APLIKASI KEAMANAN SMS PADA PONSEL CERDAS (SMARTPHONE) BERBASIS ANDROID DENGAN ALGORITMA RAIL FENCE DAN ALGORITMA DATA ENCRYPTION STANDARD (DES)

SKRIPSI

Disusun Sebagai Salah Satu Syarat
untuk Memperoleh Gelar Sarjana Komputer
pada Departemen Ilmu Komputer/Informatika

Disusun Oleh :
DIEGO CESAR NUGROHO
24010314120034

DEPARTEMEN ILMU KOMPUTER/ INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO
2018

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan dibawah ini:

Nama : Diego Cesar Nugroho

NIM : 24010314120034

Judul : Aplikasi Keamanan SMS Pada Ponsel Cerdas (*Smartphone*) Berbasis Android Dengan Algoritma *Rail Fence* Dan Algoritma *Data Encryption Standard* (DES).

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 sepengetahuan 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, 30 Oktober 2018

Diego Cesar Nugroho

NIM. 24010314120034

HALAMAN PENGESAHAN

Judul : Aplikasi Keamanan SMS Pada Ponsel Cerdas (*Smartphone*) Berbasis Android Dengan Algoritma *Rail Fence* Dan Algoritma *Data Encryption Standard* (DES).

Nama : Diego Cesar Nugroho

NIM : 24010314120034

Telah diujikan pada sidang tugas akhir tanggal 15 Oktober 2018 dan dinyatakan lulus pada tanggal 15 Oktober 2018.

Semarang, 30 Oktober 2018

Mengetahui,

Ketua Departemen Ilmu Komputer / Informatika

Dr. Retno Kusumaningrum, S.Si, M.Kom.

NIP. 198104202005012001

Panitia Penguji tugas Akhir

Ketua,

Drs. Eko Adi Sarwoko, M.Kom

NIP. 196511071992031003

HALAMAN PENGESAHAN

Judul : Aplikasi Keamanan SMS Pada Ponsel Cerdas (*Smartphone*) Berbasis Android Dengan Algoritma *Rail Fence* Dan Algoritma *Data Encryption Standard* (DES).

Nama : Diego Cesar Nugroho

NIM : 24010314120034

Telah diujikan pada sidang tugas akhir tanggal 15 Oktober 2018.

Semarang, 30 Oktober 2018

Dosen Pembimbing

Drs. Suhartono, M.Kom.

NIP. 195504071983031003

ABSTRAK

*Short Message Service (*SMS*)* merupakan salah satu fasilitas yang disediakan oleh ponsel cerdas (*Smartphone*). Dalam pengiriman pesan menggunakan SMS akan melewati *Short Message Service Center* (SMSC) sebelum dikirimkan ke tujuan. Pada saat pesan di SMSC sangat rentan terhadap penyadapan oleh siapapun. Akibatnya, pesan tersebut dapat diketahui oleh orang yang tidak berhak untuk mengetahuinya. Kriptografi dapat digunakan untuk mengamankan pesan. Algoritma kriptografi sangat banyak, antara lain *Rail Fence* dan algoritma DES. Dengan algoritma tersebut, pesan dapat dienkripsi dan didekripsi untuk mengamankan pesan. Untuk itu dibangun Aplikasi Keamanan SMS (RFD) pada *platform* Android yang mampu melakukan pengiriman pesan yang dienkripsi dan dekripsi. Hasil pengujian Android Profiler menyatakan bahwa aplikasi RFD menggunakan kapasitas CPU dibawah 10%, menggunakan memori dibawah 100 MB, tidak menggunakan *network* dan menggunakan energi yang normal. Dan berdasarkan kuisoner dengan 32 responden menyatakan bahwa 96,9% aplikasi mudah dioperasikan, 87,5% tampilan aplikasi menarik, 96,9% aplikasi membantu menjaga kerahasiaan SMS, 90,6% aplikasi berjalan lancar, 84,4 aplikasi berjalan stabil, 93,8% nyaman menggunakan aplikasi dan 78,1% aplikasi tidak membebani sistem Android.

