

SKIRIPSI

**IMPLEMENTASI ENKRIPSI DAN DEKRIPSI DATA MENGGUNAKAN
METODE ALGORITMA RSA DAN MEMANFAATKAN RC2CRYPTO
SERVICE PROVIDER PADA KOMPONENT .NET FRAMEWORK 2.0**



Disusun oleh :

NEFIANTI

No. Mhs : 06.12.1672

Jenjang : Strata Satu

JURUSAN SISTEM INFORMASI

SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER

"AMIKOM "

YOGYAKARTA

2009

**IMPLEMENTASI ENKRIPSI DAN DEKRIPSI DATA MENGGUNAKAN
METODE ALGORITMA RSA DAN MEMANFAATKAN RC2CRYPTO
SERVICE PROVIDER PADA KOMPONENT .NET FRAMEWORK 2.0**

SKRIPSI

Diajukan sebagai salah satu syarat untuk menyelesaikan jenjang
pendidikan Strata Satu pada Sekolah Tinggi Manajemen
Informatika dan Komputer

Disusun Oleh :

Nefianti

No. Mhs : 06.12.1672
Jurusan : Sistem Informasi
Jenjang : Strata Satu

**SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA**

2009

HALAMAN PENGESAHAN

**IMPLEMENTASI ENKRIPSI DAN DEKRIPSI DATA MENGGUNAKAN
METODE ALGORITMA RSA DAN MEMANFAATKAN RC2CRYPTO
SERVICE PROVIDER PADA KOMPONEN .NET FRAMEWORK 2.0**

SKRIPSI

Diajukan sSebagai Syarat Kelulusan Jenjang Strata-1

Jurusan Sistem Informasi

Disusun Oleh :

Nefianti

06.12.672

Telah diterima dan di setujui oleh Dosen Pembimbing Skripsi

STMIK AMIKOM YOGYAKARTA

Mengetahui :

Ketua STMIK AMIKOM :



(M. Suyanto, Prof. DR., M.M.)

Dosen Pembimbing :



(Arief Setyanto, S.Si, MT)

HALAMAN BERITA ACARA

IMPLEMENTASI ENKRIPSI DAN DEKRIPSI DATA MENGGUNAKAN METODE RSA DAN MEMANFAATKAN RC2CRYPTO SERVICE PROVIDER PADA KOMPONEN .NET FRAMEWORK 2.0

Telah di persentasikan dan di uji di hadapan penguji pada :

Hari/Tanggal : Kamis, 10 Agustus 2009

Tempat : Gedung II, Lantai II, STMIK AMIKOM YOGYAKARTA

Ruang : Pixel

Jam : 13.30

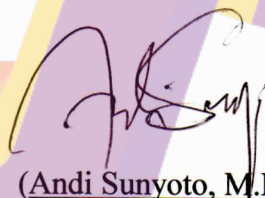
Susunan Panitia Penguji :

Penguji I :




(Arief Setyanto, S.Si,MT)

Penguji II :



(Andi Sunyoto, M.Kom)

Penguji III :



(Sudarmawan, MT)

PERSEMABAHAN

Assalumiailaikum WR, WB

**Alhamdulillah Rabbil'aalamin, terimakasih kehadiran ALLAH SWT,
atas limpahan rahmat dan hidayatNYA dan Sholawat dan Salam
tercurahkan kepada Junujungan kita, Nabi Muhammad SAW.**

Skripsi ini aku persembahkan untuk :

Bapak dan Ibu tersayang, terima kasih atas do'a
serta dukungannya, baik secara moril maupun
materil.

Adik-adikku tercinta yang selalu memberiku
semangat untuk terus maju.
Seluruh keluargaku yang tersebar di pulau-pulau
di Indonesia.

Bapak arif setyanto yang telah memberikan
bimbingan skripsi.
Almamaterku Stmik AMIKOM.

