

DAFTAR ISI

	Halaman
LEMBAR JUDUL	i
LEMBAR PERNYATAAN	ii
LEMBAR PENGESAHAN NASKAH SKRIPSI	iii
LEMBAR PEDOMAN PENGGUNAAN SKRIPSI	iv
SURAT PERNYATAAN ORISINALITAS	v
KATA PENGANTAR	vi
ABSTRAK	viii
ABSTRACT	ix
DAFTAR ISI	x
DAFTAR GAMBAR	xiii
DAFTAR TABEL	xv
DAFTAR LAMPIRAN	xvi
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Tujuan	4
1.4 Manfaat	4
BAB II TINJAUAN PUSTAKA	5
2.1 Tinjauan Umum Kriptografi	5
2.2 Teori Bilangan	6
2.2.1 Bilangan Bulat dan Sifat-Sifat Pembagian	6
2.2.2 Aritmetika Modulo	7
2.2.3 Bilangan Prima	8
2.3 Operasi XOR	8
2.3.1 Sifat-Sifat Operasi XOR	9
2.4 Kode ASCII	10
2.5 Terminologi Kriptografi	10
2.5.1 Jenis Kriptografi	11

2.6 Kriptografi Kurva Eliptik	13
2.6.1 Jenis Algoritma Kriptografi Eliptik	14
2.6.2 Kurva Eliptik pada F_p	15
2.6.3 Aturan Penjumlahan Dua Titik pada Kurva Elips	15
2.6.4 Parameter Domain Kurva Eliptik	18
2.7 Algoritma Elgamal	18
2.8 Algoritma Kriptografi Kurva Eliptik Elgamal	20
2.9 <i>One Time Pad</i>	21
2.10 Pemrograman Java	22
BAB III METODE PENELITIAN	25
BAB IV PEMBAHASAN	28
4.1 Kriptografi Kurva Eliptik Elgamal Dengan <i>One Time Pad</i>	28
4.1.1 <i>Input</i> Bilangan (a, b) dan Bilangan prima p	29
4.1.2 Representasi Titik	29
4.1.2.1 Mencari Residu Kuadratis Modulo	30
4.1.2.2 Menentukan Pasangan Beraturan	30
4.1.2.3 Penjumlahan dan Penggandaan Titik Kurva Eliptik	31
4.1.3 <i>Input</i> Plainteks dan Kunci Privat d	32
4.1.4 Enkripsi Pesan Teks Menggunakan Kriptografi Kurva Eliptik Elgamal Dengan <i>One Time Pad</i>	32
4.1.4.1 Membangkitkan Sepasang Kunci	33
4.1.4.2 Enkripsi Pesan Teks Dengan Algoritma Kriptografi Kurva Eliptik Elgamal	34
4.1.4.3 Konversi Hasil Enkripsi Kurva Eliptik Elgamal Menjadi Notasi Biner	34
4.1.4.4 Membangkitkan Kunci <i>Pad</i>	35
4.1.4.5 Enkripsi Menggunakan <i>One Time Pad</i>	35
4.1.4.6 Konversi Notasi Biner Menjadi ASCII	36
4.1.5 <i>Input</i> Ciperteks, Kunci <i>One Time Pad</i> , dan Kunci Privat d	36
4.1.6 Dekripsi Ciperteks Menggunakan Kriptografi Kurva Eliptik Elgamal Dengan <i>One Time Pad</i>	37

4.1.6.1	Konversi Ciperteks ke Notasi Biner	37
4.1.6.2	Dekripsi Ciperteks Menggunakan <i>One Time Pad</i>	38
4.1.6.3	Konversi Biner Menjadi Karakter ASCII.....	39
4.1.6.4	Dekripsi Ciperteks Menggunakan Kurva Eliptik Elgamal	39
4.2	Penyelesaian Secara Manual Contoh Kasus Kriptografi Kurva Eliptik Elgamal dengan <i>One Time Pad</i> pada Pesan Teks	40
4.2.1	Mencari Residu Kuadratis Modulo	40
4.2.2	Penentuan Pasangan Berurutan $(x, y) \in F_p$	41
4.2.3	Penjumlahan dan Penggandaan Titik Kurva Eliptik	43
4.2.4	Pembangkitkan Sepasang Kunci.....	45
4.2.5	Proses Enkripsi Kurva Eliptik Elgamal.....	46
4.2.6	Konversi Ciperteks Kurva Eliptik Elgamal ke Bentuk Notasi Biner	48
4.2.7	Bangkitkan Kunci <i>Pad</i>	49
4.2.8	Proses Enkripsi Menggunakan <i>One Time Pad</i>	50
4.2.9	Konversi Bentuk Biner Ciperteks Menjadi ASCII	51
4.2.10	Proses Dekripsi <i>One Time Pad</i>	53
4.2.11	Proses Dekripsi Kurva Eliptik Elgamal	54
4.3	Implementasi Program.....	55
4.3.1	Prosedur Membangkitkan Parameter	55
4.3.2	Prosedur Enkripsi.....	56
4.3.3	Prosedur Dekripsi.....	57
BAB V	PENUTUP	59
5.1	Kesimpulan	59
5.2	Saran	60
DAFTAR	PUSTAKA	61
LAMPIRAN		