



**Integrasi Algoritma AES Untuk Mengamankan Data pada
Aplikasi SMS Gateway Berbasis Android Smartphone**



Oleh:

UNIVERSITAS
Wishnu Hadi Wicaksono

41505010069

MERCU BUANA

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



**Integrasi Algoritma AES Untuk Mengamankan Data pada
Aplikasi SMS Gateway Berbasis Android Smartphone**

Laporan Tugas Akhir

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

UNIVERSITAS
MERCU BUANA

Oleh:

Wishnu Hadi Wicaksono

41505010069

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

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NIM : 41505010069

Nama : Wishnu Hadi Wicaksono

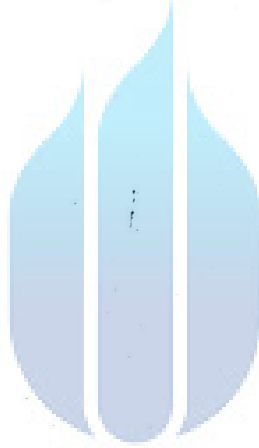
Judul Skripsi : Integrasi Algoritma AES Untuk Mengamankan Data pada
Aplikasi SMS Gateway Berbasis Android *Smartphone*.

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

Jakarta, 10 September 2013



(Wishnu Hadi Wicaksono)



UNIVERSITAS
MERCU BUANA

LEMBAR PENGESAHAN


Yang bertanda tangan di bawah ini menyatakan bahwa Laporan Tugas

Akhir dari mahasiswa berikut ini:

NIM : 41505010069
Nama : Wishnu Hadi Wicaksono
Jurusan : Teknik Informatika
Fakultas : Ilmu Komputer
Judul Skripsi : Integrasi Algoritma AES Untuk Mengamankan Data pada
Aplikasi SMS Gateway Berbasis Android Smartphone.

Telah disetujui untuk disahkan sebagai Laporan Tugas Akhir.

Jakarta, 10 September 2013



Abdi Wahab, S.Kom., MT
Pembimbing



Sabar Rudiarto, S.Kom., M.Kom

Koord. Tugas Akhir Teknik Informatika



Tri Daryanto, S.Kom., MT
KaProdi Teknik Informatika

UNIVERSITAS
MERCU BUANA

KATA PENGANTAR

Alhamdulillah, puji syukur kehadiran Allah SWT. Karena dengan anugerah yang telah diberikan sehingga tugas akhir ini berhasil diselesaikan dengan semaksimal mungkin, walaupun masih jauh dari nilai sempurna. Karena semua yang sempurna hanyalah milik Allah SWT.

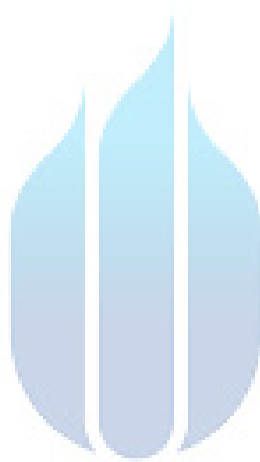
Selama pembuatan tugas akhir ini tidak sedikit bantuan yang didapatkan dari berbagai pihak. Oleh karena itu, dalam kesempatan ini dengan segala kerendahan hati ingin menyampaikan terima kasih yang sebesar-besarnya kepada :

1. Bapak Tri Daryanto, S.Kom., MT selaku KaProdi Teknik Informatika Universitas Mercu Buana Jakarta.
2. Bapak Abdi Wahab, S.Kom., MT selaku pembimbing tugas akhir yang sangat sabar dalam membimbing dan banyak membantu dalam pengerjaan tugas akhir ini.
3. Bapak Sabar Rudiarto, S.Kom., M.Kom selaku Koordinator Tugas Akhir Teknik Informatika Jakarta.
4. Seluruh Dosen Pengajar pada Jurusan Teknik Informatika yang tidak dapat disebutkan satu per satu.
5. Kedua orang tua saya yang selalu memberikan doa dan semangatnya.

Laporan tugas akhir ini masih jauh dari sempurna, oleh karena itu kritik dan saran yang sifatnya membangun sangat diperlukan untuk memperbaiki mutu penelitian selanjutnya.

