

**APLIKASI ENKRIPSI DAN DEKRIPSI SMS BERBASIS ANDROID
MENGUNAKAN ALGORITMA RC6**

SKRIPSI



disusun oleh

Alfian Chandra Alviana

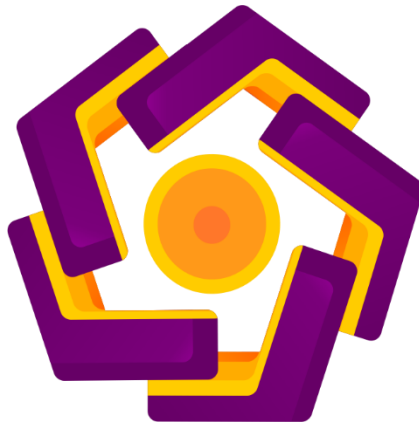
14.21.0759

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016**

**APLIKASI ENKRIPSI DAN DEKRIPSI SMS BERBASIS ANDROID
MENGUNAKAN ALGORITMA RC6**

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai gelar Sarjana
pada Program Studi Teknik Informatika



disusun oleh

Alfian Chandra Alviana

14.21.0759

**PROGRAM SARJANA
PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2016**

PERSETUJUAN

SKRIPSI

APLIKASI ENKRIPSI DAN DEKRIPSI SMS BERBASIS ANDROID MENGUNAKAN ALGORITMA RC6

yang dipersiapkan dan disusun oleh

Alfian Chandra Alviana

14.21.0759

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 8 Oktober 2016

Dosen Pembimbing,


Rizqi Sukma Kharisma, M.Kom
NIK. 190302215

PENGESAHAN

SKRIPSI

APLIKASI ENKRIPSI DAN DEKRIPSI SMS BERBASIS ANDROID MENGUNAKAN ALGORITMA RC6

yang dipersiapkan dan disusun oleh

Alfian Chandra Alviana

14.21.0759

telah dipertahankan di depan Dewan Penguji
pada tanggal 26 Mei 2016

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Rizqi Sukma Kharisma, M.Kom
NIK. 190302215

M. Rudyanto Arief, MT
NIK. 190302098

Ferry Wahyu Wibowo, S.Si., M.Cs
NIK. 190302235

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 31 Mei 2016



Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang berada 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 disuatu institusi pendidikan tinggi manapun, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau tidak diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Segala sesuatu terkait dengan naskah dan karya yang telah dibuat adalah menjadi tanggung jawab saya pribadi.

