



UNIVERSITAS
MERCU BUANA

**PENGAMANAN SMS PADA TELEPON SELULAR
DENGAN MENGGUNAKAN ALGORITMA RC6**

SKRIPSI

Oleh :

CICI SUCIPTA
NIM : 41505120076

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2009



UNIVERSITAS
MERCU BUANA

PENGAMANAN SMS PADA TELPON SELULAR DENGAN MENGGUNAKAN ALGORITMA RC6

Diajukan Untuk Melengkapi Salah Satu Syarat
Memperoleh Gelar Sarjana Komputer

Oleh :

Cici Sucipta
NIM : 41505120076

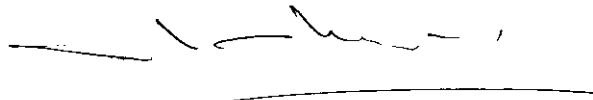
PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2009

LEMBAR PERSETUJUAN

NIM : 41505120076
Nama : CICI SUCIPTA
Judul Skripsi : PENGAMANAN SMS PADA TELEPON SELULAR
DENGAN MENGGUNAKAN ALGORITMA RC6

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI

JAKARTA, 27 AGUSTUS 2009



Drs. Achmad Kodar, MT
Pembimbing



Devi Fitriyah, S.Kom., MTI
Koord. Skripsi Teknik Informatika



Abdusy Syarif, ST., MT
KaProdi Teknik Informatika

KATA PENGANTAR

Puji syukur kami panjatkan kehadirat Allah SWT, yang atas berkat rahmat dan hidayahnya penulis dapat menyelesaikan skripsi ini dengan baik dengan segala keterbatasan yang dimiliki oleh penulis. Skripsi ini kami ajukan untuk memenuhi tugas mata kuliah Skripsi di Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Mercu Buana.

Pembuatan Aplikasi Pengamanan SMS Pada Telepon Selular Dengan Menggunakan Algoritma RC6 ini dimaksudkan untuk menggali potensi kemungkinan penggunaan algoritma RC6 ini sebagai alat bantu untuk mengamankan komunikasi yang sudah sangat banyak digunakan di seluruh dunia ini yaitu SMS. Dengan demikian, diharapkan komunikasi yang sudah sangat populer ini bisa pula digunakan untuk kepentingan lain dengan lebih aman.

Selama pengerjaan sampai dengan pelaporan skripsi ini, kami mendapatkan banyak sekali bantuan dari berbagai pihak. Oleh karena itu, perkenankanlah kami untuk memberikan rasa terima kasih kepada :

1. Orang tua kami yang selama ini telah memberikan inspirasi, bimbingan serta kasih sayangnya kepada kami dalam melaksanakan skripsi ini.
2. Istriku tercinta, Raeny Damayanti, yang secara terus menerus memberikan bantuan serta dukungan kepada kami sehingga terselesaikannya skripsi ini.
3. Anak-anakku tersayang, Annabel Putri Martiza dan Amadea Putri Zafira, yang telah memberikan inspirasi dan merelakan waktu mereka untuk digunakan kami dalam menyelesaikan studi kami.

4. Bapak Drs. Achmad Kodar, MT, selaku pembimbing yang dengan tulus hati telah membimbing kami dalam menyelesaikan skripsi ini.
5. Ibu Devi Fitriana S.Kom MTI sebagai Koordinator Skripsi yang telah banyak memberikan dukungan dalam pelaksanaan skripsi ini.
6. Bapak Abdus Syarif ST. MT, selaku ketua jurusan yang tidak hanya memberikan bimbingan tetapi memberikan semangat dan dukungan yang penuh kepada kami sehingga kami dapat menyelesaikan penulisan skripsi ini.
7. Bapak Ir. Fajar Masya MMSI, yang telah banyak membantu memberikan masukan serta inspirasi dalam penyelesaian skripsi ini.
8. Teman-teman seangkatan yang telah memberikan semangat dan bantuan selama kami menyelesaikan studi.
9. Semua pihak yang telah membantu kami yang tidak dapat kami sebutkan satu persatu.