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

Jakarta, Agustus 2013



(Wishnu Hadi Wicaksono)

UNIVERSITAS
MERCU BUANA

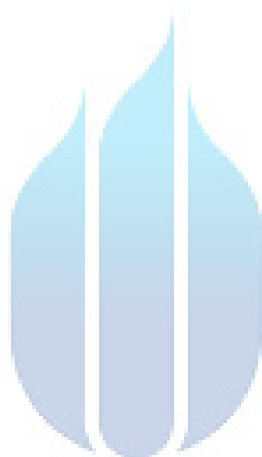
DAFTAR ISI

JUDUL LUAR	i
JUDUL DALAM	ii
LEMBAR PERNYATAAN	iii
LEMBAR PENGESAHAN	iv
KATA PENGANTAR	v
ABSTRAK	vii
ABSTRACT	viii
DAFTAR ISI	ix
DAFTAR GAMBAR	xiv
DAFTAR TABEL	xiv
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	3
1.3 Maksud dan Tujuan	3
1.4 Batasan Masalah	3
1.5 Metodologi Penelitian	4
1.5.1 Metode Penelitian	4
1.6 Diagram Alir Penelitian	6
1.7 Sistematika Penulisan	7
BAB II LANDASAN TEORI	9
2.1 Pengertian <i>Short Messaging Service</i> (SMS)	9

2.1.1	<i>Concatenated SMS Message / Long SMS Message</i>	10
2.1.2	SMS Center (SMSC).....	10
2.2	SMS Gateway.....	11
2.2.1	<i>Client Server SMS Gateway</i>	12
2.2.2	Cara Kerja <i>Client Server</i>	13
2.3	Pengertian Balita	14
2.3.1	Klarifikasi Perkembangan Balita	14
2.3.2	Pengertian Berat Badan Balita	16
2.4	Gammu	16
2.5	Kriptografi	16
2.5.1	Pengertian Algoritma	21
2.5.2	Algoritma Berdasarkan Jenis Kunci	22
2.5.2.1	Algoritma Simetris	22
2.5.2.2	Algoritma Asimetris	23
2.5.3	Algoritma Berdasarkan Mode Bit	25
2.5.3.1	Algoritma Block Cipher	25
2.5.3.1.1	<i>Electronic Code Book (ECB)</i>	25
2.5.3.1.2	<i>Chiper Block Chaining (CBC)</i>	26
2.5.3.1.3	<i>Chiper Feed Back (CFB)</i>	28
2.5.3.1.4	<i>Output Feed Back (OFB)</i>	29
2.5.3.2	Algoritma Stream Chiper	30
2.5.3.2.1	<i>Synchronous Stream Chiper</i>	31
2.5.3.2.2	<i>Self-Synchronous Stream Chiper</i>	32
2.6	Android.....	32

2.6.1	Fitur-fitur yang terdapat pada Android	33
2.6.2	Arsitektur Android	33
2.6.3	Daur Hidup Dari Aktivitas Aplikasi Di Android	34
2.7	AES (<i>Advance Encryption Standard</i>).....	36
2.7.1	Algoritma AES (<i>Advance Encryption Standard</i>).....	37
2.7.2	Putaran Proses Enkripsi dan Deskripsi	37
2.8	Pemrograman Java	39
2.9	JCE (<i>Java Cryptography Extension</i>).....	40
2.10	Layanan Keamanan (<i>Security Services</i>)	41
2.11	Metode Pengujian <i>Black Box</i>	43
2.12	Yii <i>Framework</i>	44
2.13	PHP.....	45
2.13.1	Sejarah PHP	45
2.13.2	Syarat Untuk Menjalankan PHP	46
2.13.3	Contoh Script PHP	46
2.14	<i>Database MySQL</i>	47
BAB III ANALISA DAN PERANCANGAN		51
3.1	Analisa Sistem	51
3.1.1	Deskripsi Sistem	51
3.1.2	Analisa Kebutuhan	53
3.1.2.1	Kebutuhan Awal.....	54
3.2	Perancangan Sistem.....	55
3.3	Integrasi Aplikasi SMS dengan Modul Enkripsi.....	57
3.4	Perancangan Basis Data	59

