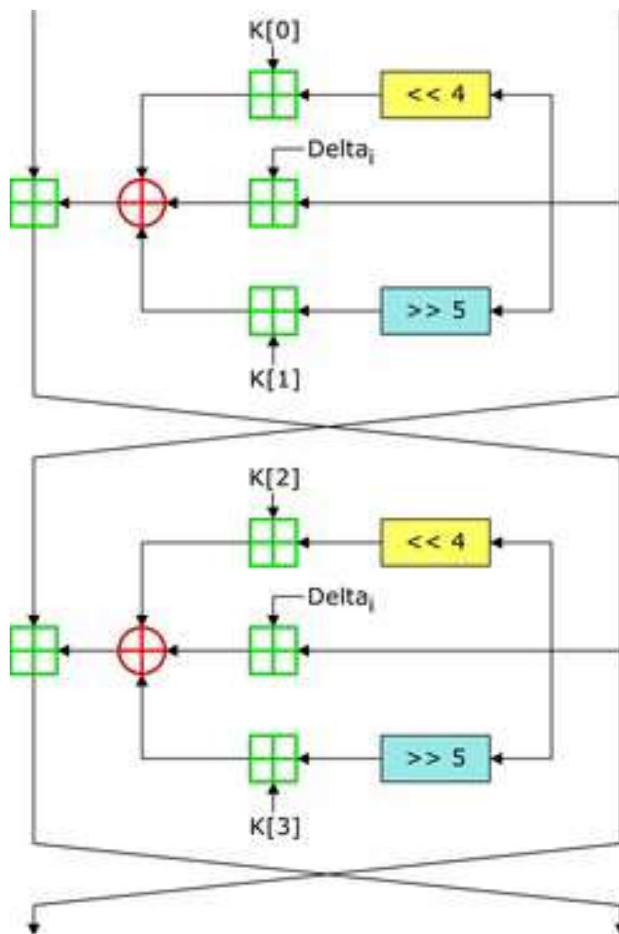
pengamanan secara fisik hingga penggunaan algoritma matematika yang membuat data tidak dapat dipahami. Istilah lain yang senada dengan confidentiality adalah secrecy dan privacy.

2. Integritas data adalah layanan penjagaan perubahan data dari pihak yang tidak berwenang. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi pesan oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam pesan yang sebenarnya. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (digital signature). Pesan yang telah ditandatangani menyiratkan bahwa pesan yang dikirim adalah asli.
3. Otentikasi adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (user authentication atau entity authentication) maupun mengidentifikasi kebenaran sumber pesan (data origin authentication). Dua pihak yang saling berkomunikasi harus dapat mengotentikasi satu sama lain sehingga ia dapat memastikan sumber pesan. Pesan yang dikirim melalui saluran komunikasi juga harus diotentikasi asalnya. Otentikasi sumber pesan secara implisit juga memberikan kepastian integritas data, sebab jika pesan telah dimodifikasi berarti sumber pesan sudah tidak benar. Oleh karena itu, layanan integritas data selalu dikombinasikan dengan layanan otentikasi sumber pesan. Di dalam kriptografi, layanan ini direalisasikan dengan menggunakan tanda-tangan digital (digital signature). Tanda-tangan digital menyatakan sumber pesan.

4. Nirpenyangkalan (non-repudiation) adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan. (*Anandia Zelvina; 2012 : 58*)

#### **2.4 Algoritma TEA(*Tiny Encryption Algorithm*)**

TEA adalah algoritma *block cipher* yang diciptakan oleh *David J. Wheeler* dan *Roger M. Needham* dari *Cambridge University* tahun 1994. Hal yang paling menonjol dari TEA adalah kesederhanaan implementasi, ketiadaan *S-Box* maupun *P-Box* dan kecepatan yang tinggi. TEA beroperasi dalam ukuran blok 64 bit dan panjang kunci 128 bit. TEA berbasiskan jaringan *Feistel* dan memiliki 32 putaran. Kunci K pertama-tama akan dibagi menjadi 4 kunci internal yaitu K[0..3] masing-masing panjangnya 32 bit. Setiap putaran TEA terdiri atas dua *ronde Feistel* (lihat gambar II.3). Penjadwalan kunci TEA sangat sederhana, yaitu untuk ronde ganjil digunakan K[0] dan K[1], sedangkan untuk ronde genap digunakan K[2] dan K[3]. (*Khandar William ; 2010 : 2*)



**Gambar 2.2 Satu putaran enkripsi dalam jaringan Feistel milik TEA**  
*Sumber : Khandar William ; 2010*

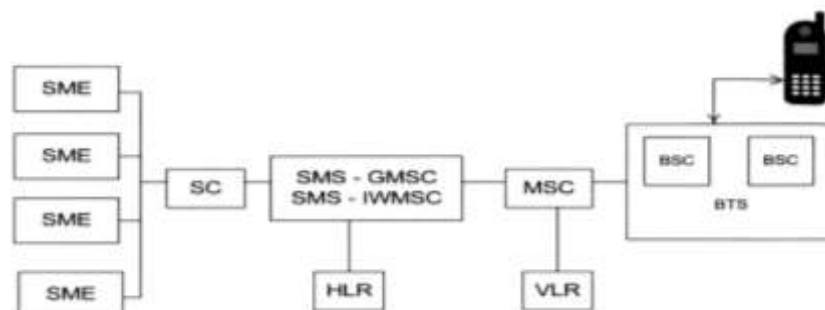
## 2.5 Short Message Service (SMS)

Short Message Service (SMS) adalah salah satu fasilitas dari teknologi GSM yang memungkinkan mengirim dan menerima pesan-pesan singkat berupa text dengan kapasitas maksimal 160 karakter dari Mobile station (MS). Kapasitas maksimal ini tergantung dari alfabet yang digunakan, untuk alfabet latin maksimal 160 karakter, dan untuk non-latin misalnya alfabet arab atau china

maksimal 70 karakter. Dalam arsitektur layanan SMS dalam jaringan GSM, terdapat beberapa bagian, yaitu :

1. Terminal Equipment (TE), perangkat yang digunakan, contoh : HP.
2. Mobile Equipment (ME), terdiri dari pemancar radio, display dan DSP
3. Base Transceiver Station (BTS), terdiri dari pemancar radio untuk berkomunikasi dengan mobile station (MS)
4. Base Station Controller (BSC), mengatur radio resources untuk satu atau lebih BTS
5. Mobile Switching Center (MSC), melaksanakan fungsi seperti registrasi, authentication, update lokasi dll
6. Home Location Register (HLR), database yang memiliki data pelanggan tetap
7. SMS Centre (SMSC), mengatur proses pengiriman dan penerimaan pesan dari atau menuju SME sesuai dengan proses store and forward
8. Email Gateway, sebuah gateway yang menghubungkan antara SMS dengan email pada internet. (*Adrian Imantaka ; 2015:3*)

Jaringan GSM yang terintegrasi dengan service SMS memiliki beberapa tambahan subsistem, seperti gambar berikut ini.



**Gambar 2.3 Elemen jaringan dan arsitektur SMS**

*Sumber : Adrian Imantaka ; 2015*

## 2.6 Eclipse

Eclipse adalah sebuah IDE (Integrated Development Environment) untuk mengembangkan perangkat lunak dan dapat dijalankan di semua platform. Adapun tiga sifat dari Eclipse adalah sebagai berikut. pertama Multi-platform dimana target sistem operasi Eclipse adalah Microsoft Windows, Linux, Solaris, AIX, HP-UX dan Mac OS X. kedua adalah multi-language, hal mana Eclipse dikembangkan dengan bahasa pemrograman Java, akan tetapi Eclipse mendukung pengembangan aplikasi berbasis bahasa pemrograman lainnya, seperti C/C++, Cobol, Python, Perl, PHP, dan lain sebagainya. Dan yang terakhir adalah Multi-role yaitu selain sebagai IDE untuk pengembangan aplikasi, Eclipse pun bisa digunakan untuk aktivitas dalam siklus pengembangan perangkat lunak, seperti dokumentasi, test perangkat lunak, pengembangan web, dan lain sebagainya. Eclipse pada saat ini merupakan salah satu IDE favorit dikarenakan gratis dan open source, yang berarti setiap orang dapat melihat kode pemrograman perangkat lunak ini. Selain itu, kelebihan dari Eclipse yang membuatnya populer adalah kemampuannya untuk dapat dikembangkan oleh pengguna dengan komponen yang dinamakan plug-in. Konsep Eclipse adalah IDE yang terbuka, mudah diperluas untuk apa saja, dan tidak untuk sesuatu yang spesifik. Jadi, Eclipse tidak saja untuk mengembangkan program Java, akan tetapi dapat digunakan untuk berbagai macam keperluan, cukup dengan menginstal plug-in yang dibutuhkan (*Alicia Sinsuw ; 2013 :3*)

## **2.7 Android**

*Android* adalah sistem operasi untuk telepon seluler yang berbasis Linux, yang mencakup *system* operasi, *middleware* dan aplikasi. *Android* tidak terikat ke satu merek telepon seluler. *Android* menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri hingga dapat digunakan oleh berbagai peranti mobile. Beberapa fitur utama dari *Android* antara lain WiFi hotspot, Multi-touch, Multitasking, GPS, support java, mendukung banyak jaringan (GSM/EDGE, IDEN, CDMA, EV-DO, UMTS, Bluetooth, Wi-Fi, LTE, and WiMAX) dan juga kemampuan dasar telepon seluler pada umumnya. (*Alicia Sinsuw ; 2013 :3*)

### **2.7.1 Android SDK (Software Development Kit)**

Android SDK adalah tools API (Application Programming Interface) yang diperlukan untuk mengembangkan aplikasi pada platform Android menggunakan bahasa pemrograman Java. Beberapa fitur-fitur Android yang paling penting adalah mesin Virtual Dalvik yang dioptimalkan untuk perangkat mobile, integrated browser berdasarkan engine open source WebKit, Grafis yang dioptimalkan dan didukung oleh libraries grafis 2D, grafis 3D berdasarkan spesifikasi opengl ES 1.0 (Opsional akselerasi perangkat keras), kemudian SQLite untuk penyimpanan data (database). Fitur-fitur android lainnya termasuk media yang mendukung audio, video, dan gambar, juga ada fitur bluetooth, EDGE, 3G dan WiFi, dengan fitur kamera, GPS, dan kompas. Selanjutnya fitur yang juga turut disediakan adalah lingkungan Development yang lengkap dan kaya termasuk

perangkat emulator, tools untuk debugging, profil dan kinerja memori, dan plugin untuk IDE Eclipse. (Alicia Sinsuw ; 2013 :2)

### **2.7.2 AVD (*Android Virtual Device*)**

*Android Virtual Device* merupakan emulator untuk menjalankan aplikasi android yang tampilannya dapat dilihat pada gambar 1. Setiap AVD terdiri dari sebuah profil perangkat keras yang dapat mengatur pilihan untuk menentukan fitur hardware emulator. Misalnya, menentukan apakah menggunakan perangkat kamera, apakah menggunakan keyboard QWERTY fisik atau tidak, berapa banyak memori internal, dan lain-lain. AVD juga memiliki sebuah pemetaan versi Android, maksudnya kita menentukan versi dari platform Android akan berjalan pada emulator. Pilihan lain dari AVD, misalnya menentukan skin yang kita ingin gunakan pada emulator, yang memungkinkan untuk menentukan dimensi layar, tampilan, dan sebagainya. Kita juga dapat menentukan SD Card virtual untuk digunakan dengan di emulator. (Alicia Sinsuw ; 2013 :2)

