

DAFTAR ISI

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI.....	v
DAFTAR TABEL.....	vii
DAFTAR GAMBAR	viii
DAFTAR LAMPIRAN.....	ix
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Tujuan Penelitian	4
1.4 Batasan Masalah.....	4
1.5 Sistematika Penulisan	4
BAB II TINJAUAN PUSTAKA.....	7
2.1 <i>DigitalSignature</i>	7
2.1.1 Tujuan <i>Digital Signature</i>	8
2.1.2 Prinsip Kerja <i>Digital Signature</i>	10
2.1.3 Cara Melakukan <i>Digital Signature</i>	12
2.1.4 Skenario <i>Digital Signature</i>	14
2.2 Kriptografi.....	15
2.2.1 Definisi Kriptografi.....	16
2.2.2 Termonologi Kriptografi.....	16
2.2.3 Tujuan Kriptografi	20
2.2.4 Kriptografi Kunci Asimetri	21
2.3 Sistem Kriptografi ElGamal.....	23
2.3.1 Proses Pembangkitan Pasangan Kunci.....	24
2.3.2 Proses Enkripsi.....	26
2.3.3 Proses Dekripsi	27

2.4	Fungsi Hash	27
2.4.1	Macam Fungsi Hash	28
2.4.2	Fungsi Hash Satu Arah	29
2.5	Secure Hash Algorithm (SHA)	30
2.6	Penelitian Relevan.....	31
BAB III METODOLOGI PENELITIAN		33
3.1	Prosedur Penelitian.....	33
3.2	Metode Penelitian.....	35
3.2.1	Metode Pengumpulan Data	35
3.2.2	Metode Pengembangan Perangkat Lunak	35
3.3	Instrumen Penelitian.....	37
3.3.1	Alat Penelitian.....	37
3.3.2	Bahan Penelitian.....	38
3.3.3	Skenario Pengujian.....	38
BAB IV HASIL PENELITIAN DAN PEMBAHASAN		39
4.1	Sistem Kriptografi ElGamal.....	39
4.1.1	Proses Pembuatan Kunci.....	39
4.1.2	Proses Enkripsi.....	41
4.1.3	Proses Dekripsi	45
4.2	Fungsi Hash dan SHA-512	48
4.3	Digital Signature dengan Algoritma ElGamal dan SHA-512.....	55
4.3.1	Pembentukan Kunci	55
4.3.2	Pembuatan Digital Signature	57
4.3.3	Proses Verifikasi	59
4.4	Pengujian.....	61
4.4.1	Desain Eksperimen.....	61
4.4.2	Hasil Eksperimen	63
4.5	Analisis.....	69
BAB V KESIMPULAN DAN SARAN.....		72
5.1	Kesimpulan	72
5.2	Saran.....	73
DAFTAR PUSTAKA		74