

DAFTAR ISI

HALAMAN JUDUL	i
HALAMAN PENGESAHAN	ii
HALAMAN PERNYATAAN	iii
HALAMAN PERSEMBAHAN	iv
PRAKATA	v
DAFTAR ISI	vii
DAFTAR TABEL	ix
DAFTAR LAMBANG	x
INTISARI	xii
ABSTRACT	xiii
I PENDAHULUAN	1
1.1. Latar Belakang Masalah	1
1.2. Rumusan Masalah	2
1.3. Batasan Masalah	2
1.4. Tujuan dan Manfaat Penelitian	2
1.5. Tinjauan Pustaka	3
1.6. Metodologi Penelitian	4
1.7. Sistematika Penulisan	4
II DASAR TEORI	6
2.1. Teori Bilangan	6
2.2. Grup dan Ring	18
2.3. Kriptografi	31
2.3.1. Sistem Kripto Simetris	35
2.3.2. Sistem Kripto Asimetris	37
III MASALAH LOGARITMA DISKRIT DAN PENYELESAIANNYA	39
3.1. Sistem Kripto El-Gamal	39
3.2. Masalah Logaritma Diskrit	46
3.3. Algoritma Pohlig-Hellman	47
3.4. Metode Index Calculus	59
3.5. Penyelesaian Masalah Logaritma Diskrit Pada Z_p^* Memanfaatkan Bilangan <i>Smooth</i> atas ± 1	66
3.5.1. Algoritma I	75
3.5.2. Algoritma II	77



3.6. Penggunaan Algoritma Pohlig-Hellman, Metode <i>Index Calculus</i> , Algoritma I serta Algoritma II pada Nilai p Tertentu	80
IV PENUTUP	93
4.1. Kesimpulan	93
4.2. Saran	93
DAFTAR PUSTAKA	94
A SKRIP PROGRAM PYTHON	95