Kata kunci : SMS, Keamanan, Enkripsi, Dekripsi, *Rail Fence*, DES.

ABSTRACT

Short Message Service (SMS) is one of the facilities provided by smartphones. In sending messages using SMS will pass Short Message Service Center (SMSC) before being sent to the destination. At the time the message in the SMSC is very vulnerable to wiretapping by anyone. As a result, the message can be known by people who do not have the right to know it. Cryptography can be used to secure messages. Cryptographic algorithms are numerous, including Rail Fence and DES algorithms. With this algorithm, messages can be encrypted and decrypted to secure messages. For this purpose, the SMS Security Application (RFD) was built on the Android platform that is capable of sending encrypted and decrypted messages. The Android Profiler test results state that the RFD application uses a CPU capacity below 10%, uses memory below 100MB, does not use the network and uses normal energy. And based on questionnaires with 32 respondents stated that 96.9% of applications are easy to operate, 87.5% of applications are attractive, 96.9% of applications help maintain the confidentiality of SMS, 90.6% of applications run smoothly, 84.4 applications run stable, 93,8% comfortable using the application and 78.1% of applications do not overload the Android system.

Keywords: SMS, Security, Encryption, Decryption, Rail Fence, DES**.**

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT yang telah melimpahkan segala rahmat dan hidayah-Nya sehingga penulis dapat menyelsaikan skripsi dengan judul "Aplikasi Keamanan SMS Pada Ponsel Cerdas (*Smartphone*) Berbasis Android Dengan Algoritma *Rail Fence* Dan Algoritma *Data Encryption Standard* (DES)."

Dalam pelaksanaan tugas akhir dan penyusunan dokumen tugas akhir ini, penulis menyadari banyak pihak yang membantu sehingga akhirnya dokumen ini dapat diselesaikan. Oleh karena itu, melalui kesempatan ini penulis ingin menyampaokan ucapan terima kasih yang sebesar-besarnya kepada :

1. Ibu Dr. Retno Kusumaningrum, S.Si., M.Kom. selaku Ketua Departemen Ilmu Komputer/ Informatika FSM UNDIP.
2. Bapak Helmie Arif Wibawa, S.Si., M.Cs. selaku Koordinator Tugas Akhir Departemen Ilmu Komputer/ Informatika FSM UNDIP.
3. Drs. Suhartono, M.Kom. selaku dosen pembimbing srkispsi yang telah membantu dalam membimbing dan mengarahkan penulis dalam menyelesaikan skripsi ini.
4. Orang tua dan keluarga yang telah mendukung, membantu, memaksa dan memberikan semangat kepada penulis dalam menyelesaikan skripsi ini.
5. Orang-orang yang telah mengisi kuisoner dan semua pihak yang telah membantu kelancaran dalam menyelesaikan skripsi yang tidak dapat disebutkan satu per satu.

Penulis menyadari bahwa dokumen tugas akhir ini masih jauh dari sempurna. Oleh sebab itu, saran dan kritik yang membangun sangat penulis harapkan. Akhir kata, semoga tugas akhir ini dapat bermanfaat bagi semua pihak.

Semarang, 30 Oktober 2018

Diego Cesar Nugroho

NIM. 24010314120034

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LISTING

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup, dan sistematika penulisan skripsi mengenai Aplikasi Keamanan SMS Pada Ponsel Cerdas (*Smartphone*) Berbasis Android Dengan Algoritma *Rail Fence* dan Algoritma *Data Encryption Standard* (DES).

1.1. Latar Belakang

Pada dewasa ini perkembangan teknologi dalam bidang ponsel cerdas (*Smartphone*) sangat pesat. Beragam fitur disediakan oleh *Smartphone,* bahkan hampir sama dengan fitur – fitur yang tersedia pada komputer. Sehingga para *developer* berlomba – lomba mengembangkan aplikasi untuk *Smartphone*. Perangkat lunak untuk mengembangkan aplikasi tersebut semakin banyak bermunculan, diantaranya adalah Android. Salah satu fasilitas pada *Smartphone* yang paling banyak digunakan adalah melakukan pengiriman pesan singkat melalui *Short Message Service* (SMS).

