



**PENGAMANAN SMS PADA TELEPON SELULER BERBASIS  
ANDROID MENGGUNAKAN ALGORITMA TRIPLE DES**

**M. Rival Suheri**

**41509010105**

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



**PENGAMANAN SMS PADA TELEPON SELULER BERBASIS ANDROID  
MENGGUNAKAN ALGORITMA TRIPLE DES**

*Laporan Tugas Akhir*

Diajukan Untuk Melengkapi Salah Satu Syarat  
Memperoleh Gelar Sarjana Komputer

Oleh:

M. Rival Suheri

41509010105

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

## **LEMBAR PERNYATAAN**

Yang bertanda tangan dibawah ini :

NIM : 41509010105

Nama : M. Rival Suheri

Judul Skripsi : Pengamanan SMS pada Telepon Seluler Berbasis Android

Menggunakan Algoritma Triple DES

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 didalam laporan skripsi saya terdapat unsur plagiat, maka saya siap untuk mendapatkan sanksi akademik yang terkait dengan hal tersebut.

Jakarta, 4 Mei 2013



M. Rival Suheri

## LEMBAR PERSETUJUAN

NIM : 41509010105  
Nama : M. Rival Suheri  
Jurusan : Teknik Informatika  
Fakultas : Ilmu Komputer  
Judul Skripsi : Pengamanan SMS pada Telepon Seluler Berbasis Android  
Menggunakan Algoritma Triple DES

Skripsi ini telah diperiksa dan disetujui

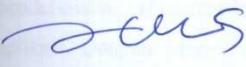
Jakarta, 4 Mei 2013

Menyetujui,

  
Raka Yusuf, S.T., M.TI

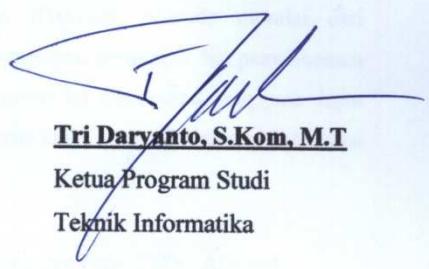
Pembimbing

Mengetahui,

  
Sabar Rudiarto, S.Kom, M.Kom

Koordinator Tugas Akhir  
Teknik Informatika

Mengesahkan,

  
Tri Daryanto, S.Kom, M.T

Ketua Program Studi  
Teknik Informatika

## **KATA PENGANTAR**

Puji syukur penulis panjatkan atas kehadirat Allah SWT, karena berkat rahmat dan karunia-Nya sehingga Tugas Akhir ini dapat terselesaikan dengan baik. Laporan tugas akhir yang berjudul "Pengamanan SMS pada Telepon Seluler Berbasis Android Menggunakan Algoritma Triple DES" ini diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu (S-1) pada Program Studi Teknik Informatika Universitas Mercu Buana. Penulis juga mengucapkan terima kasih kepada semua pihak yang telah membantu penulis sehingga laporan tugas akhir ini dapat tersusun dengan baik. Untuk itu penulis ingin mengucapkan terima kasih kepada :

1. Bapak Raka Yusuf, S.T., M.TI., selaku Pembimbing Tugas Akhir yang telah membimbing, membantu, dan memberikan saran-sarannya kepada penulis dalam menyelesaikan tugas akhir ini.
2. Bapak Tri Daryanto, S.Kom, M.T., 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. Seluruh dosen Fakultas Ilmu Komputer yang ikut memberikan semangat dan telah memberikan banyak ilmunya kepada penulis.
5. Bapak, Ibu, dan adik-adik penulis. Terima kasih atas pengorbanannya selama ini. Atas jerih payah kalian, penulis dapat merasakan dan menyelesaikan perkuliahan dengan baik. Serta selalu memberikan doa dan dukungannya yang begitu besar kepada penulis. Kasih sayang dan perjuangan kalian yang membuat penulis menjadi selalu bersemangat dikala penulis menemui keputusasaan dalam berbagai hal.
6. Keluarga Asisten Laboratorium Fakultas Ilmu Komputer. Terima kasih atas dukungan dan doanya kepada penulis sehingga dapat menyelesaikan tugas akhir ini.
7. Teman-teman seperjuangan, seluruh mahasiswa Teknik Informatika angkatan 2009 Universitas Mercu Buana yang telah memberikan semangat kepada penulis dalam menyelesaikan tugas akhir ini.

8. Beserta semua pihak yang tidak dapat penulis sebutkan satu persatu yang telah memberikan semangat dan membantu secara langsung maupun tidak langsung kepada penulis sehingga laporan ini dapat terselesaikan.

