

DAFTAR ISI

PRAKATA	iii
ARTI LAMBANG DAN SINGKATAN	vi
ABSTRACT	vii
INTISARI	viii
DAFTAR ISI	ix
DAFTAR GAMBAR	xi
DAFTAR TABEL	xiii
DAFTAR LAMPIRAN	xiv
BAB I PENDAHULUAN	2
1.1 Latar Belakang	2
1.2 Perumusan Masalah	4
1.3 Keaslian Penelitian.....	4
1.4 Tujuan Penelitian	7
1.5 Manfaat Penelitian	7
BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI	8
2.1 Tinjauan Pustaka	8
2.2 Landasan Teori	12
2.2.1 Perangkat <i>Mobile</i>	12
2.2.2 <i>Instant Messenger</i>	13
2.2.3 Jenis layanan dan format data pada <i>Instant Messenger</i>	15
2.2.4 Kriptografi.....	17
2.2.5 Algoritma pada Kriptografi.....	18
2.2.6 Perbandingan Algoritma Simetri dan Asimetri.....	19
2.2.7 Keaslian Data Digital	20
2.2.8 Tanda Tangan Digital (<i>Digital Signature</i>)	21
2.2.9 Skema pada tanda tangan digital.....	23
2.2.10 Algoritma Tanda Tangan Digital	25
2.2.11 Algoritma RSA	27
2.2.12 Algoritms DSA	28
2.2.13 Algoritma Kurva Eliptik	30
2.2.14 Perbandingan Algoritma RSA, DSA dan Kurva Eliptik	32
2.2.15 Tanda Tangan Digital berbasis Algoritma Kurva Eliptik	33
2.2.16 Enkripsi dan Dekripsi berbasis Algoritma Kurva Eliptik	36
2.2.17 <i>Finite Field</i>	37
2.2.18 Jenis-Jenis Serangan terhadap algoritma Kurva Eliptik	37
2.2.19 Pertimbangan dalam penerapan algoritma Kurva Eliptik	39
2.2.20 Parameter Domain pada Kurva Eliptik	40
2.2.21 Fungsi Hash.....	41
2.2.22 Kelebihan Metode Pengamanan Pada Penelitian	43
2.2.23 Keunggulan Algoritma Kurva Eliptik	44

BAB III METODOLOGI	45
3.1 Alat dan Bahan.....	45
3.1.1 Alat.....	45
3.1.2 Bahan	46
3.2 Jalannya Penelitian.....	47
3.3 Perancangan Sistem	49
3.3.1 Rancangan Tampilan Aplikasi Utama	49
3.3.2 Desain <i>interface</i> proses pembangkitan kunci (<i>generating</i>).....	50
3.3.3 Desain <i>user interface</i> proses penandatanganan (<i>signing</i>).....	51
3.3.4 Desain <i>user interface</i> proses verifikasi (<i>verifying</i>)	52
3.4 Perancangan Sistem Keamanan <i>Mobile IM</i>	53
3.4.1 Komunikasi pada Sistem Keamanan <i>Mobile IM</i>	53
3.4.2 Alur Komunikasi <i>Mobile IM</i> berbasis Kurva Eliptik.....	54
3.4.3 Rancangan Interaksi Pengguna <i>Mobile IM</i>	58
3.5 Pengujian.....	59
3.5.1 Aspek Pengujian	59
3.5.2 Spesifikasi <i>Emulator</i> dalam Pengujian	61
3.6 Pembahasan.....	62
3.7 Penarikan Kesimpulan	62
BAB IV HASIL DAN PEMBAHASAN.....	63
4.1 Pengujian Fungsional Aplikasi	63
4.1.1 Pembangkitan Pasangan Kunci (<i>Generating</i>).....	63
4.1.2 Pemberian Tanda Tangan (<i>Signing</i>)	64
4.1.3 Proses Pengiriman Pesan (<i>Sending</i>).....	65
4.1.4 Proses Verifikasi Tanda Tangan (<i>Verifying</i>)	66
4.2 Pengujian Metode Pengamanan pada Aplikasi <i>Mobile IM</i>	67
4.2.1 Pengujian Tanda Tangan Digital berbasis (DSA) Standar	67
4.2.2 Pengujian Tanda Tangan Digital berbasis Algoritma Kurva Eliptik	68
4.2.3. Pengujian Tingkat Efisiensi	77
4.3. Pembahasan Hasil	82
4.3.1. Metode Pengamanan berbasis Autentikasi DSA.....	82
4.3.2. Metode Pengamanan berbasis Kurva Eliptik.....	83
4.6 Kontribusi Penelitian pada Masalah <i>Mobile IM</i>	84
4.6. Keterbasan.....	85
BAB V KESIMPULAN DAN SARAN	86
5.1. Kesimpulan	86
5.2. Saran	86
DAFTAR PUSTAKA.....	87
LAMPIRAN.....	89