HALAMAN PENGESAHAN I

Tugas akhir dengan judul :

ALGORITMA RIVEST-SHAMIR-ADLEMAN (RSA) DALAM KRIPTOSISTEM KUNCI UMUM

Disusun oleh :

Nama : Nur Izzati

NIM : J2A 097 039

Telah lulus ujian sarjana pada tanggal 7 Agustus 2002

Semarang, 21 Agustus 2002

Panitia Penguji Ujian Sarjana

Jurusan Matematika

Ketua Jurusan Matematika
FMIPA Undip

Drs. Jayu Surarso, Msc. PhD
NIP. 131 764 886

Ketua

Drs. Kushartantya, MIKomp
NIP. 130 805 062

HALAMAN PENGESAHAN II

Tugas akhir dengan judul :

ALGORITMA RIVEST-SHAMIR-ADLEMAN (RSA) DALAM KRIPTOSISTEM KUNCI UMUM

Disusun oleh :

Nama : Nur Izzati

NIM : J2A 097 039

Telah Diseminarkan dan disetujui pada tanggal 7 Agustus 2002

Semarang, 21 Agustus 2002

Pembimbing I	Pembimbing II
Drs. Kushartantya,MIKomp	Aris Sugiharto, SSi
NIP. 130 805 062	NIP. 132 161 207

PERSEMBAHAN

ALLAH SWT atas penjagaanMU selama ini ...
Nabi Muhammad SAW yang telah mengajarkan nikmat islam kepadaku

Ibu Masyitoh dan bapak Mas'Udi tercinta
Mas Imank, Yunan dan de' Eva tersayang
Thanks for loving me ....

MASDUKI family atas dukungannya
Om Cham , Lik Ipah , Fandi & si endut Farah , Om Fui & Bulik Rita
Om Zahid & Bulik Eli , Nita , mba Upit dan Dede

My friends...atas persahabatan yang manis selama ini
Nana ,Yunnie , Nining , Nidyan ,Udin , Asep , Imoenk , Hidayat
All members of Math Fly' 97

Sobatku....
Anno (Let's cheer up the world !), YP
Dwinanto (thank's man ...) dan Ulin (Don't give up ...!)

Temen-temen 'Gober' Adipati Unus 13 atas keceriannya
Sharie (thanks for joggingnya ...),
Retno (thanks for understanding me),m'Tuti ,Fifi,
Dewi , Ida , Eko , Anne , Nita , m'Ima , Elis
Reni (kitiran Nagane'...), Amel Donald
deelel

And the last ...
For Kiko ,Olief and 'Pacey' ,thanks for everything

MOTTO

ALLAH tidak akan mengubah nasib seorang hamba
Jika hamba itu sendiri yang mengubahnya
(2.S Ar–raad : 11)

Kerendahan hati

Kalau engkau tidak mampu menjadi beringin yang tegak
Jadilah belukar
Belukar yang terbaik, yang tumbuh di tepi danau
Kalau engkau tak sanggup jadi belukar
Jadilah rumput
Rumput yang memperkuat tanggul pinggiran jalan
Kalau engkau tak mampu menjadi jalan raya
Jadilah jalan kecil
Jalan setapak yang membawa orang ke mata air
Tak semua orang menjadi kapten
Harus ada yang menjadi awak kapalnya
Bukan besar kecil tugas
yang menjadi tinggi rendahnya nilai dirimu
Tetapi
Arti yang dapat kau berikan untuk hidupmu
Jadilah dirimu sendiri
Sebaik–baiknya dari dirimu

KATA PENGANTAR

Alhamdulilah penulis panjatkan kepada Pemberi Nikmat Hidup Allah SWT karena dengan rahmat dan hidayatNya penulis dapat menyelesaikan tugas akhir ini.

Tugas akhir yang berjudul **"ALGORITMA RIVEST-SHAMIR-ADLEMAN (RSA) DALAM KRIPTOSISTEM KUNCI UMUM"** disusun sebagai salah satu syarat untuk memperoleh gelar sarjana strata satu pada Jurusan Matematika Fakultas MIPA Universitas Diponegoro.

