PENERAPAN ALGORITMA RSA UNTUK PENGAMANAN DATA DAN DIGITAL SIGNATURE DENGAN . NET

SKRIPSI

disusun oleh

ANDRIANUS TRIORIZKA

06.12.1748

JURUSAN SISTEM INFORMASI

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

AMIKOM

YOGYAKARTA

2010

PENERAPAN ALGORITMA RSA UNTUK PENGAMANAN DATA DAN DIGITAL SIGNATURE DENGAN . NET

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Sistem Informasi

disusun oleh

ANDRIANUS TRIORIZKA

06.12.1748

JURUSAN SISTEM INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA

2010

PERSETUJUAN

SKRIPSI

Penerapan Algoritma RSA untuk Pengamanan Data dan Digital Signature Dengan .NET

yang dipersiapkan dan disusun oleh

Andrianus Triorizka

06.12.1748

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 27 Januari 2010

Dosen Pembimbing,

Ema Utami, S.Si., M.Kom
NIK. 190302037

PENGESAHAN

SKRIPSI

Penerapan Algoritma RSA untuk Pengamanan Data dan Digital Signature Dengan .NET

yang dipersiapkan dan disusun oleh

Andrianus Triorizka

06.12.1748

telah dipertahankan di depan Dewan Penguji

pada tanggal 17 Februari 2010

Susunan Dewan Penguji

Nama Penguji	**Tanda Tangan**
Andi Sunyoto, M.Kom. **NIK. 190302052**	_____
Armadyah Amborowati, S.Kom., M.Eng. **NIK. 190302063**	_____
Ema Utami, S.Si., M.Kom. **NIK. 190302037**	_____

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 17 Februari 2010

KETUA STMIK AMIKOM YOGYAKARTA

PERNYATAAN

Saya yang bertandatangan di bawah ini menyatakan bahwa, skripsi ini merupakan karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 17 Februari 2010

Andrianus Triorizka
NIM. 06.12.1748

HALAMAN PERSEMBAHAN

Segala puji bagi Allah SWT, ku panjatkan puji syukurku hanya kepada-Nya, yang telah memberikan rahmat dan hidayah-Nya serta memberikan kesehatan dan kesabaran sehingga aku bisa menyelesaikan skripsi ini dengan baik, dan hanya kepada-Nya aku memohon pertolongan dan ampunan.

Skripsi ini aku persembahkan untuk :

- *Kedua orang tua ku yang sangat-sangat aku sayangi dan selalu aku rindukan. Terima kasih untuk semua perhatian dan do`a yang selalu ada untukku, serta selalu sabar dalam mendidik dan memberi nasihat yang begitu bermanfaat bagiku.*
- *Kakak dan adik-adikku yang sangat aku sayangi dan selalu aku rindukan, semoga kita semua bisa menjadi orang yang sukses baik dunia maupun akhirat. Amin...*
- *Teman-teman kos "M19", terima kasih untuk semua dukungan kalian. Kalian seperti keluarga kedua bagiku. Terima kasih buat saran dan kritik dari kalian yang sangat membangun diriku yang lebih baik lagi.*
- *Teman-teman SI-D '06 yang aku cintai, aku sangat bersyukur bisa mengenal kalian dalam hidupku. Terima kasih atas dukungan dan do`a kalian semua. Semoga kalian segera menyusul aku. Amin.*
- *Buat teman-teman seperjuanganku, ayo segera selesaikan misi kalian. Segera lulus dan menjadi orang sukses. Amin*

HALAMAN MOTTO

" Jadilah yang terbaik dari yang terbaik "

" Jika kau lunak terhadap dirimu, maka dunia akan keras padamu. Jika kau keras terhadap dirimu, maka dunia akan lunak padamu "

" Kegagalan merupakan awal dari suatu keberhasilan yang tertunda "

" Di atas langit masih ada langit "

" Usaha tanpa do`a akan sia-sia, dan berdo`a saja tanpa usaha tak akan ada hasilnya. Berusaha dan berdo`a adalah kunci kesuksesan "

KATA PENGANTAR

Assalamu`alaikum wr. wb.

