IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA-CRT PADA APLIKASI *INSTANT MESSAGING*

SKRIPSI

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

Disusun Oleh :

Ashari Arief

J2F009036

JURUSAN ILMU KOMPUTER/ INFORMATIKA
FAKULTAS SAINS DAN MATEMATIKA
UNIVERSITAS DIPONEGORO

2016

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 dalam daftar pustaka.

Semarang, 17 Maret 2016

Ashari Arief
J2F009036

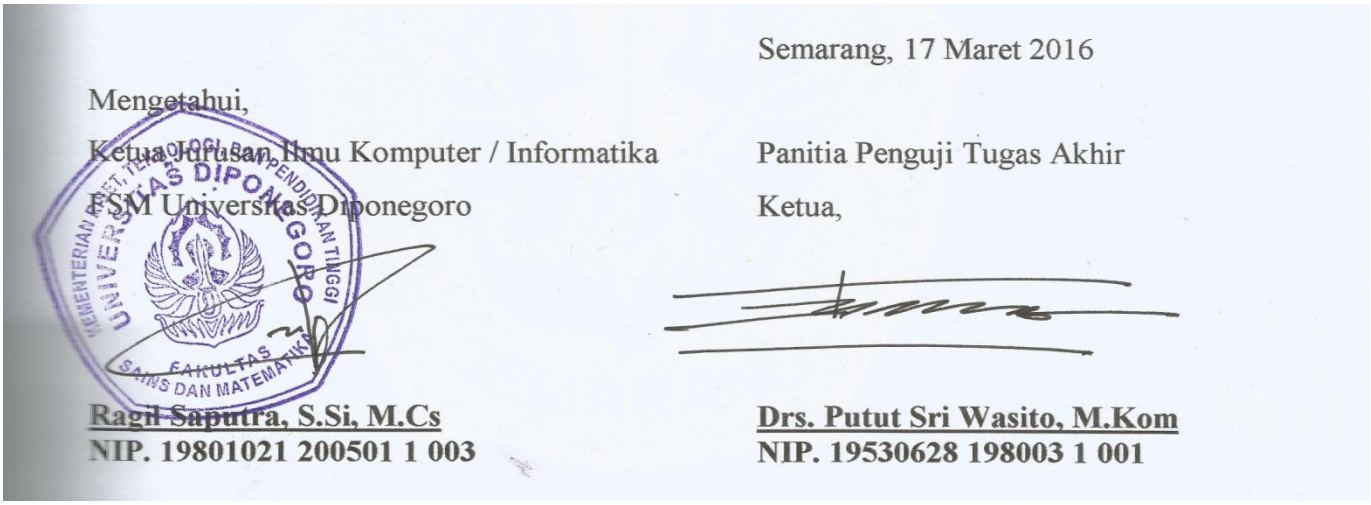
HALAMAN PENGESAHAN

Judul : Implementasi Algoritma Kriptografi RSA - CRT pada Aplikasi *Instant Messaging*

Nama : Ashari Arief

NIM : J2F009036

Telah diujikan pada sidang tugas akhir pada tanggal 14 Maret 2016 dan dinyatakan lulus pada tanggal 16 Maret 2016.



Semarang, 17 Maret 2016

Mengetahui,

Ketua Jurusan Ilmu Komputer / Informatika
FSM Universitas Diponegoro

Ragil Saputra, S.Si, M.Cs
NIP. 19801021 200501 1 003

Panitia Penguji Tugas Akhir
Ketua,

Drs. Putut Sri Wasito, M.Kom
NIP. 19530628 198003 1 001

HALAMAN PENGESAHAN

Judul : Implementasi Algoritma Kriptografi RSA - CRT pada Aplikasi *Instant Messaging*

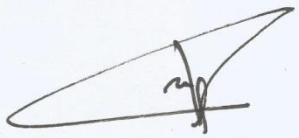
Nama : Ashari Arief

NIM : J2F009036

Telah diujikan pada sidang tugas akhir pada tanggal 14 Maret 2016.

