

# Daftar Isi

Abstrak	i
Abstract	ii
Lembar Persembahan	iii
Kata Pengantar	v
Daftar Isi	vi
Daftar Gambar	viii
Daftar Tabel	ix
<b>I Pendahuluan</b>	<b>1</b>
1.1 Latar Belakang . . . . .	1
1.2 Pernyataan Masalah . . . . .	2
1.3 Perumusan Masalah . . . . .	2
1.4 Tujuan . . . . .	2
1.5 Batasan Masalah . . . . .	2
1.6 Hipotesis . . . . .	3
1.7 Sistematika Penulisan . . . . .	3
1.8 Rangkuman . . . . .	4
<b>II Kajian Pustaka</b>	<b>5</b>
2.1 Riset Terkait . . . . .	5
2.2 Identity Based Encryption . . . . .	8
2.2.1 <i>Setup</i> . . . . .	9
2.2.2 <i>Extract</i> . . . . .	9
2.2.3 <i>Encrypt</i> . . . . .	10
2.2.4 <i>Decrypt</i> . . . . .	10
2.2.5 <i>Bilinear Map</i> . . . . .	10
2.3 <i>Elliptic Curve Cryptography</i> . . . . .	10
2.3.1 <i>Point Addition</i> . . . . .	11

2.3.2	<i>Point Doubling</i>	11
2.3.3	<i>Point Scalar Multiplication</i>	12
2.3.4	<i>Hasses's Theorem</i>	12
2.4	Rangkuman	13
<b>III Metodologi dan Desain metode</b>		<b>14</b>
3.1	Metodologi Penelitian	14
3.1.1	Metodologi Perancangan Desain IBE-ECC	15
3.1.2	Metodologi Implementasi dan Analisis	17
3.1.3	Data	18
3.1.4	Analisis Kebutuhan Metode	19
3.1.5	Matrik Pengujian	19
3.1.6	Perbandingan	20
3.2	Desain IBE-ECC	20
3.2.1	<i>Setup</i>	22
3.2.2	<i>Encrypt</i>	24
3.2.3	<i>Extract</i>	24
3.2.4	<i>Decrypt</i>	25
3.3	Implementasi pada Bahasa Pemrograman <i>Java</i>	25
3.4	Rangkuman	27
<b>IV Hasil dan Pembahasan</b>		<b>28</b>
4.1	Hasil Pengujian	28
4.1.1	Running Time	28
4.1.2	Memory Usage	35
4.1.3	Brute Force Attack	38
4.2	Pembahasan	41
4.2.1	Rangkuman	42
<b>V Kesimpulan dan Saran</b>		<b>43</b>
5.1	Kesimpulan	43
5.1.1	Saran	43
<b>Daftar Pustaka</b>		<b>44</b>
<b>Lampiran</b>		<b>46</b>