

**IMPLEMENTASI ALGORITMA RC6 UNTUK ENKRIPSI DAN
DEKRIPSI SMS BERBASIS ANDROID**

SKRIPSI



disusun oleh

Muhammad Indra

10.11.4460

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2014**

**IMPLEMENTASI ALGORITMA RC6 UNTUK ENKRIPSI DAN
DEKRIPSI SMS BERBASIS ANDROID**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika



disusun oleh

Muhammad Indra

10.11.4460

**JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2014**

PERSETUJUAN

SKRIPSI

**IMPLEMENTASI ALGORITMA RC6 UNTUK ENKRIPSI DAN
DEKRIPSI SMS BERBASIS ANDROID**

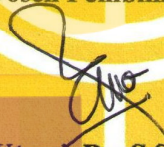
Yang dipersiapkan dan disusun oleh

Muhammad Indra

10.11.4460

Telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 29 Oktober 2013

Dosen Pembimbing,



Ema Utami, Dr. S.Si, M.Kom

NIK. 190302037

PENGESAHAN

SKRIPSI

**IMPLEMENTASI ALGORITMA RC6 UNTUK ENKRIPSI DAN
DEKRIPSI SMS BERBASIS ANDROID**

yang dipersiapkan dan disusun oleh

Muhammad Indra

10.11.4460

telah dipertahankan didepan Dewan Penguji
pada tanggal 18 Juni 2014

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Ema Utami, Dr., S.Si, M.Kom

NIK.190302037

Emha Taufiq Luthfi, ST, M.KOM

NIK. .190302125

Yuli Astuti, M.Kom

NIK.190302146

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 14 Juli 2014



KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M.Suvanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 08 Juli 2014

Muhammad Indra

10.11.4460

MOTTO

Barang siapa keluar untuk mencari ilmu maka dia berada di jalan Allah
(HR.Turmudzi)

Janganlah membanggakan dan meyombongkan diri apa-apa yang kita peroleh,
turut dan ikutilah ilmu padi makin berisi makin tunduk dan makin bersyukur
kepada yang menciptakan kita Allah SWT.

Ing Ngarsa Sung Tuladha, Ing Madya Mangun Karsa, Tut Wuri Handayani
Artinya, di depan memberikan suri teladan, di tengah membangun kemauan dan
semangat, di belakang mengikuti sambil mengoreksi dan menjada keselamatan
semuanya
(Ki Hajar Dewantara)

Urip Iku Urup, artinya Hidup itu Nyala, Hidup itu hendaknya memberi manfaat
bagi orang lain disekitar kita, semakin besar manfaat yang bisa kita berikan tentu
akan lebih baik.

Tuhan menciptakan kedua mata kita di depan karena kita harus terus melihat ke
depan, bukan ke belakang dan terpaku pada masa lalu.
(Mario Teguh)

Kadang keberhasilan baru akan tiba setelah kesulitan dialami. Maka jangan
menyerah dalam menggapai keberhasilan walau kesulitan menghadang.
(Mario teguh)

PERSEMBAHAN

Skripsi ini saya persembahkan untuk :

- Allah SWT yang telah melimpahkan ilmu pengetahuan didunia ini untuk dipelajari dan menambah imanku serta berkahMu hingga aku dapat mencapai gelar Sarjana Komputer.
- Orang tua tercinta yang selama ini berjuang membesarkanku hingga aku kuliah, do'amu selalu menyertai aku.
- Dosen pembimbing, Ema Utami, Dr., S.Si, M.Komyang telah membimbing perjalanan skripsi ini. Terima kasih banyak bu Ema, semoga ilmu pengetahuan ini menjadi manfaat yang baik bagi siapapun yang menggunakannya.
- Keluarga besar kontrakan 168 (Anis, Beni, Hakim, Arif,) yang telah ikut berjuang membantu dalam membantu menyelesaikan skripsi saya terimakasih banyak,sukses buat kita semua.
- Muhammad Anis Rosyadi teman multitalent sekaligus teman blusukan menyusuri jalan setapak.
- Kelas S1-TI 10 dan 11 semoga kita semua dalam lindungan Allah SWT
- Seluruh teman-temanku dan keluarga besar STMIK AMIKOM Yogyakarta yang tidak dapat saya sebutkan satu-persatu, terima kasih banyak.