### **2.7.3 Bahasa Pemrograman Java**

Bahasa pemrograman Java dapat dikategorikan sebagai sebuah bahasa pemrograman berorientasi objek, pemrograman terdistribusi dan bahasa pemrograman multithreaded. Objek Java dispesifikasi dengan membentuk kelas. Untuk masing-masing kelas Java, kompiler Java memproduksi sebuah file keluaran arsitektur netral yang akan jalan pada berbagai implementasi dari Java Virtual Machine (JVM). (Alicia Sinsuw ; 2013 :3)



## 2.8 Konsep UML (*Unified Modelling Language*)

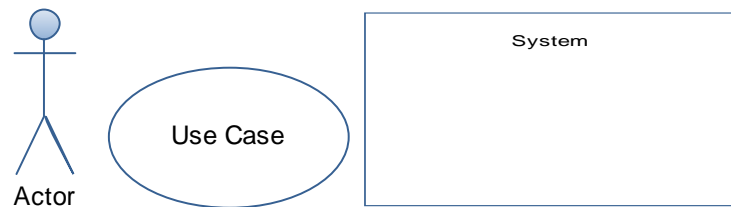
*Unified Modelling Language* (UML) adalah sebuah “bahasa” yang telah menjadi standar dalam industri untuk visualisasi, merancang dan mendokumentasikan sistem piranti lunak. UML menawarkan sebuah standar untuk merancang model sebuah sistem. Dengan menggunakan UML dapat dibuat model untuk semua jenis aplikasi piranti lunak, dimana aplikasi tersebut dapat berjalan pada piranti keras, sistem operasi dan jaringan apapun, serta ditulis dalam bahasa pemrograman apapun. Tetapi karena UML juga menggunakan class dan operation dalam konsep dasarnya, maka lebih cocok untuk penulisan piranti lunak dalam bahasa berorientasi objek seperti C++, Java, atau VB. NET. (Prastuti Sulistyorini : 2009 : 1).

### 2.8.1 Diagram – diagram UML

#### 1. *Use Case Diagram*

Use-case adalah konstruksi untuk mendeskripsikan bagaimana sistem akan terlihat di mata pengguna potensial. Use-case terdiri dari sekumpulan skenario yang dilakukan oleh seorang aktor (orang, perangkat keras, urutan waktu atau sistem yang lain). Sedangkan *Use Case Diagram* memfasilitasi komunikasi di antara analis dan pengguna serta diantara analis dan klien. *Use Case Diagram* menunjukkan 3 aspek dari sistem yaitu : *actor*, *use-case*, dan *system boundary*. *Actor* adalah pengguna sistem, biasanya mewakili peran orang, sistem yang lain atau alat yang berkomunikasi dengan *use-case*. *Use Case* adalah tugas yg

dilakukan oleh *actor*. Sekumpulan *use-case* biasanya dikelompokkan dalam suatu *group* yang disebut *System Boundary*. (Prastuti Sulistyorini : 2009 : 1). Simbol *use-case* ditunjukkan pada gambar 2.4.



**Gambar 2.4 Actor**

Sumber : (Prastuti Sulistyorini : 2009 : 1).

## 2. Activity Diagram

*Activity diagram* menggambarkan berbagai alir aktivitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, *decision* yang mungkin terjadi, dan bagaimana mereka berakhir. *Activity diagram* juga dapat menggambarkan proses paralel yang mungkin terjadi pada beberapa eksekusi (Prastuti Sulistyorini : 2009 : 1).

Simbol	Keterangan
●	Titik Awal
⦿	Titik Akhir
▭	Activity
◇	Pilihan untuk pengambilan keputusan

**Tabel 2.1 Simbol-simbol pada Activity Diagram**

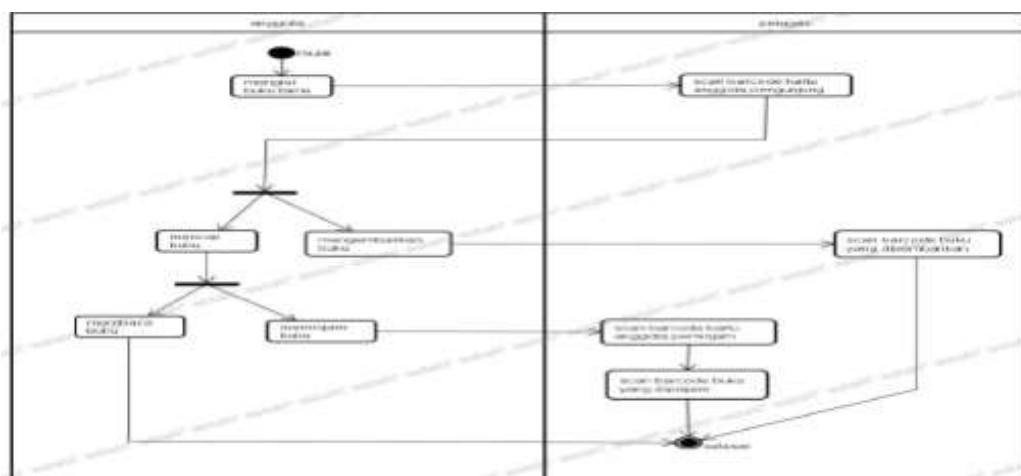
Sumber : (Prastuti Sulistyorini : 2009 : 1).

## 3. Class Diagram

*Class diagram* membantu dalam visualisas istruktur kelas-kelas dari suatu sistem dan merupakan tipe diagram yang paling banyak. *Class diagram*

memperlihatkan hubungan antar kelas dan penjelasan detail tiap-tiap kelas di dalam model desain (dalam *logical view*) dari suatu sistem. Selama proses analisis, *class diagram* memperlihatkan aturan-aturan dan tanggung jawab entitas yang menentukan perilaku sistem. Selama proses analisis, *class diagram* memperlihatkan aturan-aturan dan tanggung jawab entitas yang menentukan perilaku sistem. Selama tahap desain, *class diagram* berperan dalam menangkap struktur dari semua kelas yang membentuk arsitektur sistem yang dibuat. *Class diagram* juga merupakan pondasi untuk *component diagram* dan *deployment diagram*. (Prastuti Sulistyorini : 2009 : 4).

*Class diagram* menggambarkan struktur statis dari kelas dalam sistem anda dan menggambarkan atribut, operasi dan hubungan antara kelas. *Class diagram* membantu dalam memvisualisasikan struktur kelas-kelas dari suatu sistem dan merupakan tipe diagram yang paling banyak dipakai. Selama tahap desain, *class diagram* berperan dalam menangkap struktur dari semua kelas yang membentuk arsitektur sistem yang dibuat. (Prastuti Sulistyorini : 2009 : 4).

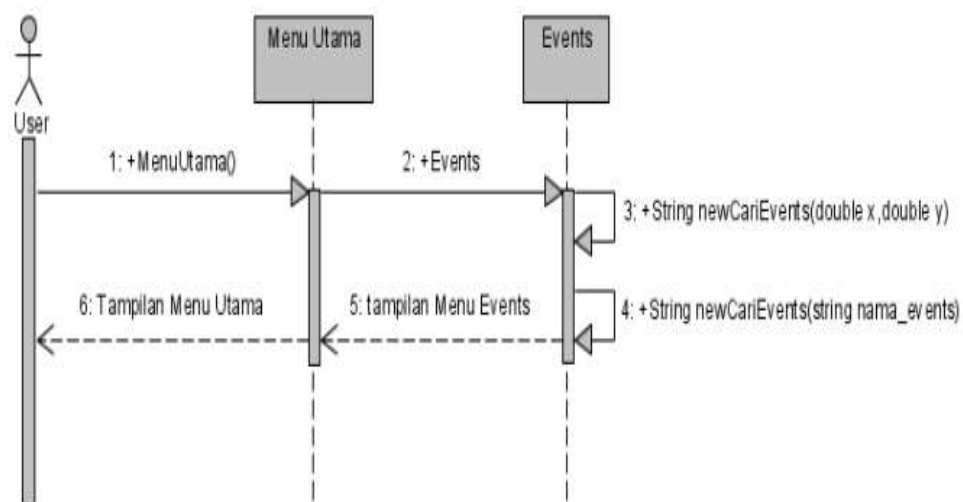


**Gambar 2.5 Contoh Simbol Class Diagram**

Sumber : (Prastuti Sulistyorini : 2009 : 4).

#### 4. Sequence diagram

Diagram sequence menjelaskan interaksi objek yang disusun dalam suatu urutan waktu. Diagram ini secara khusus berasosiasi dengan *use case*. Sequence diagram memperlihatkan tahap demi tahap apa yang seharusnya terjadi untuk menghasilkan sesuatu didalam *use case*. Diagram sequence sebaiknya digunakan diawal tahap desain atau analisis karena kesederhanaannya dan mudah untuk dimengerti. Sequence diagram menjelaskan interaksi objek yang disusun berdasarkan urutan waktu. Secara mudahnya sequence diagram adalah gambaran tahap demi tahap, termasuk kronologi (urutan) perubahan secara logis yang seharusnya dilakukan untuk menghasilkan sesuatu sesuai dengan usecase diagram. (Haviluddin : 2011 : 5).



**Gambar 2.6 Contoh Sequence Diagram**

Sumber : (S. Nofan Maulana Rachman : 2012 : 9)

*Class diagram* menggambarkan struktur statis dari kelas dalam sistem anda dan menggambarkan atribut, operasi dan hubungan antara kelas. *Class diagram* membantu dalam memvisualisasikan struktur kelas-kelas dari suatu

sistem dan merupakan tipe diagram yang paling banyak dipakai. Selama tahap desain, *class diagram* berperan dalam menangkap struktur dari semua kelas yang membentuk arsitektur sistem yang dibuat

## **BAB III**

### **ANALISIS DAN DESAIN SISTEM**

#### **3.1 Analisa Kebutuhan Sistem**

Analisa yang mengacu dengan terciptanya sistem diambil dari jurnal dengan ada permasalahan seperti pada jurnal sebelumnya dengan judul “Pembuatan Algoritma Enkripsi DES SMS Berbasis Mobile” (*Fettian; 2015 : 152*);, pada sistem jurnal ini untuk menerima dan mengirim pesan tanpa bisa membalas pesan. Maksimal karakter pesan yang dikirim yaitu 77 karakter. Hanya memiliki aplikasi yang bisa melakukan enkripsi dan dekripsi pesan. Aplikasi ini belum menyediakan layanan hapus pesan. Terdapat kunci rahasia yang harus dimasukkan untuk bisa mengenkripsi atau mendeskripsi pesan sms. Untuk masukkan kunci rahasia yang digunakan untuk mengenkripsi sms sama dengan masukan pada saat kita mendeskripsikan sms. Hal ini karena algoritma yang digunakan yaitu algoritma simetris block cipher DES (Data Encryption Standar). Maksimal karakter yang dimasukkan yaitu 8 karakter.