Semarang, 17 Maret 2016

Pembimbing



Ragil Saputra, S.Si, M.Cs

NIP. 19801021 200501 1 003

ABSTRAK

Kemajuan teknologi komputer dan telekomunikasi membantu dalam menyelesaikan banyak pekerjaan dengan cepat, akurat, dan efisien. Salah satu kemajuan teknologi komunikasi yaitu menghasilkan aplikasi *instant messaging*, namun seiring dengan kemajuan teknologi dengan semakin banyaknya pengguna yang menggunakan aplikasi *instant messaging* terdapat dampak negatif berupa penyadapan data khususnya saat terjadi komunikasi yang bersifat rahasia dan penting. Untuk menjaga kerahasiaan, integritas data, otentikasi entitas, dan otentikasi asal data diterapkan kriptografi. Salah satu algoritma kriptografi yang tidak membutuhkan saluran yang aman untuk distribusi kunci adalah algoritma RSA. Algoritma RSA dapat dimodifikasi dengan algoritma CRT (*Chinese Remainder Theorem*) untuk mempercepat proses dekripsi dan disebut dengan algoritma RSA-CRT. Penelitian ini mengimplementasikan algoritma kriptografi RSA-CRT pada aplikasi *instant messaging*. Metode untuk mempercepat proses pemangkatan menggunakan algoritma *fast modular exponentiation*. Penelitian ini menggunakan model proses *waterfall* yang diimplementasikan dengan menggunakan bahasa pemrograman vb.net dan bersifat *client-server*. Berdasarkan hasil pengujian dapat diimplentasikan algoritma RSA-CRT pada aplikasi *instant messaging* serta pengujian untuk bit n mulai dari 56 bit sampai 88 bit dapat disimpulkan proses dekripsi RSA-CRT dua kali lebih cepat dibandingkan proses dekripsi RSA.

Kata kunci : Kriptografi, Algoritma RSA-CRT, Algoritma *Fast Modular Exponentiation*, *Instant Messaging*.

ABSTRACT

The advancement of computer technology and telecommunications has helped to resolve much of problem with fast, accurate, and efficient. One of that advancement is instant messaging, but because of the growing of a number of users that use the instant messaging also the advancement of telecomunication it self, there is a negative impact in the form of tapping data, especially when there is communication of confidential and important thing. There is a cryptography, one of the method that used to maintain confidentiality, integrity, entity authentication and data origin authentication. One of the cryptography algorithm that does not require a secure channel for key distribution is the RSA algorithm. The RSA algorithm can be modified with the CRT (Chinese Remainder Theorem) algorithm to accelerate the process the decryption and called the RSA-CRT. This study implements RSA-CRT algorithm in instant messaging applications. A method to accelerate the process of exponentiation using a fast modular exponentiation algorithm. This study uses a waterfall process model as a development method that implemented by using a vb.net programming language and client-server based. Based on the test results, implementation of RSA-CRT algorithm in instant messaging application for n bits from 56 bits to 88 bits has made a conclution that RSA-CRT decryption process two times faster than RSA decryption process.

Keywords : Cryptography, RSA-CRT Algorithm, Fast Modular Exponentiation Algorithm, Instant Messaging

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 Kriptografi RSA-CRT pada Aplikasi *Instant Messaging***" sehingga dapat memperoleh gelar Sarjana Strata Satu Jurusan Ilmu Komputer/ Informatika pada Fakultas Sains dan Matematika Universitas Diponegoro.

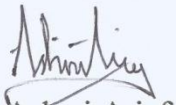
Dalam penyusunan tugas akhir ini, penulis mendapat bantuan dan dukungan dari banyak pihak. Atas peran sertanya dalam membantu dalam penyelesaian tugas akhir ini, penulis ingin mengucapkan terima kasih kepada :

1. Ibu Prof. Dr. Widowati, S.Si, M.Si selaku Dekan Fakultas Sains dan Matematika Universitas Diponegoro.
2. Bapak Ragil Saputra, S.Si, M.Cs. selaku Ketua Jurusan Ilmu Komputer/ Informatika dan dosen pembimbing yang telah membimbing dan mengarahkan Penulis dalam menyelesaikan tugas akhir ini.
3. Bapak Helmie Arif Wibawa, S.Si, M.Cs. selaku Koordinator Tugas Akhir Jurusan Ilmu Komputer/ Informatika.
4. Semua pihak yang telah membantu kelancaran dalam pelaksanaan tugas akhir ini yang tidak dapat penulis sebutkan satu per satu.

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 komputer.

