

**PENERAPAN ALGORITMA RSA DAN ALGORITMA
HUFFMAN PADA APLIKASI KRIPTOGRAFI DAN
KOMPRESI SMS BERBASIS ANDROID**

TESIS



**Oleh :
LAURENTINUS
1311601601**

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

**JAKARTA
2016**

**PENERAPAN ALGORITMA RSA DAN ALGORITMA
HUFFMAN PADA APLIKASI KRIPTOGRAFI DAN
KOMPRESI SMS BERBASIS ANDROID**

TESIS

**Diajukan untuk memenuhi salah satu persyaratan
memperoleh gelar Magister Ilmu Komputer (MKOM)**



**Oleh :
LAURENTINUS
1311601601**

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

**JAKARTA
2016**



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

LEMBAR PERNYATAAN

Saya yang bertandatangan dibawah ini,

Nama Mahasiswa : Laurentinus
Nomor Induk Mahasiswa : 1311601601
Jenjang Studi : Strata 2
Konsentrasi : Rekayasa Komputasi Terapan
Fakultas/Program : Magister Ilmu Komputer

Menyatakan bahwa TESIS yang berjudul :

Penerapan Algoritma RSA dan Algoritma Huffman pada Aplikasi
Kriptografi dan Kompresi SMS Berbasis 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 apabila di kemudian pernyataan ini tidak benar.

Jakarta, 10 Februari 2016



(.....Laurentinus.....)



**PROGRAM STUDI : MAGISTER ILMU KOMPUTER
PROGRAM PASCASARJANA
UNIVERSITAS BUDI LUHUR**

LEMBAR PENGESAHAN

Nama : Laurentinus
Nomor Induk Mahasiswa : 1311601601
Konsentrasi : Rekayasa Komputasi Terapan
Jenjang Studi : Strata 2
Judul : Penerapan Algoritma RSA dan Algoritma Huffman
Pada Aplikasi Kriptografi dan Kompresi SMS
Berbasis Android

Jakarta, 15 Februari 2016

Tim Penguji:

Tanda tangan :

Ketua,
Prof. Dr. Moedjiono, M.Sc

Anggota,
Dr. Ir. Nazori Az, M.T

Pembimbing Utama,
Mardi Hardjianto, M.kom

Pembimbing Pendamping,
Dr. Ir. Nazori Az, M.T

Ketua Program Studi

(Dr. Ir. Nazori Az, M.T)

Abstrak

Perkembangan teknologi telekomunikasi memungkinkan manusia untuk berkomunikasi salah satunya yaitu menggunakan perangkat telepon. Namun tidak adanya security yang menjamin Keamanan dan menjaga kerahasiaan data atau informasi dalam pengiriman SMS mengakibatkan pesan mudah dicuri oleh pihak yang tidak berwenang. SMS yang dikirimkan melalui BTS akan diterima Message Service Center (SMSC) Operator sehingga menimbulkan celah penyalahgunaan informasi. Salah satu cara untuk mengamankan data dari proses komunikasi data yaitu dengan kriptografi. Penelitian ini menggunakan metode penelitian statistik deskriptif. Penelitian ini dilakukan dengan melakukan analisa keamanan dengan menerapkan algoritma RSA pada aplikasi kriptografi dan kompresi SMS berbasis android. Algoritma RSA merupakan algoritma kriptografi asimetri yang menggunakan kunci publik dan kunci privat dalam enkripsi dan dekripsi untuk menghasilkan modulus dan ciphertext. Dengan aplikasi tersebut maka semua pesan yang dikirim telah dienkripsi menggunakan kunci yang digenerate, dan untuk membuka pesan tersebut maka dibutuhkan kunci yang digunakan untuk dekripsi pesan. Dikarenakan hasil ciphertext menggunakan algoritma RSA sangat panjang maka dibutuhkan kompresi text. Algoritma Huffman merupakan algoritma lossless data compression dimana kompresi data tidak menghilangkan satu byte pun dan disimpan sesuai aslinya. sehingga hasil dekompres sama dgn ciphertext original. Pengujian dilakukan menggunakan Metode Blackbox dan model ISO 9126 untuk menghasilkan aplikasi yang memiliki standarisasi tinggi.

