

**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

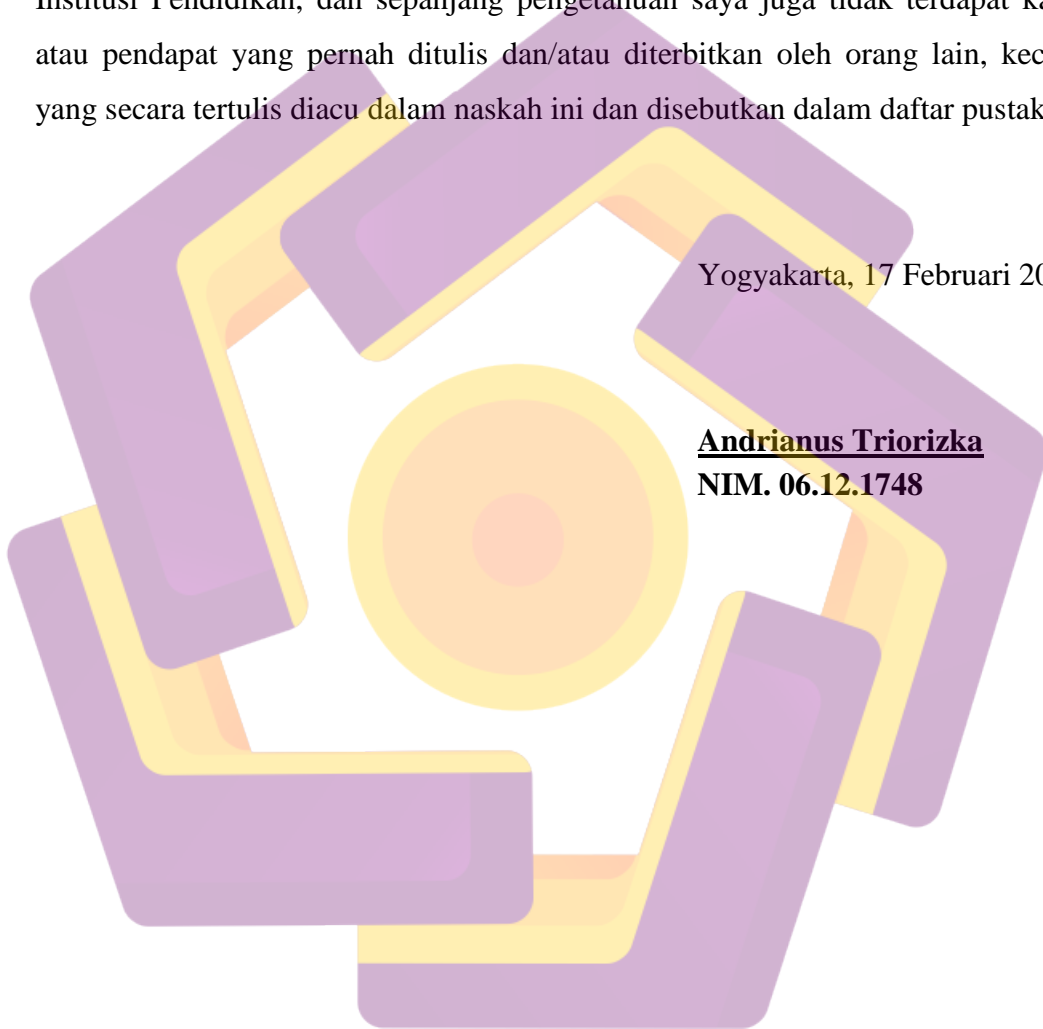
KETUA STMIK AMIKOM YOGYAKARTA

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 kehadiran 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 sumbangsuhnya 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.

