

**APLIKASI SMS ENKRIPSI PADA ANDROID DENGAN
ALGORITMA RC4 DAN BASE64**



SKRIPSI

**Disusun Sebagai Salah Satu Syarat
Untuk Memperoleh Gelar Sarjana Komputer
Pada Jurusan Ilmu Komputer / Informatika**

Disusun oleh:

M. ARIF FAUZI

24010310120002

**JURUSAN ILMU KOMPUTER / INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO**

2014

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Dengan ini saya menyatakan bahwa dalam tugas akhir / skripsi ini tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di Perguruan Tinggi dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis yang diacu pada naskah ini dan disebutkan dalam daftar pustaka.

Semarang, Juni 2014



M. Arif Fauzi

24010310120002

HALAMAN PENGESAHAN

Judul : Aplikasi SMS Enkripsi pada Android dengan Algoritma RC4 dan Base64
Nama : M. Arif Fauzi
NIM : 24010310120002

Telah diujikan pada sidang tugas akhir pada tanggal 26 Mei 2014 dan dinyatakan lulus pada tanggal 5 Juni 2014

Semarang, 5 Juni 2014

Mengetahui,

Ketua Jurusan Ilmu Komputer / Informatika



Nurdin Bahtiar, S.Si, M.T.

NIP. 19790720 200312 1 002

Mengetahui,

Panitia Penguji Tugas Akhir

Ketua

Helmie Arif Wibawa, S.Si, M.Cs

NIP 19780516 200312 1 001

HALAMAN PENGESAHAN

Judul : Aplikasi SMS Enkripsi pada Android dengan Algoritma RC4 dan Base64
Nama : M. Arif Fauzi
NIM : 24010310120002

Telah diujikan pada sidang tugas akhir pada tanggal 26 Mei 2014.

Pembimbing I,



Aris Sugiharto, S.Si, M.Kom

NIP 19710811 199702 1 004

Semarang, 5 Juni 2014

Pembimbing II,



Sutikno, S.T, M.Cs

NIP 19790524 200912 1 003

ABSTRAK

Short Message Service (SMS) adalah sebuah mekanisme pengiriman pesan singkat melalui jaringan *mobile*. *Short Message Service* (SMS) yang dikirim tidak langsung diterima oleh penerima, melainkan harus melalui *short message service center* (SMSC) terlebih dahulu. Hal ini dapat dimanfaatkan oleh orang-orang yang tidak bertanggung jawab untuk mencuri informasi dalam SMS tersebut. Salah satu alternatif yang digunakan untuk menjaga kerahasiaan SMS adalah dengan mengenkripsi SMS terlebih dahulu sebelum SMS dikirim. Metode enkripsi yang digunakan yaitu algoritma kriptografi RC4 dan base64. Aplikasi ini dibuat dengan menggunakan metode pengembangan perangkat lunak *Unified Process* dan implementasinya menggunakan bahasa pemrograman Java serta diperuntukan untuk *smartphone* dengan sistem operasi Android. Aplikasi SMS enkripsi dengan algoritma RC4 dan Base64 telah diuji dengan menggunakan metode pengujian *blackbox* dan dapat berjalan dengan baik pada *smartphone* Android sesuai dengan yang diharapkan yakni dapat mengirimkan SMS, menerima SMS serta melakukan enkripsi dan dekripsi.

Kata Kunci : RC4, Base64, Enkripsi, *Short Message Service* (SMS), Android

ABSTRACT

Short Message Service (SMS) is a mechanism of delivery of short messages over mobile networks. Short Message Service (SMS) sent was not immediately accepted by the recipient, but must go through a short message service center (SMSC) in advance. It can be used by people who are not responsible for stealing information in the SMS proficiency level. One alternative that is used to maintain the confidentiality of SMS is by encrypting SMS before SMS was sent . The encryption method used is the cryptographic algorithm RC4 and base64. This application is created using software development methods Unified Process and its implementation using the Java programming language and is intended for smartphones with Android operating system. Applications SMS encryption with RC4 and Base64 algorithm has been tested using blackbox testing methods and can run well on Android smartphones as expected, it can send SMS, receive SMS and perform encryption and decryption.