Kata Kunci : Kriptografi, Enkripsi, Dekripsi, SMS, mobile, RSA, kompresi, Huffman, android

ABSTRACT

Development of telecommunications technology allows humans to communication, one of them is using mobile phone device. Unfortunately, there are no security guarantees authenticity and confidentiality of data or information, the process delivery of SMS easily stolen by unauthorized parties because SMS sent via BTS will be accepted by Message Service Center (SMSC), And the operator can view the message contents. One of the ways to secure information from the data communication process that is uses cryptography. This research used descriptive statistics research. This research was conducted by analysing security by implementing the RSA algorithm Encryption and Decryption to SMS Application based on Android, RSA algorithm is an asymmetric cryptographic algorithm which uses a public key and a private key in the encryption and decryption to generate the modulus and ciphertext. With the application, all messages sent has been encrypted using a key that is generated, to open the message then takes the key used to decrypt the message. Because the results of the ciphertext using RSA algorithm is very long, it takes compression of the text. Huffman algorithm is an algorithm of Lossless compression that compresses the text without losing the original data so that decompress data same with the ciphertext. Testing Prototype in this research, we use the Blackbox method and ISO 9126 models to generate applications that have a high standardization.

Keywords : Cryptography, Encryption, Decryption, SMS, mobile, RSA, android

KATA PENGANTAR

Segala Puji bagi Tuhan Yesus Kristus atas segala anugrah, akal dan pikiran yang diberikan-Nya, sehingga penulis dapat menyelesaikan penelitian tesis dengan judul “PENERAPAN ALGORITMA RSA DAN ALGORITMA HUFFMAN PADA APLIKASI KRIPTOGRAFI DAN KOMPRESI SMS BERBASIS ANDROID”.

Tujuan pembuatan tesis ini yaitu 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.

Dengan segala keterbatasan, penulis menyadari pula bahwa laporan penelitian tesis ini takkan terwujud tanpa bantuan, bimbingan, dan dorongan dari berbagai pihak. Untuk itu, dengan segala kerendahan hati, penulis menyampaikan ucapan terima kasih kepada:

1. Tuhan Yesus Kristus yang telah memberikan segalanya untuk menyelesaikan laporan ini.
2. Orang Tua yang senantiasa mendoakan dan mencurahkan cinta, kasih sayang, dan dukungan baik moral maupun materil.
3. Bapak Prof. Dr. Moedjiono, M.Sc selaku Ketua STMIK Atma Luhur Pangkalpinang.
4. Bapak Mardi Hardjianto, M.kom selaku Pembimbing Laporan Tesis.
5. Teman-teman yang telah mendukung dan berjuang bersama.
6. Lisia yang terus memberi dukungan.

Penulis menyadari penulisan laporan tesis ini masih jauh dari sempurna. Maka dari itu penulis menerima kritik serta saran yang bertujuan membangun. Semoga penelitian tesis ini dapat berguna serta bermanfaat bagi semua pihak.

