

DAFTAR ISI

Halaman Judul	
Lembar Pengesahan	
Abstrak	iii
Kata Pengantar	v
Daftar Isi	vii
Daftar Gambar	x
Daftar Lampiran	xi
Daftar Singkatan	xii
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	1
1.3 Batasan Masalah	2
1.4 Tujuan Tugas Akhir	2
1.5 Metode Penelitian	3
1.6 Sistematika Penulisan	3
BAB II DASAR TEORI	5
2.1 Teknologi Java	5
2.1.1 J2ME	5
2.1.2 Konfigurasi J2ME	6
2.1.3 Profil J2ME	7
2.2 MIDlet	7
2.3 Kriptografi	7
2.3.1 Algoritma Sandi	8
2.3.1.1 Algoritma Sandi Kunci Simetris	9
2.3.1.1 Algoritma Sandi Kunci Asimetris	9
2.3.2 Fungsi Hash Kriptografis	10
2.4 Elliptic Curve Cryptography	11
2.4.1 Diffie-Hellman Problem (DHP)	11

2.4.2 Deskripsi Protokol	11
2.4.3 ECIES (<i>Elliptic Curve Integrated Encryption Scheme</i>)	12
2.4.3.1 Parameter-parameter Domain	12
2.4.3.2 Pembangkitan Pasangan Kunci (<i>Key-pair</i>)	13
2.4.3.3 ECIES Encryption	13
2.4.3.4 ECIES Decryption	14
2.5 Short Message Service (SMS)	14
2.5.1 Arsitektur GSM	14
2.5.1.1 Mobile Station (MS)	15
2.5.1.2 Base Transceiver Station (BTS)	15
2.5.1.3 Base Station Controller (BSC)	15
2.5.1.4 Mobile Switching Centre (MSC) dan Visitor Location Register (VLR)	16
2.5.1.5 Home Location Register (HLR)	16
2.5.2 Arsitektur SMS	16
2.5.2.1 Short Message Entity (SME)	17
2.5.2.2 SMS Service Centre (SMSC).....	17
2.5.2.3 Email Gateway	18
2.5.3 Aspek yang dipertimbangkan pada Keamanan SMS	18
2.6 <i>Brute Force Attack</i>	19
BAB III ANALISA DAN PERANCANGAN SISTEM	20
3.1 Teknologi Kriptografi SMS	20
3.2 Analisa Kebutuhan Sistem	21
3.2.1 Spesifikasi Perangkat Keras	21
3.2.2 Spesifikasi Perangkat Lunak	22
3.3 Batasan Perancangan	22
3.4 Input dan Output Sistem	22
3.5 Peancangan Sistem	23
3.5.1 Flowchart Sistem	25
3.5.2 Proses Pengiriman SMS	26
3.5.3 Proses Penerimaan SMS	28

BAB IV IMPLEMENTASI DAN ANALISA HASIL SISTEM	29
4.1 Perangkat Lunak Pendukung Dalam Pengembangan Sistem	29
4.2 Lingkungan Implementasi	29
4.2.1 Sistem Operasi.....	29
4.2.2 Bahasa Pemrograman	30
4.2.3 Lingkungan Perangkat Keras	30
4.2.4 Perangkat Lunak Utama Aplikasi Kriptografi SMS	30
4.3 Implementasi dan Pengujian Sistem	30
4.3.1 Pengujian Fungsionalitas Sistem Pada Emulator	30
4.3.2 Pengujian Fungsionalitas Sistem Telepon Seluler	35
4.4 Analisa Panjang Data Output	36
4.5 Analisa Penggunaan Memori Sistem	37
4.6 Analisa Waktu Proses	38
4.6.1 Aplikasi Pada PC	39
4.6.2 Aplikasi Pada Ponsel.....	39
4.6.3 Hasil Evaluasi.....	41
 BAB V KESIMPULAN DAN SARAN.....	 42
5.1 Kesimpulan	47
5.2 Saran	48
 Daftar Pustaka	 xiv