Semoga Tuhan Yang Maha Kuasa melimpahkan karunia-Nya kepada semua pihak atas bantuan yang telah diberikan kepada kami.

Kami menyadari bahwa dalam pembuatan skripsi ini masih jauh dari kesempurnaan. Oleh sebab itu kami sangat mengharapkan masukan berupa saran dan kritik yang membangun dari para pembaca. Walaupun demikian, kami berharap semoga skripsi kami ini dapat memberikan manfaat, khususnya bagi diri kami pribadi, dan bagi para pembaca pada umumnya.

Jakarta, Agustus 2009

Penulis

DAFTAR ISI

	Halaman
LEMBAR PENGESAHAN	ii
KATA PENGANTAR	iii
ABSTRACT	v
ABSTRAK	vii
DAFTAR ISI	ix
DAFTAR GAMBAR	xii
DAFTAR TABEL	xiv
BAB I PENDAHULUAN	1
1.1. Latar Belakang Masalah	1
1.2. Metodologi	4
1.3. Tujuan	5
1.4. Batasan Masalah	6
1.5. Sistematika Penulisan	7
BAB II LANDASAN TEORI	9
2.1. <i>Short Message Service</i>	9
2.1.1. Sejarah SMS	10
2.1.2. Struktur Pesan SMS	11
2.2. Kriptografi	13
2.2.1. Sejarah Kriptografi	15
2.2.2. Kriptografi Kunci-Simetri dan Nirsimetri	18

2.2.3. Tinjauan Matematis	22
2.2.4. Kriptanalisis	24
2.2.5. Kunci Lemah dan Kunci Setengah Lemah	26
2.2.6. Mode Operasi	27
2.2.7. Proses <i>Padding</i>	27
2.2.8 <i>Block Cipher</i>	28
2.3. Algoritma RC6	31
2.3.1. Pembentukan Kunci Internal	33
2.3.2 . Proses Enkripsi dan Dekripsi	37
BAB III ANALISA DAN PERANCANGAN	45
3.1. Analisis Masalah	45
3.1.1. Analisis Strktur SMS	45
3.1.2. Analisis Algoritma RC6	46
3.1.3. Analisis Penerapan Enkripsi SMS	53
3.1.4. Analisis Dampak System	55
3.2. Analisis Kebutuhan Pembangunan Aplikasi	57
3.2.1. Deskripsi Umum Sistem	57
3.2.2. Analisis Spesifikasi dan Kebutuhan Aplikasi	59
3.2.3. Model <i>Use Case</i>	62
3.2.4. Analisis Kelas	65
3.3. Perancangan Kelas	67
3.3.1. Diagram Perancangan Kelas	67
3.4. Perancangan Modul	69

3.5. Perancangan Antar Muka	71
3.5.1. Perancangan Antar Muka Menu Utama	71
3.5.2. Perancangan Antar Muka Compose Message	73
3.5.3. Perancangan Antar Muka Daftar Isi Pesan yang Disimpan	74
BAB IV IMPLEMENTASI DAN PENGUJIAN	75
4.1. Lingkungan Implementasi	75
4.2. Batasan Implementasi	76
4.3. Implementasi Kelas	76
4.3.1. Deskripsi Kelas	76
4.3.2. Operasi dan Atribut	77
4.4. Implementasi Modul	85
4.5. Implementasi Antar Muka	86
4.6. Pengujian Aplikasi	87
4.6.1. Pengujian Performansi Aplikasi	87
4.6.2. Pengujian Enkripsi dan Dekripsi	88
4.6.3. Analisa Hasil Pengujian	89
BAB V PENUTUP	91
5.1. Kesimpulan	91
5.2. Masukan dan Saran	92