Semoga Allah SWT membalas seluruh kebaikan dan selalu mencerahkan rahmat dan hidayah-Nya. Penulis menyadari sepenuhnya bahwa laporan tugas akhir ini masih jauh dari sempurna. Untuk itu, penulis mohon maaf apabila masih banyak kekurangan dalam penyusunan laporan tugas akhir ini. Semoga laporan tugas akhir ini dapat bermanfaat bagi semua pihak yang membutuhkannya. Aamiin.

Jakarta, 4 Mei 2013

M. Rival Suheri

## DAFTAR ISI

	hal
Judul	
Halaman Judul	
Lembar Pernyataan .....	iii
Lembar Persetujuan .....	iv
Kata Pengantar .....	v
Abstrak .....	vii
Abstract .....	viii
Daftar Isi.....	ix
Daftar Gambar.....	xiii
Daftar Tabel .....	xv
Daftar Kode.....	xvi
<b>BAB I PENDAHULUAN</b>	
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah .....	2
1.3 Tujuan dan Manfaat.....	3
1.4 Batasan Masalah .....	3
1.5 Metode Penelitian .....	4
1.6 Sistematika Penulisan.....	5
<b>BAB II LANDASAN TEORI</b>	
2.1 Kriptografi .....	7
2.1.1 Kriptografi Klasik .....	8
2.1.2 Kriptografi Modern .....	9
2.1.3 Rangkaian Bit dan Operasinya pada Kriptografi Modern.....	9
2.2 Algoritma dan Kunci.....	10
2.2.1 Algoritma Kunci-Simetris.....	11
2.2.1.1 Chiper Aliran ( <i>Stream Chiper</i> ).....	11
2.2.1.2 Chiper Blok ( <i>Block Chiper</i> ) .....	12
2.2.2 Algoritma Kunci-Asimetris.....	14

2.3 Mode Operasi Chiper Blok .....	15
2.3.1 Electronic Code Book (ECB).....	15
2.3.2 Chiper Block Chaining (CBC) .....	16
2.4 Triple DES .....	18
2.4.1 DES .....	19
2.4.2 Proses Kunci .....	21
2.4.3 Proses Enkripsi .....	23
2.4.4 Proses Dekripsi .....	26
2.5 Fungsi Hash.....	27
2.5.1 Fungsi Hash Satu-Arah ( <i>One-way Hash</i> ).....	28
2.6 Short Messages Service (SMS).....	28
2.7 Java.....	29
2.8 Extensible Markup Language (XML) .....	29
2.9 Eclipse .....	30
2.10 Eclipse Plug-in .....	32
2.10.1 Android Development Tools (ADT).....	32
2.11 Android .....	33
2.11.1 Arsitektur Perangkat Lunak Android .....	33
2.11.2 Komponen Dasar Aplikasi Android.....	35
2.11.2.1 Activity.....	35
2.11.2.2 Intent .....	37
2.11.2.3 Service.....	37
2.11.2.4 Content Provider .....	37
2.11.3 Android Manifest .....	38
2.12 Resources pada Android .....	38
2.13 Rekayasa Perangkat Lunak .....	39
2.13.1 Metodologi Rekayasa Perangkat Lunak.....	40
2.14 Unified Modelling Language .....	42
2.14.1 Diagram <i>Use Case</i> .....	45
2.14.2 Diagram Aktivitas ( <i>Activity Diagram</i> ).....	46
2.14.3 Diagram Kelas ( <i>Class Diagram</i> ).....	47
2.14.4 Diagram <i>Sequence</i> ( <i>Sequence Diagram</i> ) .....	49

2.15 Pengujian <i>Black-Box</i> .....	50
---------------------------------------	----

### **BAB III ANALISIS DAN PERANCANGAN**

3.1 Analisis Kebutuhan .....	51
3.2 Analisis Struktur Pesan SMS .....	52
3.3 Analisis Sistem.....	53
3.4 Analisis Efek pada Sistem.....	55
3.5 Analisis Proses Encoding Array Byte ke String Heksadesimal .....	56
3.6 Analisis Algoritma .....	58
3.7 Pemodelan <i>Use Case Diagram</i> .....	59
3.8 Perancangan Sistem .....	62
3.8.1 Tujuan Perancangan Sistem .....	62
3.8.2 Pemodelan <i>Activity Diagram</i> .....	62
3.8.3 Pemodelan <i>Class Diagram</i> .....	67
3.8.4 Pemodelan <i>Sequence Diagram</i> .....	69
3.8.4.1 <i>Sequence Diagram</i> membuat pesan baru .....	69
3.8.4.2 <i>Sequence Diagram</i> melihat pesan masuk.....	70
3.8.4.3 <i>Sequence Diagram</i> memilih menu pengaturan bahasa .....	71
3.8.4.4 <i>Sequence Diagram</i> melihat tentang aplikasi .....	72
3.8.4.5 <i>Sequence Diagram</i> memilih option menu bantuan .....	73
3.9 Perancangan Antarmuka Pengguna .....	74
3.9.1 Antarmuka halaman Utama.....	74
3.9.2 Antarmuka halaman Buat pesan baru .....	75
3.9.3 Antarmuka halaman Kotak masuk .....	75
3.9.4 Antarmuka halaman Pengaturan .....	76
3.9.5 Antarmuka halaman Tentang .....	77
3.9.6 Antarmuka halaman menu Bantuan .....	78

### **BAB IV IMPLEMENTASI DAN PENGUJIAN**

4.1 Implementasi Program dan Antarmuka.....	79
4.1.1 Menampilkan Menu Utama .....	79
4.1.2 Mengenkripsi dan Mengirim Pesan .....	83
4.1.3 Mendekripsi dan Menampilkan Pesan .....	91
4.1.4 Mengganti Bahasa Antarmuka Aplikasi .....	97

4.2 Pengujian Aplikasi.....	102
4.2.1 Lingkungan Pengujian .....	102
4.2.2 Skenario Pengujian Aplikasi.....	103
4.2.3 Pengujian Enkripsi dan Dekripsi.....	104
4.2.4 Pengujian Keamanan Pesan .....	106
4.2.5 Dokumen Hasil Pengujian Aplikasi.....	110
4.2.6 Analisis Hasil Pengujian .....	112

## **BAB V PENUTUP**

5.1 Kesimpulan.....	113
5.2 Saran .....	114

## **DAFTAR PUSTAKA**

## **LAMPIRAN**

## DAFTAR GAMBAR

hal

Gambar 2.1 Proses enkripsi dan dekripsi .....	11
Gambar 2.2 Skema algoritma kunci simetris .....	11
Gambar 2.3 Skema enkripsi dan dekripsi pada cipher blok.....	13
Gambar 2.4 Skema algoritma kunci asimetris .....	14
Gambar 2.5 Mode electronic code book (ECB).....	16
Gambar 2.6 Mode cipher block chaining (CBC) .....	17
Gambar 2.7 Jaringan <i>Feistel</i> untuk satu putaran.....	19
Gambar 2.8 Skema jaringan <i>Feistel</i> algoritma enkripsi DES secara keseluruhan .....	20
Gambar 2.9 Proses pembangkitan kunci kunci internal.....	22
Gambar 2.10 Rincian komputasi fungsi $f$ .....	23
Gambar 2.11 Skema algoritma Triple DES .....	25
Gambar 2.12 Skema cara kerja SMS .....	28
Gambar 2.13 Arsitektur dari eclipse .....	30
Gambar 2.14 Arsitektur dari perangkat lunak sistem android .....	34
Gambar 2.15 Siklus hidup dari sebuah activity .....	36
Gambar 2.16 Contoh sederhana AndroidManifest.xml .....	38
Gambar 2.17 Model <i>waterfall</i> .....	40
Gambar 2.18 Hirarki diagram pada UML.....	44
Gambar 3.1 Struktur pesan SMS.....	52
Gambar 3.2 Arsitektur sistem .....	54
Gambar 3.3 Diagram Alir Algoritma DES .....	58
Gambar 3.4 Use case diagram aplikasi Crypto Messenger.....	59
Gambar 3.5 Activity diagram untuk membuat pesan baru .....	63
Gambar 3.6 Activity diagram untuk melihat pesan masuk .....	64
Gambar 3.7 Activity diagram untuk memilih menu pengaturan bahasa.....	65
Gambar 3.8 Activity diagram untuk melihat tentang aplikasi .....	66
Gambar 3.9 Activity diagram untuk memilih option menu bantuan .....	66

Gambar 3.10 Class diagram aplikasi Crypto Messenger .....	67
Gambar 3.11 Sequence diagram membuat pesan baru .....	70
Gambar 3.12 Sequence diagram melihat pesan masuk.....	71
Gambar 3.13 Sequence diagram memilih menu pengaturan bahasa.....	72
Gambar 3.14 Sequence diagram melihat tentang aplikasi .....	73
Gambar 3.15 Sequence diagram memilih option menu bantuan .....	73
Gambar 3.16 Rancangan antarmuka halaman Utama .....	74
Gambar 3.17 Rancangan antarmuka halaman Buat pesan baru.....	75
Gambar 3.18 Rancangan antarmuka halaman Kotak masuk .....	76
Gambar 3.19 Dialog dekripsi pesan .....	76
Gambar 3.20 Rancangan antarmuka halaman Pengaturan.....	77
Gambar 3.21 Rancangan antarmuka halaman Tentang.....	77
Gambar 3.22 Rancangan antarmuka halaman Bantuan .....	78
Gambar 4.1 Tampilan antarmuka halaman menu Utama .....	80
Gambar 4.2 Tampilan antarmuka halaman Buat pesan baru .....	84
Gambar 4.3 Tampilan kotak dialog halaman kotak masuk dan hasil dekripsi.....	92
Gambar 4.4 Tampilan pesan kesalahan.....	95
Gambar 4.5 Tampilan menu pilihan bahasa.....	99
Gambar 4.6 Tampilan program John the Ripper.....	107
Gambar 4.7 Hasil dari percobaan <i>brute force</i> menggunakan John the Ripper ....	107
Gambar 4.8 Tampilan kotak dialog ketika membuka program Hashcat.....	108
Gambar 4.9 Tampilan program Hashcat .....	108
Gambar 4.10 Hasil dari percobaan <i>brute force</i> menggunakan Hashcat .....	109

## **DAFTAR TABEL**

hal

Tabel 2.1 Jumlah pergeseran bit pada setiap putaran.....	21
Tabel 2.2 Mode enkripsi dan dekripsi Triple DES .....	27
Tabel 2.3 Notasi diagram Use Case .....	45
Tabel 2.4 Notasi diagram aktifitas .....	46
Tabel 2.5 Notasi diagram kelas .....	48
Tabel 2.6 Notasi diagram <i>sequence</i> .....	49
Tabel 3.1 Spesifikasi skenario use case membuat pesan baru .....	60
Tabel 3.2 Spesifikasi skenario use case melihat pesan masuk.....	60
Tabel 3.3 Spesifikasi skenario use case memilih menu pengaturan bahasa .....	61
Tabel 3.4 Spesifikasi skenario use case melihat tentang aplikasi .....	61
Tabel 3.5 Spesifikasi skenario use case memilih option menu bantuan .....	62
Tabel 4.1 Skenario pengujian <i>Black-Box</i> pada aplikasi .....	103
Tabel 4.2 Pengujian enkripsi pesan.....	104
Tabel 4.3 Pengujian dekripsi pesan.....	105
Tabel 4.4 Dokumen hasil pengujian <i>Black-Box</i> pada aplikasi.....	110

## DAFTAR KODE

hal

Kode 3.1 Konversi array byte ke string heksadesimal.....	57
Kode 4.1 Menampilkan halaman utama.....	79
Kode 4.2 <i>ScrollView</i> pada halaman utama .....	80
Kode 4.3 <i>LinearLayout</i> pada halaman utama .....	81
Kode 4.4 Beberapa <i>item</i> pada halaman utama .....	81
Kode 4.5 Kode program untuk tombol Buat pesan baru.....	81
Kode 4.6 Kode program untuk tombol Kotak masuk .....	82
Kode 4.7 Kode program untuk tombol Pengaturan .....	82
Kode 4.8 Menampilkan halaman Buat pesan baru.....	83
Kode 4.9 <i>RelativeLayout</i> pada halaman Buat pesan baru .....	84
Kode 4.10 Kotak input untuk memasukkan nomor telepon.....	84
Kode 4.11 Kotak input untuk memasukkan kunci .....	85
Kode 4.12 Kotak input untuk mengisi pesan .....	85
Kode 4.13 Mengenkripsi dan mengirimkan pesan.....	85
Kode 4.14 Mendeklarasikan sebuah <i>StringBuilder</i> .....	86
Kode 4.15 Mendeklarasikan kunci pertama.....	87
Kode 4.16 Mendeklarasikan kunci kedua .....	87
Kode 4.17 Metode MD5 pada kelas Triple DES .....	88
Kode 4.18 Mendeklarasikan kunci ketiga .....	88
Kode 4.19 Mendeklarasikan algoritma Triple DES .....	89
Kode 4.20 Mode operasi Enkripsi-Dekripsi-Enkripsi pada kelas Triple DES.....	91
Kode 4.21 Menampilkan halaman Kotak masuk .....	92
Kode 4.22 <i>LinearLayout</i> pada halaman Kotak masuk .....	93
Kode 4.23 <i>ListView</i> pada halaman Kotak masuk.....	93
Kode 4.24 Mendeklarasikan <i>ListView</i> dan <i>ListAdapter</i> .....	93
Kode 4.25 Mendekripsi dan menampilkan pesan .....	94
Kode 4.26 Menampilkan pesan kesalahan .....	95
Kode 4.27 Mode operasi Dekripsi-Enkripsi-Dekripsi pada kelas Triple DES .....	96

Kode 4.28 Menampilkan halaman Pengaturan .....	97
Kode 4.29 <i>Event listener</i> pada pengaturan bahasa.....	97
Kode 4.30 <i>ListPreference</i> pada halaman Pengaturan .....	98
Kode 4.31 Beberapa entri pada array untuk <i>ListPreference</i> .....	99
Kode 4.32 Beberapa entri <i>string</i> pada file strings.xml di dalam folder <i>values</i> ....	101
Kode 4.33 Beberapa entri <i>string</i> pada file strings.xml di dalam folder <i>values-id</i> .....	101