DAFTAR ISI

LEMBAR PENGESAHAN

LEMBAR PERNYATAAN

ABSTRAK i

ABSTRACT ii

KATA PENGANTAR iii

DAFTAR ISI v

DAFTAR GAMBAR ix

DAFTAR TABEL xi

DAFTAR ISTILAH xii

BAB I PENDAHULUAN 1

1.1. Latar Belakang Masalah 1

1.2. Identifikasi Masalah 4

1.3. Maksud dan Tujuan 4

1.4. Batasan Masalah 5

1.5. Metodologi Penelitian 6

1.6. Sistematika Penulisan 7

BAB II LANDASAN TEORI 9

2.1. Penyandian data (Kriptografi) 9

2.1.1. *Chipper* 11

2.1.1.1 Kriptografi Simetri 11

2.1.1.2 Kriptografi Asimetri 12

2.1.2. *Message diggest/Digital fingerprint* 13

2.1.3 *Digital Signature* 13

2.2 Algoritma RSA 14

2.2.1 Fungsi Totient Euler 16

2.2.2 Algoritma Pembangkitan Kunci 16

2.2.3 Proses Enkripsi pesan 18

2.2.4 Proses Dekripsi pesan 19

2.3 Fungsi hash satu arah (SHA) 20

2.3.1 Secure Hash Function 21

2.3.2 SHA-1 22

2.4 Tanda Tangan Digital (*Digital Signature*) 26

2.4.1 Proses pembentukan tanda tangan digital (*signing*) 28

2.4.2 Proses verifikasi tandatangan digital (*Verifying*) 29

2.5 Serangan Terhadap Kriptografi 29

2.6 MMS (Multimedia Messaging Service) 30

2.7 Pemrograman berorientasi objek 32

2.7.1 Kelas dan Objek 32

2.7.2 Pewarisan (*inheritance*) 32

2.7.3 Polimorfisme (*Polymorfism*) 33

2.7.4 Pengkapsulan (*Encapsulation*) 33

2.8 J2ME 33

2.8.1 J2ME Configuration 34

2.8.2 J2ME Profile 35

2.8.3 Midlet 36
2.8 Unified Modelling language (UML) 38
2.9.1 Tujuan UML 38
2.9.2 Diagram dan Teknik pemodelan UML 39
2.9.2.1 Diagram Struktur 40
2.9.2.2 Diagram perilaku 41
2.9.4 Notasi dalam UML 42
BAB III ANALISIS DAN PERANCANGAN SISTEM 47
3.1. Gambaran Umum 47
3.2 Analisis Kebutuhan 47
3.2.1 Masukan 48
3.2.2 Keluaran 49
3.3 Perancangan Sistem 49
3.3.1 Use Case Diagram 50
3.3.1.1 Skenario Uses Case 50
3.3.1.2 Class Diagram 54
3.3.2 Sequence Diagram 56
3.3.2.1 Sequence Diagram Untuk *Use case login* 56
3.3.2.2 *Sequence* Diagram untuk *Use case* Mengetik MMS. 56
3.3.2.3 *Sequence* Diagram untuk *use case* Mengirim MMS. 57
3.3.2.4 *Sequence* Diagram untuk *use case* Menerima MMS 57
3.3.2.5 *Sequence* Diagram untuk *use case* Membaca MMS. 58
3.3.2.6 *Sequence* Diagram *use case* Menggenerate kunci 58

3.3.3 *Activity Diagram* 58

3.3.3.1 Activity Diagram untuk use case mengetikkan dan mengirimkan MMS 59

3.3.3.2 Actifity Diagram untuk use case Menerima MMS ... 60

3.3.3.3 Actifity Diagram untuk use case Membaca MMS 61

BAB IV IMPLEMENTASI DAN PENGUJIAN 62

4.1. Spesifikasi perangkat keras pendukung 62

4.2 Spesifikasi perangkat lunak pendukung 63

4.3 Batasan Fungsionalitas Sistem 63

4.4 Implementasi Sistem 63

4.5 Pengujian Sistem 69

4.5.1 Pengujian Fungsionalitas Sistem 70

4.5.2 Pengujian Performasi Sistem 72

4.5.2.1 Analisis proses signing dan verifying 74

4.5.2.2 Pengujian pengaruh banyaknya teks terhadap waktu proses signing dan verifying 77

BAB V KESIMPULAN DAN SARAN 78

5.1 Kesimpulan 78

5.2 Saran 79

DAFTAR PUSTAKA 80

LAMPIRAN A 82

LAMPIRAN B 83