RANCANG BANGUN APLIKASI KRIPTOGRAFI SMS MENGGUNAKAN ALGORITMA RIJNDAEL BERBASIS ANDROID

SKRIPSI

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

Disusun Oleh:
FAHD RYIFIH
J2F007012

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 suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan di dalam daftar pustaka.

Semarang, 23 Juli 2014

Fahd Ryifih
J2F007012

HALAMAN PENGESAHAN

Judul : Rancang Bangun Aplikasi Kriptografi SMS Menggunakan Algoritma Rijndael Berbasis Android

Nama : Fahd Ryifih

NIM : J2F007012

Telah diujikan pada sidang tugas akhir pada tanggal 15 Juli 2014 dan dinyatakan lulus pada tanggal 23 Juli 2014

Semarang, 24 Juli 2014

Mengetahui,
Ketua Jurusan Ilmu Komputer / Informatika
FSM Universitas Diponegoro,

Nurdin Bahtiar, S.Si, M.T.
NIP. 1979 0720 2003 12 1 002

Panitia Penguji Tugas Akhir
Ketua,

Dra. Indriyati, M.Kom
NIP. 1952 0610 1983 03 2 001

HALAMAN PENGESAHAN

Judul : Rancang Bangun Aplikasi Kriptografi SMS Menggunakan Algoritma Rijndael Berbasis Android

Nama : Fahd Ryifih

NIM : J2F007012

Telah diujikan pada sidang tugas akhir pada tanggal 15 Juli 2014.

Semarang, 24 Juli 2014

Pembimbing Utama

Beta Noranita, S.Si, M.Kom

NIP. 1973 0829 1998 02 2 001

ABSTRAK

Salah satu hasil teknologi telekomunikasi yang banyak digunakan adalah Short Message Service (SMS). Dengan menggunakan SMS, pengguna dapat saling bertukar pesan teks dengan pengguna lain. Proses pengiriman pesan melalui SMS tidak memiliki standar keamanan tertentu, sehingga semua orang yang memiliki hak khusus dan kemampuan yang cukup dapat dengan mudah mengetahui isi pesan SMS yang dikirim. Keamanan dan kerahasiaan pesan SMS tidak dapat terpenuhi dalam proses pengiriman SMS. Untuk memenuhi aspek kerahasiaan dan keamanan pesan yang dikirimkan, diperlukan aplikasi yang menerapkan teknik kriptografi. Dengan teknik kriptografi, pesan SMS yang dikirim hanya dapat dibaca atau dilihat oleh orang yang memiliki otoritas untuk membaca pesan SMS tersebut. Aplikasi Kriptografi SMS Rijndael dibangun untuk mengatasi permasalahan tersebut. Rijndael merupakan sebuah algoritma yang kuat dan aman serta telah menjadi algoritma standar internasional untuk proses pengenkripsian data. Aplikasi ini mengimplementasikan algoritma Rijndael dalam proses enkripsi dan dekripsi pesannya serta dibangun menggunakan bahasa pemrograman java-android sehingga dapat diimplementasikan pada telepon seluler berbasis android. Hasil keluaran dari aplikasi ini berupa pesan SMS yang dapat dimengerti maknanya jika kunci dekripsi yang dimasukkan benar dan dapat pula berupa pesan SMS yang tidak dapat dimengerti maknanya jika kunci dekripsi yang dimasukkan salah.

Kata kunci: Kriptografi, SMS, Enkripsi, Dekripsi, Rijndael, Android.

ABSTRACT

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. Sending messages by SMS have not security standard, so make all of the people with privilege and the enough capability is able to known the sent messages. Security and privacy of messages, cannot be implemented in the process of sending SMS. To achieve privacy and security aspects of the message, an application is required to apply cryptography techniques. With cryptography techniques, the message can only read or seen by people who have the authority to read the message. Rijndael SMS Cryptography Application is developed to solve those problems. Rijndael is strong and save algorithm that has become an international standard algorithm for data encryption process. This Application is developed using the Rijndael algorithm and built using java-android technology that can be implemented in android mobile phones. The output of this application is messages that the meaning can only be understood if the decryption key inputted is correct and vice versa.

