

DAFTAR ISI

	Halaman
PERNYATAAN	i
ABSTRAK	ii
KATA PENGANTAR	iii
UCAPAN TERIMA KASIH	iv
DAFTAR ISI	v
DAFTAR TABEL	ix
DAFTAR GAMBAR	x
DAFTAR LAMPIRAN	xi
ARTI LAMBANG	xii
 BAB 1 PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	2
1.3 Batasan Masalah.....	2
1.4 Tujuan Penulisan	3
1.5 Manfaat Penulisan	3
 BAB 2 LANDASAN TEORI	
2.1 Kriptografi.....	4
2.1.1. Sejarah Kriptografi.....	5
2.1.2. Algoritma Kriptografi	7
2.1.2.1. Algoritma Kriptografi Simetris.....	7
2.1.2.2. Algoritma Kriptografi Asimetris	8
2.1.3. Sistem Kriptografi	9
2.2 Bilangan Bulat.....	10

2.2.1	Divisibility.....	10
2.2.2	Algoritma Pembagian.....	12
2.2.3	Representasi Bilangan Bulat	13
2.2.4	Pembagi Persekutuan Terbesar	15
2.2.5	Algoritma Euclid.....	17
2.2.6	Algoritma Euclid yang Diperluas.....	18
2.2.7	Bilangan Prima.....	19
2.3	Struktur Aljabar.....	20
2.3.1	Pemetaan	21
2.3.2	Grup.....	21
2.3.3	Ring dan Field	22
2.4	Konsep Dasar Matematika dalam Algoritma RSA	23
2.4.1	Persamaan Kongruen.....	24
2.4.2	Residue Class	26
2.4.3	Residue Class Ring.....	27
2.4.4	Multiplikatif Grup Residue	29
2.4.5	Teorema Fermat	31
2.4.6	Metode Fast Exponentiation.....	33
2.4.7	Tes Keprimaan	34
2.4.7.1	Tes Fermat.....	34
2.4.7.2	Bilangan Carmichael.....	35
2.4.7.3	Tes Miller-Rabin	35
2.5	Digital Signature	36
2.5.1	Layanan Keamanan	36

BAB 3 KRIPTOGRAFI RSA

3.1	Sistem ASCII.....	39
3.2	Algoritma Kriptografi RSA.....	40

Chandra Putra Devha, 2013

Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi Rivest Shank Adleman (RSA)

3.2.1	Proses Pembangkitan Kunci.....	42
3.2.2	Proses Enkripsi.....	48
3.2.3	Proses Dekripsi.....	51
3.3	Digital Signature Algoritma Kriptografi RSA	53
3.3.1.	Konsep Digital Signature	53
3.3.2.	Algoritma Digital Signature Kriptografi RSA	54
3.2.3.1	Proses Pembangkitan Kunci.....	55
3.2.3.2	Proses Sign Digital Signature.....	59
3.2.3.3	Proses Verifikasi Digital Signature	61
3.4	Keamanan RSA	65
3.5	Kelebihan dan Kekurangan RSA	66

BAB 4 IMPLEMENTASI DAN UJI COBA

4.1	Sarana Implementasi	74
4.2	Implementasi Algoritma RSA.....	75
4.2.1.	Deklarasi Nama Program, Unit, Variabel dan Tipe Data.....	75
4.2.2.	Fungsi dan Prosedur	76
4.3	Uji Coba Program.....	84
4.3.1.	Bahan Pengujian.....	84
4.3.2.	Pengujian Program	84
4.3.2.1	Pengujian Proses Input Bilangan Prima	84
4.3.2.2	Pengujian Proses Pembangkitan Kunci	85
4.3.2.3	Pengujian Proses Enkripsi dan Dekripsi	88
4.4	Perbandingan Uji Coba	89
4.4.1	Perbandingan Uji Coba Terhadap Waktu Proses Pembangkitan Kunci	90
4.4.2	Perbandingan Uji Coba Terhadap Waktu Proses Enkripsi.....	94

Chandra Putra Devha, 2013

Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi Rivest Shank Adleman (RSA)