Penulis menyadari bahwa penyusunan tugas akhir ini dapat berjalan dengan baik karena adanya dukungan dari berbagai pihak. Untuk itu, penulis menyampaikan terima kasih kepada :

1. Bapak Drs. Bayu Surarso, MSc PhD sebagai Ketua Jurusan Matematika Fakultas MIPA Universitas Diponegoro.
2. Bapak Drs. Kushartantya, MIKomp sebagai Pembimbing I yang telah memberikan bimbingan dan pengarahan kepada penulis.
3. Bapak Aris Sugiharto, Ssi sebagai Pembimbing II yang telah membimbing penulis selama penyusunan tugas akhir ini.
4. Bapak Drs. Suhartono, MIKomp sebagai dosen wali yang telah membantu dan membimbing penulis selama belajar di Jurusan Matematika Fakultas MIPA Universitas Diponegoro.
5. Para Dosen Pengajar Jurusan Matematika Fakultas MIPA Universitas Diponegoro, sehingga pengetahuan yang diberikan sangat bermanfaat dalam penyusuna Tugas Akhir ini.

Penulis menyadari bahwa penyusunan tugas akhir ini masih jauh dari sempurna, sehingga kritik dan saran yang membangun dari pembaca sangat penulis harapkan. Semoga tugas akhir ini bermanfaat untuk para pembaca.

Semarang , Agustus 2002

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR LAMPIRAN

DAFTAR SIMBOL

+	:	Operasi penjumlahan
-	:	Operasi pengurangan
.	:	Operasi perkalian
/	:	Operasi pembagian
=	:	Sama dengan
≠	:	Tidak sama dengan
<	:	Kurang dari
≤	:	Kurang dari atau sama dengan
>	:	Lebih dari
≥	:	Lebih dari atau sama dengan
mod	:	Modulo
a≡b	:	a kongruen b
a≡b	:	a tidak kongruen terhadap b
⇒	:	Jika ... maka ...
⇔	:	Jika dan hanya jika
∀	:	Untuk semua
∃	:	Terdapat beberapa
∃!	:	Terdapat dengan tunggal
Z	:	Himpunan bilangan bulat
Z^+	:	Himpunan bilangan bulat positif
Z_n	:	Himpunan bilangan bulat modulo n
Z_n^*	:	Himpunan grup multikatif dari Z_n

W,X,Y	:	Himpunan
$x \in X$	:	x adalah elemen himpunan X
$\lvert X \rvert$	:	Banyaknya elemen dari himpunan X
f,g	:	Fungsi
$f: X \mapsto Y$	:	Fungsi f dari himpunan X ke himpunan Y
f^{-1}	:	Fungsi invers
fog	:	Fungsi komposit
f_k	:	Fungsi dengan *Informasi Trapdoor* k
φ	:	Fungsi Euler
a | b	:	a membagi b
gcd(a,b)	:	Greatest Common Divisor dari a dan b
lcm (a,b)	:	Least Common Multiple dari a dan b
$a \equiv b \bmod n$	:	a kongruen ke b modulo n
A	:	Alphabet
M	:	Ruang Plainteks
P	:	Ruang Plainteks dalam bentuk bilangan
C	:	Ruang Ciperteks
K	:	Ruang Kunci
S	:	Ruang Plainteks yang ditandatangani
e	:	Nilai Eksponen Enkripsi pada Kunci enkripsi
d	:	Nilai Eksponen Dekripsi pada kunci dekripsi
n	:	Nilai Modulus
k	:	Kunci penandatanganan

l	:	Kunci verifikasi
e^*	:	Kunci enkripsi milik penyusup
d^*	:	Kunci dekripsi milk penyusup
m	:	Plainteks
c	:	Ciperteks
c^*	:	Ciperteks yang dimanipulasi penyusup
s	:	Plainteks yang ditandatangani dan elemen dari S
m_i	:	Plainteks dengan indeks-i
p_i	:	Plainteks dalam bentuk bilangan dengan indeks-I
c_i	:	Ciperteks dengan indeks-i
e_i	:	Kunci enkripsi dengan indeks-i
d_i	:	Kunci dekripsi dengan indeks-i
E_e	:	Fungsi Enkripsi dengan kunci e
D_d	:	Fungsi Dekripsi dengan kunci d
E_{e_i}	:	Fungsi Enkripsi dengan kunci e indeks-i
D_{d_i}	:	Fungsi Dekripsi dengan kunci d indeks-i
E_{e^*}	:	Fungsi Enkripsi dengan kunci e^*
D_{d^*}	:	Fungsi Dekripsi dengan kunci d^*
S_k	:	Fungsi Penandatanganan dengan kunci k
V_l	:	Fungsi Verifikasi dengan kunci l
B_i	:	Entiti dalam Komunikasi
$S_k(B_i \| e_i)$	:	Fungsi Penandatanganan sertikat digital dengan kunci k
$V_l(B_i \| e_i)$	:	Fungsi Verifikasi sertifukat digital dengan kunci l