KATA PENGANTAR

Puji dan syukur penulis persembahkan untuk Allah SWT yang telah memberikan rahmat, hidayah dan kekuatan sehingga penulis dapat menyelesaikan skripsi ini sesuai dengan waktu yang diinginkan penulis. Tidak lupa sholawat dan salam penulis haturkan pada junjungan umat yaitu Nabi Muhammad SAW, yang telah menyebarkan agama Islam sehingga penulis dan seluruh umat Islam dapat merasakan indahnya Islam.

Skripsi ini disusun sebagai salah satu syarat kelulusan bagi setiap mahasiswa STMIK AMIKOM Yogyakarta. Selain itu juga merupakan suatu bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang program Strata-1 dan untuk memperoleh gelar Sarjana Komputer.

Dengan selesainya skripsi ini, maka penulis tidak lupa mengucapkan terima kasih kepada:

1. Bapak Prof. Dr. M. Suyanto, MM Selaku Ketua STMIK AMIKOM Yogyakarta.
2. Bapak Sudarmawan, MT. Selaku ketua jurusan Teknik Informatika STMIK AMIKOM Yogyakarta.
3. Ibu Ema Utami, Dr., S.Si, M.Kom Selaku dosen pembimbing yang telah banyak memberikan pengarahan bagi penulis dalam pembuatan skripsi.
4. Bapak dan Ibu Dosen STMIK AMIKOM Yogyakarta yang telah banyak memberikan ilmunya selama penulis kuliah.
5. Semua keluarga besar penulis terutama untuk kedua orang tua yang tidak bosan-bosannya memberikan dukungan, semangat, dan doa kepada penulis.

6. Teman-teman Saya yang telah membantu dan mendukung saat Saya menyusun skripsi ini
7. Semua pihak yang tidak dapat penulis sebutkan satu persatu yang telah membantu baik dukungan moril maupun materiil, pikiran, dan tenaga dalam penyelesaian skripsi ini.

Penulis tentunya menyadari bahwa pembuatan skripsi ini masih banyak kekurangan dan kelemahannya. Oleh karena itu penulis berharap kepada semua pihak agar dapat menyampaikan kritik dan saran yang membangun untuk menambah kesempurnaan skripsi ini. Namun penulis tetap berharap skripsi ini akan bermanfaat bagi semua pihak yang membacanya.

Yogyakarta, 08 Juli 2014

Penyusun

DAFTAR ISI

SKRIPSI.....	i
HALAMAN JUDUL	i
PERSETUJUAN.....	ii
PENGESAHAN.....	iii
PERNYATAAN.....	iv
MOTTO	v
PERSEMBAHAN.....	vi
KATA PENGANTAR.....	vii
DAFTAR ISI.....	ix
DAFTAR TABEL	xiii
DAFTAR GAMBAR.....	xiv
INTISARI.....	xviii
ABSTRACT.....	xix
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Rumusan Masalah.....	3
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	5
1.6 Metodologi Pengumpulan Data.....	5
1.7 Sistematika Penulisan.....	6
BAB II LANDASAN TEORI.....	8
2.1 Konsep Dasar <i>Kriptografi</i>	8
2.1.1 Pengertian <i>Kriptografi</i>	8
2.1.2 Pengenalan Algoritma <i>Kriptografi</i>	8
2.1.3 Tujuan <i>Kriptografi</i>	9
2.2 Macam-macam Algoritma <i>Kriptografi</i>	11
2.2.1 Algoritma Simetri (Konvensional).....	11