#### **3.2 Sistem Yang Sedang Berjalan**

Analisis terhadap suatu sistem yang sedang berjalan merupakan suatu langkah penting dalam pemahaman permasalahan yang ada sebelum dilakukannya pengambilan keputusan atau tindakan dalam menyelesaikan permasalahan tersebut. Setelah dilakukan analisis terhadap sistem yang berjalan, langkah berikutnya adalah melakukan perancangan sistem baru. Dimana dalam

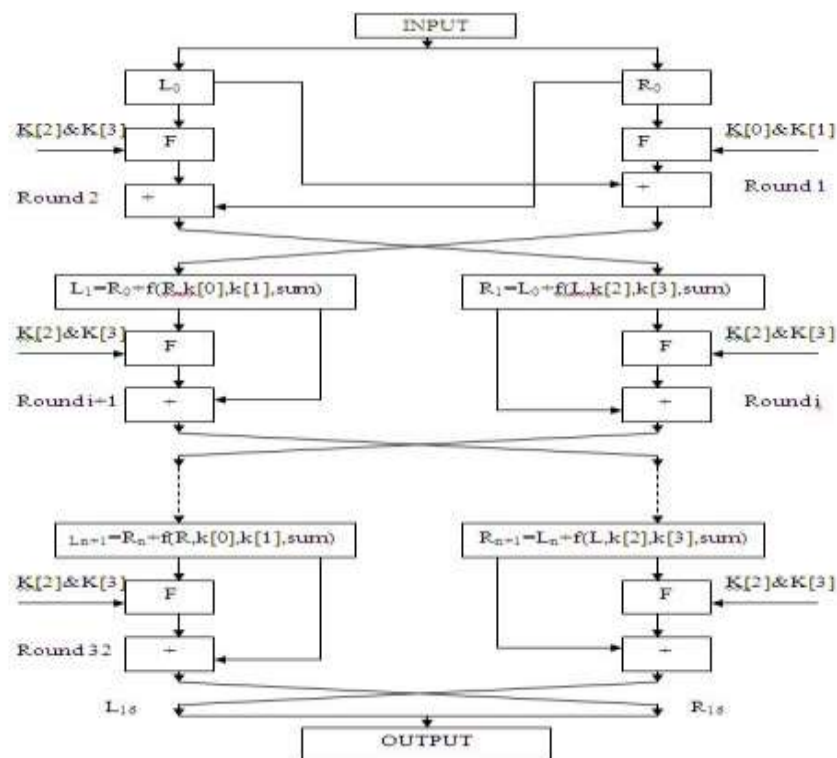
perancangan sistem ini dapat memberikan gambaran tentang sistem yang akan dibuat. Salah satu dukungan yang ada pada perangkat seluler, pengguna dapat menggunakan pesan *SMS* atau dalam bahasa Indonesia adalah pesan singkat. Banyak pengguna telepon seluler yang menggunakan layanan ini, dikarenakan biaya yang cukup murah dan hanya menggunakan teks dalam berkomunikasi. Namun tingkat keamanan pada layanan *SMS* tidak ada tetapi masih belum terjamin dalam pengamanan pesan teks terkirim atau diterima. Hal ini yang cenderung menimbulkan bahaya bagi pengguna yang memiliki pesan-pesan pribadi penting, sehingga dapat disalah gunakan oleh pihak yang tidak bertanggung jawab. Di dalam keamanan komputer dikenal sebuah teknik kriptografi, yang difungsikan untuk penyandian pesan. Berdasarkan kepentingan dan kerahasiaan sebuah pesan diperlukannya sebuah cara untuk mengamankan suatu pesan atau informasi dengan menggunakan teknik kriptografi. Saat ini sudah banyak berkembang algoritma kriptografi yang mendukung untuk mengamankan suatu pesan atau informasi yang ada dari orang atau pihak yang tidak berhak untuk mengakses data atau informasi tersebut. Salah satu teknik kriptografi adalah menggunakan algoritma *Tiny Encryption Algorithm (TEA)*. *TEA* adalah algoritma *block cipher* yang diciptakan oleh *David J. Wheeler* dan *Roger M. Needham* dari *Cambridge University* tahun 1994. Hal yang paling menonjol dari *TEA* adalah kesederhanaan implementasi, ketiadaan *S-Box* maupun *P-Box* dan kecepatan yang tinggi. Penulis mencoba untuk membangun sebuah aplikasi yang dapat mengamankan pesan teks *SMS* dengan algoritma kriptografi *Tiny Encryption Algorithm (TEA)*.



### 3.3 Algoritma TEA (*Tiny Encryption Algorithm*)

*Tiny Encryption Algorithm* (TEA) merupakan suatu algoritma sandi yang diciptakan oleh David Wheeler dan Roger Needham dari Computer Laboratory, Cambridge University, England pada bulan November 1994. Algoritma ini merupakan algoritma penyandian *block cipher* yang dirancang untuk penggunaan memory yang seminimal mungkin dengan kecepatan proses yang maksimal.

Sistem penyandian TEA menggunakan proses *feistel network* dengan menambahkan fungsi matematik berupa penambahan dan pengurangan sebagai operator pembalik selain XOR. Hal ini dimaksudkan untuk menciptakan sifat non-linearitas. Pergeseran dua arah (ke kiri dan ke kanan) menyebabkan semua bit kunci dan data bercampur secara berulang ulang. Struktur penyandian TEA terlihat pada gambar 3.1 sebagai berikut:

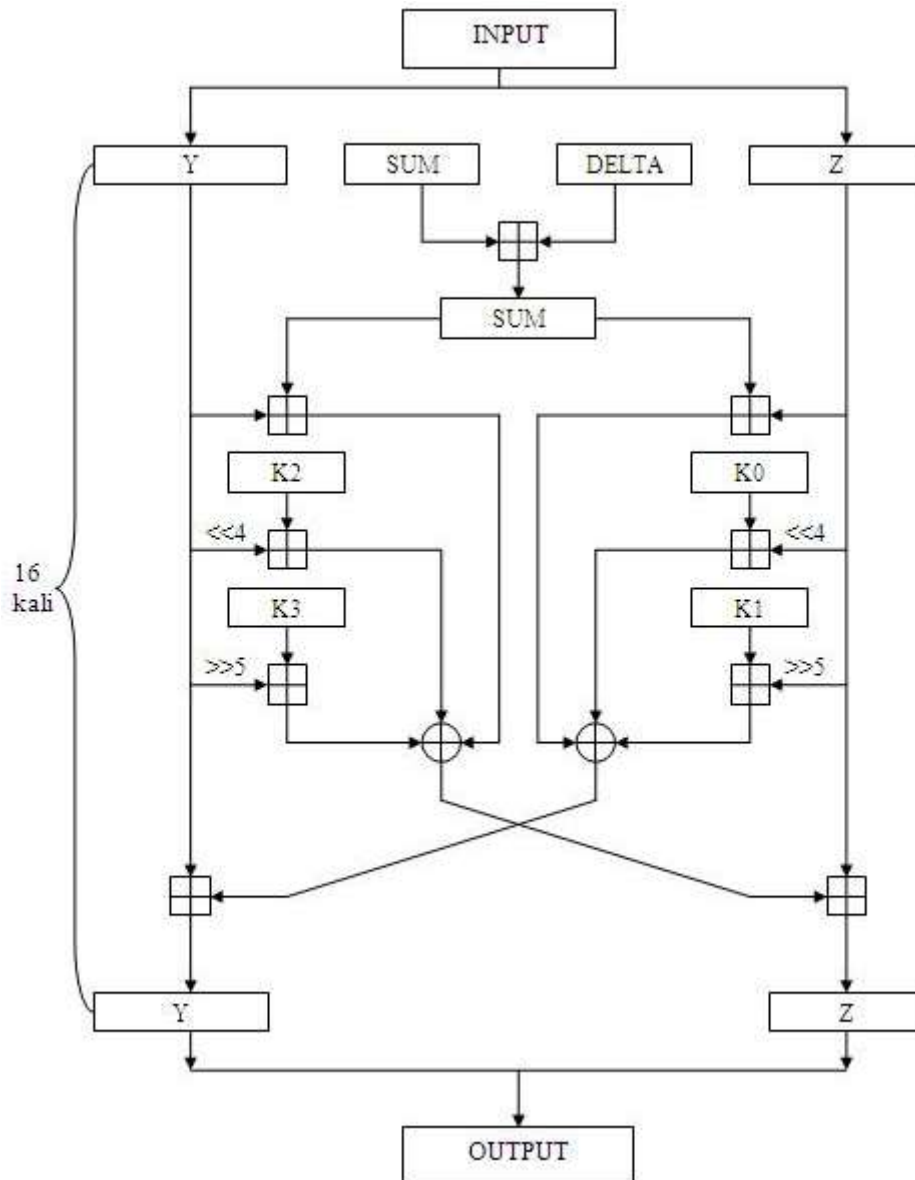


Gambar 3.1 Algoritma TEA

TEA memproses 64-bit input sekali waktu dan menghasilkan 64-bit output. TEA menyimpan 64-bit input kedalam  $L_0$  dan  $R_0$  masing masing 32-bit, sedangkan 128-bit kunci disimpan kedalam  $k[0]$ ,  $k[1]$ ,  $k[2]$ , dan  $k[3]$  yang masing masing berisi 32-bit. Diharapkan teknik ini cukup dapat mencegah penggunaan teknik *exshautive search* (teknik pencarian solusi secara solusi *brute force* atau percobaan terhadap semua kunci yang mungkin, untuk masalah yang melibatkan pencarian elemen dengan sifat khusus, biasanya di antara objek-objek kombinatorik seperti permutasi, kombinasi, atau himpunan bagian dari sebuah himpunan) secara efektif. Hasil outputnya akan disimpan dalam  $L_{16}$  dan  $R_{16}$ .

Bilangan delta berasal dari *golden number*, digunakan  $\delta = (\sqrt{5} - 1)2^{31}$ . Suatu bilangan delta ganda yang berbeda digunakan dalam setiap roundnya sehingga tidak ada bit dari perkalian yang tidak berubah secara teratur. Berbeda dengan struktur *feistel* yang semula hanya mengoperasikan satu sisi yaitu sisi sebelah kanan dengan sebuah fungsi  $F$ , pada algoritma TEA kedua sisi dioperasikan dengan sebuah fungsi yang sama yaitu fungsi  $F$  ( $L_0 = L_0 + (((R_0 \ll 4) + k[0]) \wedge R_0 + \text{sum}^{\wedge}((R_0 \gg 5) + k[1]))$ ) dan  $R_0 = R_0 + (((L_0 \ll 4) + k[2]) \wedge L_0 + \text{sum}^{\wedge}((L_0 \gg 5) + k[3]))$ ) untuk satu round TEA.

Struktur dari penyandian dengan algoritma untuk satu cycle (dua round) dapat dilihat pada gambar 3.2 berikut:



**Gambar 3.2** Satu Cycle TEA (dua round)

Proses diawali dengan *input-bit* teks sebanyak 64-bit, kemudian 64-bit teks tersebut dibagi menjadi dua bagian, yaitu sisi kiri ( $L_0$ ) sebanyak 32-bit dan sisi kanan ( $R_0$ ) sebanyak 32-bit. Setiap bagian teks akan dioperasikan sendiri-sendiri.  $R_0$  ( $Z$ ) akan digeser ke kiri sebanyak empat (4) kali dan ditambahkan dengan kunci  $k[0]$ , sementara itu  $Z$  ditambah dengan sum (delta) yang merupakan konstanta. Hasil penambahan ini di-XOR-kan dengan penambahan sebelumnya. Langkah

selanjutnya di-XOR-kan dengan hasil penambahan antara  $Z$  yang digeser kekanan sebanyak lima (5) kali dengan kunci  $k[1]$ . Hasil tersebut kemudian ditambahkan dengan  $L_0$  ( $Y$ ) yang akan menjadi  $R_1$ .

