



**IMPLEMENTASI APLIKASI SMS TERSANDIKAN  
DENGAN ALGORITMA AES PADA  
PLATFORM ANDROID**

**Agus Sarjuni**  
**41509010002**

UNIVERSITAS  
MERCU BUANA

**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS MERCU BUANA JAKARTA  
2013**



UNIVERSITAS  
MERCU BUANA

IMPLEMENTASI APLIKASI SMS TERSANDIKAN DENGAN ALGORITMA AES  
PADA PLATFORM ANDROID

*Laporan Tugas Akhir*

Diajukan Untuk Melengkapi Salah Satu Syarat  
Memperoleh Gelar Sarjana Komputer

Oleh: Agus

Sarjuni

41509010002

UNIVERSITAS  
MERCU BUANA

PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS ILMU KOMPUTER  
UNIVERSITAS MERCU BUANA JAKARTA  
2013

## LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

NIM : 41509010002  
Nama : Agus Sarjuni  
Judul Skripsi : Implementasi Aplikasi SMS Tersandikan Dengan Algoritma AES pada Platform Android

Menyatakan bahwa skripsi dengan judul diatas adalah hasil karya saya sendiri dan bukan plagiat kecuali kutipan-kutipan dan teori-teori yang digunakan dalam skripsi ini. Apabila ternyata ditemukan di dalam laporan skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 20 Februari 2013



UNIVERSITAS  
MERCU BUANA

## LEMBAR PENGESAHAN

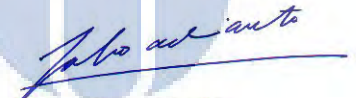
Yang bertanda tangan dibawah ini menyatakan bahwa laporan tugas akhir ini dari mahasiswa berikut ini :

Nim : 41509010002  
Nama : Agus Sarjuni  
Jurusan : Teknik Informatika  
Fakultas : Ilmu Komputer  
Judul Skripsi : Implementasi Aplikasi SMS Tersandikan Dengan Algortima AES  
Pada Platform Android

Skripsi ini telah diperiksa dan disetujui.

Jakarta, 21 Februari 2013

Menyetujui,



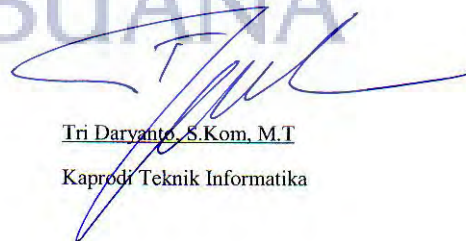
Joko Adiarto, M.Inf.Sys

Mengetahui,



Sabar Rudiarto, S.Kom, M.Kom  
Koord. Tugas Akhir Teknik Informatika

Mengesahkan,



Tri Daryanto, S.Kom, M.T  
Kaprod. Teknik Informatika

## KATA PENGANTAR

Puji syukur Alhamdulillah kehadirat Allah SWT yang telah melimpahkan segala rahmat dan karuniaNya, sehingga penulis dapat menyelesaikan laporan tugas akhir yang merupakan salah satu persyaratan untuk menyelesaikan program studi strata satu (S1) pada Jurusan Teknik Informatika Universitas Mercu Buana.

Penulis menyadari bahwa laporan tugas akhir 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 tugas akhir ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Bapak Joko Adiarto M.Inf.Sys, selaku Pembimbing Tugas Akhir pada Jurusan Teknik Informatika Universitas Mercu Buana, yang telah berkenan meluangkan waktunya serta memberi dukungan dan pengarahan hingga laporan dan aplikasi tugas akhir ini selesai.
2. Bapak Tri Daryanto, S. Kom. MT, selaku Ketua Program Studi Teknik Informatika Universitas Mercu Buana.
3. Bapak Sabar Rudiarto, S. Kom, M. Kom, selaku Koordinator Tugas Akhir pada Jurusan Teknik Informatika Universitas Mercu Buana.
4. Bapak dan Ibu tercinta yang telah mendukung penulis baik spirit maupun materi.
5. Orang tua dan Kakak tercinta yang telah mendukung penulis dalam segala hal.
6. Teman-teman yang telah bersedia berbagi ilmu, pengalaman motivasi, semangat, dan doa kepada penulis. Serta mahasiswa-mahasiswi Teknik Informatika, khususnya angkatan 2009 yang bersama-sama berjuang bersama penulis meraih gelar Strata-1 (S1).

