

KRIPTOGRAFI TRIPLE DES DAN RC6 UNTUK PENGAMANAN SMS PADA SMARTPHONE ANDROID

TESIS



**OLEH:
RENDI PRASETYA
1211601834**

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

**JAKARTA
2015**

KRIPTOGRAFI TRIPLE DES DAN RC6 UNTUK PENGAMANAN SMS PADA SMARTPHONE ANDROID

TESIS

Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer (M.Kom)



**OLEH:
RENDI PRASETYA
1211601834**

**PROGRAM STUDI: MAGISTER ILMU KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

**JAKARTA
2015**



PROGRAM STUDI: MAGISTER KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama Mahasiswa : Rendi Prasetya
Nomor Induk Mahasiswa : 1211601834
Program Studi : Magister Ilmu Komputer
Konsentrasi : Rekayasa Komputasi Terapan
Fakultas/Program : Pascasarjana

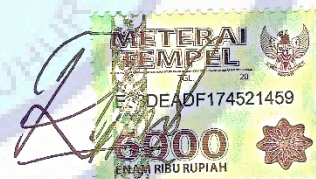
menyatakan bahwa Tesis yang berjudul:

***Kriptografi Triple DES dan RC6 untuk Pengamanan SMS pada Smartphone
Android***

1. merupakan hasil karya tulis ilmiah sendiri dan bukan merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain,
2. saya ijin untuk dikelola oleh Universitas Budi Luhur sesuai dengan norma hukum dan etika yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan saya bersedia menerima konsekuensi apapun sesuai aturan yang berlaku apabila di kemudian hari pernyataan ini tidak benar.

Jakarta, 21 Pebruari 2015



(Rendi Prasetya)



PROGRAM STUDI: MAGISTER KOMPUTER (MKOM)
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR

LEMBAR PENGESAHAN

Nama Mahasiswa : Rendi Prasetya
Nomor Induk Mahasiswa : 1211601834
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Strata 2
Judul Tesis : Kriptografi Triple DES dan RC6 untuk
Pengamanan SMS pada *Smartphone* Android

Telah diperiksa, diuji dan dipertahankan dalam sidang ujian Tesis pada hari Sabtu, tanggal 21 Pebruari 2015, dan disetujui oleh Tim Penguji Tesis.

Jakarta, 21 Pebruari 2015

Tim Penguji:

Tanda Tangan:

Ketua,

(Prof. Dr. Moedjiono M.Sc)

Anggota,

(Samidi M.M, M.Kom)

Pembimbing Utama,

(Dr. Ir. Nazori AZ MT)

Pembimbing Pendamping,

(Samidi M.M, M.Kom)

Ketua Program Studi

(Dr. Ir. Nazori AZ MT)

ABSTRAK

Short message service (SMS) merupakan sebuah layanan yang banyak diaplikasikan dan digunakan pada sistem komunikasi tanpa kabel. Namun, layanan ini tidak menjamin keamanan dan kerahasiaan pesan yang dikirimkan. Proses enkripsi pada layanan ini hanya dilakukan antara *mobile station* dan *base transceiver station*, sedangkan pada bagian lainnya masih rentan. Oleh karena itu, pada penelitian ini diusulkan sebuah proses enkripsi layanan SMS pada smartphone Android sebelum pesan tersebut dikirimkan ke *mobile station*. Algoritma kriptografi yang digunakan adalah Triple DES dan RC6, yang merupakan algoritma yang memiliki tingkat keamanan yang sangat baik, tetapi merupakan algoritma yang sederhana. Penelitian ini merupakan jenis penelitian terapan, pengumpulan data dilakukan dengan observasi, studi pustaka dan wawancara. Metode yang digunakan dalam menganalisis dan merancang sistem adalah metode analisis dan perancangan berorientasi objek menggunakan *unified modelling language*. Pengujian dengan pendekatan *blackbox* menggunakan: *Focus Group Discussion*, pengujian kualitas dengan mengadaptasi model ISO 9126, dan pengujian menggunakan *web service tools* AppThwack untuk mengetahui kualitas perangkat lunak yang dibangun dan juga untuk membandingkan performa penggunaan CPU dan memori antara kedua algoritma yang digunakan. Hasil yang didapatkan pada penelitian ini secara keseluruhan sangat baik, dengan persentase hasil pengujian FGD sebesar 100% dan hasil pengujian dengan mengadaptasi model ISO 9126 sebesar 88,65%, dan hasil pengujian menggunakan *web service tools* AppThwack sebesar 99% tanpa adanya bugs, dengan penggunaan CPU dan memori pada algoritma RC6 yang lebih baik dibandingkan dengan algoritma Triple DES, dengan terjadi perbedaan yang tidak signifikan.