Dengan menyebut nama Allah SWT. Yang Maha Pengasih lagi Maha Penyayang, puji syukur kehadirat Allah SWT. yang telah melimpahkan rahmat, taufiq dan hidayah-Nya sehingga penulis dapat menyelesaikan Skripsi ini dengan judul "**PENERAPAN ALGORITMA RSA UNTUK PENGAMANAN DATA DAN DIGITAL SIGNATURE DENGAN .NET"**

Penulisan Skripsi ini ditujukan untuk memenuhi salah satu syarat dalam memperoleh gelar Sarjana S1 pada Jurusan Sistem Informasi pada Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.

Selesainya skripsi ini tidak terlepas dari dukungan berbagai pihak yang telah memberikan dorongan moril maupun spiritual dan juga bimbingan ilmu pengetahuan. Oleh karena itu, pada kesempatan yang berbahagia ini penulis mengucapkan rasa terima kasih yang sebesar-besarnya kepada :

1. Bapak Prof. Dr. Muhammad Suyanto, M.M., selaku Ketua STMIK AMIKOM Yogyakarta.
2. Bapak Drs. Bambang Sudaryatno, M.M., selaku Ketua Jurusan Sistem Informasi STMIK AMIKOM Yogyakarta.
3. Ibu Ema Utami, S.Si., M.Kom., selaku Dosen Pembimbing yang sangat membantu dalam proses bimbingan.
4. Seluruh Dosen dan Staf Pengajar STMIK AMIKOM Yogyakarta yang telah memberikan ilmu pengetahuan selama kuliah.

5. Teman-teman seperjuangan yang selalu memberi semangat yang luar biasa.
6. Dan semua pihak yang telah memberikan dukungan dan sumbangsihnya sehingga terselesaikannya skripsi ini.

Penulis sangat menyadari bahwa penulisan skripsi ini masih belum sempurna, oleh sebab itu penulis mengharapkan kritik dan saran yang dapat melengkapi skripsi ini demi membangun kesempurnaan dalam pengembanganya lebih lanjut.

Akhir kata semoga dengan adanya penelitian ini dapat lebih bermanfaat bagi penulis sendiri, pembaca dan pihak yang membutuhkan.

Wassalamu`alaikum wr. wb.

Yogyakarta, Februari 2010

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Kriptografi adalah ilmu dan seni untuk menjaga keamanan data dengan melakukan enkripsi dan deskripsi dengan memanfaatkan model matematika tertentu, dan salah satu model yang digunakan yaitu *asymmetric cryptography* dengan menentukan kunci publik dan kunci privat. Di dalam model kriptosistem yang dibangun ini terdapat algoritma dan fungsi yang memanfaatkan kriptografi. RSA yang merupakan algoritma pada enkripsi public key. RSA merupakan salah satu algoritma yang paling maju dalam bidang kriptografi public key. RSA dipercaya dalam mengamankan dengan menggunakan kunci yang cukup panjang.

Model kriptosistem ini juga akan melakukan digital signature dengan memanfaatkan fungsi hash MD5, digunakan untuk melakukan pengujian integritas sebuah file. Dengan model kriptosistem ini diharapkan dapat membantu pengguna dalam mengamankan data yang sangat penting dan rahasia sekaligus dapat berkomunikasi secara aman dengan relasinya diseluruh dunia melalui internet maupun melalui jaringan yang lainnya.

Kata-kunci : Kriptografi, Asymmetric Cryptography, Algoritma RSA, Algoritma MD5, Model Kriptosistem, Jaringan.

ABSTRACT

Cryptography is the science and art to maintain data security with encryption and description using a specific mathematical models, and one model of asymmetric cryptography used to determine the public key and private key. In this cryptosystem model have algorithms and functions that make use of cryptography. RSA is an algorithm in public key encryption. RSA is one of the most advanced algorithms in the field of public key cryptography. RSA is believed in using secure key long enough.

The cryptosystem model will also perform a digital signature by using the MD5 hash function, used for testing the integrity of a file. Kriptosistem model is expected to help users in securing critical data and confidential and can communicate securely with the relationship over the world via the Internet or through other networks.

Keywords *: Cryptography, Asymmetric Cryptography, RSA algorithm, MD5 Algorithm, Cryptosystem Model, Network.*