7. Semua pihak yang tidak dapat penulis sebutkan satu persatu yang telah memberikan dorongan dan membantu serta memberikan saran baik secara langsung maupun tidak langsung kepada penulis sehingga laporan ini dapat terselesaikan.

Semoga Allah SWT membalas kebaikan dan selalu mencurahkan hidayah serta taufikNya, Amin.

Jakarta, 20 Februari 2013

Penulis



UNIVERSITAS  
MERCU BUANA

## DAFTAR ISI

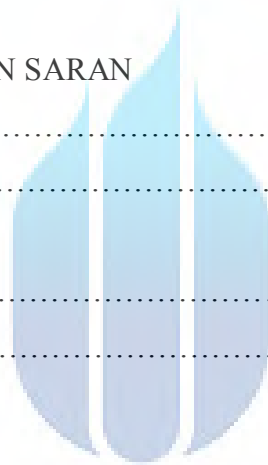
	Hal.
JUDUL	
HALAMAN JUDUL.....	i
LEMBAR PERNYATAAN.....	ii
LEMBAR PENGESAHAN.....	iii
ABSTRAK.....	iv
<i>ABSTRACT</i> .....	v
KATA PENGANTAR.....	vi
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	xii
DAFTAR TABEL.....	xv
DAFTAR ISTILAH.....	xvi
BAB I PENDAHULUAN	
1.1 Latar Belakang.....	1
1.2 Perumusan Masalah.....	2
1.3 Batasan Masalah.....	2
1.4 Tujuan dan Manfaat.....	3
1.5 Metode Penelitian.....	3
1.6 Sistematika Penulisan.....	5
BAB II LANDASAN TEORI	
2.1 SMS ( <i>Short Message Service</i> ) .....	7
2.1.1 Cara Kerja SMS.....	8
2.2 Kriptografi.....	8
2.3 Algoritma AES ( <i>Advanced Encryption Standard</i> ) .....	10

2.3.1 Deskripsi AES.....	10
2.3.2 Proses Enkripsi AES.....	11
2.3.2.1 <i>Add Roundkey</i> .....	12
2.3.2.2 <i>SubBytes</i> .....	13
2.3.2.3 <i>Shiftrows</i> .....	14
2.3.2.4 <i>MixColumns</i> .....	15
2.3.3 Proses Dekripsi AES.....	15
2.3.3.1 <i>InshifRows</i> .....	16
2.3.3.2 <i>InvSubBytes</i> .....	17
2.3.3.3 <i>InvMixColumns</i> .....	17
2.4 Bahasa Pemrograman Java.....	18
2.5 Android.....	18
2.5.1 Versi Sistem Operasi Android.....	19
2.6 Android SDK ( <i>Software Development Kit</i> ) .....	24
2.7 Eclipse.....	24
2.8 ADT ( <i>Android Development Tools</i> ) .....	25
2.9 Intent.....	25
2.10 Perangkat Lunak.....	25
2.11 UML ( <i>Unified Modelling Language</i> ) .....	27
2.11.1 <i>Use Case Diagram</i> .....	28
2.11.2 <i>Activity Diagram</i> .....	29
2.11.3 <i>Class Diagram</i> .....	30
2.11.4 <i>Sequence Diagram</i> .....	30
2.12 <i>White Box</i> .....	31
2.13 <i>Black Box</i> .....	32
<b>BAB III ANALISA DAN PERANCANGAN</b>	
3.1 Analisa Perangkat Lunak.....	33
3.2 Analisa Kebutuhan.....	33
3.3 Diagram alir Pemodelan Proses.....	34