Keywords : RC4, Base64, Encryption, *Short Message Service* (SMS), Android

KATA PENGANTAR

Segala puji syukur bagi Allah SWT atas karunia-Nya yang diberikan kepada penulis sehingga penulis dapat menyelesaikan penulisan laporan Tugas Akhir ini.

Laporan Tugas Akhir yang berjudul **“Aplikasi SMS Enkripsi pada Android dengan Algoritma RC4 dan Base64”** disusun sebagai salah satu syarat untuk memperoleh gelar sarjana komputer pada jurusan Ilmu Komputer / Informatika Universitas Diponegoro. Pada penelitian Tugas Akhir ini, mahasiswa dituntut untuk mengimplementasikan ilmu yang telah didapatkan di bangku perkuliahan untuk menyelesaikan suatu permasalahan yang ada dengan menggunakan teknik penelitian ilmiah.

Pada penyusunan laporan ini, tentulah Penulis banyak mendapat bimbingan dan bantuan dari berbagai pihak. Untuk itu, pada kesempatan ini penulis mengucapkan rasa hormat dan terima kasih kepada :

1. Dr. Muhammad Nur, DEA, selaku Dekan Fakultas Sains dan Matematika (FSM) Universitas Diponegoro
2. Nurdin Bahtiar, S.Si, M.T, selaku Ketua Jurusan Ilmu Komputer / Informatika FSM UNDIP
3. Indra Waspada, S.T, M.T, selaku Dosen Koordinator Tugas Akhir Jurusan Ilmu Komputer / Informatika FSM UNDIP
4. Aris Sugiharto, S.Si, M.Kom, selaku Dosen Pembimbing I yang telah membantu dalam proses bimbingan hingga terselesaikannya laporan Tugas Akhir ini.
5. Sutikno, S.T, M.Cs, selaku Dosen Pembimbing II yang telah membantu dalam proses bimbingan hingga terselesaikannya laporan Tugas Akhir ini.
6. Teman Jurusan Ilmu Komputer/ Informatika, khususnya angkatan 2010 yang senasib sepenanggungan.
7. Semua pihak yang telah membantu kelancaran dalam pelaksanaan Tugas Akhir, yang tidak dapat penulis sebutkan satu persatu.

Penulis menyadari bahwa dalam laporan ini masih banyak kekurangan baik dari segi materi ataupun dalam penyajiannya karena keterbatasan kemampuan dan pengetahuan Penulis. Oleh karena itu, kritik dan saran sangat penulis harapkan.

Semoga laporan ini dapat bermanfaat bagi pembaca pada umumnya dan penulis pada khususnya.

Semarang, Juni 2014
Penulis,

M. Arif Fauzi

DAFTAR ISI

	Hal
HALAMAN PERNYATAAN KEASLIAN SKRIPSI.....	ii
HALAMAN PENGESAHAN	iii
ABSTRAK	v
ABSTRACT	vi
KATA PENGANTAR.....	vii
DAFTAR ISI	ix
DAFTAR GAMBAR.....	xi
DAFTAR TABEL	xiii
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	2
1.3. Tujuan dan Manfaat	2
1.4. Ruang Lingkup	2
1.5. Sistematika Penulisan	3
BAB II LANDASAN TEORI.....	4
2.1. <i>Short Message Service</i> (SMS)	4
2.2. Android	7
2.3. Konsep Berorientasi Objek	10
2.4. <i>Unified Process</i>	12
2.5. <i>Unified Modelling Language</i>	15
2.6. Kriptografi	21
2.7. Algoritma Kriptografi RC4.....	23
2.8. Base64.....	25
BAB III DEFINISI KEBUTUHAN, ANALISIS, DAN PERANCANGAN	27
3.1. Definisi Kebutuhan	27
3.1.1. Gambaran Umum	27
3.1.2. Model Use case	32
3.1.3. Kebutuhan Non-fungsional Perangkat Lunak	41
3.2. Analisis	41
3.2.1. <i>Use Case Realization</i> Tahap Analisis	41

