

Daftar Isi

| | |
|--|-----|
| ABSTRAK | i |
| ABSTRACT | ii |
| LEMBAR PERSEMBAHAN | iii |
| KATA PENGANTAR | v |
| DAFTAR ISI | vi |
| DAFTAR GAMBAR | ix |
| DAFTAR TABEL | xi |
| DAFTAR ISTILAH | xii |
| BAB I PENDAHULUAN | |
| 1.1 Latar Belakang | 1 |
| 1.2 Perumusan Masalah..... | 2 |
| 1.3 Batasan Masalah..... | 2 |
| 1.4 Tujuan..... | 2 |
| 1.5 Hipotesa Awal | 2 |
| 1.6 Metodologi Penyelesaian | |
| 1.6.1 Metodologi Penyelesaian Tugas Akhir | 3 |
| 1.6.2 Metodologi Penyelesaian Masalah | 4 |
| 1.7 Sistematika Penulisan | 4 |
| BAB II LANDASAN TEORI | |
| 2.1 SMS (<i>Short Message Service</i>) | |
| 2.1.1. Jaringan SMS | 6 |
| 2.1.2 Struktur Pesan SMS | 7 |
| 2.1.3 Format PDU (<i>Protokol Data Unit</i>) SMS..... | 8 |
| 2.2 Kriptografi | |
| 2.2.1 Istilah dalam Kriptografi | 9 |
| 2.2.2 Tujuan Kriptografi | 9 |
| 2.2.3 Kriptografi Kunci Simetri dan Kriptografi Kunci Asimetri | 10 |
| 2.2.4 Serangan Terhadap Kriptografi | 10 |
| 2.3 Algoritma RC6 | |
| 2.3.1 Operasi dasar | 12 |
| 2.3.2 Pembentukan Kunci Internal | 12 |
| 2.3.3 Algoritma Enkripsi | 13 |
| 2.3.4 Algoritma Dekripsi | 15 |
| 2.4 Algoritma RSA | |
| 2.4.1 Algoritma Pembangkitan Pasangan Kunci | 16 |
| 2.4.2 Algoritma Enkripsi dan Dekripsi | 17 |

BAB III PERANCANGAN SISTEM

| | |
|---|----|
| 3.1 Analisis Sistem | |
| 3.1.1 Deskripsi Sistem..... | 19 |
| 3.1.2 Analisis Kebutuhan Sistem | 19 |
| 3.1.3 Spesifikasi Perangkat Keras | 19 |
| 3.1.4 Spesifikasi Perangkat Lunak | 20 |
| 3.1.5 Parameter Masukan dan Keluaran..... | 20 |
| 3.2 Perancangan Sistem | |
| 3.2.1 Diagram Blok Sistem..... | 21 |
| 3.2.2 <i>Use Case</i> Diagram | 21 |
| 3.2.3 <i>Class</i> Diagram | 26 |
| 3.2.4 <i>Sequence</i> Diagram | |
| 3.2.4.1 <i>Sequence</i> Diagram Memasukkan <i>Password</i> | 27 |
| 3.2.4.2 <i>Sequence</i> Diagram Mengganti <i>Password</i> | 27 |
| 3.2.4.3 <i>Sequence</i> Diagram Membangkitkan Kunci RC6 | 28 |
| 3.2.4.4 <i>Sequence</i> Diagram Mengenkripsi Kunci RC6..... | 28 |
| 3.2.4.5 <i>Sequence</i> Diagram Mengenkripsi Pesan | 29 |
| 3.2.4.6 <i>Sequence</i> Diagram Mengirim Kunci dan Pesan terenkripsi/ Mengirim SMS | 29 |
| 3.2.4.7 <i>Sequence</i> Diagram Menyimpan SMS | 30 |
| 3.2.4.8 <i>Sequence</i> Diagram Mendekripsi Kunci RC6..... | 30 |
| 3.2.4.9 <i>Sequence</i> Diagram Mendekripsi Pesan | 31 |
| 3.2.5 <i>Deployment</i> Diagram | 31 |

BAB IV IMPLEMENTASI

| | |
|---|----|
| 4.1 Lingkungan Implementasi | |
| 4.1.1 Lingkungan Perangkat Keras (<i>hardware</i>) | |
| 4.1.1.1 Spesifikasi Nokia 6630..... | 33 |
| 4.1.1.2 Spesifikasi Nokia N70 | 33 |
| 4.1.2 Lingkungan Perangkat Lunak (<i>software</i>)..... | 33 |
| 4.2 Batasan Sistem | 33 |
| 4.3 Implementasi <i>Interface</i> | |
| 4.3.1 <i>Interface Login</i> | 34 |
| 4.3.2 <i>Interface</i> Menu Utama | 34 |
| 4.3.3. <i>Interface Change Password</i> | 34 |
| 4.3.4 <i>Interface Create SMS</i> | 35 |
| 4.3.5 <i>Interface Inbox</i> | 38 |
| 4.3.6 <i>Interface Outbox</i> | 41 |

BAB V PENGUJIAN DAN ANALISIS

| | |
|--|----|
| 5.1 Pengujian Sistem | |
| 5.1.1 Tujuan Pengujian..... | 43 |
| 5.1.2 Skenario Pengujian | 43 |
| 5.2 Gambar Grafik dan Analisis Hasil Pengujian | |
| 5.2.1 Analisis Skenario Pengujian Fungsionalitas Sistem..... | 51 |
| 5.2.2 Perbandingan Waktu Enkripsi dan Dekripsi Pesan | 53 |

| | |
|---|----|
| 5.2.2.1 Perbandingan Waktu Enkripsi dan Dekripsi Pesan dengan Panjang Kunci yang Sama | 53 |
| 5.2.2.2 Perbandingan Waktu Enkripsi dan Dekripsi Pesan dengan Jumlah Round yang Sama | 58 |
| 5.2.3 Perbandingan Waktu Enkripsi dan Dekripsi Pesan dengan Menggunakan Kunci RC6 dan Kunci RSA | 65 |
| 5.3 Analisis <i>Exhaustive Key Search Attack/Brute Force Attack</i> | 67 |
| 5.4 Analisis Serangan Kriptanalisis Diferensial | 69 |
| 5.5 Analisis Data <i>Dependent Rotation</i> | 69 |

BAB VI KESIMPULAN DAN SARAN

| | |
|----------------------|----|
| 6.1 Kesimpulan | 70 |
| 6.2 Saran | 70 |

| | |
|-----------------------------|----|
| DAFTAR PUSTAKA | 71 |
| LAMPIRAN A | 72 |
| LAMPIRAN B | 78 |
| LAMPIRAN C | 80 |