3.3.1 Diagram alir Proses utama Aplikasi SMS AesDroid.....	34
3.3.2 Diagram alir Proses Enkripsi Algoritma AES pada 128 bit.....	35
3.3.3 Diagram alir Proses Enkripsi Algoritma AES pada 128 bit.....	36
3.4 Perancangan Sistem.....	37
3.4.1 Pemodelan <i>Use Case Diagram</i> dan Skenario.....	37
3.4.2 Pemodelan <i>Activity Diagram</i> .....	41
3.4.2.1 <i>Activity Diagram</i> untuk memilih Tab Menu SMS.....	41
3.4.2.2 <i>Activity Diagram</i> untuk memilih Tab Menu Inbox.....	43
3.4.2.3 <i>Activity Diagram</i> untuk memilih Option Menu Tentang Aplikasi.....	44
3.4.2.4 <i>Activity Diagram</i> untuk memilih Option Menu Petunjuk.....	45
3.4.2.5 <i>Activity Diagram</i> untuk memilih Option Menu Keluar.....	46
3.4.3 Pemodelan <i>Sequence Diagram</i> .....	47
3.4.3.1 <i>Sequence Diagram</i> memilih Tab Menu SMS.....	47
3.4.3.2 <i>Sequence Diagram</i> memilih Tab Menu Inbox.....	48
3.4.3.3 <i>Sequence Diagram</i> memilih Option Menu Tentang Aplikasi.....	50
3.4.3.4 <i>Sequence Diagram</i> memilih Option Menu Petunjuk.....	50
3.4.3.5 <i>Sequence Diagram</i> memilih Option Menu Keluar.....	51
3.4.4 Pemodelan Class Diagram.....	52
3.5 Perancangan Antarmuka.....	53
3.5.1 Perancangan Halaman <i>SplashScreen</i> .....	53
3.5.2 Perancangan Halaman Pengiriman SMS Enkripsi.....	54
3.5.3 Perancangan Halaman <i>Inbox</i> SMS.....	55
3.5.4 Perancangan Halaman Dekripsi SMS.....	56
3.5.5 Perancangan Option Menu.....	57
BAB IV IMPLEMENTASI DAN PENGUJIAN	
4.1 Kebutuhan Perangkat Keras dan Perangkat Lunak.....	59
4.2 Implementasi Aplikasi.....	61
4.2.1 Tampilan <i>SplashScreen</i> .....	61
4.2.2 Tampilan Tab Menu.....	62

4.2.3 Tampilan Halaman SMS Enkripsi.....	63
4.2.4 Tampilan <i>Inbox</i> SMS.....	66
4.2.5 Tampilan Dekripsi SMS.....	67
4.3 Pengujian Aplikasi.....	69
4.3.1 Pengujian <i>White Box</i> .....	69
4.3.1.1 Pengujian <i>White Box</i> pada Proses Enkripsi Pesan SMS	69
4.3.1.2 Pengujian <i>White Box</i> pada Proses Dekripsi Pesan SMS	75
4.3.2 Pengujian <i>Black Box</i> .....	82
4.3.3 Analisa Hasil.....	84
BAB V KESIMPULAN DAN SARAN	
5.1 Kesimpulan.....	85
5.2 Saran.....	86
DAFTAR PUSTAKA.....	87
LAMPIRAN.....	89



