



**DESAIN, MEKANISME DAN ANALISA SECURE SMS
ENKRIPSI UNTUK PENGAMANAN LAYANAN KOMUNIKASI
MOBILE BERBASIS SMS**

TESIS

UNIVERSITAS
Oleh
MERCU BUANA
ASWIN HADI NASUTION
55410120012

**PROGRAM MAGISTER TEKNIK ELEKTRO
PROGRAM PASCASARJANA
UNIVERSITAS MERCU BUANA
2015**



UNIVERSITAS
MERCU BUANA

**DESAIN, MEKANISME DAN ANALISA SECURE SMS
ENKRIPSI UNTUK PENGAMANAN LAYANAN KOMUNIKASI
MOBILE BERBASIS SMS**

TESIS

**Diajukan sebagai Salah Satu Syarat untuk Menyelesaikan Program
Pascasarjana Program Magister Teknik Elektro**

UNIVERSITAS
MERCU BUANA

Oleh

ASWIN HADI NASUTION

55410120012

**UNIVERSITAS MERCU BUANA
PROGRAM PASCASARJANA**

PENGESAHAN TESIS

Judul : DESAIN, MEKANISME DAN ANALISA SECURE SMS
ENKRIPSI UNTUK PENGAMANAN LAYANAN
KOMUNIKASI MOBILE BERBASIS SMS
Nama : Aswin Hadi Nasution
Nim : 55410120012
Program : Pascasarjana Program Magister Teknik Elektro
Konsentrasi : Manajemen Telekomunikasi
Tanggal : Februari 2015

Pembimbing Utama



(Prof. Dr. -Ing. Mudrik Alaydrus)

Mengesahkan :

Direktur Pascasarjana

**Ketua Program Studi
Magister Teknik Elektro**



(Prof. Dr. Didik J. Rachbini)



(Prof. Dr. -Ing. Mudrik Alaydrus)

PERNYATAAN

Saya yang bertandatangan di bawah ini menyatakan dengan sebenar-benarnya bahwa seluruh tulisan dan pernyataan dalam Tesis ini:

Judul : DESAIN, MEKANISME DAN ANALISA SECURE SMS
ENKRIPSI UNTUK PENGAMANAN LAYANAN
KOMUNIKASI MOBILE BERBASIS SMS

Nama : Aswin Hadi Nasution

NIM : 554 10120012

Program : Pascasarjana Program Magister Teknik Elektro

Konsentrasi : Manajemen Telekomunikasi

Tanggal : Februari 2015

Merupakan hasil studi pustaka, penelitian lapangan, dan karya saya sendiri dengan bimbingan Pembimbing yang ditetapkan dengan Surat Keputusan Ketua Program Studi Magister Teknik Elektro Universitas Mercu Buana.

Tesis ini belum pernah diajukan untuk memperoleh gelar magister pada program sejenis di perguruan tinggi lain. Semua informasi, data, dan hasil pengolahannya yang digunakan, telah dinyatakan secara jelas sumbernya dan dapat diperiksa kebenarannya.

UNIVERSITAS
MERCU BUANA

Jakarta, Februari 2015



Aswin Hadi Nasution

KATA PENGANTAR

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

Alhamdulillah, segala puji syukur kepada Allah SWT atas segala rahmat dan hidayah-Nya sehingga penulisan tesis dengan judul: “DESAIN, MEKANISME DAN ANALISA SECURE SMS ENKRIPSI UNTUK PENGAMANAN LAYANAN KOMUNIKASI MOBILE BERBASIS SMS ” dapat diselesaikan dengan baik. Penulisan ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Magister Teknik Program Studi Teknik Elektro, kekhususan Manajemen Telekomunikasi pada Universitas Mercu Buana.

Penyelesaian Tesis ini tak lepas dari bantuan berbagai pihak. Dengan segala kerendahan hati, saya menghaturkan terima kasih yang sebesar-besarnya kepada :

1. Prof. Dr. –Ing. Mudrik Alaydrus selaku Ketua Program Studi Magister Teknik Elektro Universitas Mercu Buana dan dosen Pembimbing yang telah banyak meluangkan waktu untuk memberikan pengarahan, diskusi dan bimbingan serta persetujuan sehingga saya dapat menyelesaikan tesis ini dengan baik
2. Kedua orang tua dan mertua atas segala doa restunya selama ini sehingga saya dapat melalui setiap rintangan dengan selamat dan penuh kesabaran. Semoga Allah SWT juga memberikan keselamatan dunia dan akhirat kepada keduanya, Amin.
3. Istriku Fitriany Kadevi dan anakku tersayang Alyanada Andini Nasution yang telah member banyak inspirasi dan semangat, terima kasih atas dukungan dan doanya.
4. Kakak Diah Umiati Nasution, Syarifah Umri Nasution dan Adikku Arbi Yasfi Nasution. Terima Kasih atas doa dan dukungannya.
5. Partnerku Galih dan Narno yang sudah memberi sumbangsih pemikiran dalam penyelesaian tesis ini.

6. Segenap teman–teman angkatan MTEL-8 Program Studi Magister Teknik Elektro Universitas Mercu Buana.

Begitu pula ucapan terima kasih kepada semua pihak yang tidak sempat saya sebutkan satu per satu atas jasa-jasanya dalam membantu dan menumbuhkan gairah optimisme saya, baik secara langsung maupun tidak langsung.

Dengan menyadari berbagai kekhilafan yang bukan tidak mungkin akan terdapat dalam tulisan ini, penulis sangat mengharapkan adanya kritik dan saran yang bersifat membangun terhadap Tesis ini.

Akhir kata dengan segala kerendahan hati penulis berharap semoga Tesis ini dapat bermanfaat bagi penelitian-penelitian selanjutnya.

