IMPLEMENTASI SUPER ENKRIPSI ALGORITMA *SHIFT-COLUMNAR CIPHER* DAN RIJNDAEL UNTUK APLIKASI SMS BERBASIS SISTEM OPERASI ANDROID

SKRIPSI

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

Disusun Oleh:
DENY KRIS SAWUNGSETYA
J2F008016

JURUSAN ILMU KOMPUTER / INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO
2015

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, 28 Agustus 2015

Deny Kris Sawungsetya
J2F008016

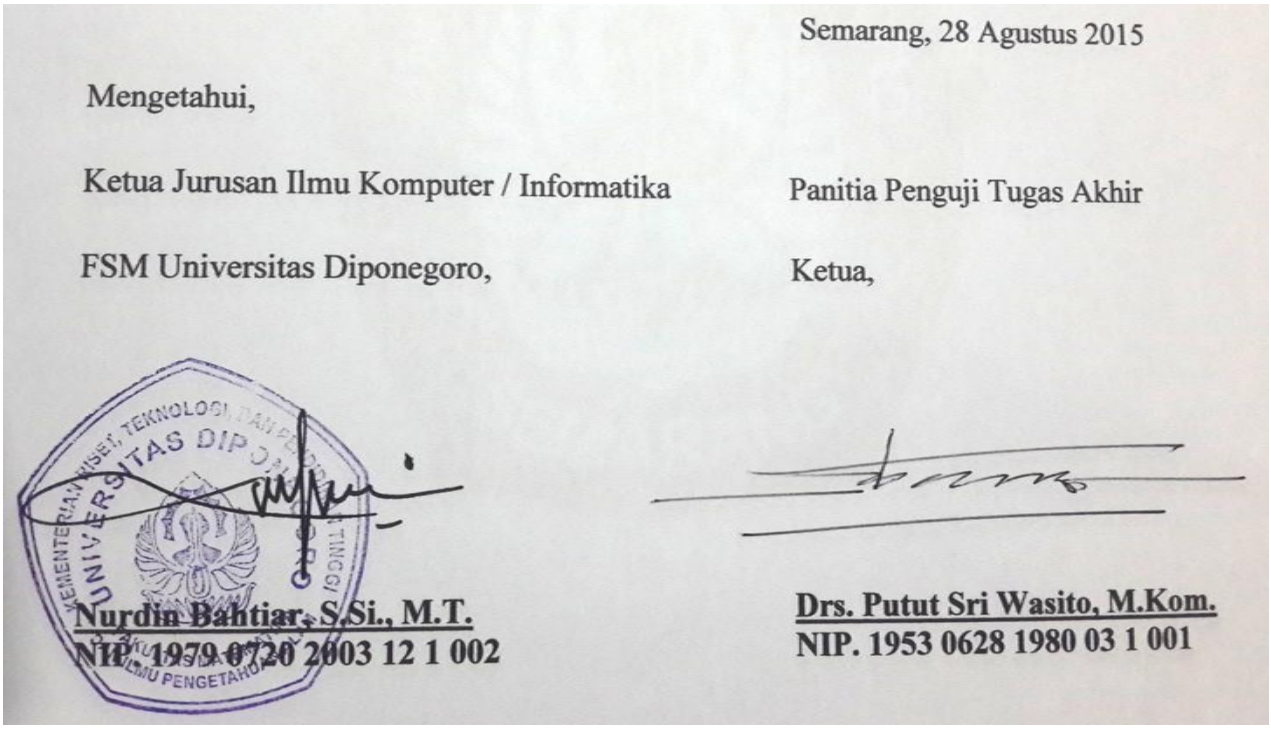
HALAMAN PENGESAHAN

Judul : Implementasi Super Enkripsi Algoritma *Shift-Columnar Cipher* dan Rijndael untuk Aplikasi SMS Berbasis Sistem Operasi Android

Nama : Deny Kris Sawungsetya

NIM : J2F008106

Telah diujikan pada sidang tugas akhir pada tanggal 28 Agustus 2015 dan dinyatakan lulus pada tanggal 28 Agustus 2015.