Semarang, 16 Maret 2016



Ashari Arief

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I
PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup, dan sistematika penulisan penelitian mengenai Implementasi Algoritma Kriptografi RSA - CRT pada Aplikasi *Instant Messaging.*

1.1. Latar Belakang

Komunikasi merupakan elemen terpenting dari manusia sebagai makhluk sosial. Salah satu cara berkomunikasi yaitu dengan surat menyurat. Di era globalisasi, surat menyurat telah tergantikan oleh *email* atau surat elektronik. *Email* merupakan komponen utama yang paling banyak digunakan dalam komunikasi informasi saat ini (Supriyanto, 2007). Namun komunikasi yang terjadi disaat ini apabila menggunakan *email* masih dianggap kurang cepat. Hal ini disebabkan karena sebagian besar *email* tidak bersifat *real time.* Sebagai contoh pengirim *email* tidak tahu apakah penerima *email* sedang online atau tidak sehingga pengirim tidak tahu kapan *email* tersebut akan dibaca atau dibalas.

Kemajuan teknologi komputer dan telekomunikasi membantu dalam menyelesaikan banyak pekerjaan dengan cepat, akurat, dan efisien. Salah satu kemajuan teknologi komunikasi yaitu menghasilkan aplikasi *instant messaging* atau pesan instan. *Instant messaging* merupakan fasilitas komunikasi *chatting* untuk para pengguna internet sehingga *user* dapat berkomunikasi dengan cara mengirimkan pesan berupa *text* dengan *user* lain (Zuliarso & Februariyanti, 2013). Namun seiring dengan kemajuan teknologi, dengan semakin banyaknya pengguna yang menggunakan aplikasi *instant messaging* terdapat dampak negatif berupa penyadapan data khususnya saat terjadi komunikasi yang bersifat rahasia dan penting sehingga aspek keamanan dalam pertukaran informasi dianggap penting.

Kriptografi adalah ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas, dan otentikasi asal data (Menezes, et al., 1996). Kriptografi bertujuan agar informasi yang bersifat rahasia dan dikirim melalui suatu jaringan,

seperti LAN atau *internet*, tidak dapat diketahui dan dimanfaatkan oleh orang lain atau pihak yang tidak berkepentingan.

RSA merupakan algoritma kriptografi kunci publik atau sering disebut kunci asimetrik (kunci enkripsi dan kunci dekripsi berbeda) sehingga tidak membutuhkan saluran yang aman untuk distribusi kunci. RSA ditemukan oleh tiga peneliti dari MIT (*Massachussets Institute of Technology*), yaitu Ronald Linn Rivest, Adi Shamir, dan Len Adleman pada tahun 1977 (Rivest, et al., 1978). Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor - faktor prima .

CRT (*Chinese Remainder Theorem*) merupakan suatu algoritma untuk mengurangi perhitungan aritmatika modular dengan modulus besar untuk perhitungan yang sama untuk masing-masing faktor dari modulus (Tilborg, 2005). CRT dapat memperpendek ukuran bit eksponen dekripsi *d* (merupakan kunci publik RSA atau RSA-CRT) dengan cara menyembunyikan *d* pada sistem kongruen sehingga mempercepat waktu dekripsi serta dapat digunakan bersama algoritma RSA yang disebut RSA - CRT.

Algoritma asimetris seperti RSA dapat diterapkan dalam pesan instan yang dibangun menggunakan bahasa pemrograman java tanpa mengurangi kecepatan, tidak terdapat delay yang berpengaruh dalam percobaan yang dilakukan pada setiap user, serta tidak ada pesan yang tidak utuh sampai ke tujuan pada setiap percobaan (Khairan, et al., 2014).

Algoritma RSA dapat diimplementasikan dalam program soket klien-server dengan menggunakan PHP yang dimana tingkat keamanan RSA yang baik yaitu tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi faktor primanya (Sulun, 2008).

Algoritma RSA menggunakan CRT empat kali lebih cepat untuk dekripsi dibandingkan algoritma RSA biasa (tanpa CRT), sehingga dekripsi pada algoritma RSA lebih efektif dengan menggunakan CRT (Shinde & Fadewar, 2008).

Untuk meningkatkan keamanan dari segi pengiriman pesan yang dibuat dalam saluran yang tidak aman serta modifikasi algoritma RSA dengan menggunakan teorema CRT agar dapat dibandingkan dengan algoritma RSA, perlu dibangun sebuah aplikasi *instant messaging* dengan mengimplementasikan algoritma kriptografi RSA – CRT.

1.2. Rumusan Masalah

Berdasarkan uraian latar belakang di atas, maka rumusan masalahnya adalah bagaimana mengimplementasikan algoritma kriptografi RSA - CRT pada aplikasi *instant messaging.*

1.3. Tujuan Manfaat

Tujuan yang ingin dicapai dalam penelitian ini adalah dapat diimplementasikannya algoritma kriptografi RSA – CRT pada aplikasi *instant messaging* serta dapat dibandingkan dengan algoritma kriptografi RSA.