Yogyakarta, 31 Mei 2016



Alfian Chandra Alviana
14.21.0759

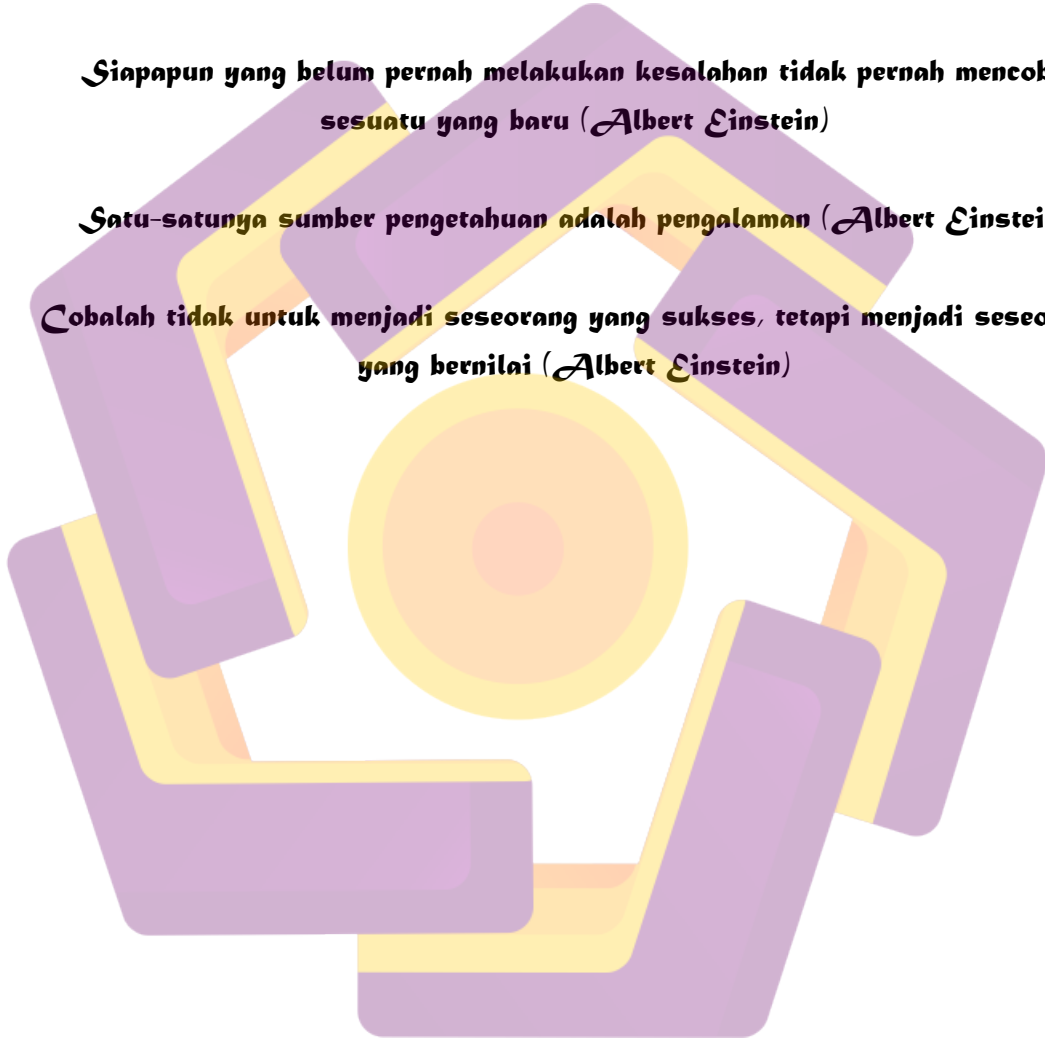
MOTTO

**sabarlah memang akan ada orang di masa depanmu yang malu dan menyesal
karena meremehkanmu saat muda
(Mario Teguh)**

**Siapapun yang belum pernah melakukan kesalahan tidak pernah mencoba
sesuatu yang baru (Albert Einstein)**

Satu-satunya sumber pengetahuan adalah pengalaman (Albert Einstein)

**Cobalah tidak untuk menjadi seseorang yang sukses, tetapi menjadi seseorang
yang bernilai (Albert Einstein)**



HALAMAN PERSEMBAHAN

Dengan mengucapkan alhamdulillah sebagai tanda rasa syukur kepada Allah SWT dan suri tauladanku Nabi Muhammad SAW yang selalu memberikan rahmatnya sehingga Skripsi ini dapat selesai. Adapun karya ini saya persembahkan untuk:

1. Kedua orang tua dan keluarga besar saya yang senantiasa memberikan dukungannya baik moral maupun materi dan selalu membimbing saya dengan do'a dan limpahan kasih sayang yang tak terbatas.
2. Bapak Rizqi Sukma Kharisma yang telah membimbing dari awal sampai akhir skripsi ini.
3. My sweetie "Sri Hastuti" saya persembahkan karya kecil ini buatmu, terimakasih atas, perhatian, semangat, dan kesabaran yang telah memberikanku semangat dan inspirasi dalam menyelesaikan Skripsi ini.
4. Buat shabat dan teman Indro, Wira, Rudi, Rayi, Surya, Eka, Yudi, Vira, Hendra, Aan, Arum, Yola, terimakasih atas do'a dan dukungan kalian, smoga kalian sukses.
5. Teman seperjuangan 14.TT.01. Terimakasih semoga yang masih skripsi cepat wisuda dan smoga sukses.
6. Dosen-dosen amikom yang telah memberi ilmu selama 2 tahun ini.
7. Semua pihak yang tidak bisa saya sebutkan satu persatu, yang telah membantu demi terselesaikannya skripsi ini. Terimakasih untuk semua bantuannya.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadiran Allah SWT yang senantiasa melimpahkan rahmat dan hidayahnya pada kita sehingga laporan skripsi ini dapat terselesaikan dengan baik.

Laporan skripsi ini penulis ajukan sebagai syarat kelulusan program Strata 1 jurusan Teknik Informasi pada Sekolah Tinggi Manajemen Informatika dan Komputer, STMIK Amikom Yogyakarta.