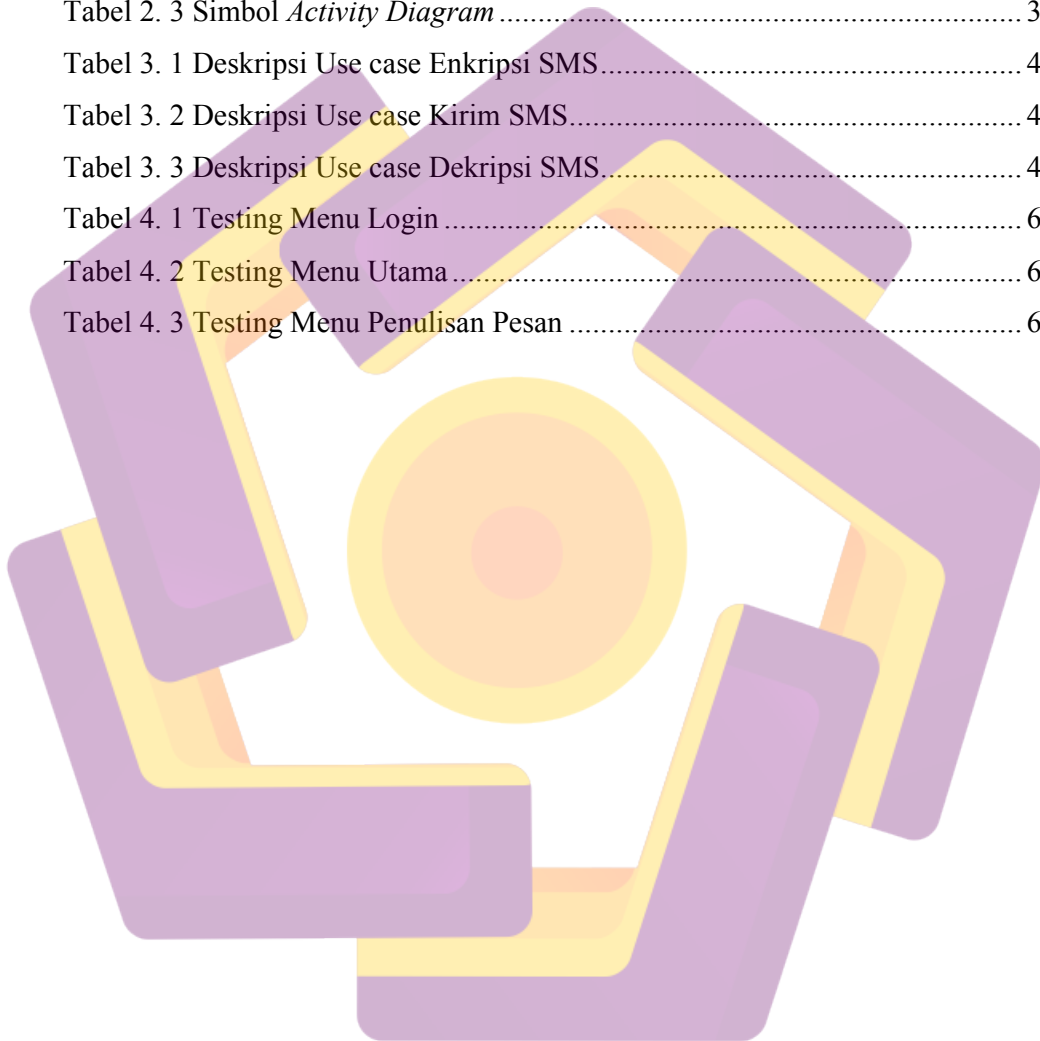
2.2.2	Algoritma Asimetri.....	13
2.2.3	Fungsi Hash.....	14
2.3	Sejarah Algoritma Rivest Code 6 (RC6)	15
2.3.1	Algoritma RC6	15
2.3.2	Key Expansion Algorithm	16
2.3.3	Algoritma Enkripsi	17
2.4	SMS (<i>Short Message Service</i>).....	21
2.4.1	Pengertian <i>Short Message Service</i> (SMS)	21
2.4.2	Cara Kerja SMS.....	22
2.4.3	Keuntungan SMS.....	23
2.5	Android	23
2.5.1	Pengertian Android.....	23
2.5.2	Sejarah Android.....	24
2.5.3	Arsitektur Android.....	24
2.6	UML (<i>Unified Modelling Language</i>)	27
2.6.1	Pengenalan UML.....	27
2.6.2	Tujuan UML.....	27
2.6.3.1	<i>Use Case Diagram</i>	28
2.6.3.2	<i>Activity Diagram</i>	30
2.6.3.3	<i>Sequence Diagram</i>	31
2.6.3.4	<i>Class Diagram</i>	32
2.7	Java	33
2.7.1	Pengertian Java.....	33
2.7.2	Sejarah Java.....	34
2.7.3	Java Platform.....	34
2.7.4	Struktur Pemrograman Java	35
2.8	Konsep OOP (<i>Object Oriented Programming</i>).....	35
2.9	Perangkat Lunak Yang Digunakan.....	37
2.9.1	Eclipse Integrated Development Environment (Eclipse IDE)	37
2.9.2	Android Software Development Kit (SDK).....	37
2.9.3	Android Development Tool (ADT) Plugins	37