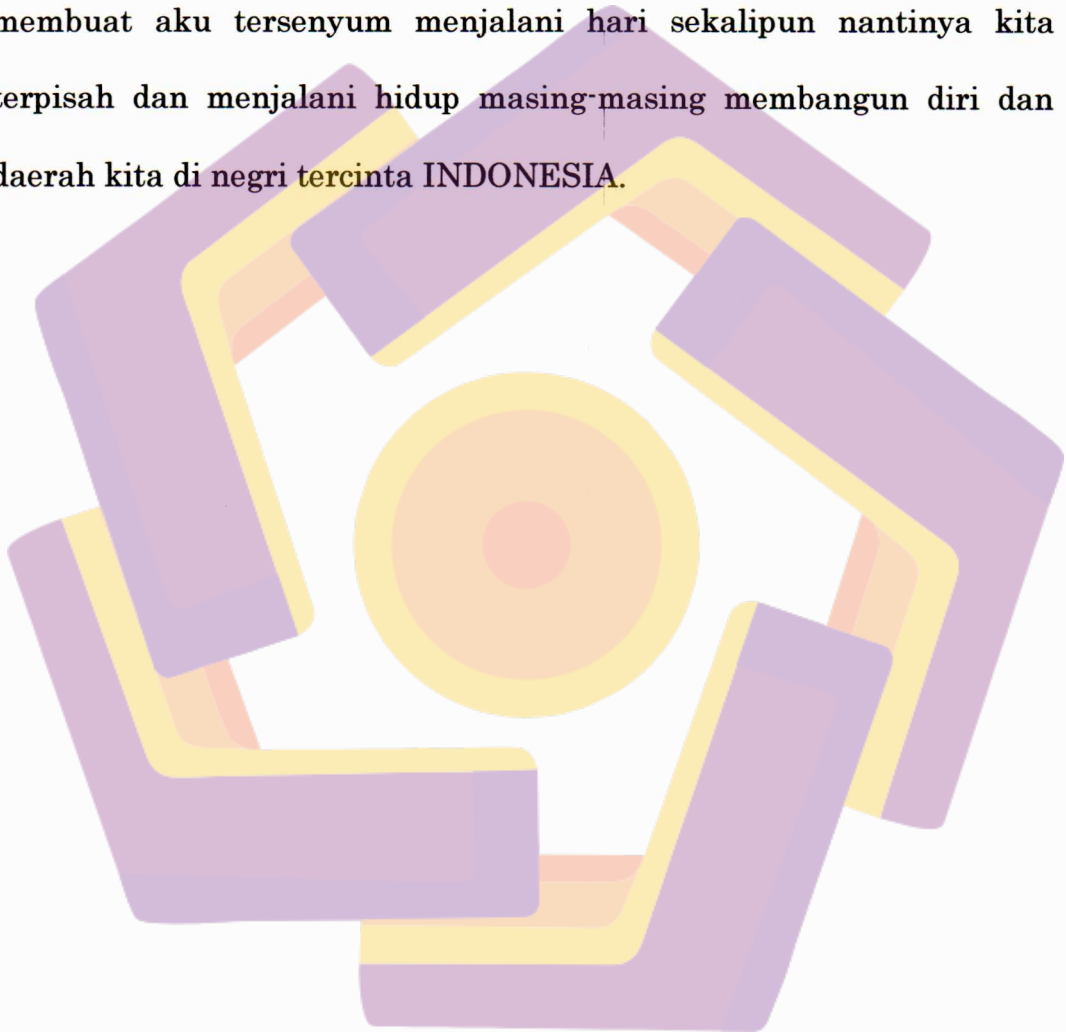
Teman dekatku (Adi) yang selalu memberiku
semangat dan perhatian.

Kaka saya (Ade dan Koko) yang telah membarikan
semangat dan dukungan

Semua Sahabat-sahabat saya, sahabat
seperjuanganku baik di Sulawesi, papua maupun di
Yogyakarta

Atau dimanapun kalian berada saat ini
Terimah kasih

Lewat lantunan doa, semangat, cinta, kasih sayang, tawa dan canda dalam kebersamaan menjadikan motivasi dalam masa-masa menjalani perkuliahan ini sampai aku selesai, semua itu tidak akan pernah habis dan akan tertanam dalam jiwa ku yang akan selalu membuat aku tersenyum menjalani hari sekalipun nantinya kita terpisah dan menjalani hidup masing-masing membangun diri dan daerah kita di negeri tercinta INDONESIA.