Dalam penyusunan laporan skripsi ini penulis banyak mendapat bimbingan dari berbagai pihak, maka dalam kesempatan ini penulis mengucapkan banyak terimakasih kepada:

1. Bapak Prof. Dr. Suyanto, MM, selaku ketua, STMIK Amikom Yogyakarta.
2. Bapak Sudarmawan, M.T, selaku ketua jurusan Teknik Informatika S1 Sekolah Tinggi Manajemen Informatika dan Komputer Amikom Yogyakarta.
3. Bapak Rizqi Sukma Kharisma yang telah membimbing dari awal sampai akhir skripsi ini.
4. Bapak M.Rudyanto Arief, MT dan bapak Ferry Wahyu Wibowo, S.Si., M.Cs

Penulis menyadari bahwa skripsi ini masih ada kekurangan, untuk itu segala kritik dan saran yang sifatnya membangun akan penulis terima dengan terbuka, demi kesempurnaan skripsi ini. Selain itu jika ada hal-hal yang tidak berkenan dalam skripsi ini penulis mohon maaf yang sebesar-besarnya. Smoga skripsi ini bermanfaat bagi penulis dan khususnya semua pihak.

Yogyakarta 31 Mei 2016



Penulis

DAFTAR ISI

HALAMAN JUDUL.....	i
HALAMAN PERSETUJUAN.....	ii
HALAMAN PENGESAHAN.....	iii
HALAMAN KEASLIAN	iv
MOTTO	v
HALAMAN PERSEMBAHAN	vi
KATA PENGANTAR	vii
DAFTAR ISI.....	viii
DAFTAR TABEL.....	xii
DAFTAR GAMBAR	xiii
INTISARI.....	xv
<i>ABSTRACT</i>	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	2
1.3 Batasan Penelitian	2
1.4 Maksud dan Tujuan Penelitian.....	2
1.5 Metode Penelitian.....	3
1.5.1 Metode Pengumpulan Data.....	3
1.5.2 Metode Analisis	3
1.5.3 Metode Perancangan	4
1.6 Sistematika Penulisan	4
BAB II LANDASAN TEORI	6
2.1 Tinjauan Pustaka	6
2.2 SMS.....	8
2.1 Cara Kerja SMS	9
2.3 Kriptografi.....	9
2.3.1 Komponen-komponen Kriptografi	10

2.3.2	Algoritma Kriptografi.....	11
2.4	Algoritma Kriptografi RC6.....	11
2.4.1	<i>Key Expansion Algorithm</i>	12
2.4.2	Algoritma Enkripsi Kriptografi RC6.....	12
2.4.3	Algoritma Dekripsi Kriptografi RC6.....	15
2.4.4	Keamanan Algoritma Kriptografi RC6	16
2.5	SDLC	16
2.6	Java.....	17
2.6.1	Sejarah Java.....	17
2.6.2	Pengertian Java.....	18
2.6.3	Java Platform.....	18
2.7	Android Studio.....	18
2.8	Whitebox Testing.....	19
2.9	Blackbox Testing	19
2.10	Android.....	19
2.8.1	<i>The Dalvik Virtual Machine (DVM)</i>	19
2.8.2	Android SDK (Software Development Kit).....	20
2.8.3	Arsitektur Android.....	20
2.11	Perangkat Pendukung.....	21
2.9.1	<i>Unified Modeling Language</i>	21
2.9.2	<i>Use Case</i>	21
2.9.3	<i>Class Diagram</i>	23
2.9.4	<i>Activity Diagram</i>	23
2.9.5	<i>Sequence Diagram</i>	24
BAB III ANALISIS DAN PERANCANGAN		25
3.1	Tinjauan Umum	25
3.2	Analisis Sistem.....	25
3.2.1	Analisis Kebutuhan Sistem.....	25
3.2.1.1	Kebutuhan Fungsional	25
3.2.1.2	Kebutuhan Nonfungsional	26
3.2.2	Analisis Kelayakan Sistem.....	27