BAB III ANALISIS DAN PERANCANGAN.....	39
3.1 Tinjauan Umum.....	39
3.2 Analisis Sistem.....	39
3.2.1 Analisis Kelemahan Sistem.....	39
3.2.2 Analisis Kebutuhan Sistem.....	41
3.2.2.1 Kebutuhan Fungsional.....	41
3.2.2.2 Kebutuhan Non Fungsional.....	42
3.2.3 Analisis Kelayakan sistem.....	43
3.2.3.1 Analisis Kelayakan Teknologi.....	44
3.2.3.2 Analisis Kelayakan Operasional.....	44
3.2.3.3 Analisis Sistem Operasi.....	44
3.2.3.4 Analisis Kebutuhan Pengguna.....	45
3.2.3.5 Analisis Kelayakan Hukum.....	45
3.3 Perancangan sistem.....	45
3.3.1 Perancangan UML.....	46
3.3.1.1 Use Case Diagram.....	47
3.3.1.2 Class Diagram.....	50
3.3.1.3 <i>Sequence Diagram</i>	51
3.3.1.4 <i>Activity Diagram</i>	53
3.3.2 Perancangan <i>Interface</i>	55
3.3.2.1 Rancangan Tampilan Login.....	56
3.3.2.2 Rancangan Tampilan Menu Utama.....	56
3.3.2.3 Rancangan Antar Muka Tampilan Tulis Pesan.....	57
3.3.2.4 Rancangan Antar Muka Tampilan Penerima.....	58
3.3.2.5 Rancangan Antar Muka Tampilan Bantuan.....	58
3.3.2.6 Rancangan Tampilan About.....	59
BAB IV IMPLEMENTASI DAN PEMBAHASAN.....	60
4.1 Implementasi.....	60
4.1.1 Uji Coba Sistem dan Program.....	60
4.1.1.1 <i>White Box Testing</i>	60
4.1.1.2 <i>Black Box Testing</i>	61

4.1.2	Manual Program	70
4.1.2.1	<i>Splash Screen</i>	70
4.1.2.2	Tampilan Menu Login	71
4.1.2.3	Form Menu Utama	72
4.1.2.4	Form Tulis Pesan	72
4.1.2.5	Form Kotak Masuk	74
4.1.2.6	Form Bantuan	74
4.1.2.7	Form About	75
4.1.2.8	Form Pengaturan Keamanan	76
4.1.3	Manual Instalasi	76
4.1.4	Pengembangan Sistem	79
4.2	Pembahasan	79
4.2.1	Pembahasan Listing Program	79
4.2.1.1	<i>Class SplashScreen</i>	79
4.2.1.2	<i>Class Login</i>	80
4.2.1.3	<i>Class Menu Utama</i>	82
4.2.1.4	Pembuatan <i>Class</i> Tulis Pesan	85
4.2.1.5	Pembuatan <i>Class</i> Inbox	89
4.2.1.6	Pembuatan <i>Class</i> Baca SMS	90
4.2.1.7	Pembuatan <i>Class</i> RC6	92
4.2.1.8	<i>Class</i> Pembuatan Menu Bantuan	98
BAB V PENUTUP		99
5.1	Kesimpulan	99
5.2	Saran	99
DAFTAR PUSTAKA		101