SMS adalah salah satu layanan yang digunakan untuk mengirimkan pesan singkat antara pengguna *Smartphone* dengan biaya yang murah dan cepat. Jangkauan global SMS lebih luas dan tidak memerlukan permintaan pertemanan untuk melakukan pengiriman dan penerimaan SMS. Meskipun SMS dipandang sebagai teknologi kuno, tetapi SMS memiliki peran penting dalam menghubungkan sebagian besar teknologi modern, seperti penggunaan *two-factor authentication* (2FA) yang masih popular digunakan sampai sekarang (Cohen, 2018).

Pada proses pengiriman dan penerimaan SMS dibutuhkan suatu media transmisi berupa jalur komunikasi *Global Sistem for Mobile Communication* (GSM). Pesan yang dikirimkan terlebih dahulu disimpan pada *Short Message Service Center* (SMSC) sebelum SMS tersebut dikirimkan ke tujuan. Pada proses ini sangat rentan terhadapan penyadapan oleh siapapun yang memiliki akses ke dalam SMSC (Lubis, 2013). Akibatnya, informasi penting dalam pesan tersebut dapat diketahui oleh orang yang tidak berhak untuk mengetahuinya. Untuk itu dibutuhkan suatu cara untuk mengamankan pesan.

Pengamanan pesan dapat dilakukan dengan menggunakan salah satu teknik penyandian. Ilmu yang mempelajari penyandian biasa disebut dengan kriptografi.

Dalam kriptografi terdapat metode yang cukup penting, salah satunya adalah enkripsi (*encryption*). Enkripsi adalah proses mengubah pesan asli(*plaintext*) ke bentuk kode – kode yang tidak dapat dibaca (*ciphertext*). Sedangkan proses untuk mengembalikan *ciphertext* menjadi *plaintext* disebut dekripsi (*decryption*) (Ariyus, 2008). Ada beberapa algoritma di dalam kriptografi, diantaranya yaitu *Rail Fence*, dan *Data Encryption Standard* (DES).

Algoritma *Rail Fence* merupakan salah satu bentuk teknik transposisi atau permutasi karakter dengan berdasarkan tingkatan nilai untuk enkripsi dan dekripsi (Siahaan, 2016). Menurut Jayadilaga dalam penelitian yang berjudul "Kriptografi Hybrid Algoritma *Rail Fence* Dan ElGamal Dalam Pengamanan Data Berbasis Teks", algoritma *Rail Fence* memiliki kelebihan kecepatan proses enkripsi dan dekripsi (Jayadilaga, 2017). Algoritma *Rail Fence* memiliki kelemahan mudah dipecahkan, dikarenakan semua karakter *plaintext* masih ada dan hanya mengalami perubahan posisi (Siahaan, 2016).

Sedangkan algoritma DES merupakan algoritma simetri dengan enkripsi maupun dekripsi menggunakan kunci yang sama (Ariyus, 2008). Algoritma ini telah banyak digunakan dalam menyelesaikan permasalahan yang berkaitan dengan pengamanan pesan. Menurut Solichin Zaki dalam penelitian yang berjudul "Aplikasi Pengamanan Citra Dengan Algoritma DES dan Transformasi Wavelet Diskrit", algoritma DES memiliki keunggulan kemanan kunci (Zaki, 2011). Tetapi algoritma DES memiliki kerentanan terhadap serangan *brute force attack* (Schneier, 1996).

Menurut Adeem Akhtar dalam penelitian yang berjudul "Enhancing the Security of Simplified DES Algorithm Using Transposition and Shift Rows", apabila dua algoritma digabung antara algoritma S-DES dan algoritma *transposition* menyebabkan keamanan sangat ketat dan hampir tidak mungkin untuk diputus dan dipecahkan (Adeem Akhtar, 2017).