3.2.2.1	Analisa Kelayakan Teknologi.....	27
3.2.2.2	Analisa Kelayakan Operasional.....	28
3.2.2.3	Analisa Kelayakan Operasi.....	28
3.2.2.4	Analisa Kelayakan Hukum.....	28
3.3	Perancangan Sistem.....	29
3.3.1	Perancangan UML.....	29
3.3.1.1	<i>Use Case Diagram</i>	29
3.3.1.2	<i>Class Diagram</i>	32
3.3.1.3	<i>Activity Diagram</i>	32
3.3.1.4	<i>Sequence Diagram</i>	37
3.3.2	Perancangan Interface.....	42
3.3.2.1	Rancangan Tampilan Menu Utama.....	42
3.3.2.2	Rancangan Tampilan Tulis Pesan.....	43
3.3.2.3	Rancangan Tampilan Penerima.....	44
3.3.2.4	Rancangan Tampilan Pesan Terkirim.....	45
3.3.2.5	Rancangan Tampilan Informasi.....	46
3.3.2.6	Rancangan Tampilan Bantuan.....	47
3.3.2.7	Rancangan Tampilan Tentang.....	48
BAB IV	IMPLEMENTASI DAN PEMBAHASAN	49
4.1	Implementasi.....	49
4.1.1	Implementasi Algoritma Enkripsi RC6.....	49
4.1.2	Implementasi Algoritma Dekripsi RC6.....	50
4.1.3	Implementasi Interface Menu Utama.....	50
4.1.3.1	Pembahasan Listing Program menu utama.....	51
4.1.4	Implementasi Interface Tulis Pesan.....	53
4.1.4.1	Pembahasan Listing Program Tulis Pesan.....	53
4.1.5	Implementasi Interface <i>Inbox</i> dan <i>Outbox</i>	58
4.1.5.1	Pembahasan Listing Program <i>Inbox</i>	58
4.1.5.2	Pembahasan Listing Program <i>Outbox</i>	61
4.1.6	Implementasi Interface Baca Pesan.....	62
4.1.6.1	Pembahasan Listing Program Baca Pesan.....	63

4.1.7 Implementasi Interface Menu Informasi.....	65
4.1.7.1 Pembahasan Listing Program Menu Informasi	65
4.1.8 Implementasi Interface Bantuan	66
4.1.8.1 Pembahasan Listing Program Bantuan.....	67
4.1.9 Implementasi Interface About	67
4.1.9.1 Pembahasan Listing Program Tentang	68
4.1.9.2 Listning Program Class RC6.java.....	68
4.2 Pengujian Aplikasi	73
4.2.1 <i>Whitebox Testing</i>	73
4.2.2 <i>Blackbox Testing</i>	74
4.2.2.1 Uji Coba Berbagai Jenis <i>Smartphone</i>	76
4.2.3 Pemeliharaan Sistem	76
4.2.4 Proses Upload APK pada Google Playstore.....	77
4.2.5 Distribusi	80
4.2.6 Instalasi Manual.....	83
BAB V PENUTUP.....	82
5.1 Kesimpulan	86
5.2 Saran.....	87
DAFTAR PUSTAKA	xvii

DAFTAR TABEL

Tabel 2.1 Tinjauan Pustaka.....	6
Tabel 2.2 Tinjauan Pustaka.....	7
Tabel 2.3 Tinjauan Pustaka.....	8
Tabel 2.4 Simbol use case diagram.....	22
Tabel 2.5 Simbol Class diagram.....	23
Tabel 2.6 Simbol Activity diagram.....	24
Tabel 2.4 Simbol Sequence diagram.....	24
Tabel 3.1 Kebutuhan Hardware.....	26
Tabel 3.2 Spesifikasi Smartphone.....	26
Tabel 3.3 Kebutuhan Software.....	27
Tabel 3.4 Deskripsi Use case enkripsi SMS.....	30
Tabel 3.5 Deskripsi Use case kirim SMS.....	30
Tabel 3.6 Deskripsi Use case dekripsi.....	31
Tabel 4.1 Testing Menu Utama.....	75
Tabel 4.1 Testing Tulis Pesan.....	75
Tabel 4.1 Testing Inbox dan Outbox.....	75
Tabel 4.1 Testing Baca Pesan.....	75
Tabel 4.1 Testing Menu Informasi.....	75
Tabel 4.1 Testing Bantuan.....	76
Tabel 4.1 Testing Tentang.....	76
Tabel 4.1 Hasil uji coba aplikasi pada berbagai jenis smartphone.....	76

