

## DAFTAR ISI

<b>LEMBAR PENGESAHAN</b> . . . . .	<b>ii</b>
<b>LEMBAR PERNYATAAN ORISINALITAS</b> . . . . .	<b>iii</b>
<b>ABSTRAK</b> . . . . .	<b>iv</b>
<b>ABSTRACT</b> . . . . .	<b>v</b>
<b>KATA PENGANTAR</b> . . . . .	<b>vi</b>
<b>UCAPAN TERIMA KASIH</b> . . . . .	<b>vii</b>
<b>DAFTAR ISI</b> . . . . .	<b>ix</b>
<b>DAFTAR GAMBAR</b> . . . . .	<b>xi</b>
<b>DAFTAR TABEL</b> . . . . .	<b>xii</b>
<b>DAFTAR SINGKATAN</b> . . . . .	<b>xiii</b>
<b>I PENDAHULUAN</b> . . . . .	<b>1</b>
1.1 Latar Belakang Masalah . . . . .	1
1.2 Rumusan Masalah . . . . .	2
1.3 Tujuan dan Manfaat . . . . .	3
1.4 Batasan Masalah . . . . .	3
1.5 Metode Penelitian . . . . .	3
<b>II KONSEP DASAR</b> . . . . .	<b>5</b>
2.1 <i>Cryptography</i> . . . . .	5
2.2 Jenis <i>Cryptography</i> Berdasarkan Kunci yang Digunakan . . . . .	6
2.3 <i>Elliptic Curve Cryptography</i> (ECC) . . . . .	6
2.3.1 <i>Finite Field</i> . . . . .	8
2.4 <i>Elliptic Curve Diffie-Helman</i> (ECDH) . . . . .	9
2.5 <i>Hash</i> . . . . .	10
2.6 <i>Message Authentication Code</i> (MAC) . . . . .	10
2.7 <i>Hash Message Authentication Code</i> (HMAC) . . . . .	11

2.8	<i>Zero Knowledge Protocol (ZKP)</i>	11
2.8.1	<i>Fiat-Shamir</i>	13
<b>III</b>	<b>MODEL SISTEM DAN PERANCANGAN</b>	<b>14</b>
3.1	Gambaran Sistem	14
3.2	Perangkat	15
3.2.1	<i>Hardware</i> (Perangkat Keras)	15
3.2.2	<i>Software</i> (Perangkat Lunak)	15
3.3	Perancangan dan Proses Kerja Sistem	16
3.3.1	Perancangan Protokol Autentikasi ECC Berbasis <i>Fiat-Shamir</i>	16
3.3.2	Perancangan Protokol Autentikasi ECDH-HMAC	17
3.4	Skenario Pengujian	18
3.4.1	Tujuan Pengujian	18
3.4.2	Rancangan Pengujian Sistem	19
<b>IV</b>	<b>HASIL DAN ANALISIS</b>	<b>20</b>
4.1	Pengujian Sistem	20
4.2	Waktu Komputasi	20
4.2.1	Simulasi	20
4.2.2	Testbed	21
4.3	Delay	23
4.3.1	Simulasi	23
4.3.2	Testbed	25
4.4	Penggunaan Memori	26
4.4.1	Simulasi	27
4.4.2	Testbed	30
4.5	<i>Communication Cost</i>	30
4.5.1	Simulasi	31
4.5.2	Testbed	31
<b>V</b>	<b>KESIMPULAN DAN SARAN</b>	<b>33</b>
5.1	Kesimpulan	33
5.2	Saran	34
	<b>DAFTAR PUSTAKA</b>	<b>35</b>
	<b>LAMPIRAN</b>	<b>1</b>