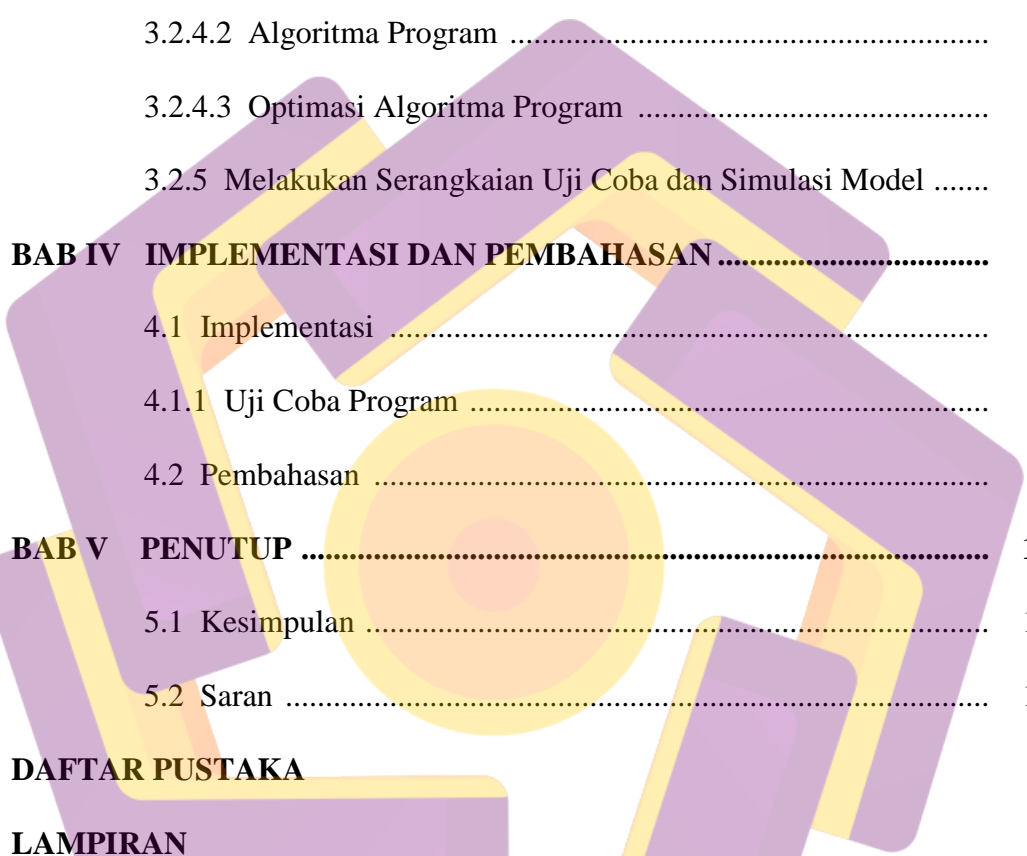
Yogyakarta, Februari 2010

Penulis

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PERSETUJUAN	ii
HALAMAN PENGESAHAN	iii
HALAMAN PERNYATAAN	iv
HALAMAN PERSEMBAHAN	v
HALAMAN MOTTO	vi
KATA PENGANTAR	vii
DAFTAR ISI	ix
DAFTAR TABEL	xii
DAFTAR GAMBAR	xiii
INTISARI	xvi
ABSTRACT	xvii
BAB I PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah	2
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
1.6 Metodologi Penelitian	4
1.7 Sistematika Penulisan	5
BAB II LANDASAN TEORI	6

2.1 Tinjauan Pustaka	6
2.2 Landasan Teori	12
2.2.1 Konsep Dasar Kriptografi	12
2.2.2 Model Algoritma RSA	16
2.2.2.1 Deskripsi RSA	16
2.2.2.2 Algoritma RSA	17
2.2.2.3 Kinerja RSA	18
2.2.2.4 Keamanan RSA	20
2.2.3 <i>Digital Signature</i> (Tanda Tangan Digital)	20
2.2.3.1 <i>Digital Signature</i> Dengan Menggunakan Fungsi <i>Hash</i> Satu Arah	22
2.2.4 Model Algoritma MD5	23
2.2.5 Dot (.) NET Framework	24
2.2.6 Konsep Pemodelan Sistem	25
2.2.6.1 Flowchart	25
2.2.7 Perangkat Lunak yang Digunakan	27
2.2.7.1 Microsoft Visual Studio 2008	27
BAB III ANALISIS DAN PERANCANGAN SISTEM	31
3.1 Analisis Kebutuhan Sistem	31
3.1.1 Kebutuhan Perangkat Keras	31
3.1.2 Kebutuhan Perangkat Lunak	32
3.2 Perancangan Sistem	33
3.2.1 Melakukan Studi Pustaka	33



3.2.2	Persiapan Dalam Penelitian	33
3.2.3	Perancangan Antarmuka	34
3.2.4	Penerapan Algoritma	42
3.2.4.1	Flowchart Program	43
3.2.4.2	Algoritma Program	46
3.2.4.3	Optimasi Algoritma Program	51
3.2.5	Melakukan Serangkaian Uji Coba dan Simulasi Model	54
BAB IV	IMPLEMENTASI DAN PEMBAHASAN	58
4.1	Implementasi	58
4.1.1	Uji Coba Program	58
4.2	Pembahasan	81
BAB V	PENUTUP	102
5.1	Kesimpulan	102
5.2	Saran	103
DAFTAR PUSTAKA		
LAMPIRAN		