3.2.2. <i>Analysis Class</i>	44
3.3. Perancangan	46
3.3.1. <i>Use case</i> Realization Tahap Perancangan	46
3.3.2. Perancangan Antarmuka	52
3.3.3. Kelas Perancangan	56
BAB IV IMPLEMENTASI DAN PENGUJIAN	58
4.1. Implementasi.....	58
4.1.1. Spesifikasi Perangkat	58
4.1.2. Implementasi Class	58
4.1.3. Implementasi <i>Database</i>	59
4.1.4. Implementasi Antarmuka	59
4.2. Pengujian	68
4.2.1. Lingkungan Pengujian.....	68
4.2.2. Rencana Pengujian	69
4.2.3. Pelaksanaan Pengujian	69
4.2.4. Evaluasi Pengujian	69
BAB V PENUTUP	70
5.1. Kesimpulan	70
5.2. Saran	70
DAFTAR PUSTAKA	71
LAMPIRAN 1	73

DAFTAR GAMBAR

	Hal
Gambar 2.1 Proses Pengiriman SMS	4
Gambar 2.2 Proses Pengiriman SMS Antar Teknologi Jaringan yang Berbeda	5
Gambar 2.3 Arsitektur Android.....	9
Gambar 2.4 Contoh Kelas	10
Gambar 2.5 Hubungan Fase dengan Workflow dalam Unified Process	13
Gambar 2.6 Contoh Dependency.....	16
Gambar 2.7 Contoh Association.....	16
Gambar 2.8 Contoh Generalization	17
Gambar 2.9 Ilustrasi Enkripsi dan Dekripsi	22
Gambar 2.10 Ilustrasi Encoding dan Decoding Base64	26
Gambar 3.1 Deskripsi Umum Aplikasi SMS	27
Gambar 3.2 Alur Proses Aplikasi SMS	28
Gambar 3.3 Alur Proses Enkripsi	29
Gambar 3.4 Alur Proses Dekripsi.....	31
Gambar 3.5 Use Case Diagram	33
Gambar 3.6 Activity Diagram Menulis SMS	34
Gambar 3.7 Activity Diagram Akses Inbox	35
Gambar 3.8 Activity Diagram Akses Outbox	35
Gambar 3.9 Activity Diagram Enkripsi Pesan	36
Gambar 3.10 Activity Diagram Dekripsi Pesan	37
Gambar 3.11 Analysis Class Use Case Menulis SMS	42
Gambar 3.12 Analysis Class Use Case Akses Inbox	42
Gambar 3.13 Analysis Class Use Case Akses Outbox.....	43
Gambar 3.14 Analysis Class Use Case Enkripsi Pesan.....	43
Gambar 3.15 Analysis Class Use Case Dekripsi Pesan	43
Gambar 3.16 Realisasi Use Case Menulis SMS.....	46
Gambar 3.17 Sequence Diagram Menulis SMS.....	47
Gambar 3.18 Realisasi Use case Akses Inbox.....	48

Gambar 3.19 Sequence Diagram Akses Inbox	48
Gambar 3.20 Realisasi Use case Akses Outbox	49
Gambar 3.21 Sequence Diagram Akses Outbox	49
Gambar 3.22 Realisasi Use Case Enkripsi Pesan	50
Gambar 3.23 Sequence Diagram Enkripsi Pesan	51
Gambar 3.24 Realisasi Use case Dekripsi Pesan.....	51
Gambar 3.25 Sequence Diagram Dekripsi Pesan	52
Gambar 3.26 Sketsa Tampilan Awal Aplikasi SMS Enkripsi.....	53
Gambar 3.27 Sketsa Tampilan Menulis SMS Aplikasi SMS Enkripsi	53
Gambar 3.28 Sketsa Tampilan Inbox Aplikasi SMS Enkripsi	54
Gambar 3.29 Sketsa Tampilan DecryptSMS Aplikasi SMS Enkripsi.....	54
Gambar 3.30 Sketsa Tampilan Outbox Aplikasi SMS Enkripsi	55
Gambar 3.31 Sketsa Tampilan ShowOutbox Aplikasi SMS Enkripsi	55
Gambar 3.32 Sketsa Tampilan Enkripsi Pesan Aplikasi SMS Enkripsi.....	56
Gambar 3.33 Sketsa Tampilan Dekripsi Pesan Aplikasi SMS Enkripsi	56
Gambar 4.1 Antarmuka Halaman Main	60
Gambar 4.2 Antarmuka Menulis SMS	60
Gambar 4.3 Antarmuka Inbox	61
Gambar 4.4 Antarmuka DecryptSMS	61
Gambar 4.5 Antarmuka Outbox	62
Gambar 4.6 Antarmuka ShowOutbox	62
Gambar 4.7 Antarmuka Enkripsi Pesan	63
Gambar 4.8 Antarmuka Dekripsi Pesan	63