Manfaat yang diharapkan dari penelitian ini adalah untuk meningkatkan keamanan data atau informasi pada saat menggunakan *instant messaging*.

1.4. Ruang Lingkup

Ruang lingkup dalam pembuatan aplikasi *instant messaging* menggunakan algoritma kriptografi RSA – CRT dan penelitian ini adalah sebagai berikut :

1. Data yang diamankan berupa teks.
2. Aplikasi ini dapat menampung maksimal 1.350 karakter untuk n yaitu hasil dari p (bilangan prima) dikali q (bilangan prima) yang digunakan untuk membangkitkan kunci RSA atau RSA-CRT yang lebih kecil dari 1.000.000, untuk n lebih besar sama dengan 1.000.000 dapat menampung maksimal 1.800 karakter setiap pengiriman pesan.
3. Aplikasi ini dapat menggunakan bilangan integer di atas 40 serta p dan q harus berbeda.
4. Aplikasi ini dapat digunakan untuk 2 pengguna yang terhubung dalam 1 server, 2 pengguna tersebut harus terhubung ke server terlebih dahulu.
5. Pengujian dilakukan untuk bit n mulai dari 56 bit sampai 88 bit.
6. Aplikasi menggunakan algoritma kriptografi RSA – CRT dan algoritma kriprografi RSA sebagai pembanding.
7. Aplikasi akan dibangun menggunakan pemrograman berorientasi objek serta menggunakan bahasa pemrograman *Visual Basic.net*.
8. Aplikasi yang dibuat berbasis *desktop* yang bersifat *client-server*.
9. Aplikasi *instant messaging* dibuat dengan pemrograman soket berbasis TCP.
10. Model pengembangan perangkat lunak menggunakan model proses *waterfall*.

1.5. Sistematika Penulisan

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

BAB I PENDAHULUAN

Bab ini membahas latar belakang, rumusan masalah, tujuan dan manfaat, ruang lingkup, dan sistematika penulisan penelitian mengenai Implementasi Algoritma Kriptografi RSA - CRT pada Aplikasi *Instant Messaging*.

BAB II TINJAUAN PUSTAKA

Bab ini menyajikan tinjauan pustaka yang berhubungan dengan topik penelitian. Tinjauan pustaka yang digunakan dalam penyusunan penelitian ini meliputi kriptografi, sistem kriptografi, faktor persekutuan terbesar (*Greatest Common Divisor*), *extended euclid*, invers, algoritma *fast modular exponentiation*, sistem kriptografi RSA, algoritma RSA, *chinese remainder theorem* (CRT), RSA dengan CRT (RSA-CRT), *instant messaging*, pemrograman soket dengan TCP, *unified modeling language* (UML), dan model proses *waterfall*.

BAB III ANALISIS DAN PERANCANGAN

Bab ini berisi tentang analisis perangkat lunak dan perancangan perangkat lunak. Analisis perangkat lunak meliputi analisis permasalahan dan analisis kebutuhan diantaranya kebutuhan fungsional yang dijelaskan dengan definisi aktor, definisi *use case*, skenario *use case* dan *use case diagram* serta kebutuhan non-fungsional. Perancangan perangkat lunak meliputi perancangan diagram diantaranya pemodelan dengan *class diagram*, *sequence diagram*, *activity diagram*, dan *deployment diagram*, perancangan algoritma kriptografi RSA-CRT pada aplikasi *instant messaging* diantaranya mengolah server dan *client*, mengolah kunci, dan mengolah pesan, serta perancangan antarmuka diantaranya perancangan antarmuka server dan perancangan antarmuka *client*.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi tentang implementasi perangkat lunak dan pengujian perangkat lunak. Implementasi perangkat lunak meliputi spesifikasi perangkat, implementasi *class,* implementasi algoritma kriptografi RSA-CRT pada aplikasi *instant messaging*, dan implementasi antarmuka. Pengujian perangkat lunak meliputi lingkungan pengujian, rencana pengujian, pelaksanaan pengujian, serta analisa hasil pengujian.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dari hasil pembuatan aplikasi *instant messaging* dengan menerapkan algoritma kriptografi RSA-CRT dan saran-saran untuk pengembangan selanjutnya.