

## DAFTAR ISI

	Halaman
HALAMAN JUDUL .....	i
HALAMAN PENGESAHAN .....	ii
ABSTRAK .....	iii
ABSTRACT .....	iv
HALAMAN MOTO .....	v
HALAMAN PERSEMBAHAN .....	vi
KATA PENGANTAR .....	vii
DAFTAR ISI .....	viii
DAFTAR TABEL .....	x
DAFTAR GAMBAR .....	xi
DAFTAR ALGORITMA .....	xii
DAFTAR LAMPIRAN .....	xiii
DAFTAR NOTASI DAN SIMBOL .....	xiv
BAB I    PENDAHULUAN .....	1
1.1. Latar Belakang .....	1
1.2. Perumusan Masalah .....	3
1.3. Batasan Masalah .....	3
1.4. Tujuan .....	4
1.5. Manfaat .....	4
BAB II    LANDASAN TEORI .....	5
2.1. Tinjauan Pustaka .....	5
2.1.1. Grup Siklis .....	5
2.1.2. Lapangan Berhingga .....	6
2.1.3. Lapangan Berhingga Prima ( $F_p$ ) .....	7
2.1.4. Grup <i>Elliptic</i> atas $F_p$ .....	8
2.1.5. <i>Public Key Cryptosystem</i> .....	9
2.2. Kerangka Pemikiran .....	10

BAB III	METODE PENELITIAN .....	12
	3.1. Studi Literatur .....	12
	3.2. Implementasi Program .....	12
BAB IV	PEMBAHASAN .....	14
	4.1. Kriptografi Kurva <i>Elliptic</i> .....	14
	4.1.1. Kurva <i>Elliptic</i> atas $F_p$ .....	16
	4.1.2. Aritmetika Kurva <i>Elliptic</i> atas $F_p$ .....	17
	4.1.3. Parameter Domain Kurva <i>Elliptic</i> .....	20
	4.2. ElGamal ECC atas $F_p$ .....	21
	4.2.1. Algoritma <i>Generalized ElGamal Encryption</i> atas $F_p$ ...	21
	4.2.2. Algoritma ElGamal ECC .....	22
	4.3. Implementasi ElGamal ECC .....	24
	4.3.1. Algoritma Perkalian Skalar Kurva <i>Elliptic</i> .....	25
	4.3.2. Implementasi ElGamal ECC pada <i>Software Matlab</i> ...	28
	4.3.2.1. Program Penentuan Kunci .....	32
	4.3.2.2. Program Enkripsi ElGamal ECC .....	34
	4.3.2.3. Program Dekripsi ElGamal ECC .....	37
	4.3.3. Analisa Waktu dan Hasil Implementasi ElGamal ECC .....	40
	4.3.3.1. Analisa Waktu Aritmetika Kurva <i>Elliptic</i> ...	40
	4.3.3.2. Analisa Waktu Representasi <i>Plaintext</i> .....	41
	4.3.3.3. Analisa Waktu Enkripsi dan Dekripsi ElGamal ECC .....	42
	4.3.3.4. Hasil Implementasi ElGamal ECC .....	43
BAB V	PENUTUP .....	49
	5.1. Kesimpulan .....	49
	5.2. Saran .....	50
	DAFTAR PUSTAKA .....	51
	LAMPIRAN .....	53