DAFTAR TABEL

	Hal
Tabel 2.1 Tabel PDU	7
Tabel 2.2 Notasi Use Case Diagram.....	18
Tabel 2.3 Simbol Activity Diagram	19
Tabel 2.4 Simbol Class Diagram.....	19
Tabel 2.5 Simbol Stereotype	20
Tabel 2.6 Simbol Sequence Diagram	21
Tabel 2.7 Tabel Base64	25
Tabel 3.1 Daftar Aktor.....	32
Tabel 3.2 Daftar Use Case.....	32
Tabel 3.3 Detail Use Case Menulis SMS	38
Tabel 3.4 Detail Use case Akses Inbox	39
Tabel 3.5 Detail Use Case Akses Outbox	39
Tabel 3.6 Detail Use Case Enkripsi Pesan	40
Tabel 3.7 Detail Use Case Dekripsi Pesan	41
Tabel 3.8 Hasil Identifikasi Analysis Class.....	44
Tabel 3.9 Daftar Tanggung Jawab dan Atribut Analysis Class	45
Tabel 3.10 Identifikasi Class Perancangan Use Case Menulis SMS.....	46
Tabel 3.11 Identifikasi Class Perancangan Use Case Akses Inbox.....	47
Tabel 3.12 Identifikasi Class Perancangan Use Case Akses Outbox	49
Tabel 3.13 Identifikasi Class Perancangan Use Case Enkripsi Pesan.....	50
Tabel 3.14 Identifikasi Class Perancangan Use Case Enkripsi Pesan.....	51
Tabel 3.15 Hasil Identifikasi Kelas Perancangan.....	57
Tabel 3.16 Rancangan Tabel Outbox	57
Tabel 4.1 Implementasi Class.....	59
Tabel 4.2 Rancangan Implementasi Tabel	59
Tabel 4.3 Tabel Rencana Pengujian	69

BAB I

PENDAHULUAN

Bab ini menyajikan latar belakang, rumusan masalah, tujuan dan manfaat dan ruang lingkup mengenai tugas akhir aplikasi sms enkripsi pada android dengan algoritma RC4 dan base64.

1.1. Latar Belakang

Perkembangan teknologi di bidang telekomunikasi dari tahun ke tahun mengalami kemajuan yang pesat, hal ini dapat dilihat dari semakin banyaknya ponsel pintar (*smartphone*) yang digunakan oleh masyarakat. Dari berbagai macam sistem operasi yang digunakan pada *smartphone*, sistem operasi Android yang paling menguasai pasar, terlihat dari pangsa pasar android pada kuartal kedua tahun 2013 sebanyak 79% di seluruh dunia[1].

Smartphone memiliki berbagai macam fitur yang dapat digunakan diantaranya *telephone*, *video call*, *Short Message Service (SMS)*, *internet* dan lain sebagainya. Dari sekian banyak fitur tersebut yang masih banyak digunakan adalah layanan SMS. Sayangnya layanan SMS tidak menjamin keamanan atau kerahasiaan pesan yang disampaikan[5]. Pesan yang bersifat personal tidak dijamin sampai ke penerima tanpa dicuri informasinya oleh orang lain.

Pesan yang dikirim tidak langsung diterima oleh penerima, melainkan harus melalui *short message service center (SMSC)* terlebih dahulu. SMSC yaitu sistem yang mengelola pesan singkat dalam jaringan nirkabel. Hal ini dapat dimanfaatkan oleh orang-orang yang tidak bertanggung jawab untuk mencuri informasi dalam pesan tersebut.