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

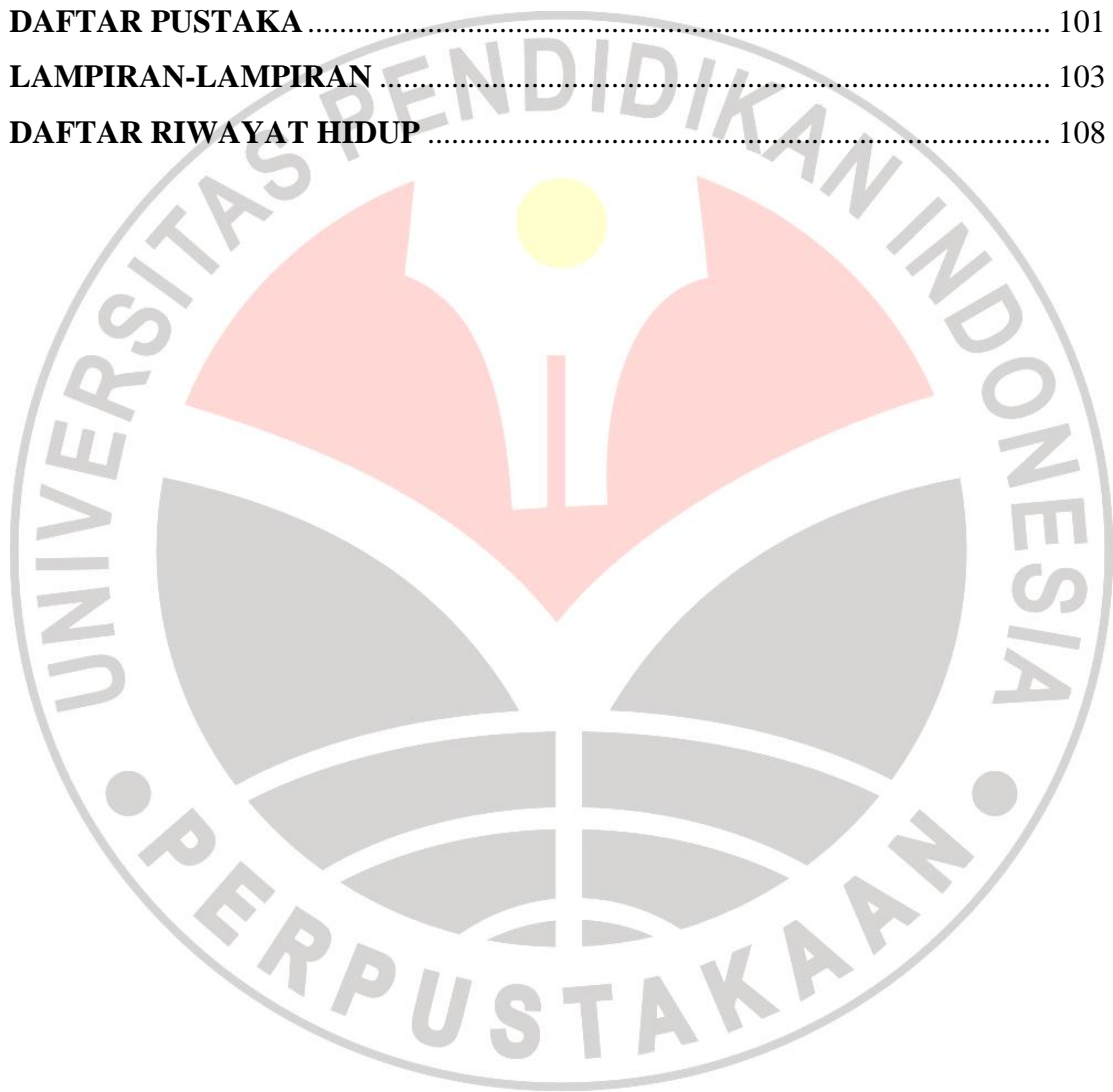
BAB 5 KESIMPULAN DAN SARAN

5.1 Kesimpulan..... 99
5.2 Saran..... 100

DAFTAR PUSTAKA 101

LAMPIRAN-LAMPIRAN 103

DAFTAR RIWAYAT HIDUP 108



Chandra Putra Devha, 2013

Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi Rivest Shank Adleman (RSA)