Sisi sebelah kiri akan mengalami proses yang sama dengan sisi sebelah kanan.  $L_0$  ( $Y$ ) akan digeser ke kiri sebanyak empat (4) kali lalu ditambahkan dengan kunci  $k[2]$ , sementara itu,  $Y$  ditambah dengan sum (delta). Hasil penambahan ini di-XOR-kan dengan penambahan sebelumnya. Langkah selanjutnya di-XOR-kan dengan hasil penambahan antara  $Y$  yang digeser ke kanan sebanyak lima (5) kali dengan kunci  $k[3]$ . Hasil tersebut kemudian ditambahkan dengan  $R_0$  ( $Z$ ) yang akan menjadi  $L_1$ .

### **3.4 Analisis Proses Enkripsi Algoritma TEA**

Untuk melakukan enkripsi, proses diawali dengan input-bit teks terang sebanyak 64-bit. Kemudian 64-bit teks terang tersebut dibagi menjadi dua bagian, yaitu sisi kiri ( $L_0$ ) sebanyak 32-bit dan sisi kanan ( $R_0$ ) sebanyak 32-bit. Setiap bagian teks terang akan dioperasikan sendiri-sendiri.  $R_0$  ( $z$ ) akan digeser ke kiri sebanyak empat (4) kali dan ditambahkan dengan kunci  $k[0]$ . Sementara itu  $z$  ditambah dengan sum (delta) yang merupakan konstanta. Hasil penambahan ini di-XOR-kan dengan penambahan sebelumnya. Kemudian di-XOR-kan dengan hasil penambahan antara  $z$  yang digeser kekanan sebanyak lima (5) kali dengan kunci  $k[1]$ . Hasil tersebut kemudian ditambahkan dengan  $L_0$  ( $y$ ) yang akan menjadi  $R_1$ . Untuk lebih memahami dapat dilihat pada blok diagram proses enkripsi algoritma TEA berikut ini.

Sisi sebelah kiri akan mengalami proses yang sama dengan sisi sebelah kanan. L0 (y) akan digeser kekiri sebanyak empat (4) kali dan ditambahkan dengan kunci k[2]. Sementara itu Y ditambah dengan sum (delta). Hasil penambahan ini di-XOR-kan dengan penambahan sebelumnya. Kemudian di-XOR-kan dengan hasil penambahan antara Y yang digeser kekanan sebanyak lima (5) kali dengan kunci k[3]. Hasil tersebut kemudian ditambahkan dengan R0 (Z) yang akan menjadi L1.

Misalkan :

Plaintext : bukubaca

Kunci : S1 ILMU KOMPUTER

Bagi plaintext menjadi 2 blok kedalam blok R dan blok L :

R = baca

L = buku

Begitu juga dengan kunci, menjadi 4 blok k[0], k[1], k[2], k[3] :

k[0] = S1spasiI

k[1] = LMUspasi

k[2] = KOMP

k[3] = UTER

ubah plaintext serta kunci dalam kode ASCII kemudian ke biner dengan proses sebagai berikut :

b → 98 → 01100010

a → 97 → 01100001

c → 99 → 01100011

a → 97 → 01100001

b → 98 → 01100010

u → 117 → 01110101

k → 107 → 01101011

u → 117 → 01110101

S → 83 → 01010011

l → 49 → 00110001

Spasi → 32 → 00100000

I → 73 → 01001001

L → 76 → 01001100

M → 77 → 01001101

U → 85 → 01010101

Spasi → 32 → 00100000

K → 75 → 01001011

O → 79 → 01001111

M → 77 → 01001101

P → 80 → 01010000

U → 85 → 01010101

T → 84 → 01010100

E → 69 → 01000101

R → 82 → 01010010

Sehingga didapat :

Cipher R (Z) : 01100010 01100001 01100011 01100001

Cipher L (Y) : 01100010 01110101 01101011 01110101

K[0] : 01010011 00110001 00100000 01001001

K[1] : 01001100 01001101 01010101 00100000

K[2] : 01001011 01001111 01001101 01010000

K[3] : 01010101 01010100 01000101 01010010

Cipher R (Z) akan mengalami pergeseran bit ke kiri sebanyak 4 bit dan pergeseran bit ke kanan sebanyak 5 bit.

Cipher R (Z) : 01100010 01100001 01100011 01100001

Menjadi

Zsl ( Z shift left) : 00100110 00010110 00110110 00010110

Zsr ( R shift right) : 00010011 00001011 00011011 00001011

Zsl ditambah dengan kunci k[0] :

Zsl : 00100110 00010110 00110110 00010110

K[0] : 01010011 00110001 00100000 01001001  


---

 01110111 00110111 00110110 01011111

Sedangkan Zsr ditambah dengan k[1] :

Zsr : 00010011 00001011 00011011 00001011

K[1] : 01001100 01001101 01010101 00100000  


---

 01011111 01001111 01011111 00101011

Kemudian Cipher R (Z) tidak mengalami pergeseran bit ditambahkan dengan bilangan delta, dimana bilangan delta yang digunakan secara konstan yaitu : 9E3779B9 atau dalam biner : 10011110 00110111 01111001 10111001.

R (Z) : 01100010 01100001 01100011 01100001

Delta : 10011110 00110111 01111001 10111001

11111110 01110111 01111011 11111001

Kemudian di XOR kan dengan cipher Zsl yang ditambah k[0] :

11111110 01110111 01111011 11111001

01110111 00110111 00110110 01011111

10001001 01000000 01001101 10100110

Kemudian di XOR kan dengan Zsr yang ditambah k[1] :

10001001 01000000 01001101 10100110

01011111 01001111 01011111 00101011

11010110 00001111 00010010 10001101

Untuk cipher L (Y) proses yang terjadi pada dasarnya sama seperti pada cipher R (Z), yakni cipher L (Y) juga yang mengalami pergeseran bit ke kiri sebanyak 4 bit dan ke kanan sebanyak 5 bit.

Cipher L (Y) : 01100010 01110101 01101011 01110101

Menjadi

Ysl : 00100110 01010111 10110110 01010111

Ysr : 00010011 10101011 01011011 10101011

Lsl ditambah dengan k[2] :

Ysl : 00100110 01010111 10110110 01010111

K[2] : 01001011 01001111 01001101 01010000

01101111 01011111 11111111 01010111



Ysr ditambah dengan k[3] :

```

Ysr   : 00010011 10101011 01011011 10101011
K[3]  : 01010101 01010100 01000101 01010010
-----
       01010111 11111111 01011111 11111011

```

Cipher L (Y) yang tidak mengalami pergeseran ditambahkan dengan delta

```

L (Y) : 01100010 01110101 01101011 01110101
Delta  : 10011110 00110111 01111001 10111001
-----
       11111110 01110111 01111011 11111101

```

Kemudian di XOR kan dengan Ysl yang ditambah k[2] :

```

11111110 01110111 01111011 11111101
01101111 01011111 11111111 01010111
-----
10010001 00101000 10000100 10101010

```

Kemudian di XOR kan dengan Ysr yang ditambah k[3] :

```

10010001 00101000 10000100 10101010
01010111 11111111 01011111 11111011
-----
11000110 11010111 11011011 01010001

```

Hasil akhir cipher R (Z) ditambahkan dengan cipher L (Y) yang tidak mengalami pergeseran, yang mana hasilnya akan dijadikan cipher L1 (Y1) untuk round berikutnya. Demuikian juga halnya hasil akhir pada cipher L (Y) akan ditambahkan dengan cipher R (Z) yang tidak mengalami pergeseran yang akan dijadikan cipher R1 (Z1) pada round berikutnya :

```

R (Z) : 11010110 00001111 00010010 10001101
L (Y) : 01100010 01110101 01101011 01110101
      -----
      11110110 01111111 01111011 11111101    L1(Y1)
L (Y) : 11000110 11010111 11011011 01010001
R (Z) : 01100010 01100001 01100011 01100001
      -----
      11100110 11110111 11111011 01110001    R1(Z1)

```

Demikian penjelasan proses enkripsi yang terjadi pada 2 round (1 cycle), untuk round berikutnya dilakukan proses yang sama seperti round sebelumnya, hanya saja untuk proses round yang selanjutnya menggunakan cipher hasil round sebelumnya.

### 3.5 Analisis Proses Deskripsi Algoritma TEA

Untuk proses deskripsi pada algoritma TEA sama halnya dengan proses enkripsinya. Hanya saja terjadi perbedaan pada penjadwalan kuncinya yaitu pada proses enkripsi untuk cipher R yang mengalami pergeseran bit ke kiri sebanyak 4 bit digunakan kunci k[0] pada proses deskripsi digunakan kunci k[1], untuk cipher R yang mengalami pergeseran ke kanan sebanyak 5 bit menggunakan kunci [1] pada proses deskripsi menggunakan kunci k[0]. Begitu juga halnya dengan cipher L, pada proses enkripsi untuk cipher L yang mengalami pergeseran ke kiri sebanyak 4 bit menggunakan kunci k[2] pada yang mengalami Pergeseran proses deskripsi digunakan kunci k[3]. Untuk cipher L yang mengalami pergeseran kekanan sebanyak 5 bit digunakan kunci k[3] pada proses deskripsi digunakan kunci k[2].

### 3.6 Teknik pemecahan Masalah

Adapun teknik pemecahan masalah tentang perancangan aplikasi keamanan sms yang dibuat terdiri dari beberapa poin yaitu sebagai berikut:

1. Untuk langkah awal analisa terhadap perancangan yang akan dibangun terutama tentang keamanan sms yang menggunakan perangkat *android*.
2. Menentukan perangkat yang dibutuhkan dalam membangun aplikasi seperti perangkat keras maupun perangkat lunak.
3. Merancang sistem yang nantinya akan di implementasikan pada aplikasi yang akan dibangun.
4. Terakhir proses uji coba terhadap *inputan*, proses ataupun *output* aplikasi, apakah sudah sesuai dengan perancangan yang telah direncanakan sebelumnya.

