IMPLEMENTASI ALGORITMA RSA
PADA APLIKASI PENGAMAN CITRA DIGITAL
BERBASIS ANDROID

SKRIPSI

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

Disusun Oleh:
Puspita Dewi Nurmalasari
J2F008062

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

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Saya yang bertanda tangan di bawah ini :

Nama : Puspita Dewi Nurmalasari

NIM : J2F008062

Judul : Implementasi Algoritma RSA pada Alikasi Pengaman Citra Digital Berbasis Android

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, 31 Agustus 2015

Puspita Dewi Nurmalasari
NIM. J2F008062

HALAMAN PENGESAHAN

Judul : Implementasi Algoritma RSA pada Alikasi Pengaman Citra Digital Berbasis Android

Nama : Puspita Dewi Nurmalasari

NIM : J2F008062

Telah diujikan pada sidang Tugas Akhir tanggal 31 Agustus 2015 dan dinyatakan lulus pada tanggal 31 Agustus 2015.

Semarang, 31 Agustus 2015

Mengetahui,

Ketua Jurusan Ilmu Komputer / Informatika FSM UNDIP,	Panitia Penguji Tugas Akhir Ketua,
Nurdin Bahtiar, S.Si, M.T	Helmie Arif Wibawa, S. Si, M.Cs
NIP. 19790720 200312 1 002	NIP. 19780516 200312 1 001

HALAMAN PENGESAHAN

Judul : Implementasi Algoritma RSA pada Alikasi Pengaman Citra Digital Berbasis Android

Nama : Puspita Dewi Nurmalasari

NIM : J2F008062

Telah diujikan pada sidang Tugas Akhir tanggal 31 Agustus 2015.

Semarang, 31 Agustus 2015

Pembimbing,

Aris Sugiharto, S.Si, M.Kom.

NIP. 19710811 199702 1 004

ABSTRAK

Penggunaan media informasi berupa gambar dari jaman dulu sudah sering digunakan. Bahkan dalam kehidupan sehari-hari pun erat kaitannya dengan media gambar. Akan tetapi, penggunaan informasi melalui media gambar mempunyai beberapa kelemahan. Salah satunya adalah kemudahan melakukan manipulasi citra oleh pihak-pihak tertentu dengan bantuan teknologi yang berkembang sekarang ini. Sebagai upaya dalam peningkatan pengamanan informasi media gambar dan perlindungan privasi atas kepemilikan media gambar maka diterapkanlah sebuah algoritma kriptografi. Untuk memenuhi aspek keamanan dan perlindungan privasi, diperlukan aplikasi yang menerapkan teknik kriptografi. Aplikasi RSAdroid dibangun dengan menerapkan algoritma RSA (Rivest Shamir Adleman) dan diimplementasikan pada *smartphone* berbasis sistem operasi Android versi 4.2 *Jelly Bean*. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan-bilangan besar menjadi faktor prima.

Kata Kunci : Kriptografi, Citra, Algoritma RSA, Android, *Smartphone*

ABSTRACT

The use of media information such as images have often used from the past. Even in everyday life is too closely associated with media images. However, the use of information through the media image has some weakness. One of which is the ease of doing image manipulation by certain parties with help of the developing technology. As effort in improving information security of media images and privacy protection of media images ownership, then applied a cryptography algorithm. To fulfill the safety and privacy protection of images, it need an application that implements cryptograpgic techniques. RSAndroid application is built by applying the RSA(Rivest Samir Adleman) Algorithm and implemented on smartphone based on Android operating system version 4.2 Jelly Bean. The security of RSA Algorithm lies in the difficullty of factoring large number into prime factors.

Keywords : Cryptography, Images, RSA Algorithm, Android, Smartphone

KATA PENGANTAR

Segala puji penulis ucapkan kehadirat Allah SWT yang telah melimpahkan rahmat dan hidayah-Nya sehingga penulis dapat menyusun tugas akhir yang berjudul "Implementasi Algoritma RSA pada Alikasi Pengaman Citra Digital Berbasis Android " sehingga dapat memperoleh gelar sarjana strata satu 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 membantu dalam penyelesaian tugas akhir ini, penulis ingin mengucapkan terima kasih kepada :

1. Prof. Dr. Widowati, S.Si, M.Si selaku Dekan FSM UNDIP.
2. Nurdin Bachtiar, S.Si, M.T selaku Ketua Jurusan Ilmu Komputer / Informatika FSM UNDIP.
3. Aris Sugiharto, S.Si, M.Kom. selaku dosen pembimbing yang senantiasa membimbing, memberikan dukungan, semangat, serta masukan bagi penulis dalam menyelesaikan tugas akhir ini.
4. Indra Waspada, S.T, M. TI selaku Koordinator Tugas Akhir dan dosen wali yang memberikan arahan dalam bidang akademik, serta bapak / ibu dosen lainnya yang telah memberikan pelajaran yang sangat berharga kepada penulis, serta bapak / ibu dosen lainnya yang telah memberikan pelajaran yang sangat berharga kepada penulis.
5. Semua pihak yang telah membantu hingga selesainya tugas akhir ini, yang tidak dapat penulis sebutkan satu persatu.

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.

Semarang, Agustus 2015

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Bab ini menyajikan latar belakang masalah, rumusan masalah, tujuan dan manfaat, ruang lingkup, dan sistematika penulisan tugas akhir mengenai Implementasi Algoritma RSA pada Aplikasi Pengaman Citra Digital Berbasis Android.