Keywords: Cyptography, SMS, Encryption, Decryption, Rijndael, Android.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyusun tugas akhir yang berjudul "**Rancang Bangun Aplikasi Kriptografi SMS Menggunakan Algoritma Rijndael Berbasis Android**."

Tugas akhir ini disusun sebagai salah satu syarat untuk memperoleh gelar sarjana strata satu pada Jurusan Ilmu Komputer / Informatika Fakultas Sains Dan Matematika Universitas Diponegoro Semarang.

Dalam penyusunan tugas akhir ini, penulis mendapat bantuan dan dukungan dari banyak pihak. Atas peran sertanya dalam membantu dalam penyelesaian tugas akhir ini, penulis ingin mengucapkan terima kasih kepada:

1. Bapak Dr. Muhammad Nur, DEA selaku Dekan Fakultas Sains dan Matematika Universitas Diponegoro.
2. Bapak Nurdin Bahtiar, S.Si, M.T Ketua Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro.
3. Bapak Indra Waspada, ST, M.TI selaku Koordinator Tugas Akhir Jurusan Ilmu Komputer / Informatika Fakultas Sains dan Matematika Universitas Diponegoro.
4. Ibu Beta Noranita, S.Si, M.Kom selaku pembimbing I yang telah meluangkan waktu untuk membimbing dan mengarahkan Penulis dalam menyelesaikan tugas akhir ini.
5. Bapak dan Ibu dosen Jurusan Ilmu Komputer / Informatika FSM UNDIP.
6. Orang tua saya Bapak Holidy Ramlan dan Ibu Radiyem Wongso Taruno yang tak pernah berhenti memberikan yang terbaik untuk anak-anaknya.
7. Keluarga besar Ramlan dan Wongso Taruno yang selalu memberikan dukungan dan doa.
8. Abilerim semua, spesial untuk Ainurrizan, Alfa Rizky Hadi M dan Teguh Setyawan.
9. Teman-teman yang telah memberikan bantuan dan semangatnya hingga terselesaikannya Laporan Tugas Akhir ini, spesial untuk Jati Wahyu Aji, Rachman Muliawan Darmawan, Romadhoni Rosyid, Isa Kurniawan, Ervian Chandra, Rahmad Budi N, Akhwal Sadida, Nastiti Nuryani, Lusiana K, Widodo MS, Isa Ferry C, dan Indra Novian P.

10. Semua pihak yang telah membantu hingga selesainya tugas akhir ini, yang tidak dapat penulis sebutkan satu persatu. Semoga Allah membalas segala kebaikan yang telah Anda berikan kepada penulis.

Penulis menyadari bahwa masih banyak kekurangan dalam penyusunan laporan tugas akhir ini, untuk itu penulis mohon maaf dan mengharapkan saran serta kritik yang membangun dari pembaca. Semoga laporan tugas akhir ini dapat bermanfaat bagi pengembangan ilmu dan pengetahuan, khususnya pada bidang Informatika.

Semarang, 23 Juli 2014

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup, serta sistematika penulisan laporan tugas akhir mengenai Rancang Bangun Aplikasi Kriptografi SMS Menggunakan Algoritma Rijndael Berbasis Android.

1.1. Latar Belakang

Perkembangan teknologi pada era sekarang ini sudah sangat pesat, salah satu yang terus berkembang adalah teknologi di bidang telepon seluler. Seiring perkembangan teknologi telepon seluler, fitur-fitur yang terdapat di dalamnya mengalami perkembangan. Mulai dari fitur percakapan, *Short Messaging Service* (SMS), *Multimedia Messaging Service* (MMS), kamera, koneksi internet, pemutar lagu, dan *instant messaging* atau *chatting* maupun *push-email* yang memungkinkan untuk mengirim atau menerima *email* selayaknya SMS. Salah satu dari banyaknya fitur yang ada, fitur yang paling penting dan mudah digunakan serta murah adalah pengiriman data berupa teks yang lebih dikenal dengan nama SMS.

SMS adalah sebuah layanan yang dilaksanakan dengan sebuah telepon seluler untuk mengirim atau menerima pesan-pesan pendek. Pada mulanya SMS dirancang sebagai bagian daripada *Global System for Mobile Communication* (GSM) fase pertama, tetapi sekarang sudah didapatkan pada jaringan bergerak lainnya termasuk jaringan *Universal Mobile Telecommunications System* (UMTS) (Hendra, 2010).