### 3.7 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 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*.
2. Perangkat Keras (*Hardware*)

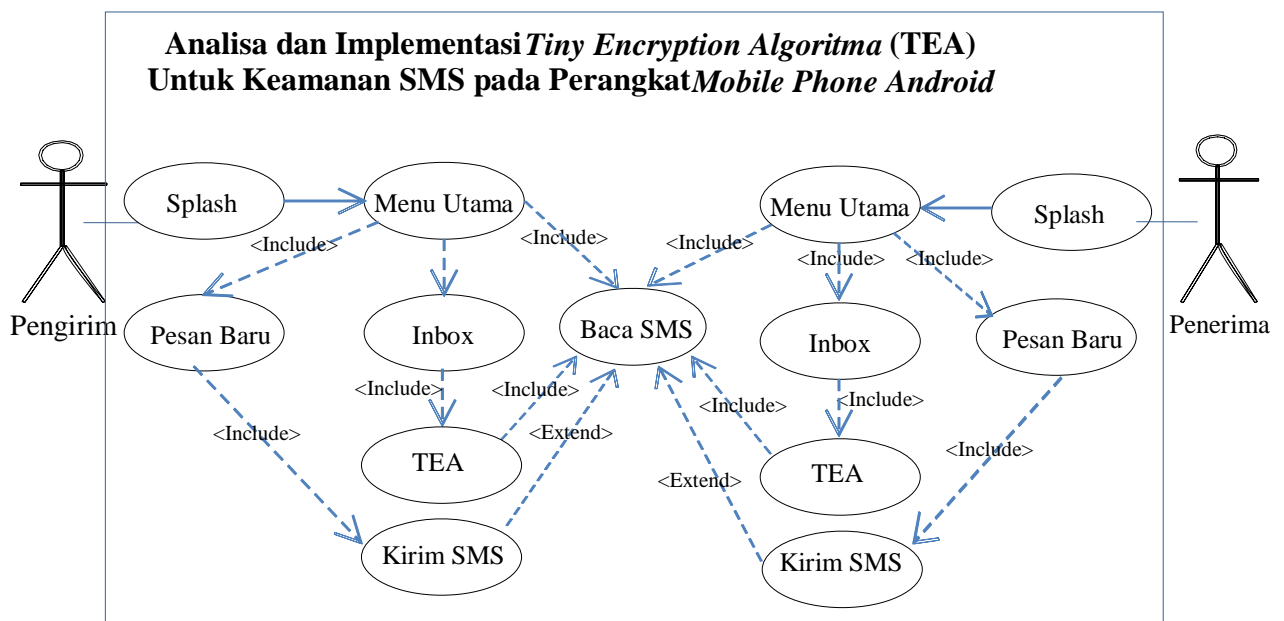
- a. Komputer yang setara *Core i3*.
- b. *Smartphone Android* dengan OS 4.1 atau di atasnya.
- c. *Mouse, keyboard*.

### 3.8 Desain Sistem Usulan

Pada proses perancangan ini akan dijelaskan mengenai beberapa rancangan aplikasi yang akan dikerjakan yang menggunakan perangkat *android* yaitu sebagai berikut:

#### 3.8.1 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 3.3 berikut.



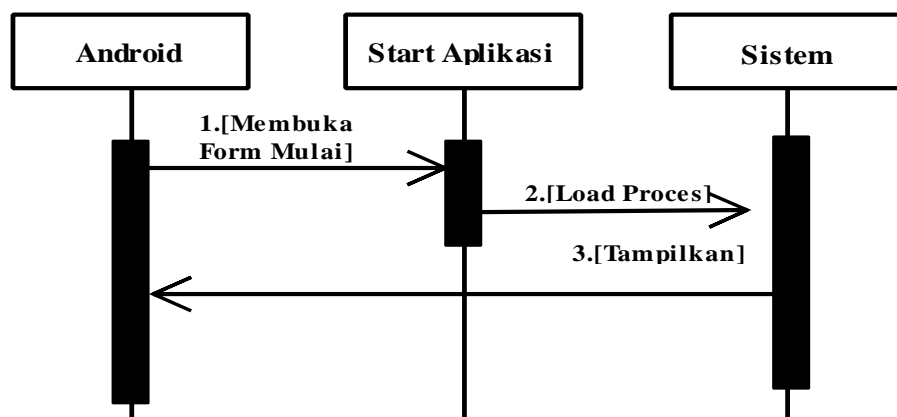
**Gambar 3.3 Use Case Diagram**

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

### 3.8.2 Sequence Diagram

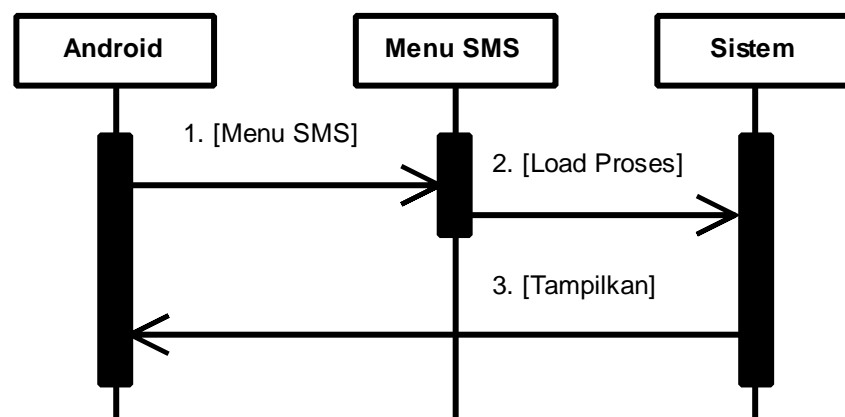
*Sequence* diagram yang digunakan untuk menggambarkan sistem pada sebuah adegan untuk proses penggunaan aplikasi. Berikut ini adalah *Sequence* diagram yang dirancang.

1. *Sequence* Diagram *Start* Aplikasi, untuk diagram proses *start* aplikasi dapat dilihat pada gambar 3.4 berikut.



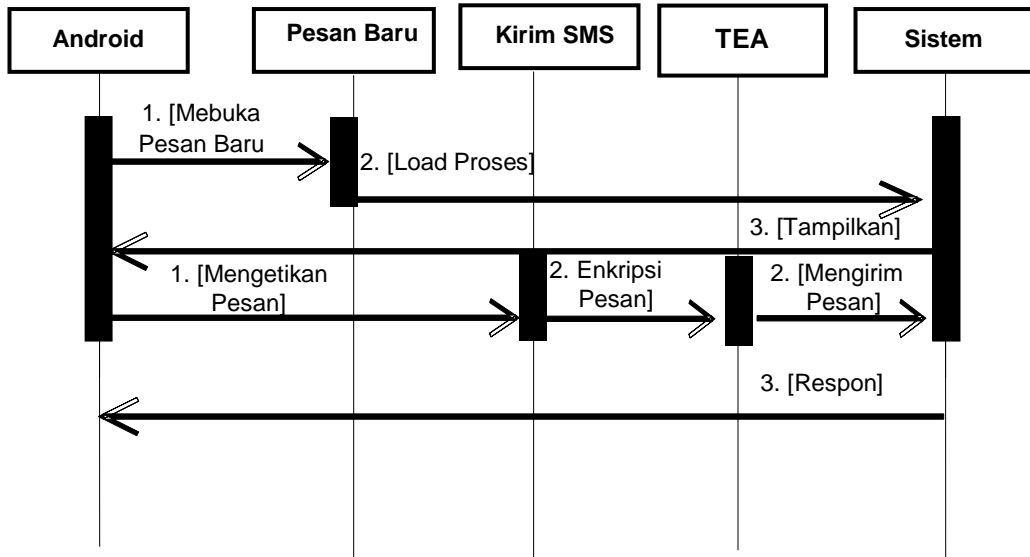
Gambar 3.4 *Sequence* Diagram *Start* Aplikasi

2. *Sequence* Diagram menampilkan *Menu SMS*, untuk diagram proses menampilkan *Menu SMS* dapat dilihat pada gambar 3.5 dibawah ini.



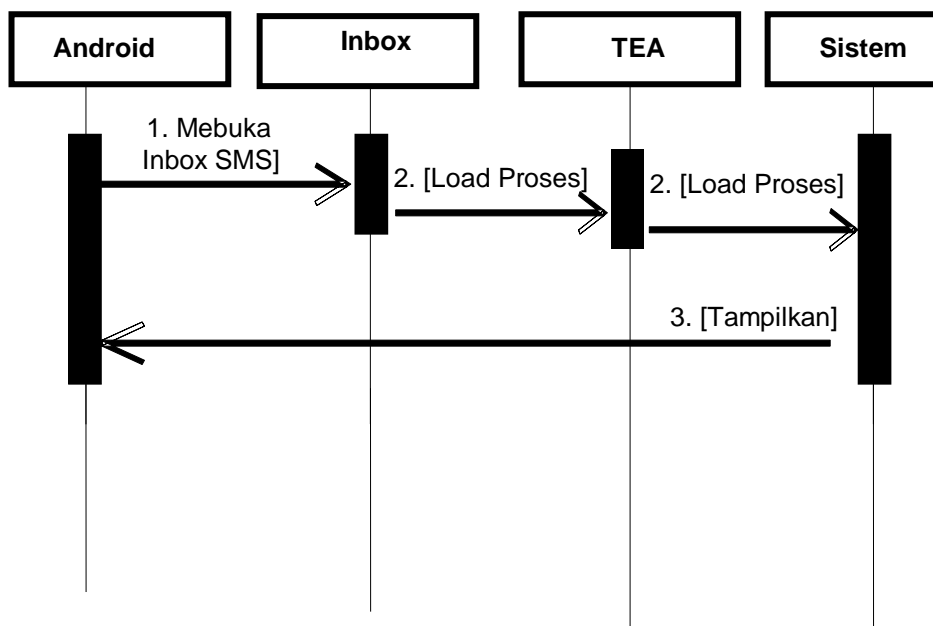
Gambar 3.5 *Sequence* Diagram Menampilkan *Menu SMS*

3. *Sequence Diagram Mengirim SMS*, untuk diagram proses Mengirim SMS dapat dilihat pada gambar 3.6 berikut.



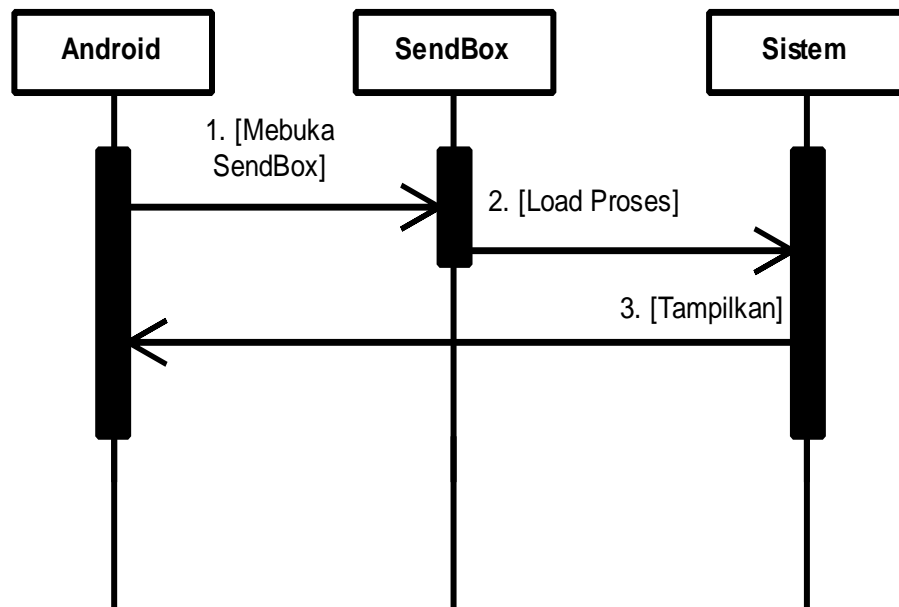
**Gambar 3.6 Sequence Diagram Mengirim Pesan**

4. *Sequence Diagram Pesan Masuk*, untuk diagram Pesan Masuk dapat dilihat pada gambar 3.7 dibawah ini.