MOTTO

“Ilmu itu sahabat akrab dalam kesepian, sahabat dalam keterasingan, pengawas dalam kesendirian, penunjuk jalan kearah yang benar, penolong di saat sulit dan simpanan saat kematian”

“ketika waktu pagi tiba jangan menunggu sampai sore, hiduplah dalam batasan hari ini dengan sseluruh semangat yang ada untuk menjadi lebih baik di hari ini”

Dan

“Ilmu adalah hidu, cinta dan keabadian”

“Hidup adalah perjuangan, maka janganlah menyerah hanya karena satu kegagalan”.

INTISARI

Aplikasi ini dibuat untuk tujuan mengamankan data dengan menggunakan teknik enkripsi dan dekripsi. Dalam hal ini data yang diamankan adalah *file* teks yang berbasis *.txt dan *file* non-teks yaitu file gambar dan pdf.

Sedangkan metode yang digunakan adalah Algoritma RSA, metode ini akan mengubah karakter-karakter pada plainteks menjadi bilangan bulat positif dengan rumus tertentu. Untuk *file* teks menggunakan metode Algoritma RSA dan *RC2CryptoServiceProvider* pada komponen .NET Framework digunakan untuk *file* non teks. Aplikasi ini dibangun dengan menggunakan bahasa pemrograman Visual Basic 2005 dan berdiri diatas .Net Framework.

Kata Kunci : *RC2CryptoServiceProvider*, Algoritma RSA, Enkripsi, Dekripsi,

KATA PENGANTAR

Assalamu 'alaikum Wr. Wb,

Dengan mengucapkan puji syukur penulis panjatkan kehadiran Allah SWT karena dengan rahmat dan hidayah-Nya penulis dapat menyelesaikan karya tulis yang berjudul *Implementasi Enkripsi Dan Dekripsi Data Menggunakan Metode Algoritma RSA Dan Memanfaatkan RC2Crypto Service Provider Pada Komponen .NET Framework 2.0* dengan baik. Maksud dan tujuan dari penulisan karya tulis ini adalah guna melengkapi dan memenuhi sebagian syarat yang telah ditentukan oleh STMIK AMIKOM Yogyakarta untuk menyelesaikan Program Strata Satu (S1).

Penyusunan laporan ini dapat selesai berkat adanya bantuan, bimbingan, arahan, dan motivasi dari berbagai pihak. Untuk itu pada kesempatan ini penyusun tidak lupa menghaturkan rasa terima kasih yang tulus kepada:

1. Bapak M. Suyanto, Prof. DR., M.M., selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
2. Bapak Drs. Bambang Sudaryatno, M.M, selaku ketua jurusan Sistem Informasi jenjang Strata Satu Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
3. Bapak Arif Setyanto, S.Si.,MT ,selaku Dosen Pembimbing.
4. Seluruh dosen dan staf karyawan Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM di Yogyakarta.

5. Bapak dan Ibu, Adik-adik saya, ka'adi, Pak Kost dan Ibu Kost, semua keluarga saya, dan sahabat-sahabat saya yang tersebar di seluruh pulau di Indonesia.
6. Buat Kaka saya Martini, S.kom dan Koko, Sahabat-sahabat saya Fitri Wahyuni, Murni Sulaiman, kaka saya Ade dan Koko terima kasih banyak.

Penulis menyadari bahwa didalam penulisan karya tulis ini masih jauh dari sempurna, oleh karena itu kritik dan saran yang bersifat membangun sangatlah penulis harapkan guna perbaikan laporan karya tulis ini pada masa yang akan datang dan menambah wawasan dan pengembangan ilmu yang telah penulis peroleh selama ini.