Banyak dilakukan penelitian dalam keamanan SMS sampai pada saat ini, antara lain : "Development of a Secure SMS Application using Advanced Encryption Standard (AES) on Android Platform" oleh Muhammad Noman Riaz (Humam, 2018), "Enkripsi SMS dengan Menggunakan One Time Pad (OTP) dan Kompresi Lempel-Ziv-Welch (LZW)" oleh Fitria Diani (Fitri Diani, 2018) dan "Peningkatan Keamanan Algoritma DES Pada Aplikasi Enkripsi Sms Android Menggunakan Algoritma AES 256 Bit" oleh Muhammad Humam (Humam, 2018).

Kombinasi algoritma *Rail Fence* dan DES merupakan inovasi yang digunakan untuk pengamanan pesan, untuk itu perlu dibangun suatu aplikasi berjudul "Aplikasi Keamanan SMS Pada Ponsel Cerdas (*Smartphone*) Berbasis Android Dengan Algoritma *Rail Fence* dan Algoritma *Data Encryption Standard* (DES)".

1.2. Rumusan Masalah

Berdasarkan permasalahan yang telah disampaikan pada latar belakang, perumusan masalah dalam penelitian ini adalah bagaimana membuat Aplikasi Keamanan SMS Pada Ponsel Cerdas (*Smartphone*) Berbasis Android Dengan Algoritma *Rail Fence* dan Algoritma *Data Encryption Standard* (DES) untuk mengirim SMS terenkripsi dan mendekripsi SMS.

1.3. Tujuan dan Manfaat

Tujuan yang ingin dicapai dari penelitian ini adalah menghasilkan sebuah aplikasi berbasis Android yang dapat digunakan untuk pengiriman SMS terenkripsi dan mendekripsi SMS dengan algoritma *Rail Fence* dan *Data Encryption Standard* (DES).

Manfaat dari penelitian ini adalah aplikasi yang dapat mengirimkan suatu SMS teracak.

1.4. Ruang Lingkup

Pada penelitian ini perlu adanya batasan-batasan yang akan dikerjakan agar tidak melebihi target yang akan diteliti:

1. Data masukan berupa SMS.
2. Panjang 1 SMS atau 160 karakter yang disesuaikan dengan *Global Sistem for Mobile Communication* (GSM).
3. Aplikasi SMS ini menggunakan perangkat mobile ber-*platform* Android minimum versi 4.0 atau API level 14 (*IceCreamSandwich*).
4. Proses enkripsi dan dekripsi menggunakan dua algoritma, yaitu *Rail Fence* dan DES.
5. Menggunakan pengujian *User Acceptance* dan *Android Profiler.*
6. Bahasa pemrograman yang digunakan adalah *Java.*

1.5. Sistematika Penulisan

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

BAB I PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, serta ruang lingkup tugas akhir mengenai Aplikasi Keamanan SMS Pada Ponsel Cerdas (*Smartphone*) Berbasis Android Dengan Algoritma *Rail Fence* dan Algoritma *Data Encryption Standard* (DES).

BAB II TINJAUAN PUSTAKA

Bab ini merupakan teori-teori penunjang yang digunakan sebagai landasan dalam pembuatan Aplikasi Keamanan SMS Pada Ponsel Cerdas (*Smartphone*) Berbasis Android Dengan Algoritma *Rail Fence* dan Algoritma *Data Encryption Standard* (DES).

BAB III ANALISIS DAN DESAIN

Bab ini menyajikan tahapan proses pembangunan perangkat lunak menggunakan model pengembangan *Object Oriened Analysis Design (*OOAD*)*. Pada bab ini disajikan *analysis* kebutuhan dan perancangan apikasi.

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini menyajikan tahapan proses pembangunan perangkat lunak menggunakan model pengembangan OOAD. Pada bab ini disajikan fase impelementasi, pengujian dan analisis hasil dari aplikasi.

BAB V PENUTUP

Bab ini berisikan kesimpulan dan saran dari penulis untuk pengembangan lebih lanjut dari penelitian serupa.