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

FSM UNDIP

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.

Semarang, 5 Juni 2014

Pembimbing I,	Pembimbing II,
Aris Sugiharto, S.Si, M.Kom	**Sutikno, S.T, M.Cs**
NIP 19710811 199702 1 004	**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 tesebut. 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

DAFTAR GAMBAR

Hal

DAFTAR TABEL

Hal

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 quartal 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 sebaginya. 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 tesebut.

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 sebaginya. 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 ciphetext 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 kerahasian 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 kemanan (*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.