Akhir kata semoga penulisan karya tulis ini dapat bermanfaat bagi penulis dan juga bagi para pembaca. Terima kasih.

Wassalamu' alaikum Wr. Wb

Yogyakarta, 10 Agustus 2009


(Nefianti S.kom)

DAFTAR ISI

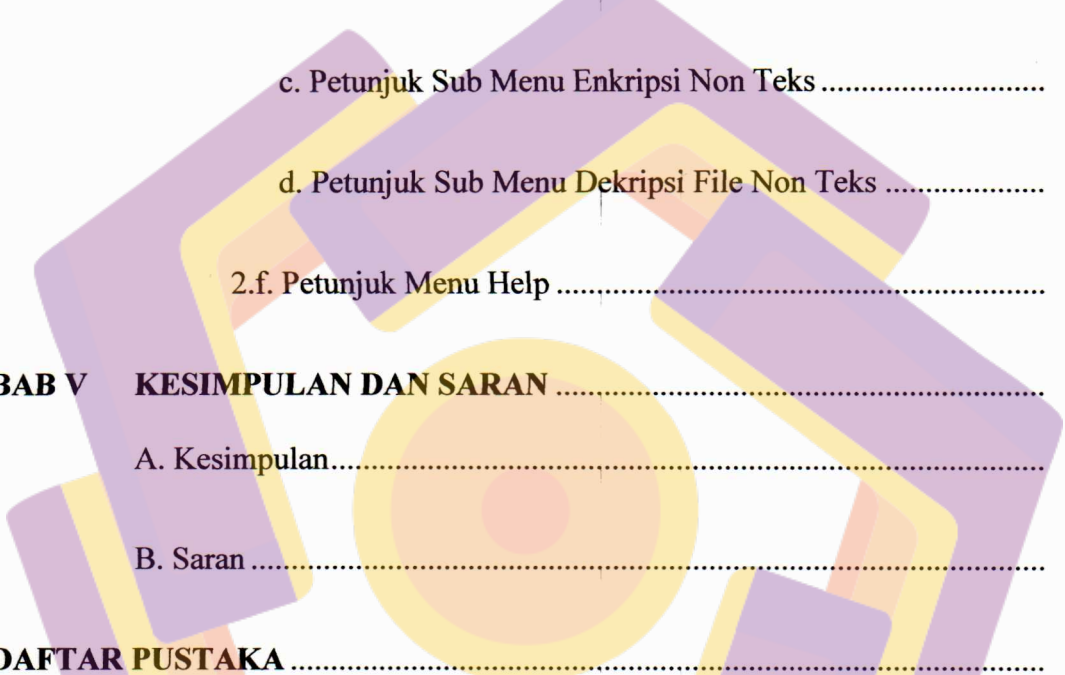
HALAMAN SAMPUL	i
HALAMAN JUDUL	ii
HALAMAN PERSETUJUAN	iii
HALAMAN PENGESAHAN	iv
HALAMAN PERSEMBAHAN	v
MOTTO	vii
INTISARI	viii
KATA PENGANTAR	x
DAFTAR ISI	xi
DAFTAR GAMBAR	xix
DAFTAR TABEL	xx
BAB I PENDAHULUAN	1
A. Latar Belakang Masalah.....	1
B. Rumusan Masalah	2
C. Batasan masalah	3
D. Tujuan Penelitian.....	3
E. Manfaat Penelitian.....	4
F. Sistematika Penulisan.....	4
BAB II LANDASAN TEORI	6
A. Dasar Teori.....	6
1. Kriptografi.....	6

1.a. Mekanisme Kriptografi.....	7
1.b. Kriptografi Asimtrik.....	9
2. RSA.....	11
2.a. Sejarah RSA	11
2.b. Keamanan RSA	12
2.c. Perumusan Algoritma RSA	14
2.d. Algoritma Enkripsi Dan Dekripsi	16
B. Perangkat Lunak.....	19
1. Visual Basic 2005.....	19
1.a. Area Kerja Visual Basic .NET	19
1.b. Variabel Dan Tipe data Dalam Visual Basic .NET.....	21
1.c. Operator Visual Basic.....	22
1.d. Fungsi-Fungsi Dalam Visual Basic.....	24
2. Net Framework.....	27
3. Teori Pengembangan Perangkat Lunak.....	28
3.a. DFD (Data Flow Diagram).....	28
3.b. Flowchart Program.....	32
BAB III ANALISIS DAN PERANCANGAN SISTEM.....	34

