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 ijinkan 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 Disscussion*, 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 kehadirat 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

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

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