



## DAFTAR ISI

<b>HALAMAN JUDUL</b> . . . . .	<b>i</b>
<b>HALAMAN PENGESAHAN</b> . . . . .	<b>ii</b>
<b>HALAMAN PERNYATAAN</b> . . . . .	<b>iii</b>
<b>HALAMAN PERSEMBAHAN</b> . . . . .	<b>iv</b>
<b>HALAMAN MOTTO</b> . . . . .	<b>v</b>
<b>PRAKATA</b> . . . . .	<b>vi</b>
<b>DAFTAR ISI</b> . . . . .	<b>viii</b>
<b>DAFTAR LAMBANG</b> . . . . .	<b>x</b>
<b>INTISARI</b> . . . . .	<b>xi</b>
<b>ABSTRACT</b> . . . . .	<b>xii</b>
<b>I PENDAHULUAN</b> . . . . .	<b>1</b>
1.1 Latar Belakang dan Permasalahan . . . . .	1
1.2 Tujuan dan Manfaat Penelitian . . . . .	3
1.3 Tinjauan Pustaka . . . . .	3
1.4 Metode Penelitian . . . . .	4
1.5 Sistematika Penulisan . . . . .	5
<b>II DASAR TEORI</b> . . . . .	<b>7</b>
2.1 Sejarah Kriptografi . . . . .	7
2.2 Aspek-Aspek dalam Kriptografi . . . . .	8
2.3 Fungsi Satu Arah ( <i>One Way Function</i> ) . . . . .	10
2.4 Dasar Struktur Aljabar . . . . .	14
2.5 Ring Polinomial dan Lapangan Hingga . . . . .	18
2.6 Persamaan Kurva Eliptik . . . . .	27
2.7 Himpunan Titik Rasional Kurva Eliptik . . . . .	33
2.8 Geometri Proyektif Kurva Eliptik . . . . .	39
2.9 Operasi pada Himpunan Kurva Eliptik . . . . .	52
2.10 Struktur Grup Kurva Eliptik . . . . .	61
2.11 Fungsi Bilinear . . . . .	65
<b>III Fungsi Rasional, Divisor Utama dan Grup Picard</b> . . . . .	<b>68</b>
3.1 Divisor pada Grup Kurva Eliptik . . . . .	68
3.2 Polinomial pada Kurva Eliptik . . . . .	71
3.3 Fungsi Rasional pada Kurva Eliptik . . . . .	74
3.4 Divisor Utama pada Grup Kurva Eliptik . . . . .	82



3.5	Grup Picard dan Eksistensi Fungsi Rasional dari Suatu Divisor . . .	97
<b>IV</b>	<b>SUBGRUP TORSI DAN WEIL PAIRING . . . . .</b>	<b>111</b>
4.1	Subgrup Torsi dari Grup Kurva Eliptik . . . . .	111
4.2	Akar-Akar ke- $n$ dari Unity . . . . .	133
4.3	Weil Pairing . . . . .	134
<b>V</b>	<b>KRIPTOGRAFI KURVA ELIPTIK DAN KRIPTANALISIS BERBA- SIS PAIRING . . . . .</b>	<b>149</b>
5.1	Kriptografi Kurva Eliptik . . . . .	149
5.2	<i>MOV Attack</i> . . . . .	171
<b>VI</b>	<b>KESIMPULAN . . . . .</b>	<b>181</b>
	<b>DAFTAR PUSTAKA . . . . .</b>	<b>184</b>