3.5	Perancangan Antarmuka.....	60
3.6	Skenario Pengujian.....	61
3.6.1	Pengujian <i>Black Box</i>	62
3.6.2	Layanan Keamanan (<i>Security Services</i>).....	63
BAB IV IMPLEMENTASI DAN PENGUJIAN.....		64
4.1	Ruang Lingkup Pendukung Implementasi	64
4.1.1	Ruang Lingkup Perangkat Keras	64
4.1.2	Ruang Lingkup Perangkat Lunak.....	65
4.2	Implementasi Basis Data	65
4.3	Implementasi Antarmuka	66
4.3.1	Icon Aplikasi	66
4.3.2	Form Input.....	67
4.3.3	Aplikasi <i>Client Server</i>	67
4.4	Implementasi Sistem	68
4.4.1	Implementasi Aplikasi SMS Gateway	69
4.4.1.1	Tahapan Enkripsi Data	69
4.4.1.2	Tahapan Kirim Data	69
4.4.1.3	Tahapan Dekripsi Data	71
4.5	Hasil Pengujian Menggunakan <i>Black Box</i>	72
4.6	Hasil Pengujian Menggunakan Layanan Keamanan (<i>Security Services</i>).....	72
4.7	Hasil Pengujian Data yang Terenkripsi dan Terdekripsi.....	73
BAB V KESIMPULAN DAN SARAN.....		74
5.1	Kesimpulan.....	74
5.2	Saran.....	74



UNIVERSITAS
MERCU BUANA

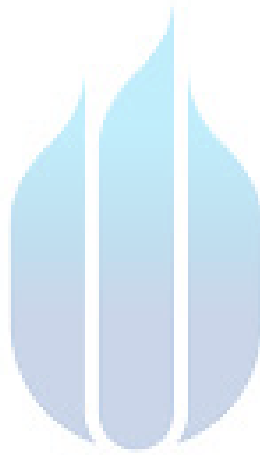
DAFTAR GAMBAR

Gambar 1.5.1 Linear Sequential Model	6
Gambar 1.6.1 Diagram Alir Penelitian	7
Gambar 2.1.1 Cara Kerja SMS	11
Gambar 2.2.1 Cara Kerja SMS <i>Gateway</i>	11
Gambar 2.2.2 Konsep Pengembangan SMS <i>Gateway</i>	12
Gambar 2.5.1 Skema Enkripsi dan Dekripsi	20
Gambar 2.5.2 Diagram Proses Enkripsi dan Dekripsi Algoritma Simetris	22
Gambar 2.5.3 Diagram Proses Enkripsi dan Dekripsi Algoritma Asimetris	24
Gambar 2.5.4 Skema Mode Operasi ECB	26
Gambar 2.5.5 Skema Mode CBC	27
Gambar 2.5.6 Skema Mode Operasi CFB	29
Gambar 2.5.7 Skema Mode Operasi OFB	30
Gambar 2.6.1 Arsitektur Android	34
Gambar 2.6.2 Daur Hidup Aktifitas Android	35
Gambar 2.7.1 Diagram Proses Enkripsi	38
Gambar 2.7.2 Diagram Proses Dekripsi	38
Gambar 2.11.1 <i>Black Box Testing</i>	44
Gambar 3.1.1 <i>Usecase</i> Diagram Aplikasi SMS	52
Gambar 3.1.2 <i>Usecase</i> Diagram Aplikasi <i>Client Server</i>	53
Gambar 3.2.1 <i>Usecase</i> Diagram Pengguna	56
Gambar 3.2.2 Diagram <i>Activity</i> Rancangan Sistem	56
Gambar 3.2.3 <i>Sequence</i> Diagram Rancangan Sistem	57

Gambar 3.3.1 Proses Integrasi JCE dengan Aplikasi SMS.....	58
Gambar 3.3.2 Diagram <i>Activity</i> Enkripsi	59
Gambar 3.5.1 Perancangan Antarmuka Aplikasi SMS	61
Gambar 4.2.1 Implementasi Tabel Inbox.....	65
Gambar 4.2.2 Implementasi Tabel Balita	66
Gambar 4.3.1 Icon Aplikasi SMS Gateway	66
Gambar 4.3.2 Form Input Aplikasi SMS Gateway	67
Gambar 4.3.3 Halaman Awal.....	67
Gambar 4.3.4 Menu Inbox	68
Gambar 4.3.5 Menu Balita	68
Gambar 4.7.1 Data yang Terenkripsi	73
Gambar 4.7.2 Data yang Terdekripsi	73

DAFTAR TABEL

Tabel 1 Jumlah Putaran Pengoperasian AES	37
Tabel 2 Tabel Inbox	60
Tabel 3 Tabel Balita	60
Tabel 4 Skenario Pengujian Keamanan Menggunakan <i>Data Confidentiality</i>	63
Tabel 5 Hasil Pengujian <i>Black Box</i>	72
Tabel 6 Hasil Pengujian Menggunakan <i>Data Confidentiality</i>	72



UNIVERSITAS
MERCU BUANA