Kata kunci: SMS, Enkripsi, Kriptografi, Triple DES, RC6, Unified Modelling Language, ISO 9126

ABSTRACT

Short message service (SMS) is a service that is widely applied and used in wireless communication systems. However, this service does not guarantee the security and confidentiality of messages sent. The encryption process in this service is only performed between the mobile station and base transceiver stations, while the other part is still open. Therefore, this research proposes an encryption process in SMS services on Android smartphones before the message sent to the mobile station. Cryptographic algorithm used in this research are Triple DES and RC6, which have very good level of security but have a simple algorithm. This research is an applied research, collect data by observing, literature reading and interviewing. System analysis and design used the object-oriented analysis method (the unified modeling language). Blackbox testing approach are: Focus Group Discussion (FGD), adapt ISO 9126 model, and web service testing tools AppThwack to measure the software quality and to compare the CPU and memory's performance usage between the two algorithms. The results obtained in this research is very good, with the percentage of FGD test results is 100% and the percentage of ISO 9126 test result is 88.65%, and test results using AppThwack web service tools is 99% without bugs, with the use of CPU and memory on the RC6 algorithm is better than the Triple DES algorithm, with no significant differences.

Keywords: SMS, Encryption, Cryptography, Triple DES, RC6, Unified Modelling Language, ISO 9126

KATA PENGANTAR

Assalamu'alaikum Wr. Wb.

Segala puji dan syukur senantiasa terpanjatkan kehadiran Allah SWT yang telah memberikan rahmat serta ridho-Nya sehingga penulis dapat menyelesaikan tesis yang berjudul “KRIPTOGRAFI TRIPLE DES DAN RC6 UNTUK PENGAMANAN SMS PADA SMARTPHONE ANDROID”. Salawat serta salam senantiasa tercurahkan kepada Nabi Muhammad SAW yang telah membawa risalah dan Qalam-Nya sehingga penulis dapat memahami dan melaksanakan kewajiban menuntut ilmu.

Tujuan pembuatan tesis ini adalah untuk memenuhi salah satu syarat dalam menyelesaikan jenjang Strata Dua (S-2) pada Program Studi Magister Ilmu Komputer (M.Kom) Program Pascasarjana Universitas Budi Luhur.

Dalam penyusunan proposal tesis ini, penulis menyampaikan terima kasih yang setulusnya kepada semua pihak yang telah mendukung dan memberi semangat kepada penulis dalam penulisan proposal tesis ini:

1. Bapak Dr. Ir. Nazori AZ. MT dan Bapak Samidi M.M, M.kom selaku dosen pembimbing tesis yang telah membimbing dan memotivasi penulis dalam menyelesaikan tesis ini.
2. Keluarga yang selalu memberikan semangat, dukungan dan juga do'a bagi penulis.
3. Rekan-rekan mahasiswa Pascasarjana Magister Ilmu Komputer Universitas Budi Luhur atas kebersamaan, kerja keras dan dukungan semangatnya.
4. Rekan-rekan Universitas Indraprasta PGRI yang selalu memberikan do'a, dukungan dan semangat kepada penulis.
5. Bapak dan ibu dosen pengampu mata kuliah di Pascasarjana Magister Ilmu Komputer Universitas Budi Luhur yang telah sabar dalam memberikan ilmu pengetahuan, pencerahan, dan bimbingan dalam belajar

Penulis menyadari penulisan proposal tesis ini masih jauh dari sempurna. Untuk itu penulis mengharapkan kritik dan saran yang membangun demi tercapainya penulisan yang lebih baik.

Wassalamu'alaikum Wr. Wb.