UNIVERSITAS  
**MERCU BUANA**

## DAFTAR GAMBAR

	Hal.
Gambar 2.1	Struktur pesan SMS ..... 7
Gambar 2.2	Skema sederhana cara kerja SMS ..... 8
Gambar 2.3	Diagram proses Enkripsi ..... 12
Gambar 2.4	Tabel <i>S-Box SubBytes</i> ..... 13
Gambar 2.5	Pengaruh pemetaan pada setiap <i>Bytes</i> dalam <i>State</i> ..... 14
Gambar 2.6	Transformasi <i>ShiftRows</i> ..... 14
Gambar 2.7	Ilustrasi proses Dekripsi AES ..... 16
Gambar 2.8	Transformasi <i>InvShiftRows</i> ..... 16
Gambar 2.9	Tabel <i>Inverse S-Box</i> ..... 17
Gambar 2.10	Android versi 1.1 ..... 19
Gambar 2.11	Android Cupcake ..... 20
Gambar 2.12	Android Donut ..... 21
Gambar 2.13	Android Eclair ..... 21
Gambar 2.14	Android Froyo ..... 22
Gambar 2.15	Android Gingerbread ..... 22
Gambar 2.16	Android Honeycomb ..... 23
Gambar 2.17	Android ICS ..... 23
Gambar 2.18	Android Jelly Bean ..... 24
Gambar 2.19	<i>Software Engineering Layer</i> ..... 27
Gambar 2.20	Komponen-komponen <i>Use Case Diagram</i> ..... 27
Gambar 2.21	Komponen-komponen <i>Sequence Diagram</i> ..... 27
Gambar 3.1	Diagram Alir Aplikasi SMS AesDroid ..... 34
Gambar 3.2	Diagram alir Proses Enkripsi Algoritma AES 128bit ..... 35
Gambar 3.3	Diagram alir Proses Dekripsi Algoritma AES 128bit ..... 36
Gambar 3.4	<i>Use Case Diagram</i> Aplikasi SMS AesDroid ..... 37

Gambar 3.5	<i>Activity</i> Diagram untuk memilih Tab Menu SMS .....	42
Gambar 3.6	<i>Activity</i> Diagram untuk memilih Tab Menu <i>Inbox</i> .....	43
Gambar 3.7	<i>Activity</i> Diagram untuk memilih Option Menu Tentang Aplikasi.....	44
Gambar 3.8	<i>Activity</i> Diagram untuk memilih Option Menu Petunjuk.....	45
Gambar 3.9	<i>Activity</i> Diagram untuk memilih Option Menu Keluar .....	46
Gambar 3.10	<i>Sequence</i> Diagram memilih Tab Menu SMS .....	48
Gambar 3.11	<i>Sequence</i> Diagram memilih Tab Menu <i>Inbox</i> .....	49
Gambar 3.12	<i>Sequence</i> Diagram untuk memilih Option Menu Tentang Aplikasi.....	50
Gambar 3.13	<i>Sequence</i> Diagram untuk memilih Option Menu Petunjuk.....	51
Gambar 3.14	<i>Sequence</i> Diagram untuk memilih Option Menu Keluar .....	51
Gambar 3.15	<i>Class</i> Diagram Aplikasi SMS AesDroid .....	52
Gambar 3.16	Rancangan Tampilan <i>SplashScreen</i> .....	53
Gambar 3.17	Rancangan Tampilan Pengiriman SMS Enkripsi .....	54
Gambar 3.18	Rancangan Tampilan <i>Inbox</i> SMS .....	53
Gambar 3.19	Rancangan Tampilan Dekripsi SMS.....	56
Gambar 3.20	Rancangan Tampilan Option Menu .....	53
Gambar 4.1	Tampilan <i>Splashscreen</i> .....	61
Gambar 4.2	Tampilan Tab Menu .....	62
Gambar 4.3	Tampilan Halaman Pengiriman SMS dan Hasil Enkripsi .....	65
Gambar 4.4	Tampilan Halaman <i>Inbox</i> SMS .....	66
Gambar 4.5	Tampilan Halaman Dekripsi SMS dan Hasil Pesan Dekripsi .....	68
Gambar 4.6	Grafik Alir Pseudocode Proses Enkripsi .....	73



