

DAFTAR ISI

| | |
|--|-------------|
| HALAMAN JUDUL | i |
| HALAMAN PENGESAHAN PEMBIMBING | ii |
| HALAMAN PENGESAHAN PENGUJI | iii |
| SURAT PERNYATAAN KARYA ASLI TUGAS AKHIR | iv |
| PERNYATAAN BEBAS PLAGIAT | v |
| HALAMAN PERSEMBAHAN | vi |
| ABSTRAK | vii |
| ABSTRACT | viii |
| KATA PENGANTAR | ix |
| DAFTAR ISI | x |
| DAFTAR TABEL | xiii |
| DAFTAR GAMBAR | xiv |
| DAFTAR PERSAMAAN | xvi |
| DAFTAR MODUL | xvii |
| BAB I PENDAHULUAN | 1 |
| 1.1. Latar Belakang | 1 |
| 1.2. Rumusan Masalah..... | 2 |
| 1.3. Batasan Masalah | 2 |
| 1.4. Tujuan Penelitian | 2 |
| 1.5. Manfaat Penelitian | 2 |
| 1.6. Metode Penelitian dan Pengembangan Sistem | 2 |
| 1.7. Sistematika Penulisan | 3 |
| BAB II TINJAUAN PUSTAKA | 4 |
| 2.1. Kriptografi | 4 |
| 2.1.1. Kriptografi Asimetris..... | 4 |
| 2.2. Model Keamanan CIAAN | 5 |
| 2.2.1. <i>Confidentiality</i> | 5 |
| 2.2.2. <i>Integrity</i> | 5 |
| 2.2.3. <i>Availability</i> | 5 |
| 2.2.4. <i>Authenticity</i> | 5 |
| 2.2.5. <i>Non-repudiation</i> | 5 |
| 2.3. Rivest Shamir Adleman (RSA) | 6 |
| 2.3.1. Pembangkitan Kunci..... | 6 |

| | | |
|---|--|-----------|
| 2.3.2. | Enkripsi dan Dekripsi | 7 |
| 2.4. | Secure Hash Algorithm 256 (SHA256)..... | 7 |
| 2.5. | Tanda Tangan Digital | 10 |
| 2.6. | Sertifikat Digital | 11 |
| 2.6.1. | Public Key Cryptography Standards (PKCS#10)..... | 12 |
| 2.7. | Dokumen Elektronik..... | 13 |
| 2.8. | Portable Document Format (PDF)..... | 13 |
| 2.9. | Studi Pustaka (State of The Art)..... | 14 |
| BAB III METODOLOGI DAN PENGEMBANGAN SISTEM | | 17 |
| 3.1. | Metodologi Penelitian..... | 17 |
| 3.2. | Identifikasi Masalah | 18 |
| 3.3. | Studi Literatur | 18 |
| 3.4. | Analisis Kebutuhan Sistem..... | 18 |
| 3.4.1. | Kebutuhan Fungsional | 18 |
| 3.4.2. | Kebutuhan Non-Fungsional..... | 18 |
| 3.5. | Metodologi Pengembangan Sistem | 19 |
| 3.6. | Perancangan Sistem | 19 |
| 3.6.1. | Perancangan Arsitektur..... | 19 |
| 3.6.2. | Perancangan Proses | 20 |
| 3.6.2.1. | Flowchart Pembuatan Sertifikat PKCS#10 | 21 |
| 3.6.2.2. | Flowchart Pembangkitan Pasangan Kunci RSA | 24 |
| 3.6.2.3. | Flowchart Hashing Template PKCS#10..... | 25 |
| 3.6.2.4. | Flowchart Enkripsi PKCS#10 | 28 |
| 3.6.2.5. | Flowchart Tanda Tangan PDF..... | 30 |
| 3.6.3. | Perancangan Antarmuka..... | 32 |
| 3.6.4. | Rancangan Pengujian | 33 |
| BAB IV HASIL DAN PEMBAHASAN | | 35 |
| 4.1. | Rancangan Pengujian | 35 |
| 4.1.1. | Halaman Request Sertifikat | 35 |
| 4.1.2. | Halaman Tanda Tangan PDF | 39 |
| 4.1.3. | Halaman <i>Verify</i> PDF..... | 45 |
| 4.2. | Pengujian | 47 |
| 4.2.1. | Pengujian Verifikasi Data Integrity | 48 |
| 4.2.2. | Pengujian Verifikasi Tanda Tangan Digital | 51 |

| | | |
|-----------------------|--|-----------|
| 4.2.3. | Pengujian Verifikasi Sertifikat Digital | 54 |
| 4.2.4. | Pengujian <i>Man-In-The-Middle</i> (MITM)..... | 58 |
| 4.2.5. | Hasil Pengujian..... | 62 |
| 4.3. | Pembahasan | 63 |
| BAB V | | 64 |
| 5.1. | Kesimpulan | 64 |
| 5.2. | Saran | 64 |
| DAFTAR PUSTAKA | | 65 |
| LAMPIRAN | | 69 |