A. Analisis Perancangan Sistem	34
1. Analisis Kebutuhan Sistem	34
2. Kebutuhan Perangkat Keras	34
3. Kebutuhan Perangkat Lunak	35
B. Perancangan Sistem.....	35
1. Diagram Alir Data.....	35
1.a. Diagram Konteks.....	36
1.b. DFD level 0	36
1.c. DFD level 1 proses 1 menu kunci	38
1.d. DFD level 1 proses 2 menu enkripsi	38
1.e. DFD level 1 proses 3 menu dekripsi	39
1.f. DFD level 2	40
2. Flowchart Sistem.....	40
2.a Flowchart Membangkitkan Pasangan Kunci.....	42
2.b. Flowchart Program Enkripsi Teks	44
2.c. Flowchart Program Dekripsi Teks	45
2.d. Flowchart Program Enkripsi Non Teks.....	48
2.e. Flowchart Program Dekripsi Non Teks.....	49

3. Perancangan Input Output.....	50
3.a. Rancangan Form Utama	50
3.b. Rancangan Form Membangkitkan Pasangan Kunci	51
3.c. Rancangan Form Enkripsi Teks	52
3.d. Rancangan Form Dekripsi Teks.....	53
3.e. Rancangan Form Enkripsi File Non Teks	54
3.f Rancangan form Kunci Enkripsi File Non Teks	55
3.g. Rancangan Form Dekripsi File Non Teks.....	55
3.h. Rancangan Form Password	56
3.i. Rancangan Form Kesalahan.....	56
3.j. Rancangan Form Informasi.....	57
3.k. Rancangan Form Help	57
BAB IV STRUKTUR, UJI COBA, PEMBAHASAN SISTEM DAN	
PETUNJUK PENGGUNAAN PERANGKAT LUNAK.....	58
A. Stuktur Aplikasi Atau Arsitektur Perangkat Lunak	58
B. Uji Coba	61
1. Dasar Uji Coba	61
2. Kesalahan-kesalahan Program	61

3. Uji Coba Dan Hasil	62
3.a. Uji Coba dan Hasil Enkripsi Tesk	63
3.b. Tabel Uji Coba Dan Hasil Dekripsi Teks.....	65
3.c. Uji Coba Dan Hasil Enkripsi Non Teks	66
3.d. Uji Coba Dan Hasil Dekripsi Non Tek	67
C. Pembahasan.....	68
1. Fungsi Membangkitkan Pasangan kunci.....	68
1.a Mencari Bilangan Prima.....	68
1.b. Mencari kunci.....	69
2. Fungsi untuk mengenkripsi <i>file</i> teks.....	70
3. Fungsi untuk mendekripsi file teks	72
4. Fungsi untuk mengenkripsi file non teks	72
5. Funsu password.....	73
6. Fungsi untuk mendekripsi file non teks	75
D. Petunjuk Penggunaan Perangkat Lunak	76
1. Instalasi Program.....	76
2. penggunaan fungsi aplikasi	79



2.a Petunjuk menu kunci	79
2.b. petunjuk menu kriptografi	83
a. Sub Menu Enkripsi Teks	84
b. Sub Menu Dekripsi Teks.....	85
c. Petunjuk Sub Menu Enkripsi Non Teks	87
d. Petunjuk Sub Menu Dekripsi File Non Teks	90
2.f. Petunjuk Menu Help	93
BAB V KESIMPULAN DAN SARAN	94
A. Kesimpulan.....	94
B. Saran	95
DAFTAR PUSTAKA	96