## DAFTAR TABEL

		Hal.
Tabel 2.1	Tabel Perbandingan Jumlah <i>Round and Key</i> .....	11
Tabel 2.2	Tabel Jenis-jenis Diagram UML .....	27
Tabel 2.3	Tabel Notasi <i>Activity Diagram</i> .....	29
Tabel 3.1	Tabel Spesifikasi <i>Use Case Diagram</i> untuk memilih Tab Menu SMS.....	38
Tabel 3.2	Tabel Spesifikasi <i>Use Case Diagram</i> untuk memilih Tab Menu <i>Inbox</i> .....	39
Tabel 3.3	Tabel Spesifikasi <i>Use Case Diagram</i> untuk memilih Option Menu Tentang Aplikasi .....	40
Tabel 3.4	Tabel Spesifikasi <i>Use Case Diagram</i> untuk memilih Option Menu Petunjuk .....	40
Tabel 3.5	Tabel Spesifikasi <i>Use Case Diagram</i> untuk memilih Option Menu Keluar .....	41
Tabel 4.1	Tabel Perangkat Keras Tahap Pembangunan Aplikasi.....	59
Tabel 4.2	Tabel Perangkat Keras Tahap Implementasi.....	60
Tabel 4.3	Tabel Perangkat Lunak Tahap Pembangunan Aplikasi.....	60
Tabel 4.4	Tabel Perangkat Lunak Tahap Implementasi.....	60
Tabel 4.5	Tabel Skenario Pengujian Enkripsi pesan SMS .....	71
Tabel 4.6	Tabel Hasil Pengujian Enkripsi pesan SMS.....	72
Tabel 4.7	Tabel <i>Graph Matrik</i> Proses Enkripsi Pesan SMS .....	74
Tabel 4.8	Tabel Pengujian Dekripsi pesan SMS .....	76
Tabel 4.9	Tabel Hasil Dekripsi pesan SMS.....	77
Tabel 4.10	Tabel <i>Graph Matrik</i> Proses Dekripsi Pesan SMS .....	86
Tabel 4.11	Tabel Skenario Pengujian dan Hasil Pengujian <i>Black Box</i>	87

## DAFTAR ISTILAH

1. *Plaintext* : pesan asli sebelum dienkripsikan ( data asli).
2. *Ciphertext* : pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
3. Enkripsi : proses pengubahan plaintext menjadi *ciphertext*.
4. Dekripsi : kebalikan dari enkripsi yakni mengubah ciphertext menjadi *plaintext*, sehingga berupa data awal/asli.
5. Kriptografer : orang yang menggunakan algoritma kriptografi untuk merahasiakan pesan dan mendeskripsikannya kembali.
6. Kriptanalisis (*cryptanalysis*) : ilmu dan seni untuk memecahkan *chipertext*, berupa memperoleh *plaintext* dari *chipertext* tanpa mengetahui kuncinya. Pelakunya disebut kriptanalisis.
7. Kriptologi (*cryptology*) : studi mengenai kriptografi dan kriptanalisis.
8. Penyadap (*eavesdropper*) : orang yang mencoba menangkap pesan selama ditransmisikan. Penyadap sama dengan *enemy*(musuh), *interceptor*(pencegat), *attecker*(penyerang).
9. Pesan, dapat berupa data maupun informasi yang dikirim melalui kurir, media komunikasi data, atau yang disimpan didalam media perekaman.
10. *Man-in-the-middle Attack* : menyadap komunikasi data rahasia.
11. *Chiper* : aturan untuk enkripsi dan dekripsi, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi.
12. Kunci (*key*) : parameter yang digunakan untuk transformasi enkripsi dan dekripsi.
13. *Encoding* : transformasi dari plainteks menjadi kode.
14. *Decoding* : transformasi dari kode menjadi plainteks.
15. *Pseudocode*: deskripsi dari algoritma pemrograman computer yang menggunakan struktur sederhana dari beberapa bahasa pemograman tetapi bahasa tersebut hanya ditujukan agar dapat dibaca manusia.

16. *Flowgraph*: Kontrol aliran program yang direpresentasikan menggunakan representasi grafis. Flowgraph terdiri dari sekumpulan *node* dan *edge*.
17. *Independent path*: jalur dalam program yang menunjukkan paling sedikit satu kumpulan proses ataupun kondisi baru.