DAFTAR GAMBAR

Gambar 2.1 Skema cara kerja SMS	9
Gambar 3.1 Use Case diagram aplikasi	29
Gambar 3.2 Class diagram RC6SMS.....	32
Gambar 3.3 Activity diagram Mengirim SMS.....	33
Gambar 3.4 Activity diagram Menerima SMS	34
Gambar 3.5 Activity diagram Membaca Pesan Terkirim	35
Gambar 3.6 Activity diagram bantuan	36
Gambar 3.7 Activity diagram tentang.....	37
Gambar 3.8 Sequence diagram penulisan pesan	38
Gambar 3.9 Sequence diagram penerima SMS.....	39
Gambar 3.10 Sequence diagram pesan terkirim	40
Gambar 3.11 Sequence diagram bantuan.....	41
Gambar 3.12 Sequence diagram tentang.....	41
Gambar 3.13 Rancangan Tampilan Menu utama.....	43
Gambar 3.14 Rancangan Tampilan Tulis Pesan	44
Gambar 3.15 Rancangan Tampilan Penerima.....	45
Gambar 3.16 Rancangan Tampilan Pesan Terkirim	46
Gambar 3.17 Rancangan Tampilan Menu informasi	47
Gambar 3.18 Rancangan Tampilan Bantuan	48
Gambar 3.19 Rancangan Tampilan Tentang.....	48
Gambar 4.1 Tampilan Menu Utama.....	51
Gambar 4.2 Tampilan Tulis Pesan dan Tombol Kontak.....	53
Gambar 4.3 Tampilan Inbox dan Outbox	58
Gambar 4.4 Tampilan Baca SMS.....	63
Gambar 4.5 Tampilan Menu Informasi.....	65
Gambar 4.6 Tampilan Bantuan	67
Gambar 4.7 Tampilan Tentang	68
Gambar 4.8 Kesalahan Kode Program.....	74

Gambar 4.9 Memasukkan APK baru	77
Gambar 4.10 Mengisi Nama Aplikasi	77
Gambar 4.11 Mengisi Store listing aplikasi	78
Gambar 4.12 Content Rating	78
Gambar 4.13 Memilih Negara untuk didistribusikan.....	79
Gambar 4.14 Proses Upload.....	79
Gambar 4.15 Pencarian Aplikasi.....	80
Gambar 4.16 Halaman Aplikasi.....	80
Gambar 4.17 Terima Perjanjian	81
Gambar 4.18 Proses Download dan Instalasi.....	81
Gambar 4.19 Proses Instalasi Selesai.....	82
Gambar 4.20 Jumlah Download dan Rating	82
Gambar 4.21 Membuka Lokasi APK.....	83
Gambar 4.22 Tampilan Konfirmasi Penginstalan.....	84
Gambar 4.23 Tampilan proses penginstalan	84
Gambar 4.24 Tampilan Instalasi selesai	85

INTISARI

Pada skripsi ini dibangun suatu perangkat lunak yang dapat berguna untuk meningkatkan keamanan pesan yang terjadi pada komunikasi melalui SMS. SMS merupakan suatu layanan yang diberikan oleh telepon selular kepada penggunanya untuk melakukan komunikasi melalui pengiriman pesan singkat dengan biaya yang murah. SMS sangatlah populer, selain dikarenakan biayanya yang murah, pesan yang dikirimkan dapat diterima oleh penerima dengan baik dan cepat. 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 merupakan algoritma dengan parameter yang dapat bekerja pada panjang kunci yang beragam. Untuk aspek keamanannya, algoritma RC6 mengutamakan prinsip iterated cipher.

Aplikasi yang dibangun penulis mempunyai tujuan untuk meningkatkan keamanan pesan dengan menggunakan enkripsi, perangkat yang dibangun menggunakan metode Algoritma RC6 Berbasis Android. Aplikasi ini diharapkan dapat melindungi isi pesan singkat yang dikirim oleh pengirim ke nomor tujuan dan melindungi pesan agar tidak dibaca oleh orang yang tidak bertanggung jawab.

Kata Kunci : SMS, Kriptografi, Android, RC6, Enkripsi, Dekripsi

ABSTRACT

This thesis built on a software that can be useful to improve the security of the message happens to communication via SMS. SMS is a service provided by mobile phone to its users to communicate via short message delivery with a cheap cost. SMS is extremely popular, besides the cost is cheap, because messages sent can be received by recipients with good and fast. messages sent through SMS media not directly to the destination, but rather through the SMS network. On the network security, the SMS messages are extremely threatened to be read by people who are not responsible. Software built improved security messages by encryption with a message that was sent.

The software is built using the RC6 algorithm to encrypt SMS so that security can be improved. RC6 algorithm is an algorithm with parameters that can work on a variety of key length. To the security aspects, giving priority to the principle of the RC6 algorithm is iterated cipher.

The author has built applications that aim to improve the security of the message using encryption, device built using the RC6 Algorithm-based method of Android. The application is expected to protect the contents of short messages that are sent by the sender to the destination number and protect messages from being read by people who are not responsible.

Keyword : SMS, Cryptography, Android, RC6, Encryption, Decryption