Jakarta, 10 Januari 2016

Laurentinus

DAFTAR ISI

	Halaman
ABSTRAK.....	i
KATA PENGANTAR	iii
DAFTAR ISI	iv
DAFTAR GAMBAR.....	vi
DAFTAR TABEL	vii
DAFTAR LAMPIRAN	viii
 BAB I PENDAHULUAN	
1.1 Latar Belakang.....	1
1.2 Masalah Penelitian.....	3
1.2.1 Identifikasi Masalah	3
1.2.2 Batasan Masalah.....	3
1.2.3 Rumusan Masalah	4
1.3 Tujuan dan Manfaat Penelitian.....	4
1.3.1 Tujuan Penelitian.....	4
1.3.2 Manfaat Penelitian.....	5
1.4 Sistematika Penulisan	5
1.5 Daftar Pengertian	6
 BAB II LANDASAN PEMIKIRAN	
2.1 Tinjauan Pustaka	7
2.1.1 GSM (Global System for Mobile)	7
2.1.1.1 Arsitektur Jaringan GSM	7
2.1.2 SMS (Short Message Service)	9
2.1.2.1 Arsitektur Jaringan SMS	9
2.1.2.2 Struktur Pesan GSM.....	11
2.1.2.3 Layanan Aplikasi SMS.....	12
2.1.3 Keamanan Sistem	13
2.1.4 Kriptografi	13
2.1.4.1 Sistem Kriptografi	14
2.1.4.2 Kriptografi Kunci Privat dan Kunci Publik	15
2.1.5 Algoritma RSA	17
2.1.5.1 Generate Key Algoritma RSA.....	18
2.1.5.2 Enkripsi Algoritma RSA.....	18
2.1.5.3 Dekripsi Algoritma RSA	18
2.1.6 Kompresi Data	19
2.1.7 Algoritma Huffman.....	19
2.1.7.1 Graf	20
2.1.7.2 Pohon (Tree)	20
2.1.7.3 Pembentukan Pohon Huffman.....	20
2.1.7.4 Huffman Encoding.....	21
2.1.7.5 Huffman Decoding	21

2.2	Metode Pengembangan Sistem Model Prototipe	21
2.2.1	Konsep Dasar Model Prototipe	21
2.3	Analisis dan Perancangan Berorientasi Objek dengan Unified Modeling Language.....	24
2.3.1	Konsep Dasar Analisis dan Perancangan Berorientasi Objek.....	24
2.3.2	Unified Modelling Language (UML).....	25
2.4	Pengujian Perangkat Lunak.....	31
2.4.1	Strategi Pengujian Perangkat Lunak	31
2.4.2	Teknik Pengujian Perangkat Lunak	32
2.4.3	Model ISO 9126.....	34
2.5	Tinjauan Studi/Penelitian Sebelumnya.	38
2.6	Tinjauan Objek Penelitian.....	40
2.7	Kerangka konsep/Pola Pikir.	41
2.8	Hipotesis.....	42
 BAB III RANCANGAN PENELITIAN		
3.1	Metode Penelitian.....	43
3.2	Teknik Penarikan Sample.....	43
3.3	Metode Pengumpulan Data	43
3.4	Teknik Analisa Perangkat Lunak	44
3.5	Teknik Pengujian Sistem.....	44
3.5.1	Pengujian Blackbox.....	44
3.5.2	Pengujian Kualitas dengan Mengadaptasi Model ISO 9126	46
3.5.2.1	Tahapan Pengujian Sistem	46
3.5.2.2	Tahapan Pengolahan Data.....	47
3.5.3	Pengujian Menggunakan Software Testing	48
3.6	Langkah Penelitian	48
3.6.1	Perumusan Hipotesis	48
3.6.2	Pembangunan Sistem	49
3.7	Jadwal Penelitian.....	51
 BAB IV ANALISIS DAN IMPLEMENTASI PENELITIAN		
4.1	Analisis Sistem.....	53
4.1.1	Analisis Kebutuhan Sistem	53
4.1.1.1	Analisis Kebutuhan Fungsional	53
4.1.1.2	Analisis Kebutuhan NonFungsional	54
4.1.2	Use Case Diagram.....	55
4.1.2.1	Generate Key Use Case Diagram	55
4.1.2.2	Create SMS Use Case Diagram.....	57
4.1.2.3	Baca SMS Use Case Diagram	59
4.1.2.4	Info Use Case Diagram.....	60
4.1.3	Activity Diagram.....	61
4.1.3.1	Activity Diagram Generate Key	62
4.1.3.2	Activity Diagram Create SMS	63
4.1.3.3	Activity Diagram Baca SMS	64