DAFTAR TABEL

| | |
|--|----|
| Tabel 2.1 Penelitian Sebelumnya | 15 |
| Tabel 2.2 Lanjutan Penelitian Sebelumnya | 16 |
| Tabel 3.1 Skenario Pengujian Analisis Verifikasi <i>Data Integrity</i> | 33 |
| Tabel 3.2 Skenario Pengujian Analisis Verifikasi Tanda Tangan Digital | 33 |
| Tabel 3.3 Skenario Pengujian Analisis Verifikasi Sertifikat Digital | 34 |
| Tabel 3.4 Skenario Pengujian Analisis Serangan MITM | 34 |
| Tabel 4.1 Tabel Uji Analisis Verifikasi <i>Data Integrity</i> | 46 |
| Tabel 4.2 Contoh Sertifikat Digital Untuk Pengujian | 51 |
| Tabel 4.3 Lanjutan Contoh Sertifikat Digital Untuk Pengujian | 52 |
| Tabel 4.4 Tabel Uji Analisis Verifikasi Tanda Tangan Digital | 52 |
| Tabel 4.5 Contoh Sertifikat Digital Untuk Pengujian | 54 |
| Tabel 4.6 Lanjutan Contoh Sertifikat Digital Untuk Pengujian | 55 |
| Tabel 4.7 Tabel Uji Analisis Verifikasi Sertifikat Digital | 55 |
| Tabel 4.8 Contoh Sertifikat Digital Asli | 58 |
| Tabel 4.9 Contoh Sertifikat Digital Palsu | 58 |
| Tabel 4.10 Contoh Pasangan Kunci Asli | 59 |
| Tabel 4.11 Contoh Pasangan Kunci Palsu | 59 |
| Tabel 4.12 Tabel Uji Serangan MITM | 60 |
| Tabel 4.13 Hasil Seluruh Pengujian | 62 |

DAFTAR GAMBAR

| | |
|---|----|
| Gambar 2.1 Proses Enkripsi/Dekripsi | 4 |
| Gambar 2.2 Proses Sederhana Kriptografi Asimetrik | 5 |
| Gambar 2.3 <i>Initial Hash Value</i> | 9 |
| Gambar 2.4 Konstanta Putaran SHA256 | 9 |
| Gambar 2.5 Proses Tanda Tangan Digital | 11 |
| Gambar 2.6 <i>Field</i> pada Dokumen PDF | 14 |
| Gambar 3.1 Tahapan Penelitian | 17 |
| Gambar 3.2 Metodologi Pengembangan Sistem <i>Waterfall</i> | 19 |
| Gambar 3.3 Perancangan Arsitektur Aplikasi | 20 |
| Gambar 3.4 Struktur Menu Utama Aplikasi | 21 |
| Gambar 3.5 Flowchart Pembuatan Sertifikat PKCS#10 | 22 |
| Gambar 3.6 Flowchart Pembangkitan Pasangan Kunci RSA | 24 |
| Gambar 3.7 Flowchart <i>Hashing Template</i> PKCS#10 | 26 |
| Gambar 3.8 Variabel Kerja SHA256 | 27 |
| Gambar 3.9 Konstanta Putaran SHA256 | 28 |
| Gambar 3.10 Flowchart Enkripsi PKCS#10 | 29 |
| Gambar 3.11 Flowchart Proses Tanda Tangan PDF | 30 |
| Gambar 3.12 <i>Field Structure</i> pada Dokumen PDF | 31 |
| Gambar 3.13 <i>Wireframe</i> Halaman <i>Request</i> Sertifikat | 32 |
| Gambar 3.14 <i>Wireframe</i> Halaman Tanda Tangan Dokumen PDF | 32 |
| Gambar 4.1 Halaman <i>Request</i> Sertifikat | 35 |
| Gambar 4.2 Tampilan Hasil <i>Request</i> Sertifikat | 39 |
| Gambar 4.3 Tampilan Halaman Tanda Tangan Dokumen PDF | 39 |
| Gambar 4.4 Tampilan Hasil Tanda Tangan Dokumen PDF | 42 |
| Gambar 4.5 Tampilan Sertifikat X.509 di Dokumen PDF | 43 |
| Gambar 4.6 <i>Offset</i> Tanda Tangan Digital pada Dokumen PDF | 44 |
| Gambar 4.7 Komparasi <i>Hexadecimal Bytes</i> Dokumen PDF | 45 |
| Gambar 4.8 Tampilan Halaman <i>Verify</i> PDF | 45 |
| Gambar 4.9 Hasil Ekstraksi Tanda Tangan dan Sertifikat Digital | 47 |
| Gambar 4.10 Dokumen <i>Dummy</i> Asli | 47 |
| Gambar 4.11 Perubahan Visual pada Pengujian <i>Data Integrity</i> | 49 |
| Gambar 4.12 Perubahan <i>Bytes</i> pada Pengujian <i>Data Integrity</i> | 49 |
| Gambar 4.13 Dokumen PDF Adobe Tanpa Perubahan Isi | 50 |