**Gambar 3.7 Sequence Diagram Pesan Masuk**

5. *Sequence Diagram* Pesan Pesan Terkirim , untuk diagram Pesan Terkirim dapat dilihat pada gambar 3.8 berikut.

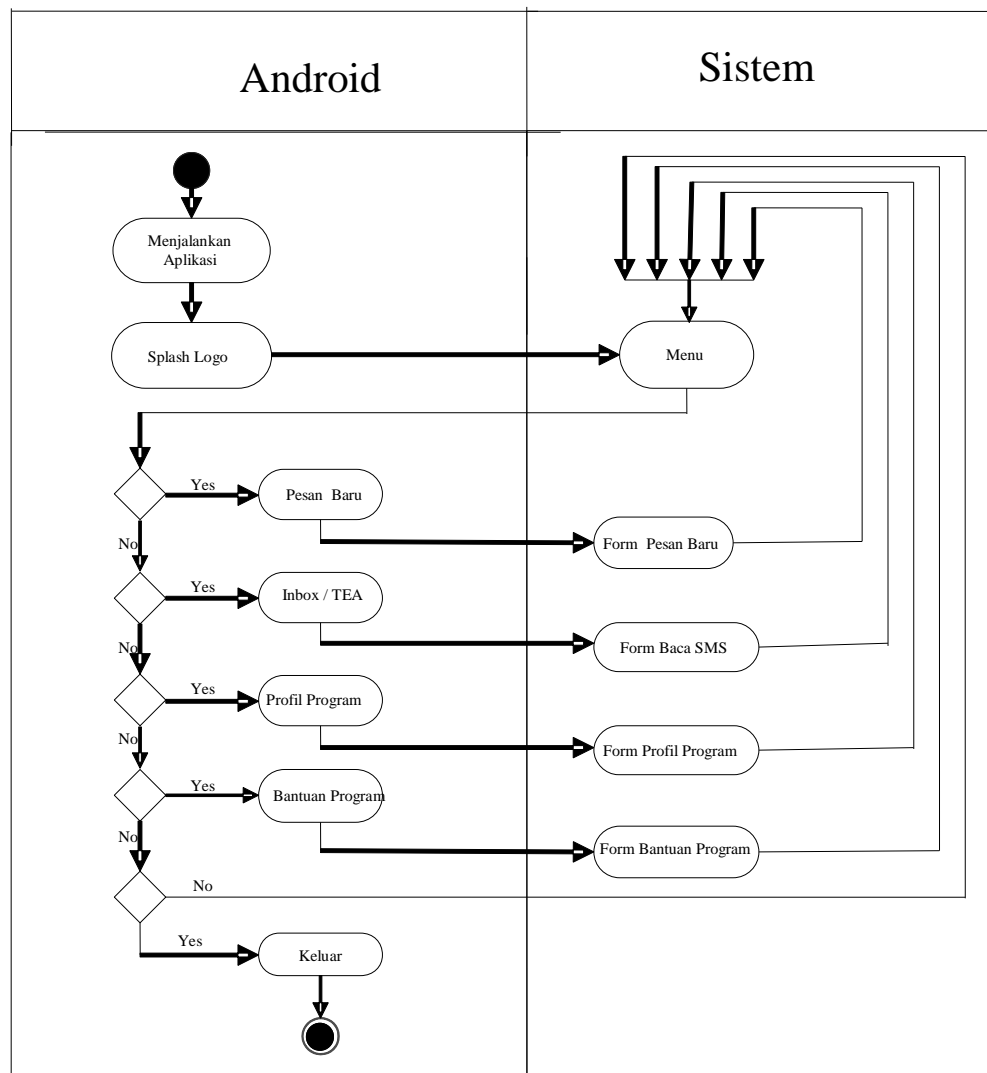


Gambar 3.8 *Sequence Diagram* Pesan Terkirim

### 3.8.3 *Activity Diagram*

*Activity Diagram* merupakan state diagram khusus, dimana sebagian besar state adalah action dan sebagian besar transisi di-*tigger* oleh selesainya state sebelumnya (*internal processing*). Oleh karena itu *activity diagram* menggambarkan behaviour internal sebuah sistem (dan interaksi antar subsistem) secara eksak, tetapi lebih menggambarkan proses-proses dan jalur0jalur aktivitaas dari level atas secara umum.

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 3.9 berikut.



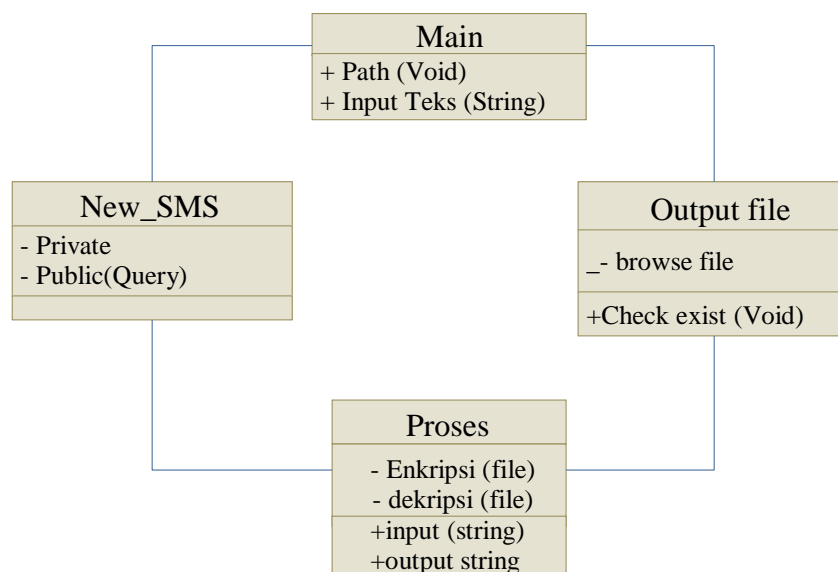
**Gambar 3.9 Activity Diagram Android**

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



### 3.8.4 Class Diagram

*Class* diagram adalah sebuah *class* yang menggambarkan struktur dan penjelasan *class*, paket, dan objek serta hubungan satu sama lain seperti *containment*, pewarisan, asosiasi, dan lain-lain. *Class* diagram juga menjelaskan hubungan antar *class* dalam sebuah sistem yang sedang dibuat dan bagaimana caranya agar mereka saling berkolaborasi untuk mencapai sebuah tujuan. *Class* diagram dari aplikasi yang dirancang dapat dilihat pada gambar 3.10 berikut.



**Gambar 3.10 Class Diagram**

### 3.9 Desain Interface

Desain *Interface* bertujuan untuk membuat interaksi pengguna sederhana dan seefisien mungkin. Bagaimana user berinteraksi dengan computer menggunakan tampilan antarmuka (*interface*) yang ada pada layar computer.

Pada rancangan aplikasi *android* terdiri dari beberapa tampilan dan menu yang dapat digunakan, rancangan tampilan yang ada pada aplikasi *android* adalah sebagai berikut.

### 3.9.1 Rancangan *Splash*

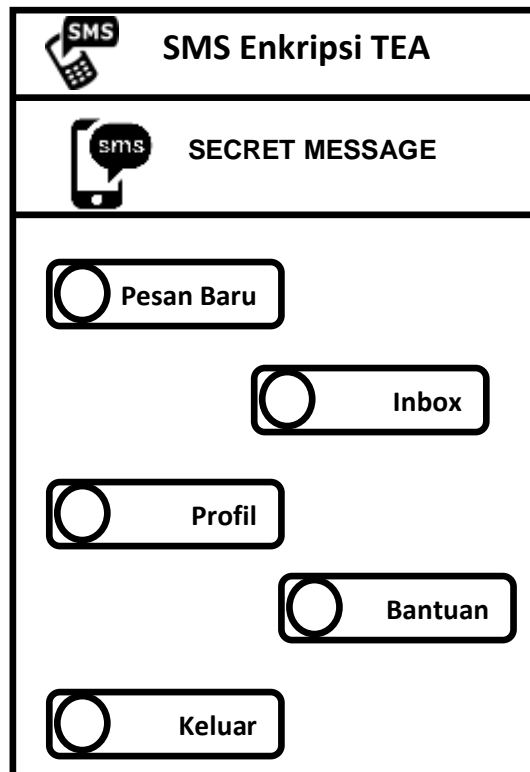
Rancangan layar *Splash* merupakan rancangan awal pembuka aplikasi, Yang dapat dilihat pada gambar 3.11 berikut.



Gambar 3.11 Rancangan *Form Splash*

### 3.9.2 Rancangan Menu

Rancangan menu adalah menu yang ada setelah pengguna masuk ke aplikasi. Yang dapat dilihat pada gambar 3.12 berikut.



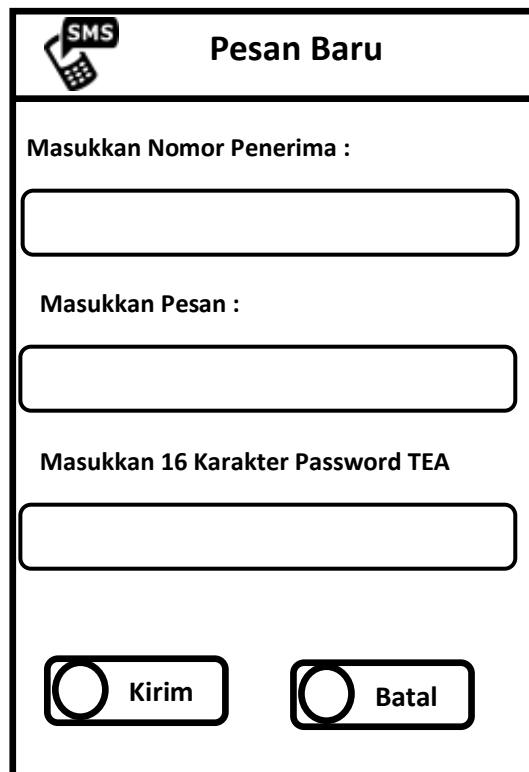
**Gambar 3.12 Rancangan Menu**

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

- a. *Pesan Baru*, merupakan menu untuk rancangan untuk membuat sms baru yaitu dengan mengetikkan text kata-kata melalui menu *new sms*.
- b. *Inbox*, merupakan menu yang digunakan untuk membuka pesan masuk dan membaca pesan masuk serta melihat pesan yang telah terkirim.
- c. *Profil*, yang merupakan menu untuk menyajikan informasi mengenai *developer* pembuat program.
- d. *Profil*, merupakan menu untuk menyajikan informasi tentang cara penggunaan aplikasi.
- e. *Exit*, untuk pengguna menutup aplikasi.

### 3.9.3 Rancangan *Pesan Baru*

*Form* ini berfungsi untuk tampilan awal pengguna sebelum masuk ke permainan. Yang dapat dilihat pada gambar 3.13 berikut.



The image shows a mobile application interface for sending a new SMS. At the top left, there is an SMS icon and the title 'Pesan Baru'. Below the title, there are three input fields: 'Masukkan Nomor Penerima:', 'Masukkan Pesan:', and 'Masukkan 16 Karakter Password TEA'. At the bottom, there are two buttons: 'Kirim' and 'Batal'.

**Gambar 3.13 Rancangan *Pesan Baru***

- Masukkan nomor penerima untuk mengirim pesan tersebut.
- Masukkan pesan adalah pesan yang akan kita kirim ke pada penerima.
- Masukkan Password yang telah kita miliki.