4.1.3.4	Activity Diagram Info	65
4.2	Perancangan Sistem.....	66
4.2.1	Konsep Proses Generate Key	67
4.2.2	Konsep Proses Create SMS	68
4.2.3	Konsep Proses Inbox	69
4.2.4	Code Algoritma RSA dan Algoritma Huffman..	70
4.2.4.1	Code Algoritma RSA	70
4.2.4.2	Code Algoritma Huffman.....	74
4.2.4.3	Proses Pengiriman Pesan.....	77
4.3	Gambaran Arsitektur Sistem	78
4.4	Implementasi Prototipe	79
4.5	Pengujian Sistem	86
4.5.1	Biaya Pengiriman SMS	86
4.5.2	Pengujian Kriptografi dan Kompresi Pengiriman SMS.....	87
4.5.3	Pengujian Kompresi Huffman	89
4.5.4	Pengujian Blackbox	90
4.5.5	Pengujian Model ISO 9126	94
4.6	Rencana Implementasi Sistem	102
4.6.1	Tahapan Rancangan Implementasi Sistem.....	102
4.6.2	Kegiatan Implementasi Sistem.....	103
BAB V PENUTUP		
5.1	Kesimpulan	104
5.2	Saran	105
DAFTAR PUSTAKA		106
LAMPIRAN-LAMPIRAN		108
RIWAYAT HIDUP SINGKAT.....		116

DAFTAR GAMBAR

Gambar	Halaman
II-1	Arsitektur Jaringan GSM..... 8
II-2	SMS Network Components 9
II-3	Struktur Pesan SMS..... 11
II-4	Kriptografi Simetri 15
II-5	Kriptografi Asimetri 17
II-6	Jenis Prototipe..... 22
II-7	Langkah-langkah pengujian perangkat lunak..... 32
II-8	Model Kualitas Perangkat Lunak ISO 9126..... 35
II-9	Kerangka Konsep Penelitian 41
III-1	Langkah-langkah pengumpulan data 47
III-2	Langkah-langkah Pembangunan Sistem 48
IV-1	Use Case Diagram Generate Key..... 55
IV-2	Use Case Diagram Create SMS 57
IV-3	Use Case Diagram Inbox 59
IV-4	Use Case Diagram Info 60
IV-5	Activity Diagram Generate Key 62
IV-6	Activity Diagram Create SMS 63
IV-7	Activity Diagram Inbox 64
IV-8	Activity Diagram Info..... 65
IV-9	Diagram Alur Prototipe..... 66
IV-10	Konsep Proses Generate Key..... 67
IV-11	Konsep Proses Create SMS..... 68
IV-12	Konsep Proses Inbox..... 69
IV-13	Konsep Arsitektur Sistem 78
IV-14	Tampilan Halaman Utama Prototipe Aplikasi Kriptografi dan Kompresi SMS 79
IV-15	Tampilan Proses Generate Key..... 80
IV-16	Tampilan Halaman Create SMS 81
IV-17	Tampilan Proses Kriptografi Pesan..... 82

IV-18	Tampilan SMS Masuk Halaman Inbox.....	83
IV-19	Halaman Dekripsi & Dekompresi SMS.....	84
IV-20	Tampilan Halaman Info Aplikasi.....	85
IV-21	Perbandingan Inbox Aplikasi SMS biasa dengan Aplikasi Kriptografi dan Kompresi.....	87
IV-22	Grafik Pengujian Black Box	94



DAFTAR TABEL

Tabel	Halaman
II-1 Elemen-elemen Use Case Diagram	26
II-2 Elemen-elemen Activity Diagram	27
II-3 Elemen-elemen Sequence Diagram	28
II-4 Elemen-elemen Class Diagram	29
II-5 Elemen-elemen Deployment Diagram.....	30
II-6 Karakteristik Kualitas Perangkat Lunak ISO 9126.....	35
II-7 Penelitian Sebelumnya.....	39
III-1 Skala Pengukuran	44
III-2 Kisi-kisi pengukuran kualitas perangkat lunak dan indikator	45
III-3 Kriteria Persentase tanggapan responden	46
III-4 Jadwal Kegiatan Penelitian.....	50
IV-1 Generate key use case aplikasi kriptografi dan kompresi SMS dengan menggunakan algoritma RSA dan algoritma Huffman.....	56
IV-2 Create SMS use case diagram aplikasi kriptografi dan kompresi SMS menggunakan algoritma RSA dan algoritma Huffman.....	58
IV-3 Inbox use case diagram aplikasi kriptografi dan kompresi SMS dengan menggunakan algoritma RSA dan Huffman	59
IV-4 Info use case diagram aplikasi kriptografi dan kompresi SMS dengan menggunakan algoritma RSA dan algoritma Huffman	61
IV-5 Perhitungan Enkripsi RSA	72
IV-6 Perhitungan Dekripsi RSA	73
IV-7 Biner Huffman.....	76
IV-8 Tabel Biaya Pengiriman SMS	86
IV-9 Pengujian Kriptografi RSA	88
IV-10 Pengujian Kompresi Huffman.....	89
IV-11 Hasil Pengujian Halaman Menu Utama	90
IV-12 Hasil Pengujian Form Generate Key	91
IV-13 Hasil Pengujian Form Create SMS	92
IV-14 Hasil Pengujian Form Inbox.....	93