DAFTAR TABEL

Tabel 2.1	Simbol-simbol dalam flowchart	26
Tabel 3.1	Spesifikasi <i>hardware</i> minimum komputer pengguna	32
Tabel 4.1	Hasil uji coba enkripsi dan <i>signature</i> teks dengan dua metode inputan teks	61
Tabel 4.2	Hasil uji coba dekripsi dan verifikasi <i>signature</i> teks dengan dua metode inputan teks	66
Tabel 4.3	File non teks yang digunakan dalam penelitian	68
Tabel 4.4	Hasil uji coba enkripsi file non teks yang digunakan dalam penelitian	72
Tabel 4.5	File non teks berekstensi <i>.enc</i> yang digunakan dalam penelitian ..	73
Tabel 4.6	Hasil uji coba dekripsi file non teks berekstensi <i>.enc</i> yang digunakan dalam penelitian	75
Tabel 4.7	File yang digunakan dalam percobaan	77
Tabel 4.8	Hasil uji coba penghancuran file	79

DAFTAR GAMBAR

Gambar 2.1 Skema enkripsi dan dekripsi secara umum	13
Gambar 2.2 Proses enkripsi dan dekripsi <i>symmetric cryptography</i>	15
Gambar 2.3 Proses enkripsi dan dekripsi <i>asymmetric cryptography</i>	16
Gambar 2.4 Algoritma RSA	18
Gambar 2.5 Skema otentikasi dengan <i>digital signature</i>	23
Gambar 2.6 Pembuatan <i>message digest</i> dengan algoritma MD5	24
Gambar 2.7 Tampilan Visual Studio 2008	29
Gambar 3.1 Rancangan form utama	35
Gambar 3.2 Rancangan form <i>key</i>	36
Gambar 3.3 Rancangan form <i>encrypt text</i>	37
Gambar 3.4 Rancangan form <i>decrypt text</i>	38
Gambar 3.5 Rancangan form <i>encrypt file</i>	39
Gambar 3.6 Rancangan form <i>decrypt file</i>	40
Gambar 3.7 Rancangan form <i>file shredder</i>	41
Gambar 3.8 Rancangan form <i>help</i>	41
Gambar 3.9 Rancangan form <i>about</i>	42
Gambar 3.10 Flowchart program enkripsi teks dan <i>digital signature</i>	43
Gambar 3.11 Flowchart program dekripsi teks dan verifikasi <i>signature data</i>	44
Gambar 3.12 Flowchart program enkripsi file	45
Gambar 3.13 Flowchart program dekripsi file	46

Gambar 4.1 Tampilan uji coba pembuatan kunci RSA	59
Gambar 4.2 Tampilan proses enkripsi dan <i>signature</i> teks	63
Gambar 4.3 Tampilan proses dekripsi dan verifikasi <i>signature</i> teks	64
Gambar 4.4 Informasi <i>signature</i> data cocok	65
Gambar 4.5 Informasi <i>signature</i> data tidak cocok	65
Gambar 4.6 Tampilan hasil proses enkripsi file non teks	69
Gambar 4.7 Informasi kunci cocok.....	70
Gambar 4.8 Pesan kesalahan pada penginputan kunci.....	70
Gambar 4.9 <i>Dialog box</i>	71
Gambar 4.10 Informasi enkripsi file berhasil	71
Gambar 4.11 Tampilan hasil proses dekripsi file non teks	74
Gambar 4.12 Informasi dekripsi file berhasil	75
Gambar 4.13 Tampilan proses penghancuran file	77
Gambar 4.14 Pesan konfirmasi	78
Gambar 4.15 Pesan penghancuran file sukses	78
Gambar 4.16 Tampilan hasil eksekusi menu <i>send mail</i>	80
Gambar 4.17 Tampilan hasil eksekusi menu <i>reference</i>	80
Gambar 4.18 Struktur model kriptosistem	81
Gambar 4.19 Tampilan form utama	82
Gambar 4.20 Tampilan form <i>key</i>	84
Gambar 4.21 Tampilan form <i>encrypt text</i>	86
Gambar 4.22 Tampilan form <i>decrypt text</i>	89
Gambar 4.23 Tampilan form <i>encrypt file</i>	92

Gambar 4.24 Tampilan form <i>decrypt file</i>	95
Gambar 4.25 Tampilan form <i>file shredder</i>	97
Gambar 4.26 Tampilan menu <i>reference</i>	100
Gambar 4.27 Tampilan form <i>about</i>	101



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 decryption 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.*