Semarang, 28 Agustus 2015

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,

Drs. Putut Sri Wasito, M.Kom.
NIP. 1953 0628 1980 03 1 001

iii

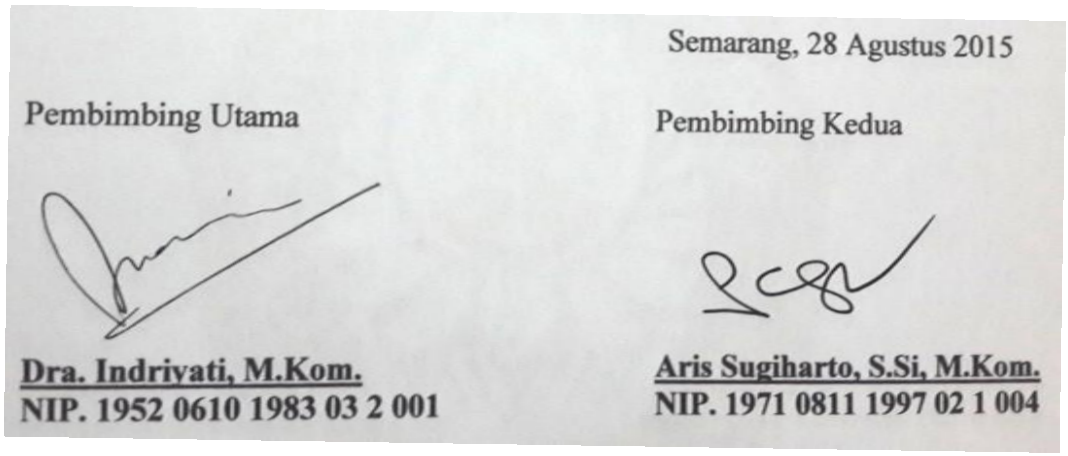
HALAMAN PENGESAHAN

Judul : Implementasi Super Enkripsi Algoritma *Shift-Columnar Cipher* dan Rijndael untuk Aplikasi SMS Berbasis Sistem Operasi Android

Nama : Deny Kris Sawungsetya

NIM : J2F008106

Telah diujikan pada sidang tugas akhir pada tanggal 28 Agustus 2015.



ABSTRAK

Short Message Service (SMS) merupakan salah satu hasil perkembangan teknologi informasi dibidang proses pengiriman data melalui telepon genggam. Dengan menggunakan SMS, pengguna dapat saling bertukar pesan teks dengan pengguna lain. Dalam proses pengiriman SMS tersebut telah dilakukan pengamanan data dengan melakukan enkripsi menggunakan algoritma A5. Namun hal tersebut menimbulkan persoalan baru yaitu terjadinya penyadapan (spoofing) data SMS dengan menembus sistem keamanan algoritma A5 tersebut. Dengan begitu proses pengiriman pesan melalui layanan SMS belum menjamin kerahasiaan pesan dan perlindungan terhadap pemalsuan serta pengubahan pesan yang tidak diinginkan. Dengan menerapkan teknik kriptografi pada proses pembuatan SMS pada device pengguna maka keamanan isi pesan dapat lebih terjaga. Dengan teknik kriptografi, pesan SMS yang dikirim hanya dapat dibaca atau dilihat oleh orang yang memiliki otoritas untuk membaca pesan SMS tersebut. Aplikasi Secure Message Service dibangun untuk mengatasi permasalahan keamanan tersebut. Aplikasi ini dibangun dengan bahasa pemrograman Java sehingga dapat diimplementasikan pada telepon genggam dengan sistem operasi Android. Pengamanan pesan pada aplikasi ini menggunakan super enkripsi tiga algoritma kriptografi sekaligus yaitu algoritma Shift Cipher, Rijndael, dan Columnar Cipher. Setiap algoritma memiliki kunci masing-masing pada tahap enkripsi dan dekripsi yang bersifat simetris. Pesan SMS yang dikirim merupakan hasil akhir dari proses enkripsi ketiga algoritma kriptografi tersebut berturut-turut. Implementasi super enkripsi dengan menggabungkan tiga algoritma kriptografi berjalan dengan baik pada aplikasi Secure Message Service ini dalam memberikan proteksi keamanan yang lebih kepada isi pesan SMS.