DAFTAR TABEL

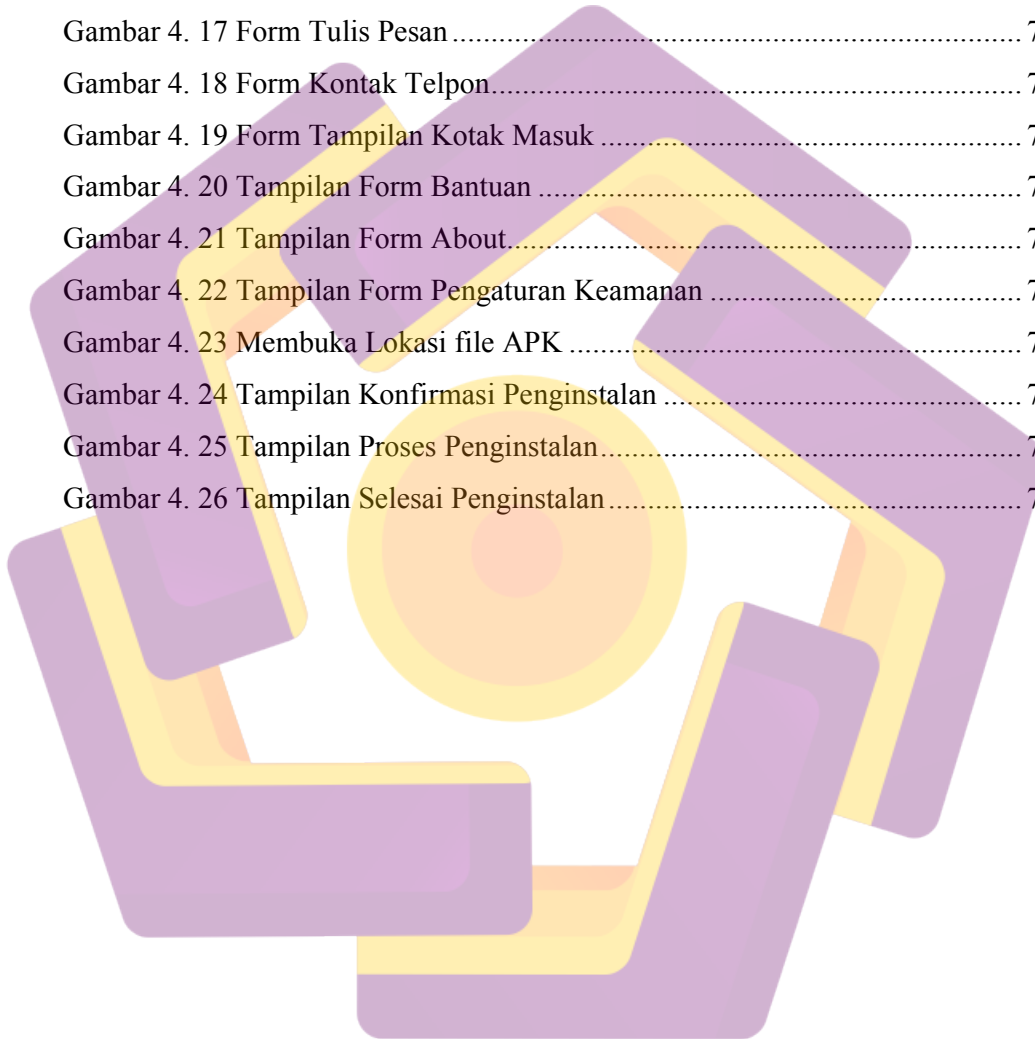
Tabel 2. 1 Sejarah Android	24
Tabel 2. 2 Simbol <i>Use Case Diagram</i>	29
Tabel 2. 3 Simbol <i>Activity Diagram</i>	31
Tabel 3. 1 Deskripsi Use case Enkripsi SMS.....	48
Tabel 3. 2 Deskripsi Use case Kirim SMS.....	48
Tabel 3. 3 Deskripsi Use case Dekripsi SMS.....	49
Tabel 4. 1 Testing Menu Login	62
Tabel 4. 2 Testing Menu Utama	63
Tabel 4. 3 Testing Menu Penulisan Pesan	66



DAFTAR GAMBAR

Gambar 2. 1 Model sederhana Sistem Kriptografi Simetris	12
Gambar 2. 2 Model sederhana Sistem Kriptografi Simetris	14
Gambar 2. 3 Diagram Enkripsi RC6.....	20
Gambar 2. 4 Gambar Skema Cara Kerja SMS.....	22
Gambar 2. 5 Arsitektur Android.....	25
Gambar 3. 1 <i>Use Case Diagram</i> Aplikasi.....	47
Gambar 3. 2 <i>Class Diagram</i> RHSms	51
Gambar 3. 3 <i>Sequence Diagram</i> Kirim SMS.....	52
Gambar 3. 4 <i>Sequence Diagram</i> Penerima SMS.....	52
Gambar 3. 5 <i>Sequence Diagram</i> Menu Bantuan.....	53
Gambar 3. 6 <i>Sequence Diagram</i> Menu Tentang Aplikasi	53
Gambar 3. 7 <i>Activity Diagram</i> mengirim Pesan	54
Gambar 3. 8 <i>Activity Diagram</i> Menerima SMS.....	55
Gambar 3. 9 Rancangan Tampilan Login	56
Gambar 3. 10 Rancang Tampilan Menu Utama	57
Gambar 3. 11 Rancangan Form Tulis Pesan	57
Gambar 3. 12 Rancangan Tampilan Form Penerima.....	58
Gambar 3. 13 Rancangan Tampilan Form Bantuan	59
Gambar 3. 14 Rancangan Tampilan Menu About	59
Gambar 4. 1 Kesalahan pada Kode Program	61
Gambar 4. 2 Testing Tombol Login	62
Gambar 4. 3 Testing Tombol Tulis Pesan.....	64
Gambar 4. 4 Testing Tombol Inbox	64
Gambar 4. 5 Testing Tombol About.....	65
Gambar 4. 6 Testing Tombol Help	65
Gambar 4. 7 Testing Tombol Pengaturan Keamanan.....	66
Gambar 4. 8 Testing Tombol Tambah Kontak.....	67
Gambar 4. 9 Testing Tombol Enkripsi Pesan	68
Gambar 4. 10 Testing Tombol Kirim Pesan	68
Gambar 4. 11 Peringatan No Tujuan Belum Diisi.....	69