Walaupun SMS merupakan bagian dari kemampuan standar GSM fase pertama, SMS masih merupakan layanan yang banyak digunakan oleh masyarakat. Bahkan berdasarkan survei yang dilakukan oleh Nielsen Mobile di Amerika pada kuartal ke-dua tahun 2008, pelanggan telepon seluler di Amerika Serikat lebih banyak menggunakan SMS dibanding melakukan percakapan telepon (Reardon, 2008). Berbagai kemudahan yang ditawarkan oleh SMS antara lain adalah informasi sesuai permintaan, pengunduhan nada dering, sampai dengan transaksi perbankan atau *mobile banking*.

Proses pengiriman pesan melalui layanan SMS tidak memiliki format keamanan tertentu dan tidak menjamin kerahasiaan pesan dan perlindungan terhadap pemalsuan serta pengubahan pesan yang tidak diinginkan. Hal tersebut dikarenakan pesan SMS mulai dienkripsi di *Base Transceiver Station* (BTS), sehingga ada peluang untuk melakukan SMS *spoofing* pada saat pengiriman pesan SMS dari telepon seluler menuju BTS. Pada proses enkripsi pesan SMS di BTS pun, algoritma yang digunakan adalah algoritma A5 yang memang merupakan algoritma enkripsi standar GSM yang telah diketahui kelemahannya dan dapat dibuka dengan mudah oleh kriptoanalis (Soeryowardhana, 2012).

Selain itu, pada umumnya kerahasiaan pesan yang dikirim melalui SMS masih bersifat terbuka. Artinya seseorang dengan hak akses dan kemampuan yang cukup, dapat dengan mudah membaca informasi yang dikirimkan. Selain itu pesan yang dikirim melalui SMS merupakan pesan dalam format yang mudah dimengerti oleh siapapun karena tidak ada pengamanan tertentu di dalamnya. Oleh sebab itu, sangatlah berbahaya apabila pesan yang dikirim melalui SMS tersebut berisi pesan rahasia yang sebenarnya bukan untuk kalangan umum. Untuk memenuhi aspek kerahasiaan dan keamanan pesan yang dikirim melalui SMS, maka diperlukan teknik kriptografi. Dengan teknik kriptografi, pesan yang dikirim melalui SMS hanya akan dapat dibaca atau dilihat oleh orang yang memiliki otoritas untuk membaca pesan tersebut.

Kriptografi adalah salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu informasi. Kriptografi merupakan kajian ilmu dan seni untuk menjaga suatu pesan atau data informasi agar data tersebut aman. Kriptografi mendukung kebutuhan dari dua aspek keamanan informasi, yaitu perlindungan terhadap kerahasiaan data informasi *(secrecy)* dan perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan *(authenticity)* (Wibowo, 2004).

Algoritma kriptografi yang baik akan memerlukan waktu yang lama untuk memecahkan data yang telah disandikan. Seiring dengan perkembangan teknologi komputer maka dunia teknologi informasi membutuhkan algoritma kriptografi yang lebih kuat dan aman. Saat ini, *Advanced Encryption Standard* (AES) merupakan

algoritma kriptografi yang cukup aman untuk melindungi data atau informasi yang bersifat rahasia. AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh *National Institute of Standard and Technology* (*NIST).* AES sendiri adalah algoritma kriptografi dengan menggunakan algoritma Rijndael yang dapat mengenkripsi dan mendekripsi blok data sepanjang 128 bit dengan panjang kunci 128 bit, 192 bit, atau 256 bit (Wibowo, 2004).

Untuk membangun aplikasi yang berorientasi pada perangkat kecil yang bersifat *mobile*, ada beberapa sistem operasi yang saat ini populer digunakan pada perangkat telepon seluler seperti *iOS, BlackBerry, Windows Phone* dan juga Android. Dari beberapa sistem operasi telepon seluler tersebut, android menjadi yang paling diunggulkan oleh para pengguna dan juga produsen telepon seluler dikarenakan sifatnya yang *open source* dan fiturnya yang sangat menarik, semenjak perkembanganya pada tahun 2005 dan dirilis pertama kali pada 2008 android sudah memiliki banyak pengguna yang tersebar dari seluruh dunia.