Kata kunci: Kriptografi, SMS, Enkripsi, Dekripsi, Rijndael, Shift, Columnar.

ABSTRACT

Short Message Service (SMS) is one of the information technology development results in the field of data sending process through the mobile phone. By using SMS, users could exchange text messages with other phone users. In the SMS delivery process had been carried out with the data security encryption use an algorithm A5. However This raises a new issue that could the interception (spoofing) SMS data to penetrate the security system of the A5 algorithm. So the process of sending messages via SMS service did not have guarantee the confidentiality of the messages also protection against counterfeiting and the unwanted conversion of messages. By applying cryptographic techniques in the making process of the SMS, the message content security could be maintained. With cryptographic techniques, SMS messages which was sent could only be read or seen by people who had the authority to read that SMS message. Secure Message Service applications were built to address that security issues. This application was built with the Java programming language that could be implemented on mobile phones with Android operating system. In this application, the process of securing message used super encryption with three cryptographic algorithms at once, that was Shift Cipher, Rijndael, and Columnar Cipher Algorithms. Each algorithm had an individual key at the encryption and decryption stage which were symmetrical. The sent SMS messages were the end result of the encryption process of three successive cryptographic algorithm. Implementation super encryption with combining three cryptographic algorithms runs well on Secure Message Service application is in provided security protection to the contents of SMS messages.

Keywords: Cyptography, SMS, Encryption, Decryption, Rijndael, Shift, Columnar.

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Tuhan Yesus Kristus yang telah melimpahkan berkat dan karunia-Nya sehingga penulis dapat menyusun tugas akhir yang berjudul "Implementasi Super Enkripsi Algoritma *Shift-Columnar Cipher* dan Rijndael untuk Aplikasi SMS Berbasis Sistem Operasi 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. Ibu Prof. Dr. Widowati, S.Si, M.Si selaku Dekan Fakultas Sains dan Matematika Universitas Diponegoro.
2. Bapak Nurdin Bahtiar, S.Si, M.T selaku 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 Dra. Indriyati, M.Kom selaku pembimbing I yang telah membimbing dan mengarahkan Penulis dalam menyelesaikan tugas akhir ini.
5. Bapak Aris Sugiharto, S.Si, M.Kom selaku pembimbing II yang telah membimbing dan mengarahkan Penulis dalam menyelesaikan tugas akhir ini.
6. Semua pihak yang telah membantu hingga selesainya tugas akhir ini, yang tidak dapat penulis sebutkan satu persatu. Semoga Tuhan 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, 28 Agustus 2015

Penulis

DAFTAR ISI

DAFTAR GAMBAR

xii

DAFTAR TABEL

xv

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup, serta sistematika penulisan laporan tugas akhir mengenai Implementasi Super Enkripsi Algoritma *Shift-Columnar Cipher* dan Rijndael untuk Aplikasi SMS Berbasis Sistem Operasi Android.

1.1. Latar Belakang

Perkembangan teknologi telekomunikasi pada saat ini telah mengubah cara masyarakat dalam berkomunikasi. Pada era tahun 1910-an, komunikasi jarak jauh masih dilakukan dengan cara konvensional, yaitu dengan cara saling mengirim surat dan beberapa menggunakan telegram. Sekarang dengan adanya telepon genggam, komunikasi jarak jauh bisa dilakukan dengan cara saling mengirim pesan singkat / SMS (*Short Message Service*). Layanan pesan singkat telah membuat komunikasi dan pertukaran informasi semakin cepat melewati batas-batas negara dan budaya.

