

DAFTAR ISI

| | |
|-----------------------------------|-------------|
| Halaman Judul | ii |
| Halaman Pernyataan | iv |
| Halaman Persembahan | v |
| DAFTAR ISI | viii |
| DAFTAR TABEL | x |
| DAFTAR GAMBAR | xi |
| INTISARI | xiii |
| ABSTRACT | xiv |
| I PENDAHULUAN | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 2 |
| 1.3 Batasan Masalah | 2 |
| 1.4 Tujuan Penelitian | 3 |
| 1.5 Manfaat Penelitian | 3 |
| 1.6 Metodologi Penelitian | 3 |
| 1.7 Sistematika Penulisan | 4 |
| II TINJAUAN PUSTAKA | 6 |
| III DASAR TEORI | 8 |
| 3.1 Kriptografi | 8 |
| 3.1.1 Kriptografi Simetris | 8 |
| 3.1.2 Kriptografi Asimetris | 9 |
| 3.2 Enkripsi Homomorfis | 9 |
| 3.3 Kriptosistem RSA | 10 |
| 3.3.1 Algoritme RSA | 10 |
| 3.3.2 Algoritme RSA Termodifikasi | 11 |

| | | |
|-----------------------|---|-----------|
| 3.3.3 | Sifat Homomorfis Algoritme RSA | 13 |
| 3.4 | e-voting | 13 |
| 3.4.1 | Persyaratan <i>e-voting</i> | 14 |
| IV | ANALISIS DAN PERANCANGAN SISTEM | 16 |
| 4.1 | Gambaran Umum Penelitian | 16 |
| 4.2 | Analisis Kebutuhan Sistem | 16 |
| 4.2.1 | Skenario <i>E-voting</i> | 16 |
| 4.2.2 | Arsitektur Sistem | 18 |
| 4.2.3 | Use Case | 19 |
| 4.3 | Perancangan Algoritme Enkripsi | 21 |
| 4.3.1 | Implementasi MRSA pada Sistem <i>E-voting</i> | 21 |
| 4.3.2 | Perancangan Algoritme MRSA | 23 |
| 4.4 | Cara Kerja Sistem E-Voting | 25 |
| V | IMPLEMENTASI SISTEM | 30 |
| 5.1 | Spesifikasi | 30 |
| 5.1.1 | Spesifikasi Perangkat Lunak | 30 |
| 5.1.2 | Spesifikasi Perangkat Keras | 31 |
| 5.2 | Implementasi Algoritma | 31 |
| 5.2.1 | Implementasi Enkripsi MRSA | 32 |
| 5.2.2 | Implementasi Pembuatan dan Pengubahan Kandidat <i>e-voting</i> | 34 |
| 5.2.3 | Implementasi <i>Login</i> dan Pengubahan Password di Sistem <i>e-voting</i> | 36 |
| 5.2.4 | Implementasi Proses Pemilihan | 37 |
| 5.3 | Tampilan <i>User Interface</i> sistem | 41 |
| VI | PENGUJIAN DAN PEMBAHASAN SISTEM | 44 |
| 6.1 | Skenario Pengujian | 44 |
| 6.2 | Pengujian Kebenaran Hasil <i>e-voting</i> | 44 |
| 6.3 | Analisis Syarat <i>e-voting</i> | 46 |
| VIIPENUTUP | | 51 |
| 7.1 | Kesimpulan | 51 |
| 7.2 | Saran | 51 |
| DAFTAR PUSTAKA | | 52 |

DAFTAR TABEL

| | | |
|-----|---|----|
| 2.1 | Perbandingan algoritma dan properti homomorfik yang digunakan | 7 |
| 6.1 | Efisiensi waktu berdasarkan jumlah user dan panjang bit nilai prima pada proses memulai <i>voting</i> | 49 |
| 6.2 | Efisiensi waktu berdasarkan jumlah user dan panjang bit nilai prima pada proses pemilihan | 49 |
| 6.3 | Efisiensi waktu berdasarkan jumlah user dan panjang bit nilai prima pada proses perhitungan hasil akhir | 50 |