1.1. Latar Belakang

Perkembangan teknologi informasi yang sangat cepat memberikan manfaat yang luar biasa kepada masyarakat. Salah satu implementasinya adalah teknologi telepon selular HP (*handphone*) yang sudah sangat dekat dengan masyarakat karena memiliki fitur yang banyak. 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 sumber terbuka (*open source*). Kode dengan sumber terbuka dan lisensi perijinan pada android memungkinkan perangkat lunak untuk dimodifikasi secara bebas dan didistribusikan oleh para pembuat perangkat dan pengembang aplikasi.

Penggunaan media informasi berupa gambar dari jaman dulu sudah sering digunakan. Bahkan dalam kehidupan sehari-hari pun erat kaitannya dengan media gambar. Akan tetapi, penggunaan informasi melalui media gambar mempunyai beberapa kelemahan. Salah satu kelemahan penggunaan media informasi media gambar adalah mudah dimanipulasi oleh pihak-pihak yang memiliki kepentingan lain di dalamnya. Terlebih jika informasi berupa file gambar tersebut bersifat rahasia. Dari sinilah mengapa tingkat keamanan menggunakan media gambar telah menjadi topik penting dalam dunia komputer. Apalagi jumlah kejahatan di bidang teknologi informasi telah meningkat akhir-akhir ini (Chin, 2001).

Keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dalam sistem informasi pada saat ini. Salah satu usaha untuk mengamankan data diantaranya dengan menggunakan kriptografi. Kriptografi mendukung kebutuhan dari dua aspek keamanan informasi, yaitu perlindungan terhadap kerahasiaan informasi (*secrecy*) dan perlindungan terhadap pemalsuan dan pengubahan informasi yang tidak diinginkan (*authenticity*) (Ariyus, 2006).

Di antara algoritma kunci publik yang pernah dibuat, Algoritma RSA merupakan yang paling populer. RSA adalah metode enkripsi yang dikembangkan oleh Ron (R)ivest, Adi (S)hamir dan Leonard (A)dleman yang diperkenalkan pada tahun 1977 dan dipatenkan oleh MIT (*Massachussets Institute of Technology*). Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi bilangan faktor-faktor prima. Pemfaktoran ini dilakukan untuk memperoleh kunci *private* (Munir, 2007).

Oleh karena kelebihan algoritma RSA dalam mengenkripsi data, maka penulis mencoba untuk mengimplementasikan algoritma tersebut pada file citra digital dengan menganalisa penerapan algoritma RSA terhadap elemen penyusun citra digital (*pixel*) agar dapat menyandikan atau mengkodekan bilangan-bilangan di setiap *pixel* pada citra digital yang akan diproses.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, dapat dirumuskan permasalahan yang dihadapi, yaitu bagaimana mengimplementasikan Algoritma RSA pada Aplikasi Pengaman Citra Digital Besbasis Android.

1.3. Tujuan dan Manfaat

1.3.1. Tujuan

Tujuan yang ingin dicapai dalam penelitian tugas akhir ini adalah menghasilkan sebuah aplikasi berbasis Android yang mengimplementasikan algoritma kriptografi RSA untuk mengamankan citra digital.

1.3.2. Manfaat

Adapun manfaat yang diharapkan dari penelitian tugas akhir ini adalah untuk membantu menjaga privasi (kerahasiaan) data citra digital sehingga hanya pihak-pihak yang berkepentingan saja yang bisa mengaksesnya.

1.4. Ruang Lingkup

Dalam penyusunan tugas akhir ini, diberikan ruang lingkup yang jelas agar pembahasan lebih terarah dan tidak menyimpang dari tujuan penulisan. Ruang lingkup dalam pengimplementasian Algoritma RSA pada Alikasi Pengaman Citra Digital Berbasis Android adalah sebagai berikut :

1. Pengembangan aplikasi ini menggunakan bahasa pemrograman Java berbasis Android, IDE (*Integrated Development Environment*) Eclipse versi Kepler.
2. Menggunakan *Emulator Android* atau *Virtual Device* sebagai bentuk implementasi dari pengembangan aplikasi ini.
3. Implementasi pada emulator dan *smartphone* menggunakan sistem operasi Android versi 4.2 atau Jelly Bean.
4. Model proses yang digunakan adalah *Unified Process*.
5. Enkripsi dan dekripsi file citra digital menggunakan algoritma RSA.
6. File input berupa file citra digital berindeks warna (.png)

1.5. Sistematika Penulisan

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

BAB I. PENDAHULUAN

Bab ini berisi latar belakang, perumusan masalah, tujuan dan manfaat, ruang lingkup, dan sistematika penulisan dalam pembuatan tugas akhir.

BAB II. TINJAUAN PUSTAKA

Dalam bab ini dipaparkan mengenai dasar teori yang berhubungan dengan topik tugas akhir. Dasar teori yang digunakan dalam tugas akhir ini meliputi pengertian citra digital, kriptografi, algoritma RSA, android dan sejarah perkembangan android, *Unified Process*, UML *(Unified Model Language)*, dan Program pendukung dalam pengembangan aplikasi kriptografi untuk pengamanan citra digital berbasis android.

BAB III. FASE *INCEPTION* DAN FASE *ELABORATION*

Bab ini membahas mengenai tahap-tahap proses pembangunan perangkat lunak meliputi definisi kebutuhan, analisis, dan perancangan aplikasi untuk pengamanan citra digital berbasis android. Proses tersebut merupakan *core workflow* yang terdapat didalam *Unified Process.*

BAB IV. FASE *CONSTRUCTION*

Bab ini dipaparkan mengenai tahap-tahap proses implementasi dan pengujian sistem meliputi implementasi sistem dan pengujian Perangkat Lunak dari pengembangan aplikasi untuk pengamanan citra digital berbasis android.

BAB V. PENUTUP

Bab ini berisi kesimpulan yang diambil berkaitan dengan perangkat lunak yang dikembangkan dan saran-saran untuk pengembangan perangkat lunak lebih lanjut.