Jakarta, Pebruari 2015

DAFTAR ISI

	Halaman
LEMBAR PERNYATAAN	i
LEMBAR PENGESAHAN	ii
ABSTRAK	iii
ABSTRACT.....	iv
KATA PENGANTAR	v
DAFTAR ISI.....	vi
DAFTAR GAMBAR	ix
DAFTAR TABEL	xi
DAFTAR LAMPIRAN.....	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang.....	1
1.2 Masalah Penelitian.....	2
1.2.1 Identifikasi Masalah	2
1.2.2 Pembatasan Masalah	3
1.2.3 Rumusan Masalah	3
1.3 Tujuan dan Manfaat Penelitian.....	3
1.3.1 Tujuan Penelitian	3
1.3.2 Manfaat Penelitian	4
1.4 Tata Urut/Sistematika Penulisan	4
1.5 Daftar Pengertian.....	5
BAB II LANDASAN TEORI DAN KERANGKA KONSEP/PEMIKIRAN	7
2.1 Tinjauan Pustaka/Teori.....	7
2.1.1 Konsep Dasar	7
2.1.1.1 Android.....	7
2.1.1.2 Short Messaging Service (SMS)	8
2.1.1.3 Kriptografi	11
2.1.1.4 Enkripsi/Dekripsi	12
2.1.1.5 Algoritma Triple DES	14
2.1.1.6 Algoritma RC6	19
2.1.2 Metode Pengembangan Sistem Model Prototipe	24
2.1.2.1 Konsep Dasar Model Prototipe	24
2.1.2.2 Model Prototipe Evolusioner	27
2.1.3 Analisis dan Perancangan Berorientasi Objek dengan <i>Unified Modeling Language</i>	28
2.1.3.1 Konsep Dasar Analisis dan Perancangan Berorientasi Objek	28
2.1.3.2 <i>Unified Modelling Language (UML)</i>	30
2.1.4 <i>Development Framework</i>	37
2.1.4.1 Java.....	37

2.1.4.2 Extensible Markup Language (XML)	37
2.1.4.3 Eclipse	38
2.1.4.4 Eclipse Plug-in	40
2.1.4.5 Android Development Tools (ADT)	40
2.1.5 Focus Group Discussion (FGD)	41
2.1.6 Model Kualitas Perangkat Lunak	44
2.1.6.1 Pengertian Kualitas Perangkat Lunak	44
2.1.6.2 Model ISO 9126	45
2.1.7 Pengujian Perangkat Lunak	48
2.1.7.1 Strategi Pengujian Perangkat Lunak	48
2.1.7.2 Teknik Pengujian Perangkat Lunak	50
2.2 Tinjauan Studi/Penelitian Sebelumnya	51
2.3 Tinjauan Objek Penelitian	52
2.3.1 Hardware yang akan Digunakan	52
2.3.2 Software yang akan Digunakan	53
2.4 Kerangka Konsep/Pola Pikir Pemecahan Masalah	53
2.5 Hipotesis	54
BAB III METODOLOGI DAN RANCANGAN/DESAIN PENELITIAN	56
3.1 Metode/Jenis Penelitian	56
3.2 Sampling/Metode Pemilihan Sampel	56
3.3 Metode Pengumpulan Data	56
3.4 Instrumentasi	57
3.4.1 Hardware	57
3.4.2 Software	57
3.5 Teknik Analisis, Rancangan, dan Pengujian Data/Sistem/Prototipe Model, Rencana Strategi	58
3.5.1 Teknik Analisis Sistem	58
3.5.2 Teknik Perancangan Sistem	58
3.5.3 Teknik Pengujian Sistem	59
3.5.3.1 Pengujian dengan Focus Group Discussion (FGD)	59
3.5.3.2 Pengujian Kualitas dengan Mengadaptasi Model ISO 9126	59
3.5.3.3 Pengujian dengan Software Testing	62
3.5.4 Teknik Implementasi Sistem	63
3.6 Langkah-Langkah Penelitian	63
3.7 Jadwal Penelitian	66
BAB IV PEMBAHASAN HASIL PENELITIAN	68
4.1 Pengelompokan dan Analisis, Temuan-Temuan, dan Interpretasi	68
4.1.1 Gambaran Umum Model Prototipe	68
4.1.2 Analisis Kebutuhan Fungsional dan Non Fungsional	69
4.1.2.1 Kebutuhan Fungsional dan Non Fungsional Pengguna	69
4.1.2.2 Use Case Diagram	74