### 3.9.4 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 3.15 berikut.



**Gambar 3.14 Rancangan *Read SMS***

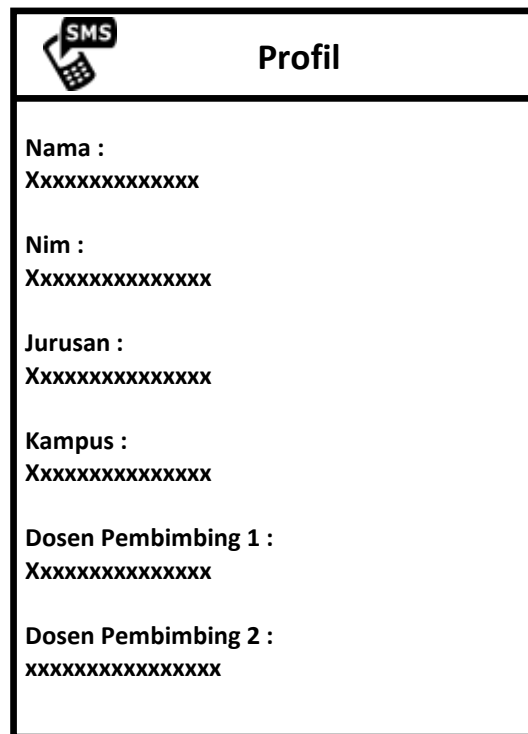
Pada gambar diatas terdapat fitur-fitur ketika pengguna menjalankan aplikasi yang diantaranya adalah sebagai berikut :

- a. *Kotak Masuk* yang digunakan untuk menampung dan menampilkan pesan masuk.
- b. *Kotak Kirim* yang berguna untuk menampung pesan terkirim .
- c. Item merupakan daftar 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.

### 3.9.5 Rancangan Form Profil

Form ini menampilkan informasi tentang penggunaan aplikasi *keamanan sms*, yang dapat dilihat pada gambar 3.15 berikut.



The image shows a form titled "Profil" with an SMS icon in the top left corner. The form contains the following fields and their corresponding placeholder text:

- Nama :  
XXXXXXXXXXXXXXXX
- Nim :  
XXXXXXXXXXXXXXXX
- Jurusan :  
XXXXXXXXXXXXXXXX
- Kampus :  
XXXXXXXXXXXXXXXX
- Dosen Pembimbing 1 :  
XXXXXXXXXXXXXXXX
- Dosen Pembimbing 2 :  
XXXXXXXXXXXXXXXX

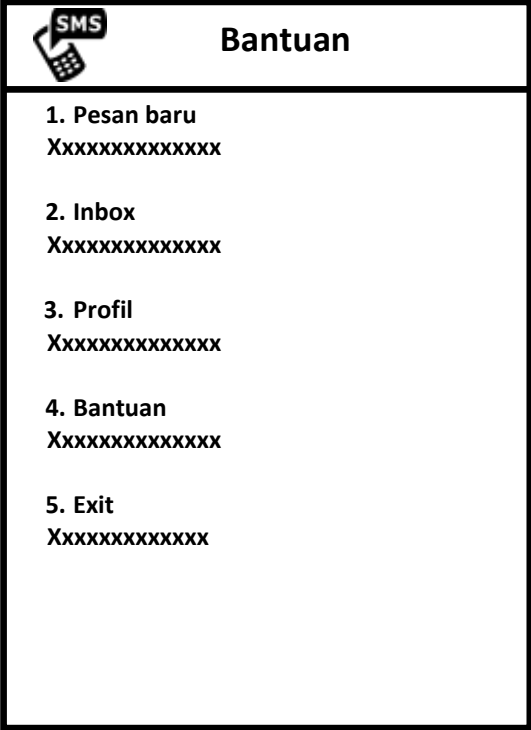
**Gambar 3.15 Rancangan Form Profil**

Di dalam form profil ini terdapat informasi mengenai:

- Nama : Asni Maisyarah Harahap
- Nim : 1514370607
- Jurusan : Sistem Komputer
- Universitas : Universitas Pembangunan Pancabudi
- Dosen pembimbing 1 : Suherman S.kom.,M.kom.
- Dosen pembimbing 2 : Akhyar Lubis S.kom.,M.kom.

### 3.9.6 Rancangan *Form Bantuan*

*Form* ini berfungsi untuk menampilkan informasi tentang cara menggunakan aplikasi keamanan sms ini, dapat dilihat pada gambar 3.16 berikut.



The image shows a wireframe for a form titled "Bantuan" (Help). At the top left, there is an icon of a mobile phone with "SMS" written above it. The title "Bantuan" is centered at the top. Below the title, there is a list of five menu items, each followed by a line of placeholder text "XXXXXXXXXXXXX":

1. Pesan baru  
XXXXXXXXXXXXX
2. Inbox  
XXXXXXXXXXXXX
3. Profil  
XXXXXXXXXXXXX
4. Bantuan  
XXXXXXXXXXXXX
5. Exit  
XXXXXXXXXXXXX

**Gambar 3.16 Rancangan *Form Bantuan***

## BAB IV

### HASIL DAN UJI COBA

#### 4.1 Hasil

Pada bab ini akan dijelaskan tampilan hasil dari aplikasi yang telah dibuat, yang digunakan untuk memperjelas tentang tampilan-tampilan yang ada pada aplikasi Keamanan SMS. Sehingga hasil implementasinya dapat dilihat sesuai dengan hasil program yang telah dibuat. Dibawah ini akan dijelaskan tiap-tiap tampilan yang ada pada program.

##### 4.1.1 Tampilan Menu *Splash*

Tampilan menu *Splash* merupakan tampilan menu pembuka atau *loading* untuk menu ke menu utama pada aplikasi. Gambar tampilan menu *Splash* ditunjukkan pada gambar 4.1. dibawah ini dan source untuk menampilkannya adalah “startActivity(new Intent("android.intent.action.MENU"));”



**Gambar 4.1 Tampilan Menu *Splash***



#### 4.1.2 Tampilan Menu Utama

Tampilan ini merupakan tampilan utama pada aplikasi yang dapat mengakses menu-menu lainnya. Pada menu ini terdapat beberapa menu yang bisa di akses diantaranya *Pesan Baru*, *Inbox*, *Profil Program*, *Bantuan Program*, *Exit Program*. Gambar tampilan Menu Utama ditunjukkan pada gambar 4.2. Dan source code untuk menampilkan menu utama adalah:

```
setContentView(R.layout.activity_main);
```



Gambar 4.2 Tampilan Menu Utama

#### 4.1.3 Tampilan Menu *Pesan Baru*

Tampilan ini merupakan tampilan akses untuk mengirim menulis sms dan mengirim sms. Untuk mengirim sms cukup meng-Klik tombol send dan secara otomatis sms akan dienkrpsi. Gambar tampilan Menu *Pesan Baru* ditunjukkan

pada gambar 4.3. dibawah ini dan source code untuk menampilkannya adalah  
“Intent it3 = new Intent(getApplicationContext(),SendSMS.class);



**Gambar 4.3 Tampilan Menu *Pesan Baru***

#### **4.1.4 Tampilan Menu *Inbox***

Tampilan ini merupakan tampilan untuk melihat *list-list* pesan masuk, pesan yang terkirim dan pesan yang tersimpan. Gambar tampilan Menu *Inbox* ditunjukkan pada gambar dibawah ini dan source code untuk menampilkannya adalah “Intent it3 = new Intent(getApplicationContext(),ReadSMS.class);



**Gambar 4.4** Tampilan Menu *Inbox*

Jika button *inbox* dipilih akan menampilkan pesan-pesan masuk yang tersimpan. Gambar tampilan Menu *Inbox* ditunjukkan pada gambar dibawah dan source code untuk menampilkannya adalah:

```
“setContentView(R.layout.activity_read);
```



**Gambar 4.5** Tampilan Menu Kotak Masuk

Jika button *Kotak Masuk* dipilih akan menampilkan pesan-pesan masuk yang tersimpan. Gambar tampilan Menu *Kotak Kirim* ditunjukkan pada gambar dibawah ini dan untuk source codenya adalah

```

“SmsManagersmsManager=SmsManager.getDefault()smsManager.sendTextMess
age(phoneNo, null, enkripsi, null, null); Toast.makeText
(getApplicationContext(), "SMS TEA Enkripsi Terkirim!", Toast
.LENGTH_LONG).show();

```



**Gambar 4.6** Tampilan Menu *Kotak Kirim*

#### 4.1.5 Pembahasan

Dalam perancangan “*Analisa dan Implementasi Tiny Encryption Algoritma (TEA) Untuk Keamanan SMS Pada Perangkat Mobile Phone*”

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

1. 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*.
2. Perangkat Keras (*Hardware*)
  - a. Komputer yang setara *Core i3*.
  - b. *Smartphone Android* dengan OS 4.1 atau di atasnya.
  - c. *Mouse, keyboard, dan Monitor*.

## **4.2 Uji Coba Sistem**

### **4.2.1 Skenario Pengujian**

Tahap ini merupakan tahap dimana akan dilakukan sebuah skenario pengujian terhadap sistem yang telah dibangun. Adapun skenario pengujian sistem yang dilakukan ialah dengan menggunakan metode pengujian sistem berupa *blackbox testing*.

Pengujian *blackbox (blackbox testing)* adalah salah satu metode pengujian perangkat lunak yang berfokus pada sisi fungsionalitas, khususnya pada input dan output aplikasi (apakah sudah sesuai dengan apa yang diharapkan atau belum). Tahap pengujian atau testing merupakan salah satu tahap yang harus ada dalam sebuah siklus pengembangan perangkat lunak (selain tahap perancangan atau

desain). Berikut pengujian sistem dengan metode *blackbox testing* yang disajikan pada tabel pengujian blackbox seperti berikut.

**Tabel 4.1 Hasil Pengujian *Black Box Testing***

<b>No</b>	<b>Skenario Pengujian</b>	<b>Test Case</b>	<b>Hasil yang diharapkan</b>	<b>Hasil Pengujian</b>	<b>Kesimpulan</b>
1	Membuka Halaman Awal Aplikasi	<i>Loading Splash</i>	Aplikasi memproses Loading Form Splash dan menuju Ke Menu Utama	Sesuai dengan yang diharapkan	<i>Valid</i>
2	Proses Enkripsi Sms	<i>Pesan Baru</i>	Ketika Sms Yang telah ditulis dan dikirim ke penerima pesan sudah di enkripsi	Sesuai dengan yang diharapkan	<i>Valid</i>
3	Menerima Pesan, Melihat Pesan, Terkirim, Simpan Pesan	Form Inbox	Aplikasi dapat menerima pesan yang dikirim melalui perangkat lain, ketika pengiriman pesan berhasil aplikasi dapat menampilkan history pesan terkirim, aplikasi dapat menyimpan pesan yang diinginkan	Sesuai dengan yang diharapkan	<i>Valid</i>

Pengujian perangkat lunak pada input dan output aplikasi (apakah sudah sesuai dengan apa yang diharapkan atau belum). Tahap uji coba salah satu tahap

yang harus ada dalam sebuah pengembangan perangkat lunak (selain tahap perancangan atau desain). Berikut hasil pengujian sistem pada tabel berikut:

**Tabel 4.2 Hasil Pengujian Sistem**

No	Plaintext	Chipertext	Key
1	Selamat Siang	AAAADRmO68vryY/XVlgBj5Mr9vk= k=	1234567891234567
2	apa kabar bro	AAAADY0ySTf4k2oKYkPkOVhKLYk= LYk=	1234567891234567
3	dimana cuy	AAAACohsvNk/p20ZvsQoSISjN/U= =	1234567890123456
4	sudah makan	AAAAC+Tn5/iA8ur3OHChf5Kzoyk= =	1234567890123456

### 4.3 Kelebihan dan Kekurangan Sistem yang dirancang

#### 4.3.1 Kelebihan Sistem

Adapun beberapa kelebihan yang dimiliki aplikasi SMS TEA ini adalah sebagai berikut :

1. Tingkat keamanan pesan terjamin sebab password yang digunakan hanya pengirim dan penerima SMS yang mengetahuinya.
2. Pengguna tidak perlu melakukan enkripsi teks pesan karena proses enkripsi secara otomatis pada saat pengguna melakukan pengiriman pesan SMS pada aplikasi ini.
3. Aplikasi SMS ini dapat dilakukan dengan *android* yang mendukung java, baik itu untuk enkripsi pesan maupun untuk deskripsi pesan yang diterima.