Gambar 4. 12 Peringatan Kolom Pesan Belum Diisi	69
Gambar 4. 13 Peringatan Kunci Belum Diisi.....	70
Gambar 4. 14 Form Splash Screen	71
Gambar 4. 15 Form Login.....	71
Gambar 4. 16 Form Menu Utama.....	72
Gambar 4. 17 Form Tulis Pesan	73
Gambar 4. 18 Form Kontak Telpon.....	73
Gambar 4. 19 Form Tampilan Kotak Masuk	74
Gambar 4. 20 Tampilan Form Bantuan	75
Gambar 4. 21 Tampilan Form About.....	75
Gambar 4. 22 Tampilan Form Pengaturan Keamanan	76
Gambar 4. 23 Membuka Lokasi file APK	77
Gambar 4. 24 Tampilan Konfirmasi Penginstalan	77
Gambar 4. 25 Tampilan Proses Penginstalan.....	78
Gambar 4. 26 Tampilan Selesai Penginstalan.....	79



INTISARI

Perkembangan teknologi telekomunikasi yang begitu pesat telah memberikan manfaat begitu besar. Dengan adanya teknologi telekomunikasi, jarak dan waktu bukan lagi menjadi sebuah kendala yang berarti. Salah satu hasil teknologi komunikasi yang sangat terkenal adalah short Message services (SMS). Dengan menggunakan sms, pengguna dapat saling bertukar teks dengan pengguna lain.

SMS sangatlah populer, selain dikarenakan biayanya yang murah, pesan yang dikirimkan dapat diterima oleh penerima dengan baik dan cepat. Namun komunikasi melalui media SMS ini bukanlah komunikasi point-to-point, pesan yang dikirimkan melalui media SMS tidak langsung sampai pada tujuan, melainkan melalui jaringan SMS. Pada jaringan SMS tersebut, keamanan pesan sangatlah terancam untuk dibaca oleh orang yang tidak bertanggung jawab. Perangkat lunak yang dibangun meningkatkan keamanan pesan dengan melakukan enkripsi terhadap pesan yang dikirimkan.

Perangkat lunak yang dibangun menggunakan algoritma RC6 untuk melakukan enkripsi SMS agar keamanan pesan dapat ditingkatkan. Algoritma RC6 adalah suatu algoritma kunci privat yang dikenal dengan kesederhanaannya. Algoritma RC6 merupakan algoritma dengan parameter yang dapat bekerja pada panjang kunci yang beragam. Untuk aspek keamanannya, algoritma RC6 mengutamakan prinsip iterated *chiper*. Software ini dapat dibuat dan dijalankan pada emulator dan smartphone android.

Kata Kunci : SMS, Enkripsi, RC6, Aplikasi Android

ABSTRACT

Rapid expansion of telecommunication technology has brought a very big benefit for us. With the existence of telecommunication technology, many constraints such as distance, location, or time can be overcome. One of the technological results in telecommunication technology is Short Message Service or usually known as SMS. By using an SMS, the subscribers can do some exchange of text messages over each other.

SMS is very popular, besides due to its low cost, the message transmitted can be received by the receiver well and quickly. But this communication through SMS media communication is not a point-to-point, the message is sent via SMS media is not directly to the purpose, but rather via the SMS network. On the SMS network, messaging security is threatened to be read by people who are not responsible. The software is built increases messaging security by encrypting the messages sent.

The software is built using the RC6 algorithm for SMS encryption for increased security messages can be improved. RC6 algorithm is an algorithm which is known as the private key simplicity. RC6 algorithm is an algorithm with parameters that can work on a long-diverse key. For the safety aspects, RC6 algorithm prioritizes the principle of iterated cipher. This software can be created and run on the emulator and android smartphones.

Keyword : SMS, Encryption, RC6, Android Apps