IV-15	Karakteristik Responden Berdasarkan umur	95
IV-16	Karakteristik Responden Berdasarkan Jenjang Studi.....	95
IV-17	Karakteristik Responden Berdasarkan Jenis Kelamin.....	95
IV-18	Tabel Skor Penilaian ISO 9126	96
IV-19	Tanggapan Responden berdasarkan Aspek Functionality.....	97
IV-20	Tanggapan Responden berdasarkan Aspek Reliability	98
IV-21	Tanggapan Responden berdasarkan Aspek Usability	99
IV-22	Tanggapan Responden berdasarkan Aspek Efisiensi.....	100
IV-23	Rangkuman Hasil Pengujian Kualitas Model ISO 9126	101
IV-24	Rencana Implementasi Sistem.....	102



DAFTAR LAMPIRAN

Lampiran	Halaman
I-1 Hasil Wawancara Responden	108
I-2 Lampiran Gambar Pengujian	109
I-3 Kuisioner Model ISO 9126.....	112



DAFTAR PUSTAKA

- [ALVIANTO 2015] Alvianto, Andi Riski, Darmaji, 2015, “Pengamanan Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android”, Jurnal Sains dan Seni ITS, No.1
- [AL-QUTAISH 2010] Al-Qutaish, Rafa E. 2010. “Quality Models in Software Engineering Literature : An Analytical and Comparative Study”, Journal of American Science.
- I. [ARIYUS 2006] ARIYUS, DONY, “ KRIPTOGRAFI KEAMANAN DATA DAN KOMUNIKASI”, YOGYAKARTA:GRAHA ILMU, 2006.
- [ARIYUS 2008] Ariyus, Dony, “Pengantar ilmu Kriptografi, Teori, Analisis & Implementasi”. Yogyakarta:Andi, 2008.
- [ASSHIDQI 2008] Asshidqi, Yanuar, Adiwijawa, Andrian Rakhmatsyah, 2008, “Aplikasi Enkripsi SMS Berbasis Java Menggunakan Algoritma RSA”, Univ. Telkom
- [BAMBANG 2010] Bambang, Hariyanto. “Esensi-esensi bahasa pemrograman Java”, Edisi Ketiga, Informatika: Bandung, 2010.
- [BRUCE 1996] Schneier, Bruce. “Applied Cryptography, Protocols, Algorithms, and Source Code in C”, New York: Wiley & Sons, Inc: 1996.
- [BUDIHANI 2012] Budihani, Herix Saputra, 2012, “Membangun Aplikasi Keamanan Data Teks dengan Metode RSA – CRT Berbasis Android”
- [BURNETT 2001] Burnett, S., & Paine, S, 2001,” *RSA Security's Official Guide to Cryptography*”, New York: McGraw-Hill.
- [CLEMENTS 2003] Clements, Tom , ” SMS – Short but Sweet”, 2003, <http://www.oracle.com/technetwork/systems/sms-155850.html> (Diakses Oktober 2015).
- [DEWANTO 2013] Dewanto, Joko, Verdy Yanto, 2013, “Pembuatan Aplikasi SMS Kriptografi RSA dengan Android”, Forum Ilmiah Vol. 10 No.2, Mei 2013