DAFTAR GAMBAR

Gambar 2.1	Skema Kriptografi Asimetri	8
Gambar 2.2	Mekanisme Kriptografi Asimetrik	10
Gambar 3.1	Diagram Konteks.....	36
Gambar 3.2	Data Flow Diagram level 0	37
Gambar 3.3	DFD Level 1 Proses 1 Menu Kunci	38
Gambar 3.4	DFD Level 1 Proses 2 Enkripsi.....	39
Gambar 3.5	DFD Level 1 Proses 3 Menu Dekripsi	39
Gambar 3.6	DFD Level 2.....	41
Gambar 3.7	Flowchart Membangkitkan Pasangan Kunci	42
Gambar 3.8	Flowchart Program Enkripsi	44
Gambar 3.9	Flowchart Program Dekripsi	45
Gambar 3.10	Flowchart Enkripsi Non Teks.....	48
Gambar 3.11	Flowchart Dekripsi Non Teks	49
Gambar 3.12	Form Utama	51
Gambar 3.13	Rancangan form Membangkitkan Pasangan Kunci	52
Gambar 3.14	Rancangan Form Enkripsi Teks	53

Gambar 3.15	Rancangan Form Dekripsi Teks	54
gambar 3.16	Rancangan Form Enkripsi File Non teks	55
Gambar 3.17	Form Kunci Enkripsi file Non Teks	55
Gambar 3.18	Rancangan Form Dekripsi File Non Teks.....	56
Gambar 3.21	Rancangan Form Informasi	57
Gambar 3.22	Rancangan Form Help	57
Gambar 4.1	Struktur Aplikasi Program.....	58
Gambar 4.2	Plainteks Dalam Bentuk Teks	62
Gambar 4.3	Hasil Enkripsi Berupa Chiperteks	64
Gambar 4.2	Setup Wizard	76
Gambar 4.3	Selection Installation Folder.....	77
Gambar 4.4	Confil Installation	77
Gambar 4.5	Installation Setup1	78
Gambar 4.6	Installation Complete	78
Gambar 4.7	Membangkitkan Pasangan Kunci.....	79
Gambar 4.8	Mencari Bilangan Prima.....	80
Gambar 4.9	Cek Kunci Publik	81
Gambar 4.10	Form Informasi	81

Gambar 4.11	Hitung Kunci Privat.....	82
Gambar 4.12	Hasil Imput Kunci	83
Gambar 4.13	Input (Plainteks) Enkripsi Teks.....	84
Gambar 4.14	Output (Chiperteks) Enkripsi Teks.....	85
Gambar 4.15	Input Chiperteks (dekripsi).....	86
Gambar 4.16	Form Dekripsi Teks.....	87
Gambar 4.17	Browse Plainteks (Enkripsi Non Teks)	88
Gambar 4.18	Password Enkripsi Non Teks	88
Gambar 4.19	Drive Penyimpanan Data	89
Gambar 4.20	Informasi (Enkripsi File Fukses).....	89
Gambar 4.21	File Output (Enkripsi Non Teks)	90
Gambar 4.22	Browse File (Dekripsi Non Teks)	91
Gambar 4.23	Password Dekripsi Non Teks	91
Gambar 4.24	Drive Folder	92
Gamabr 4.25	Informasi Dekripsi File Sukses	92
Gambar 4.26	Form Dekripsi File Non Teks.....	93
Gambar 4.27	Tampilan Help.....	93

DAFTAR TABEL

Tabel 2.1	Tipe Data Visual Basic .NET	21
Tabel 2.2	Operator Aritmatika Dalam Visual Basic .NET.....	23
Table 2.3	Simbol-simbol Yang Digunakan Dalam DFD	29
Tabel 2.4	Simbol-simbol Dalam Flowchart	33
Table 4.1	Uji Coba Dan Hasil Enkripsi Teks.....	63
Table 4.2	Uji Coba Dan Hasil Dekripsi Teks.....	65
Table 4.3	Uji Coba Dan Hasil Enkripsi Non Teks.....	66
Table 4.4	Uji Coba Dan Hasil Dekripsi Non Teks.....	67