Dengan demikian dibutuhkan suatu metode dan aplikasi yang dapat menjaga kerahasiaan pesan yang dikirim, sehingga pesan hanya dapat dibaca maknanya oleh pengirim dan penerima yang sah. Salah satu metodenya yaitu dengan mengenkripsi pesan tersebut terlebih dahulu sebelum pesan dikirim dan untuk penerima harus mendekripsi pesan terlebih dahulu agar dapat dibaca maknanya. Metode-metode yang digunakan untuk enkripsi sangat beragam mulai dari metode klasik hingga modern, klasik misalnya Vigenere, ROT13 dan Caesar, sedangkan algoritma modern misalnya

DES, RC2, RC4, RC5, RC6 dan lain sebagainya. Diantara kelima metode enkripsi modern yang telah disebutkan sebelumnya, metode enkripsi RC4 merupakan algoritma kriptografi *stream cipher* sedangkan yang lainnya merupakan algoritma kriptografi *block cipher*.

Algoritma kriptografi *stream cipher* (cipher aliran) yakni beroperasi pada *byte* tunggal, artinya proses enkripsi dan dekripsi dilakukan setiap satu *byte*, oleh karena termasuk dalam cipher aliran maka dalam proses enkripsi RC4 memakan waktu yang sangat singkat. Base64 digunakan untuk menyembunyikan *text* (dalam tugas akhir ini ciphertext hasil RC4) agar makin tidak bisa dibaca atau disalin oleh orang lain[15].

Aplikasi ini diharapkan dapat menjadi alternatif dalam pengiriman SMS yang lebih mengedepankan aspek keamanan pesan yang dikirim.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang masalah tersebut dapat dibuat rumusan masalah yaitu bagaimana membuat aplikasi sms enkripsi pada android dengan menggunakan algoritma RC4 dan base64 untuk menjaga kerahasiaan pesan yang dikirim.

1.3. Tujuan dan Manfaat

Tujuan yang ingin dicapai dari tugas akhir ini yaitu menghasilkan aplikasi sms enkripsi yang digunakan untuk menjaga kerahasiaan pesan.

Adapun manfaat yang diharapkan dari penelitian ini yaitu :

1. Dengan menggunakan aplikasi ini seseorang dapat mengirimkan suatu informasi tanpa rasa takut akan diketahuinya isi informasi yang dikirimkannya tersebut oleh orang lain.
2. Sebagai sarana pengembangan aplikasi pada bidang kewanaman (*security*).

1.4. Ruang Lingkup

Adapun ruang lingkup dalam pembuatan aplikasi sms enkripsi pada android dengan algoritma RC4 dan base64 adalah sebagai berikut:

1. Input berupa SMS
2. Spesifikasi SMS (panjang 1 pesan SMS) disesuaikan dengan standar teknologi *Global System for Mobile Communication (GSM)*
3. Aplikasi dapat digunakan untuk *smartphone* dengan sistem operasi Android versi Jelly Bean.

4. Bahasa pemrograman yang digunakan adalah Java.
5. Menggunakan aplikasi Eclipse IDE for Java Developers dalam pembuatan aplikasi enkripsi SMS ini.

1.5. Sistematika Penulisan

Sistematika penulisan yang digunakan dalam tugas akhir ini terbagi dalam beberapa pokok bahasan, yaitu:

BAB I PENDAHULUAN

Merupakan pendahuluan yang berisi latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup, serta sistematika penulisan.

BAB II DASAR TEORI

Berisi kumpulan studi pustaka yang berhubungan dengan topik tugas akhir. Dasar teori ini meliputi pengertian *Short Message Service* (SMS), sistem operasi android, konsep berorientasi objek, metode pengembangan perangkat lunak *unified process*, *unified modelling language*, algoritma kriptografi RC4 dan base64.

BAB III DEFINISI KEBUTUHAN, ANALISIS, DAN PERANCANGAN

Membahas tahap definisi kebutuhan, analisis, dan tahap perancangan, serta hasil yang didapat pada ketiga tahap tersebut.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Membahas tahap implementasi dan rincian pengujian sistem yang dibangun dengan metode *black box*.

BAB V PENUTUP

Berisi kesimpulan yang diambil berkaitan dengan sistem yang dikembangkan dan saran-saran untuk pengembangan sistem lebih lanjut.