### 4.3.2 Kekurangan Sistem

Setiap sistem yang dibangun tentunya memiliki kekurangan, adapun kekurangan yang dimiliki sistem ini adalah :

1. Password yang digunakan pengirim harus diketahui oleh penerima SMS agar pesan SMS dapat dibuka.
2. Pada aplikasi yang telah dijalankan, dalam pengiriman SMS TEA harus memasukkan *password* sebanyak 16 digit. Apabila *password* yang dimasukkan tidak mencapai 16 digit maka aplikasi akan keluar secara otomatis.
3. Pada perancangan aplikasi, tampilan interface masih memiliki kekurangan, serta butuh perbaikan dalam mendisain sistem sehingga memudahkan para pengguna dalam pemakaiannya.
4. Melihat hasil dari aplikasi yang dijalankan hanya menggunakan *password* angka, jadi masih butuh penyempurnaan sehingga dapat menggunakan huruf juga.



## **BAB V**

### **KESIMPULAN DAN SARAN**

#### **5.1 Kesimpulan**

Dari penulisan skripsi dan perancangan aplikasi ini memiliki kesimpulan. Kesimpulan adalah hasil dari keseluruhan perancangan yang dilakukan. Dalam tahapan ini merupakan hasil dari penelitian yang dirangkum dengan beberapa kesimpulan. Penulis menyimpulkan poin-poin yang menjadi kesimpulan dalam perancangan aplikasi pengamanan SMS dengan menggunakan algoritma TEA. Adapun kesimpulan tersebut dapat dijelaskan sebagai berikut :

1. Algoritma TEA dapat diimplementasikan sebagai layanan pengamanan SMS dengan berbasis *Android* untuk layanan publik.
2. Pemrograman *Java* dapat diimplementasikan kedalam bentuk pengamanan SMS dan dapat diterapkan pada perangkat *Mobile Phone Android*.
3. Aplikasi keamanan SMS ini dapat dengan mudah digunakan oleh pengguna dengan mengikuti langkah atau prosedur yang ada pada aplikasi.

#### **5.2 Saran**

Dalam perancangan ini, penulis juga memiliki saran untuk pengembangan sistem yang dapat berguna bagi pihak yang ingin melakukan pengamanan SMS, pembaca maupun penulis dikemudian hari. Beberapa saran dan masukan yang dirasa perlu untuk dituliskan yaitu sebagai berikut:

1. Service pengiriman SMS pada aplikasi hanya bisa menggunakan layanan yang ada pada SIM Card yang terdeteksi sebagai SIM 1 atau SIM utama, sehingga pada perangkat android yang memiliki dual SIM Card atau lebih tidak dapat melakukan pemilihan kartu SIM untuk melakukan proses pengiriman pesan, sehingga sebaiknya fungsi pemilihan SIM disertakan pada pengembangan aplikasi ini selanjutnya.
2. Untuk hasil dalam perancangan hanya mencakup pengamanan SMS dengan algoritma TEA, untuk pengembangan lebih lanjut dibutuhkan pengamanan dengan algoritma yang berbeda sebagai pilihan pengguna dalam melakukan pengamanannya.
3. Untuk pengamanan data dan mencegah dari penyalahgunaan, diharapkan pengembangan lebih lanjut untuk pengamanan aplikasi dari pihak yang tidak bertanggung jawab serta diharapkan penelitian dan penulisan skripsi ini dapat menjadi masukan bagi pembaca dan penulis sendiri agar pengembangan aplikasi sejenis menghasilkan layanan pengamanan SMS yang baik untuk pihak umum.

## DAFTAR PUSTAKA

- Algoritma Simetris Tiny Encryption Algorithm Dan Loki Dalam Enkripsi Dan Dekripsi Data, Jurusan Ilmu Komputer Fmipa Unila Jurusan Matematika Fmipa Unila. Vol. 4 No. 1, 2016.
- Alicia Sinsuw, Xaverius Najoan, 2013, Prototipe Aplikasi Sistem Informasi Akademik Pada Perangkat Android, Journal Teknik Elektro Dan Komputer, Program Studi Teknik Informatika, Jurusan Teknik Elektro Fakultas Teknik Universitas Sam Ratulangi Manado, Issn : 2301-8402.
- Arif Rahman, Muhammad Khoirul, 2015, Aplikasi Enkripsi Short Message Service (Sms) Berbasis Android Menggunakan Metode Xxtea, Teknik Informatika, Universitas Darul 'Ulum Jombang, Issn On Line: 2580-6017.
- Badawi, A. (2018). Evaluasi Pengaruh Modifikasi Three Pass Protocol Terhadap Transmisi Kunci Enkripsi.
- Batubara, S., Wahyuni, S., & Hariyanto, E. (2018, September). Penerapan Metode Certainty Factor Pada Sistem Pakar Diagnosa Penyakit Dalam. In Seminar Nasional Royal (SENAR) (Vol. 1, No. 1, pp. 81-86).
- Busran, Putri Mandarani, 2012, Analisa Komputasi Enkripsi Dan Dekripsi Data Gambar, Teks Dan Audio Dengan Menggunakan Algoritma Rc4 Berbasis Visual Basic 6.0, Jurnal Teknologi Informasi & Pendidikan, Vol. 5 No. 1, Issn : 2086 – 4981.
- Dahlan Abdullah, Cut Ita Erliana, 2013, Bisnis Rental Mobil Melalui Internet (E-Commerce) Menggunakan Algoritma Sha-1 (Secure Hash Algorithm-1), Program Studi Teknik Informatika, Jurusan Teknik Industri Fakultas Teknik, Universitas Malikussaleh Reuleut, Aceh Utara, Aceh-Indonesia, Volume 10 No 4, Issn : 1979-9330.
- Defni, 2014, Enkripsi Sms (Short Message Service) Pada Telepon Selular Berbasis Android Dengan Metode Rc6, Jurnal Momentum, Dosen Jurusan Teknologi Informasi Politeknik Negeri Padang, Vol.16 No.1. Issn : 1693-752x.
- Dhany, H. W., Izhari, F., Fahmi, H., Tulus, M., & Sutarman, M. (2017, October). Encryption and decryption using password based encryption, MD5, and DES. In

- International Conference on Public Policy, Social Computing and Development 2017 (ICOPOSDev 2017) (pp. 278-283). Atlantis Press.
- Fuad, R. N., & Winata, H. N. (2017). Aplikasi Keamanan File Audio Wav (Waveform) Dengan Terapan Algoritma RSA. *InfoTekJar: Jurnal Nasional Informatika dan Teknologi Jaringan*, 1(2), 113-119.
- Hariyanto, E., & Rahim, R. (2016). Arnold's cat map algorithm in digital image encryption. *International Journal of Science and Research (IJSR)*, 5(10), 1363-1365.
- Hendra, Sukiman, 2013, Aplikasi Pengaman Pertukaran Sms Pada Perangkat Android Dengan Metode Ecdh Dan Aes, Jurusan Teknik Informatika Stmik Ibbi Medan.
- Hendrawan, J. (2018). Rancang Bangun Aplikasi Mobile Learning Tuntunan Shalat. *INTECOMS: Journal of Information Technology and Computer Science*, 1(1), 44-59.
- Khairul, K., Haryati, S., & Yusman, Y. (2018). Aplikasi Kamus Bahasa Jawa Indonesia dengan Algoritma Raita Berbasis Android. *Jurnal Teknologi Informasi dan Pendidikan*, 11(1), 1-6.
- Khandar William ; 2010, Studi Mengenai Tiny Encryption Algorithm (Tea) Dan Turunan-Turunannya (Xtea Dan Xxtea), Program Studi Teknik Informatika, Institut Teknologi Bandung.
- Kurnia, D. (2017). Analisis QoS Pada Pembagian Bandwidth Dengan Metode Layer 7 Protocol, PCQ, HTB Dan Hotspot Di SMK Swasta Al-Washliyah Pasar Senen. *CESS (Journal of Computer Engineering, System and Science)*, 2(2), 102-111.
- Mariance, U. C. (2018). Analisa dan Perancangan Media Promosi dan Pemasaran Berbasis Web Menggunakan Work System Framework (Studi Kasus di Toko Mandiri Prabot Kota Medan). *Jurnal Ilmiah Core IT: Community Research Information Technology*, 6(1).
- Pradana Marlando, Wamiliana, Rico Andrian, 2016, Analisis Perbandingan
- Putri, N. A. (2018). Sistem Pakar untuk Mengidentifikasi Kepribadian Siswa Menggunakan Metode Certainty Factor dalam Mendukung Pendekatan Guru. *INTECOMS: Journal of Information Technology and Computer Science*, 1(1), 78-90.

- Rahim, R., Aryza, S., Wibowo, P., Harahap, A. K. Z., Suleman, A. R., Sihombing, E. E., ... & Agustina, I. (2018). Prototype file transfer protocol application for LAN and Wi-Fi communication. *Int. J. Eng. Technol.*, 7(2.13), 345-347.
- Ruwaida, D., & Kurnia, D. (2018). Rancang Bangun File Transfer Protocol (FTP) dengan Pengamanan Open SSL pada Jaringan VPN Mikrotik di SMK Dwiwarna. *CESS (Journal of Computer Engineering, System and Science)*, 3(1), 45-49.
- Sarif, M. I. (2017). Penemuan Aturan yang Berkaitan dengan Pola dalam Deret Berkala (Time Series).
- Sarif, M. I. Classification Of Feasibility Of Basic Food Recipients In Kelurahan Tanjung Morawa A, Tanjung Morawa Sub-District Using Naïve Bayes Classifier Algorithm.
- Sumartono, I., Siahaan, A. P. U., & Mayasari, N. (2016). An overview of the RC4 algorithm. *IOSR J. Comput. Eng.*, 18(6), 67-73.
- Tri Puji Rahayu, Yakub, Irwan Limiady, 2012, Aplikasi Enkripsi Pesan Teks (Sms) Pada Perangkat Handphone Dengan Algoritma Caesar Cipher, Program Studi Teknik Informatika, Stmik Dharma Putra Tangerang, Issn: 2089-9815.