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

DAFTAR TABEL

	Halaman
Tabel 2.1 Contoh Iterasi Algoritma Euclid yang Diperluas.....	19
Tabel 3.1 Kode ASCII.....	39
Tabel 3.2 Waktu Proses RSA.....	67
Tabel 3.3 Waktu Proses Diffie-Hellman.....	67
Tabel 3.4 Waktu Proses Enkripsi dan Dekripsi RSA.....	69
Tabel 3.5 Waktu Proses Enkripsi dan Dekripsi Elgamal.....	70
Tabel 3.6 Proses Enkripsi Menggunakan Kriptografi Elgamal.....	72
Tabel 3.7 Proses Dekripsi Menggunakan Kriptografi Elgamal.....	73
Tabel 4.1 Spesifikasi Perangkat Keras.....	74
Tabel 4.2 Spesifikasi Perangkat Lunak.....	74
Tabel 4.3 Waktu Proses Pembentukan Kunci dengan Visual Basic 6.0 ^(*)	90
Tabel 4.4 Waktu Proses Pembentukan Kunci dengan IDE Microsoft Visual Studio 2010 Ultimate ^(**)	92
Tabel 4.5 Waktu Proses Enkripsi dengan Visual Basic 6.0 ^(*)	95
Tabel 4.6 Waktu Proses Enkripsi RSA dengan aplikasi IDE Visual Studio 2010 ^(**)	97
Tabel 4.7 Perbandingan Waktu Proses Enkripsi Visual Basic 6.0 ^(*) dengan IDE Microsoft Visual Studio 2010 Ultimate ^(**)	97

Chandra Putra Devha, 2013

Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi Rivest Shank Adleman (RSA)

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

DAFTAR GAMBAR

	Halaman
Gambar 2.1 Skema Algoritma Simetris	8
Gambar 2.2 Skema Algoritma Asimetris	9
Gambar 2.3 Skema Digital Signature.....	38
Gambar 3.1 Flowchart Algoritma Pembangkitan Kunci.....	45
Gambar 3.2 Flowchart Pembangkitan Kunci Lanjutan.....	46
Gambar 3.3 Flowchart Pembangkitan Kunci Lanjutan.....	47
Gambar 3.4 Flowchart Algoritma Enkripsi.....	50
Gambar 3.5 Flowchart Proses Dekripsi	52
Gambar 3.6 Skema Digital Signature Kriptografi RSA.....	54
Gambar 3.7 Flowchart Pembangkitan Kunci Digital Signature Kriptografi RSA....	56
Gambar 3.8 Flowchart Pembangkitan Kunci Digital Signature Kriptografi RSA....	57
Gambar 3.9 Flowchart Pembangkitan Kunci Digital Signature Kriptografi RSA....	58
Gambar 3.10 Flowchart Sign Digital Signature Kriptografi RSA	60
Gambar 3.11 Flowchart Verifikasi Digital Signature Kriptografi RSA	62
Gambar 4.1 Tampilan Proses Input Bilangan Prima.....	85
Gambar 4.2 Tampilan Proses Input Bilangan Prima pada Contoh 3.1.1.1	85
Gambar 4.3 Tampilan Proses Pembangkitan Kunci	86
Gambar 4.4 Tampilan Informasi Nilai e Diterima.....	86
Gambar 4.5 Tampilan Proses Input Nilai d	86
Gambar 4.6 Tampilan Proses Pembangkitan Kunci Pada Contoh 3.1.1.1	87
Gambar 4.7 Tampilan Informasi Nilai e Diterima pada Contoh 3.1.1.1	87
Gambar 4.8 Tampilan Proses Input Nilai d pada Contoh 3.1.1.1	87
Gambar 4.9 Tampilan Proses Enkripsi dan Dekripsi	88
Gambar 4.10 Tampilan Proses Enkripsi pada Contoh 3.1.1.1	89
Gambar 4.11 Tampilan Proses Dekripsi pada Contoh 3.1.1.1	89

Chandra Putra Devha, 2013

Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi Rivest Shank Adleman (RSA)

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

DAFTAR LAMPIRAN

	Halaman
LAMPIRAN-LAMPIRAN.....	105



Chandra Putra Devha, 2013

Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi Rivest Shank Adleman (RSA)

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu