

DAFTAR ISI

	Halaman
Lembar Pengesahan	i
Abstrak	ii
Kata Pengantar	iii
Daftar Isi	v
Daftar Gambar	vii
Daftar Algoritma	viii
Daftar Tabel	ix
Daftar Lampiran	x
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian	3
1.5 Manfaat Penelitian	4
BAB II LANDASAN TEORI	5
2.1 Kriptografi	5
2.1.1 Algoritma Kriptografi	7
2.1.1.1 Algoritma Simetris	7
2.1.1.2 Algoritma Kunci Publik	8
2.1.2 Sistem Kriptografi	9
2.2 Bilangan Bulat	9
2.2.1 Divisibilitas	10
2.2.2 Representasi Bilangan Bulat	11
2.2.3 Pembagi Persekutuan Terbesar	11
2.2.4 Algoritma Euclide	13
2.3 Persamaan Kongruen dan Himpunan Bilangan Bulat Modulo	14
2.3.1 Teorema Fermat	14

	Halaman
2.3.2 Metode Fast Exponentiation	15
2.4 Tes Keprimaan	16
2.4.1 Tes Fermat	17
2.4.2 Bilangan Carmichael	18
2.4.3 Tes Miller-Rabbin	19
2.5 Masalah Logaritma Diskrit	20
2.5.1 Masalah Logaritma Diskrit pada Grup Pergandaan Bilangan Bulat Modulo Prima	20
2.6 Algoritma ElGamal	21
2.6.1 Pembentukan Kunci	22
2.6.2 Enkripsi	25
2.6.3 Dekripsi	26
2.7 Fungsi <i>Hash</i> Satu Arah	27
2.8 Tanda Tangan Digital Menggunakan Algoritma ElGamal	28
2.8.1 Proses Pembentukan Kunci	29
2.8.2 Proses Penandatanganan (<i>Signing</i>)	29
2.8.3 Proses Verifikasi	30
 BAB III METODOLOGI PENELITIAN	 31
3.1 Waktu dan Tempat Penelitian	31
3.2 Jenis Penelitian	31
3.3 Prosedur Penelitian	31
 BAB IV PEMBAHASAN	 38
4.1 Sistem Kriptografi ElGamal	38
4.1.1 Proses Pembentukan Kunci	38
4.1.1.1 Tes Fermat	38
4.1.1.2 Tes Elemen Primitif	39
4.1.1.3 Pembentukan Kunci	40
4.1.2 Proses Enkripsi	40

	Halaman
4.1.3 Proses Dekripsi	43
4.2 Fungsi Hash Satu Arah	45
4.3 Tanda Tangan Digital Menggunakan Algoritma ElGamal	46
4.3.1 Proses Pembentukan Kunci	46
4.3.2 Proses Penandatanganan	46
4.3.3 Proses Verifikasi	47
4.3.4 Contoh Pesan yang Telah Dirubah Isinya	47
4.3.4.1 Proses Verifikasi	48
4.4 Implementasi dan Uji Coba	48
4.4.1 Uji Coba Program	50
4.4.1.1 Bahan Pengujian	50
4.4.1.2 Pengujian Program	50
4.4.1.2.1 Pengujian Proses Pembentukan Kunci	51
4.4.1.2.2 Pengujian Proses Enkripsi	53
4.4.1.2.3 Pengujian Proses Dekripsi	55
BAB V KESIMPULAN DAN SARAN	57
5.1 Kesimpulan	57
5.2 Saran	58
DAFTAR PUSTAKA	59