4.1.3 Analisa Perilaku Sistem	78
4.1.3.1 <i>Activity Diagram</i>	78
4.1.3.2 <i>Sequence Diagram</i>	81
4.2 Perancangan Sistem, Prototipe Model, dan Pengujian Sistem/Prototipe Model.....	84
4.2.1 Kontruksi Sistem.....	84
4.2.1.1 Perancangan Sistem dengan <i>Class Diagram</i>	84
4.2.1.2 Konstruksi Antarmuka Prototipe.....	86
4.2.1.3 <i>Code Program Algoritma Triple DES dan RC6</i>	90
4.2.2 Ilustrasi Penggunaan Prototipe.....	95
4.2.2.1 Ilustrasi Penggunaan Prototipe untuk Membuat Pesan	95
4.2.2.2 Ilustrasi Penggunaan Prototipe untuk Membaca Pesan....	98
4.3 Pengujian Sistem	100
4.3.1 Pengujian Validasi	100
4.3.1.1 Karakteristik Responden	100
4.3.1.2 Proses Pelaksanaan FGD.....	102
4.3.1.3 Hasil Pengujian Validasi	102
4.3.1.4 Kesimpulan Hasil Pengujian Validasi dan Pembuktian Hipotesis	104
4.3.2 Pengujian Kualitas Prototipe.....	104
4.3.2.1 Karakteristik Responden	105
4.3.2.2 Pengujian dengan Mengadaptasi Model ISO 9126	106
4.3.2.3 Pengujian dengan <i>Software Testing</i>	111
4.3.3 Hasil Pengujian Perangkat Lunak	113
4.3.4 Kesimpulan Hasil Pengujian Perangkat Lunak dan Pembuktian Hipotesis.....	113
4.4 Implikasi Penelitian dan Evaluasi Keseluruhan	114
4.4.1 Aspek Sistem.....	114
4.4.2 Aspek Penelitian Lanjut	114
4.5 Rencana Implementasi Sistem.....	115
4.5.1 Tahapan Rancangan Implementasi Sistem	115
4.5.2 Kegiatan Implementasi Sistem.....	115
BAB V PENUTUP.....	117
5.1 Simpulan.....	117
5.2 Saran.....	118
5.3 Rencana Implementasi.....	118
DAFTAR PUSTAKA	120
LAMPIRAN – LAMPIRAN	123
RIWAYAT HIDUP SINGKAT	157

DAFTAR GAMBAR

Gambar	Halaman
II-1 Logo Android	8
II-2 Skema cara kerja SMS	9
II-3 Struktur pesan SMS	9
II-4 Diagram proses enkripsi dan dekripsi	12
II-5 Diagram proses enkripsi dan dekripsi algoritma simetrik.....	13
II-6 Diagram proses enkripsi dan dekripsi algoritma asimetrik.....	14
II-7 Proses pembangkitan kunci-kunci internal	15
II-8 Rincian komputasi fungsi f	16
II-9 Skema algoritma Triple DES	18
II-10 Diagram proses enkripsi RC6	23
II-11 Diagram proses dekripsi RC6	24
II-12 Model prototipe	26
II-13 Tahapan pembuatan prototipe evolusioner	28
II-14 Arsitektur dari Eclipse.....	39
II-15 Model kualitas perangkat lunak model ISO 9126	46
II-16 Langkah-langkah pengujian perangkat lunak	50
II-17 Kerangka konsep penelitian	54
III-1 Langkah-langkah penelitian	63
IV-1 Gambaran umum sistem SMS Kriptografi	68
IV-2 Actor dalam pengguna layanan SMS	75
IV-3 Use Case Diagram prototipe	75
IV-4 Activity Diagram membuat pesan baru	79
IV-5 Activity Diagram melihat pesan masuk	80
IV-6 Activity Diagram melihat tentang aplikasi	81
IV-7 Sequence Diagram membuat pesan baru	82
IV-8 Sequence Diagram melihat pesan masuk	83
IV-9 Sequence Diagram melihat tentang aplikasi	84
IV-10 Class Diagram aplikasi SMS Kriptografi	85
IV-11 Rancangan antarmuka halaman utama	87
IV-12 Rancangan antarmuka halaman buat pesan	88
IV-13 Rancangan antarmuka halaman kotak masuk	88
IV-14 Rancangan antarmuka halaman baca pesan	89
IV-15 Rancangan antarmuka halaman tentang aplikasi	89
IV-16 Halaman utama	95
IV-17 Halaman buat pesan baru	96
IV-18 Pesan yang telah terenkripsi	96
IV-19 Pesan kesalahan saat kolom kunci dan pesan belum terisi	97
IV-20 Pesan kesalahan saat nomor tujuan belum terisi	97
IV-21 Halaman kotak masuk	98

IV-22	Halaman baca pesan	98
IV-23	Hasil dekripsi pesan dengan kunci yang benar	99
IV-24	Pesan kesalahan saat kunci belum terisi	99
IV-25	Hasil dekripsi pesan dengan kunci yang salah	100
IV-26	Pesan kesalahan saat pesan yang terpilih bukan pesan terenkripsi	100
IV-27	Hasil pengujian dengan <i>AppThwack</i>	111
IV-28	Performa prototipe aplikasi SMS Kriptografi untuk algoritma RC6	112
IV-29	Performa prototipe aplikasi SMS Kriptografi untuk algoritma Triple DES	112

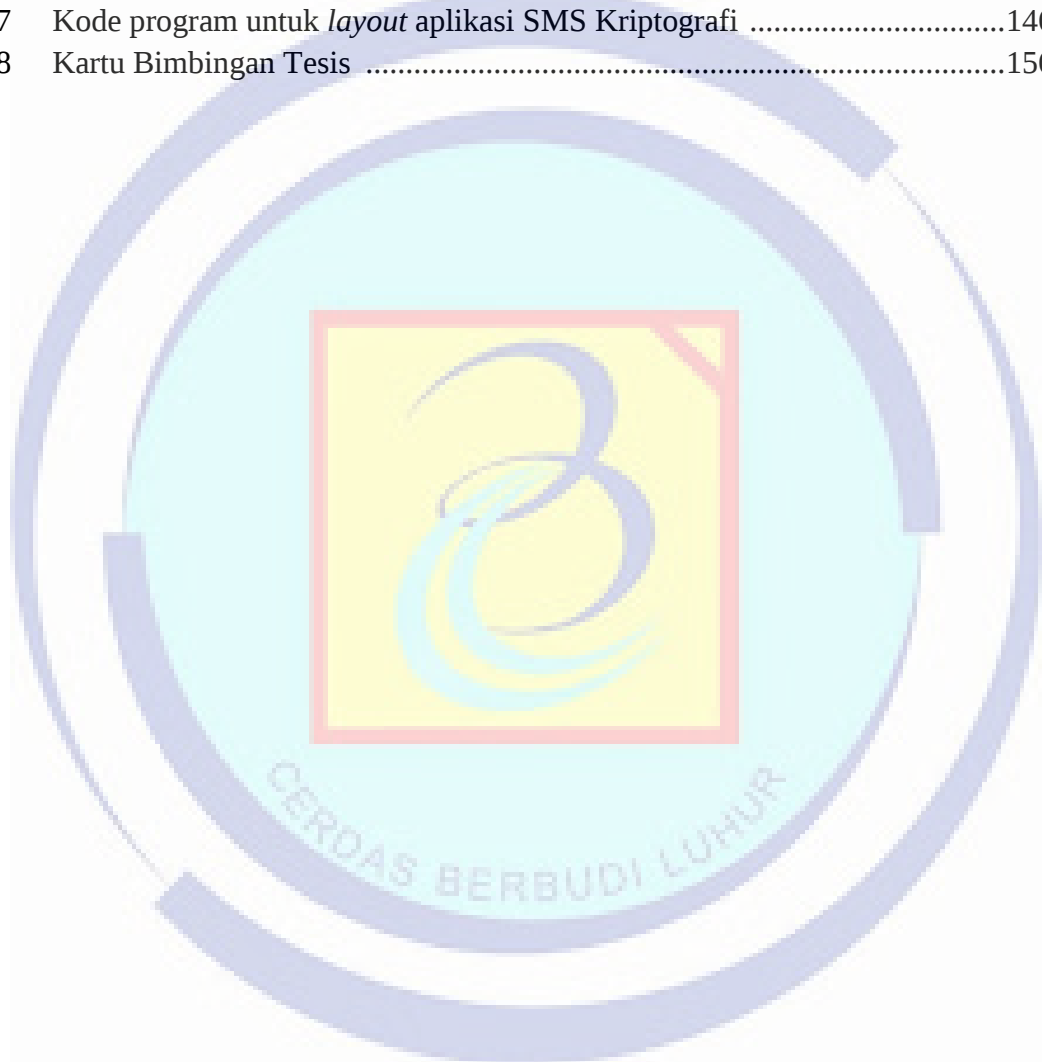


DAFTAR TABEL

Tabel	Halaman
I-1 Daftar pengertian istilah	5
II-1 Jumlah pergeseran bit pada setiap putaran	14
II-2 Mode enkripsi dan dekripsi Triple DES	19
II-3 Elemen-elemen <i>Use Case Diagram</i>	30
II-4 Elemen-elemen <i>Activity Diagram</i>	32
II-5 Elemen-elemen <i>Sequence Diagram</i>	33
II-6 Elemen-elemen <i>Class Diagram</i>	34
II-7 Elemen-elemen <i>Deployment Diagram</i>	36
II-8 Karakteristik kualitas perangkat lunak model ISO 9126	46
II-9 Tinjauan studi	51
III-1 Skala pengukuran	60
III-2 Kisi-kisi pengukuran kualitas perangkat lunak dan indikator	60
III-3 Kriteria presentase tanggapan responden	62
III-4 Jadwal penelitian	66
IV-1 Elisitasi kebutuhan fungsional dan non-fungsional tahap 1	70
IV-2 Elisitasi kebutuhan fungsional dan non-fungsional tahap 2	72
IV-3 Elisitasi kebutuhan fungsional dan non-fungsional	73
IV-4 Spesifikasi skenario <i>Use Case</i> membuat pesan baru	76
IV-5 Spesifikasi skenario <i>Use Case</i> melihat pesan masuk	77
IV-6 Spesifikasi skenario <i>Use Case</i> melihat tentang aplikasi	78
IV-7 Deskripsi responden berdasarkan jenis kelamin	101
IV-8 Deskripsi responden berdasarkan usia	101
IV-9 Deskripsi responden berdasarkan pendidikan terakhir	102
IV-10 Hasil pengujian validasi kebutuhan fungsional	103
IV-11 Deskripsi responden berdasarkan jenis kelamin	105
IV-12 Deskripsi responden berdasarkan usia	105
IV-13 Deskripsi responden berdasarkan pendidikan terakhir	106
IV-14 Kriteria persentase tanggapan responden	107
IV-15 Tanggapan responden berdasarkan aspek <i>Functionality</i>	107
IV-16 Tanggapan responden berdasarkan aspek <i>Reliability</i>	108
IV-17 Tanggapan responden berdasarkan aspek <i>Usability</i>	109
IV-18 Tanggapan responden berdasarkan aspek <i>Efficiency</i>	109
IV-19 Hasil pengujian kualitas model ISO 9126	110
IV-20 Hasil pengujian perangkat lunak	113
IV-21 Rencana implementasi sistem	115

DAFTAR LAMPIRAN