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

	Halaman
1. GAMBAR 2.1. ARSITEKTUR JARINGAN SMS	10
2. GAMBAR 2.2. STRUKTUR PESAN SMS	12
3. GAMBAR 2.3. ENKRIPSI DAN DEKRIPSI	14
4. GAMBAR 2.4. (A) SEBUAH SCYTALE (B) PESAN DITULIS SECARA HORIZONTAL	16
5. GAMBAR 2.5. MESIN ENKRIPSI ENIGMA	17
6. GAMBAR 2.6. SKEMA KRIPTOGRAFI SIMETRI.	19
7. GAMBAR 2.7. SKEMA KRIPTOGRAFI NIRSIMETRI.	20
8. GAMBAR 2.8. SKEMA CARA KERJA BLOCK CIPHER	29
9. GAMBAR 2.9. (I) PROSES ENKRIPSI ECB (II) PROSES DEKRIPSI ECB PADA SEBUAH BLOK.	30
10. GAMBAR 2.10. DIAGRAM PROSES ENKRIPSI RC6	38
11. GAMBAR 2.11. DIAGRAM PROSES DEKRIPSI RC6	40
12. GAMBAR 3.1. ARSITEKTUR GLOBAL SISTEM	57
13. GAMBAR 3.2. SKEMA KERJA SISTEM	59
14. GAMBAR 3.3. <i>USE CASE</i>	61
20. GAMBAR 3.4. DIAGRAM KELAS ANALISIS	67
21. GAMBAR 3.5. DIAGRAM KELAS PERANCANGAN	68
22. GAMBAR 3.6. INTERAKSI MODUL	71
23. GAMBAR 3.7. RANCANGAN ANTAR MUKA MENU UTAMA	72

24.	GAMBAR 3.8. PERANCANGAN TAMPILAN ANTAR MUKA <i>COMPOSE MESSAGE</i>	73
25.	GAMBAR 3.9. PERANCANGAN ANTAR MUKA DAFTAR ISI PESAN YANG DISIMPAN	74
26.	GAMBAR 4.1. GAMBAR IMPLEMENTASI ANTAR MUKA MENU UTAMA	86
27.	GAMBAR 4.2. GAMBAR IMPLEMENTASI ANTAR MUKA PENGIRIMAN PESAN	86
28.	GAMBAR 4.3. GAMBAR IMPLEMENTASI ANTAR PENERIMAAN PESAN	87

DAFTAR TABEL

	Halaman
1. TABEL 4.1. DAFTAR IMPLEMENTASI KELAS	74
2. TABEL 4.2. DAFTAR IMPLEMENTASI OPERASI : KELAS <i>INTERFACE</i>	74
3. TABEL 4.3. DAFTAR IMPLEMENTASI OPERASI : KELAS ECB	74
4. TABEL 4.4. DAFTAR IMPLEMENTASI ATRIBUT : KELAS ECB	75
5. TABEL 4.5. DAFTAR IMPLEMENTASI OPERASI : KELAS SMS <i>SENDER</i>	75
6. TABEL 4.6. DAFTAR IMPLEMENTASI ATRIBUT : KELAS SMS <i>SENDER</i>	75
7. TABEL 4.7. DAFTAR IMPLEMENTASI OPERASI : KELAS SMS <i>RECEIVE</i>	75
8. TABEL 4.8. DAFTAR IMPLEMENTASI ATRIBUT : KELAS SMS <i>RECEIVE</i>	76
9. TABEL 4.9. DAFTAR IMPLEMENTASE OPERASI : KELAS SMS <i>STORE</i>	76
10. TABEL 4.10. DAFTAR IMPLEMENTASI ATRIBUT : KELAS SMS <i>STORE</i>	76
11. TABEL 4.11. DAFTAR IMPLEMENTASI OPERASI : KELAS RC6	77
12. TABEL 4.12. DAFTAR IMPLEMENTASI ATRIBUT : KELAS RC6	77

13.	TABEL 4.13. DAFTAR IMPLEMENTASI MODUL	78
14.	TABEL 4.14. TABEL PENGUJIAN PERFORMANSI DARI APLIKASI	81
15.	TABEL 4.15. TABEL PENGUJIAN ENKRIPSI DAN DEKRIPSI	82
16.	TABEL 4.16. PENGUJIAN PENERIMAN PESAN	82