| | |
|--|----|
| Gambar 4.14 Dokumen PDF Adobe Dengan Perubahan Isi | 50 |
| Gambar 4.15 Dokumen PDF TTE Kominfo Tanpa Perubahan Isi | 51 |
| Gambar 4.16 Dokumen PDF TTE Kominfo Dengan Perubahan Isi | 51 |
| Gambar 4.17 Komparasi Perubahan Tanda Tangan Digital | 53 |
| Gambar 4.18 Dokumen PDF Adobe Dengan Penggantian Kunci Privat | 53 |
| Gambar 4.19 Dokumen PDF TTE Kominfo Dengan Penggantian Kunci Privat | 54 |
| Gambar 4.20 Dokumen PDF Adobe Dengan Sertifikat Kedaluwarsa | 56 |
| Gambar 4.21 Adobe Sertifikat Kedaluwarsa dan Pemunduran Waktu Device | 57 |
| Gambar 4.22 Dokumen PDF TTE Kominfo Dengan Sertifikat Kedaluwarsa | 57 |
| Gambar 4.23 TTE Kominfo Sertifikat Kedaluwarsa dan Pemunduran Waktu Device | 58 |
| Gambar 4.24 Pengubahan Data <i>Certificateless Digital Signature</i> | 61 |
| Gambar 4.25 Hasil Verifikasi <i>Certificateless Digital Signature</i> | 61 |
| Gambar 4.26 Pengubahan Data <i>Certified Digital Signature</i> | 61 |
| Gambar 4.27 Hasil Verifikasi <i>Certified Digital Signature</i> | 62 |

DAFTAR PERSAMAAN

| | |
|--|---|
| Persamaan 2.1 Perhitungan Nilai Modulus RSA | 6 |
| Persamaan 2.2 Perhitungan Nilai Modulus <i>Totient</i> RSA | 6 |
| Persamaan 2.3 Perhitungan Kunci Enkripsi RSA | 6 |
| Persamaan 2.4 Perhitungan Kunci Dekripsi RSA | 6 |
| Persamaan 2.5 Perhitungan Kunci Dekripsi RSA | 6 |
| Persamaan 2.6 Enkripsi RSA | 7 |
| Persamaan 2.7 Dekripsi RSA | 7 |
| Persamaan 2.8 Ekspansi Pesan SHA256 | 8 |
| Persamaan 2.9 <i>Processing Message</i> T1 SHA256 | 9 |
| Persamaan 2.10 <i>Processing Message</i> T2 SHA256 | 9 |
| Persamaan 2.11 <i>Processing Message</i> h7 SHA256 | 9 |
| Persamaan 2.12 <i>Processing Message</i> h6 SHA256 | 9 |
| Persamaan 2.13 <i>Processing Message</i> h5 SHA256 | 9 |
| Persamaan 2.14 <i>Processing Message</i> h4 SHA256 | 9 |
| Persamaan 2.15 <i>Processing Message</i> h3 SHA256 | 9 |
| Persamaan 2.16 <i>Processing Message</i> h2 SHA256 | 9 |
| Persamaan 2.17 <i>Processing Message</i> h1 SHA256 | 9 |
| Persamaan 2.18 <i>Processing Message</i> h0 SHA256 | 9 |

DAFTAR MODUL

| | |
|--|----|
| Modul Struktur 3.1 Struktur Data PKCS#10 dalam Representasi Text | 23 |
| Modul Program 4.1 Halaman <i>Request</i> Sertifikat | 36 |
| Modul Program 4.2 Pembangkitan Kunci RSA | 36 |
| Modul Program 4.3 Pembuatan Sertifikat PKCS#10 | 37 |
| Modul Program 4.4 Penerbitan Sertifikat X.509 | 38 |
| Modul Program 4.5 Halaman Tanda Tangan Dokumen PDF | 40 |
| Modul Program 4.6 <i>Sign PDF Document</i> | 41 |
| Modul Program 4.7 Ekstraksi Tanda Tangan Digital | 46 |