Disamping itu, perangkat lunak sebagai sistem operasi HP (*handphone*) juga mengalami perkembangan pesat salah satunya adalah sistem operasi Android. Android adalah sistem operasi berbasis Linux yang dirancang untuk perangkat seluler layar sentuh seperti telepon pintar (*smartphone*) dan komputer tablet. Android merupakan sistem operasi dengan dasar *open source*. Kode *open source* dan lisensi perijinan pada android memungkinkan perangkat lunak untuk dimodifikasi secara bebas dan didistribusikan oleh para pembuat perangkat, operator nirkabel dan pengembang aplikasi. Namun tidak semua perkembangan ini memberikan dampak yang menguntungkan bagi dunia komunikasi itu sendiri.

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).

Kriptografi adalah salah satu teknik yang digunakan untuk meningkatkan aspek keamanan suatu data. 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). Seiring berkembangnya zaman, kriptografi dibedakan menjadi 2, yaitu Kriptografi Klasik dan Kriptografi Modern.

Dalam kriptografi klasik dikenal dua teknik, yaitu teknik subtitusi dan teknik transposisi. Terdapat beberapa algoritma kriptografi pada teknik subtitusi, salah satunya adalah algoritma *shift cipher*. Begitu pula pada teknik transposisi dikenal algoritma *transposition cipher* dengan beberapa model antara lain adalah *columnar cipher. Shift cipher* merupakan generalisasi dari algoritma *caesar cipher*, yaitu dengan tidak membatasi jumlah pergeseran karakter. Perbedaan mendasar antara *shift cipher* dan *caesar cipher* terletak pada kuncinya. Sedangkan c*olumnar cipher* adalah salah satu jenis teknik pengenkripsian pesan dengan cara mengubah urutan huruf-huruf yang ada di dalam pesan mirip dengan anagram seperti kata “melepas” diubah menjadi “saeelpm”, tapi tentu saja *transposition cipher* mempunyai rumus atau kunci tertentu yang diperlukan agar pesan bisa dimengerti.

Dalam kriptografi modern dikenal berbagai algoritma, salah satunya adalah algoritma Rijndael yang diciptakan oleh Vincent Rijmen dan Joan Daemen yang berasal dari Belgia. Didasarkan pada aspek keamanan algoritma, kemangkusan (efisiensi), fleksibilitas, dan kebutuhan memori, pada bulan November 2001 algoritma Rijndael ditetapkan sebagai standar algoritma AES (*Advanced Encryption Standard*) yang dominan paling sedikit selama 10 tahun kedepan. Dengan tingkat keamanan yang dijadikan dasar AES tersebut diharapkan algoritma rijndael beserta algoritma *shift cipher* dan *columnar cipher* dapat diimplementasikan menjadi super enkripsi dalam aplikasi pesan singkat / SMS yang terdapat pada ponsel bersistem operasi android sehingga keamanan pesan dapat terjaga secara optimal. Super enkripsi merupakan kombinasi 2 atau lebih algoritma

kriptografi untuk mendapatkan suatu algoritma yang lebih handal (susah untuk dipecahkan).

Dengan menambahkan super enkripsi algoritma *shift cipher*, rijndael, dan *columnar cipher* secara berturut-turut pada aplikasi SMS ponsel berbasis android ini diharapkan dapat lebih mengamankan isi pesan SMS yang dikirimkan seseorang kepada orang lain. Aplikasi SMS ini juga diharapkan dapat meminimalisir terjadinya penyadapan data penting yang ada di dalam SMS. Dalam hal ini, pengembangan kriptografi dapat bermanfaat dalam membantu peningkatan keamanan data SMS sebagai objek pengiriman dalam media komunikasi jarak jauh.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang masalah di atas, dapat dirumuskan permasalahan yang dihadapi, yaitu bagaimana merancang dan membangun aplikasi yang dapat memberikan keamanan data SMS berupa kriptografi dengan menggunakan Super-Enkripsi algoritma *Shift Cipher*, Rijndael, dan *Columnar Cipher* pada sistem operasi Android.