Lampiran	Halaman
1 Daftar pedoman pertanyaan untuk wawancara	124
2 Hasil wawancara responden	125
3 Form draft elisitasi	127
4 Lembar persetujuan elisitasi	129
5 Hasil kuesioner <i>focus group discussion</i> (FGD)	130
6 Hasil kuesioner pengujian mengadaptasi model ISO 9126	138
7 Kode program untuk <i>layout</i> aplikasi SMS Kriptografi	146
8 Kartu Bimbingan Tesis	156



DAFTAR PUSTAKA

- [ALQ, 2010] Al-Qutaish, Rafa E. “*Quality Models in Software Engineering Literature: An Analytical and Comparative Study*”. Journal of American Science 6 : 166-175. 2010
- [BRU, 1996] Schneier, Bruce. “*Applied Cryptography, Protocols, Algorithms, and Source Code in C*”. New York: Wiley & Sons, Inc. 1996
- [CLE, 2007] Clements T. SMS–Short but Sweet. Sun Microsystems. <http://developers.sun.com/techtopics/mobility/midp/articles/sms/> (diakses 17 Nopember 2014)
- [DEN, 2009] Dennis, Alan. et.al. “*Systems Analysis and Design with UML – 3rd Edition*”. New York: John Wiley & Sons, Inc. 2009
- [DEX, 2007] Dexter, M. “*Eclipse And Java for Total Beginners*”. Tutorial Companion Document. 2007
- [ERI, 2012] Erik, Van. “*Standard glossary of terms used in Software Testing (V2.2)*”. ISTQB. 2012
- [HAZ, 2014] El Bakry, Hazem M. et.al. “*Implementation of a Hybrid Encryption Scheme for SMS / Multimedia Message on Android*”. International Journal of Computer Applications 85: 2. 2014
- [HOE, 1995] Hoed, B.H, “*Diskusi Kelompok Terfokus*”, Jakarta: Fakultas Sastra Universitas Indonesia. 1995
- [HOLZ, 2004] Holzner, S. “*Eclipse*”. CA: O’Reilly Media. 2004
- [KRU, 1998] Krueger, Richard A. “*Focus Group A Practical Guide for Applied Research*”. California: Sage Publication, Inc. 1998
- [KUR, 2011] Kurniawan Dwi P., Andi. “*Penerapan Algoritma Vigenere Cipher pada Aplikasi SMS Android*”. Makalah IF3058 Kriptografi – Sem. II. 2011
- [LIT, 2003] Litosseliti, L. “*Using Focus Group Discussion in Research*”. Continuum London. 2003