Dengan demikian, pengembangan aplikasi kriptografi SMS menggunakan algoritma Rijndael berbasis android ini diharapkan dapat meningkatkan aspek keamanan dalam proses pengiriman pesan SMS, sehingga mengurangi resiko bocornya pesan SMS kepada pihak yang tidak berkepentingan seperti operator telepon seluler.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, dapat dirumuskan permasalahan yang dihadapi, yaitu bagaimana mengimplementasi algoritma Rijndael dalam rancang bangun aplikasi kriptografi SMS berbasis android agar pesan SMS hanya dapat dibaca oleh orang yang memiliki otoritas untuk membacanya.

1.3. Tujuan dan Manfaat

Tujuan yang ingin dicapai dalam penelitian tugas akhir ini adalah menghasilkan sebuah aplikasi kriptografi SMS berbasis android yang mengimplementasikan algoritma Rijndael dalam proses enkripsi dan dekripsi pesan SMSnya.

Adapun manfaat yang diharapkan dari penelitian tugas akhir ini adalah aplikasi yang dikembangkan dapat digunakan sebagai media pengamanan pesan SMS, sehingga pengguna dapat mengirim dan menerima pesan SMS melalui telepon seluler tanpa diketahui oleh orang yang tidak memiliki otoritas untuk membaca pesan SMS tersebut.

1.4. Ruang Lingkup

Dalam penyusunan tugas akhir ini, diberikan ruang lingkup yang cukup jelas agar pembahasan lebih terarah dan tidak menyimpang dari tujuan penulisan. Aplikasi yang akan dikembangkan adalah aplikasi kriptografi SMS berbasis android yang mengimplementasikan algoritma Rijndael pada proses enkripsi dan dekripsi pesannya.

1) Telepon seluler yang digunakan mendukung sistem operasi Android
2) Masukan berupa pesan SMS
3) Keluaran berupa pesan SMS yang berisi karakter yang tidak dapat dimengerti maknanya *(Ciphertext)* ataupun juga dapat berupa pesan SMS yang dapat dimengerti maknanya *(Plaintext)*
4) Panjang kunci *(Cipherkey)* tidak lebih dari 16 karakter
5) Enkripsi dan dekripsi pesan SMS menggunakan algoritma Rijndael 128 bit
6) Kelancaran pengiriman dan penerimaan pesan SMS dalam *device* yang digunakan tergantung dari operator seluler sebagai penyedia jasa layanan SMS
7) Bentuk implementasinya menggunakan bahasa pemrograman Java-Android
8) Pengujian dilakukan dengan *emulator* android yang terdapat pada *Eclipse*
9) Proses pengiriman atau pertukaran informasi kunci tidak diatur dalam sistem ini.

1.5. Sistematika Penulisan

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

BAB I PENDAHULUAN

berisi uraian tentang latar belakang masalah, perumusan masalah, tujuan dan manfaat, ruang lingkup, serta sistematika penulisan laporan tugas akhir

BAB II LANDASAN TEORI

berisi penjelasan singkat konsep–konsep yang mendukung pengembangan aplikasi, meliputi konsep *Short Messaging Service*, Kriptografi, Algoritma Rijndael, Model Pengembangan Perangkat Lunak, Konsep Analisis dan Perancangan Sistem, Java, Android, dan Eclipse IDE

BAB III ANALISIS DAN PERANCANGAN

membahas proses pengembangan sistem pada tahap definisi kebutuhan, analisis dan perancangan, dengan hasilnya berupa desain dan rancangan sistem yang akan dikembangkan

BAB IV IMPLEMENTASI DAN PENGUJIAN

membahas proses pengembangan aplikasi dan hasil yang didapat pada tahap implementasi serta menerangkan rincian pengujian aplikasi yang dibangun dengan metode *black box*

BAB V PENUTUP

berisi kesimpulan yang diambil berkaitan dengan aplikasi yang dibangun dan saran untuk pengembangan lebih lanjut.