Jakarta, Februari 2015

Penulis



UNIVERSITAS
MERCU BUANA

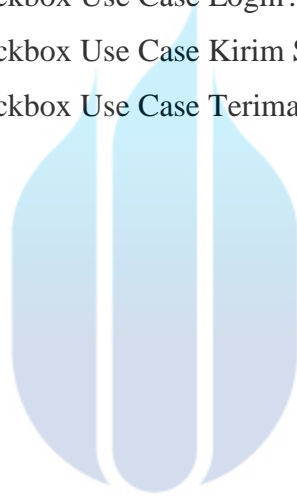
DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
LEMBAR PENGESAHAN	iii
LEMBAR PERNYATAAN KEASLIAN (ORIGINALITY)	iv
KATA PENGANTAR	v
DAFTAR ISI	vii
DAFTAR TABEL	x
DAFTAR GAMBAR	xi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	2
1.3 Tujuan Penelitian	3
1.4 Batasan Penelitian	3
1.5 Manfaat Penelitian	3
1.6 Metode Penelitian.....	3
1.7 Sistematika Penulisan	4
BAB II LANDASAN TEORI.....	5
2.1 Short Message Service (SMS)	5
2.1.1 Struktur SMS pada GSM	5
2.1.2 Prinsip Kerja SMS.....	7
2.1.3 Keamanan SMS.....	9
2.2 RSA Cryptosystem.....	10
2.2.1 <i>Generate</i> Kunci RSA	10
2.2.2 Enkripsi dan Dekripsi.....	10
2.2.3 Tanda Tangan Digital (Signing) dengan RSA	11
2.2.4 Keamanan RSA	11

2.3 Algoritma Identity Based Encryption (IBE)	12
2.4 Penelitian Yang Berkaitan.....	14
2.4.1 Hybrid Compression Encryption Technique for Securing SMS	14
2.4.2 GSM Mobile SMS/MMS using Public Key Infrastructure: m-PKI	17
2.4.3 Secure SMS Messaging	21
2.4.4 A Lookup Table Based Secure Cryptographic SMS Communication on Android Environment	23
BAB III METODOLOGI PENELITIAN	24
3.1 Studi Literatur Dan Diskusi	24
3.2 Mekanisme Kerja Secure SMS	25
3.3 Identifikasi Kebutuhan	32
3.4 Deskripsi Umum Sistem	32
3.4.1 Aplikasi Secure SMS.....	33
3.4.2 Rangkaian Proses Sistem.....	34
BAB IV PENGUJIAN DAN ANALISA	39
4.1 Pengujian Blackbox	39
4.1.1 Lingkungan Pengujian.....	39
4.1.2 Validasi Pengujian Blackbox	40
4.2 Analisa Keamanan Aplikasi.....	43
4.2.1 Pemanfaatan Password login.....	43
4.2.2 Pembuktian Matematis Otentikasi User dengan Cek Password.....	44
4.2.3 Pembuktian Confidentiality Pada Proses Enkripsi RSA.....	46
4.2.4 Pembuktian Integrity.....	49
4.2.5 Pembuktian Non-Repudiation.....	52
BAB V KESIMPULAN	54
5.1. Kesimpulan	54
5.2. Saran.....	54
DAFTAR PUSTAKA	55
DAFTAR RIWAYAT HIDUP	57

DAFTAR TABEL

Tabel 2.1	Panjang SMS	14
Tabel 2.2	Hubungan antara RSA <i>Modulus bits, maximum number of Input characters dan length of output encrypted characters</i>	15
Tabel 3.1	Perbandingan Metode Penelitian.....	30
Tabel 3.2	Peran CA dan User	32
Tabel 3.3	Deskripsi Umum Sistem.....	32
Tabel 4.1	Pengujian Blackbox Use Case Login	40
Tabel 4.2	Pengujian Blackbox Use Case Kirim SMS Enkripsi	41
Tabel 4.3	Pengujian Blackbox Use Case Terima SMS Enkripsi	42



UNIVERSITAS
MERCU BUANA

DAFTAR GAMBAR

Gambar 2.1	Arsitektur SMS.....	5
Gambar 2.2	Struktur Pesan SMS.....	7
Gambar 2.3	Arsitektur M-PKI.....	18
Gambar 2.4	Alur SMS <i>Confidential</i>	20
Gambar 2.5	Skenario Kirim Pesan.....	20
Gambar 2.6	Rangkaian Proses Pengiriman SMS Enkripsi.....	23
Gambar 3.1	Komunikasi Secure SMS.....	24
Gambar 3.2	Mekanisme Kerja Sistem Secure SMS.....	26
Gambar 3.3	Desain Secure SMS.....	27
Gambar 3.4	Flowchart Generate <i>Public</i> dan <i>privat key</i>	28
Gambar 3.5	Flowchart 2 way login.....	29
Gambar 3.6	Flowchart Penggunaan Password.....	29
Gambar 3.7	Tampilan <i>home</i> Secure SMS.....	33
Gambar 3.8	Tampilan Registrasi.....	34
Gambar 3.9	Masuk Aplikasi.....	35
Gambar 3.10	Tampilan Pengiriman Secure SMS.....	36
Gambar 3.11	Flowchart Pengiriman Secure SMS.....	37
Gambar 3.12	Flowchart Penerimaan Secure SMS.....	37
Gambar 3.13	Flowchart Kerja Sistem Secure SMS.....	38
Gambar 4.1	Tampilan Home dan Versi Perangkat.....	40
Gambar 4.2	Form Login.....	45
Gambar 4.3	Login Benar.....	45
Gambar 4.4	Login Salah.....	46
Gambar 4.5	Hasil Kirim Pesan Menggunakan Secure SMS.....	48