1.3. Tujuan dan Manfaat

Tujuan yang ingin dicapai dari penelitian tugas akhir ini adalah menghasilkan suatu perangkat lunak yang dapat memberikan keamanan sebuah data SMS yang bersifat penting, memberikan kemudahan dalam mengamankan data SMS yang akan dikirim dengan media komunikasi jarak jauh nirkabel (*handphone*).

Adapun manfaat yang diharapkan dari penelitian tugas akhir ini adalah meminimalisir gangguan yang dapat dilakukan oleh penyadap serta mengurangi kekhawatiran pengirim akan tersampaikannya data rahasia tersebut ke pihak penerima dengan keamanan yang tetap terjaga.

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. Ruang lingkup pada penyusunan tugas akhir berjudul Implementasi Super-Enkripsi Algoritma *Shift-Columnar Cipher* dan Rijndael untuk Aplikasi SMS berbasis Sistem Operasi Android ini adalah sebagai berikut:

1. Tugas akhir ini dikembangkan dengan menggunakan bahasa Pemrograman Java menggunakan IDE (*Integrated Development Environment*) Eclipse versi Juno.
2. *Input* untuk proses enkripsi dari aplikasi ini berupa teks pesan singkat sederhana (*plaintext*) dan kunci algoritma Rijndael sederhana. Sedangkan output-nya berupa *ciphertext* hasil enkripsi algoritma *Shift Cipher*, Rijndael , dan *Columnar Cipher* secara berturut-turut. Pesan yang dikirim adalah *ciphertext* hasil enkripsi algoritma *Columnar Cipher* sebagai hasil akhir dari proses super enkripsi *plaintext*.
3. *Input* untuk proses dekripsi dari aplikasi ini berupa kunci algoritma Rijndael sederhana. Sedangkan output-nya berupa *plaintext* hasil dekripsi algoritma *Columnar Cipher*, Rijndael, dan *Shift Cipher* secara berturut-turut. Pesan yang terbaca adalah *plaintext* hasil dekripsi akhir dari ketiga algoritma tersebut.
4. Kunci pada algoritma *Shift Cipher* ditentukan yaitu k = 3. Sedangkan pada algoritma *Columnar Cipher* kunci ditentukan yaitu "DENY" dengan *padding* berupa karakter "@".
5. Pergeseran pada algoritma *Shift Cipher* menggunakan sistem perhitungan bit.
6. Panjang kunci Rijndael tidak lebih dari 16 karakter dengan *padding* adalah *null*.
7. Algoritma Rijndael pada aplikasi ini menggunakan 128 bit.
8. Pengembangan sistem ini sampai tahap implementasi pada emulator yang telah disediakan oleh IDE dan juga implementasi pada *smartphone*.
9. Implementasi pada emulator dan *smartphone* menggunakan sistem operasi Android versi 4.3 atau Jelly Bean.
10. Aplikasi ini tidak membahas mengenai bagaimana cara pengirim dan penerima pesan dapat saling mengetahui kunci Rijndael yang digunakan.

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 Kriptografi, Super-Enkripsi, Algoritma *Shift Cipher*, Algoritma *Columnar Cipher*, Algoritma Rijndael, *Unified Process*, *Unified Modeling Language*, *Short Message Service*, Sistem Operasi Android, dan Eclipse IDE.

BAB III ANALISIS DAN PERANCANGAN

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

BAB IV IMPLEMENTASI DAN PENGUJIAN

membahas tentang implementasi dan pengujian sistem. Implementasi kriptografi dilakukan berdasarkan rancangan yang telah dibuat pada bab sebelumnya. Dilanjutkan dengan proses berikutnya yaitu pengujian sistem, dimana proses pengujian dilakukan dengan menguji *class* dan menguji secara diagnosis.

BAB V PENUTUP

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