

DAFTAR ISI

LEMBAR PERSETUJUAN.....	I
HALAMAN PERSEMBAHAN	II
ABSTRAK.....	III
<i>ABSTRACT</i>	IV
KATA PENGANTAR.....	V
DAFTAR ISI	VII
DAFTAR GAMBAR	X
DAFTAR TABEL.....	XI
DAFTAR ISTILAH	XII
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	4
1.3 Tujuan Penelitian.....	5
1.4 Batasan Masalah.....	5
1.5 Manfaat Penelitian	6
1.6 Kerangka Pemikiran.....	7
1.7 Metode Penelitian.....	9
1.8 Sistematika Penulisan	11
BAB II KAJIAN LITERATUR.....	15
2.1 <i>State of The Art</i>	15
2.2 Landasan Teori	28
2.2.1 Kriptografi Asimetris dan Fungsi <i>Hash</i>	28
2.2.2 <i>Content-Based Hashing</i>	30
2.2.3 <i>Digital Signature</i>	31
2.2.4 Kriptografi Simetris dan AES-GCM.....	32

2.2.5	Fungsi Derivasi Kunci (KDF) dan Argon2id.....	34
2.2.6	<i>Envelope Encryption</i>	36
2.2.7	Indikator Visual dan Interoperabilitas Validasi Dokumen Digital	37
2.2.8	<i>Public Key Infrastructure</i> dan <i>Key Revocation</i>	40
2.2.9	Algoritma RSA (Rivest-Shamir-Adleman).....	41
2.2.10	Algoritma EdDSA (<i>Edwards-Curve Digital Signature Algorithm</i>).....	43
2.2.11	<i>Hybrid-signature</i>	45
2.2.12	Ancaman Keamanan Dokumen dan <i>Replay Attack</i>	45
2.2.13	Metadata.....	46
2.2.14	<i>Design Science Research Methodology (DSRM)</i>	47
BAB III METODOLOGI.....		50
3.1	Metodologi Penelitian	50
3.1.1	Identifikasi Masalah dan Motivasi (<i>Identify Problem and Motivate</i>).....	51
3.1.2	Definisi Tujuan Solusi (<i>Define Objectives of Solution</i>).....	55
3.1.3	Desain dan Pengembangan (<i>Design and Development</i>)	56
3.1.4	Demonstrasi (<i>Demonstration</i>).....	56
3.1.5	Evaluasi (<i>Evaluation</i>).....	57
3.1.6	Komunikasi (<i>Communication</i>).....	58
3.2	Alur Penelitian	58
3.3	Alur Sistem	60
3.4	Alur Algoritma	62
3.4.1	Fase Penandatanganan	63
3.4.2	Fase Verifikasi	65
BAB IV HASIL DAN PEMBAHASAN.....		69

4.1	Implementasi Sistem	69
4.1.1	Spesifikasi Sistem	69
4.1.1.1	Perangkat Keras (<i>Hardware</i>)	69
4.1.1.2	Perangkat Lunak (<i>Software</i>).....	69
4.1.2	Halaman Unggah Dokumen.....	70
4.1.3	Halaman Penandatanganan Dokumen.....	72
4.1.4	Halaman Verifikasi Dokumen.....	75
4.1.5	Alur Implementasi Sistem.....	77
4.2	Pengujian Fungsionalitas	78
4.2.1	Skenario Pengujian.....	78
4.2.2	Analisis Fungsionalitas	83
4.3	Pengujian Kinerja.....	84
4.3.1	Durasi Penandatanganan	84
4.3.2	Durasi Verifikasi	86
4.3.3	Analisis Kinerja.....	88
4.4	Pengukuran <i>Storage Overhead</i>	89
4.4.1	Hasil Pengukuran <i>Storage Overhead</i>	89
4.4.2	Analisis Perubahan Ukuran <i>File</i>	91
4.5	Pembahasan Hasil Temuan dan Komparasi dengan Penelitian Terdahulu.....	93
4.6	Keterbatasan Sistem	95
BAB V KESIMPULAN DAN SARAN.....		97
5.1	Kesimpulan	97
5.2	Saran.....	99
DAFTAR PUSTAKA		101
LAMPIRAN.....		111

DAFTAR GAMBAR

Gambar 1.1 Diagram kerangka pemikiran	7
Gambar 2.1 Diagram alur Design Science Research Methodology	48
Gambar 3.1 Diagram alur penelitian	59
Gambar 3.2 Diagram alur sistem	60
Gambar 3.3 Diagram alur algoritma proses penandatanganan	63
Gambar 3.4 Diagram alur algoritma proses verifikasi	66
Gambar 4.1 Tangkapan layar halaman unggah dokumen	72
Gambar 4.2 Tangkapan layar halaman tanda tangan dokumen.....	73
Gambar 4.3 Tangkapan layar halaman verifikasi dokumen	76



DAFTAR TABEL

Tabel 2.1 Tabel State of The Art.....	16
Tabel 3.1 Tabel Ringkasan Input-Proses-Output Tahapan DSRM.....	50
Tabel 4.1 Tabel Hasil Pengujian Kinerja.....	79
Tabel 4.2 Hasil Pengujian Kinerja Penandatanganan	85
Tabel 4.3 Hasil Pengujian Kinerja Verifikasi	87
Tabel 4.4 Hasil Storage Overhead Setelah Penandatanganan	90



DAFTAR ISTILAH

Istilah	Keterangan	Muncul Pertama
<i>Digital Signature</i>	: Mekanisme kriptografi yang digunakan untuk menjamin keaslian identitas pengirim dan integritas dokumen digital.	1
<i>Hash</i>	: Fungsi kriptografi satu arah yang mengubah data menjadi nilai unik dengan panjang tetap.	2
<i>Man-in-the-middle</i>	: Serangan siber dimana peretas menyusup ke dalam saluran komunikasi untuk menyadap, mengelabui, atau memanipulasi pertukaran data antara kedua belah pihak yang sah secara diam-diam.	3
<i>Shadow Attacks</i>	: Serangan manipulasi dokumen digital yang mengeksploitasi fitur pembaruan fisik dokumen (seperti <i>file</i> PDF), dimana peretas menyisipkan konten berbahaya atau memodifikasi tampilan dokumen tanpa merusak validitas tanda tangan digital konvensional yang melekat di dalamnya.	3
<i>Envelope Encryption</i>	: Pola manajemen kunci dua tingkat yang memisahkan antara enkripsi data utama (<i>private key</i>) dengan enkripsi/pembungkusan kunci itu sendiri.	3
Metadata	: Informasi tambahan yang melekat pada dokumen digital untuk mendeskripsikan atau menyimpan data tertentu tanpa mengubah isi utama dokumen.	4
<i>Content-based Hashing</i>	: Metode perhitungan <i>hash</i> berdasarkan isi utama dokumen tanpa melibatkan metadata atau struktur fisik <i>file</i> .	4
<i>Payload</i>	: Data utama yang digunakan dalam proses penandatanganan atau verifikasi <i>digital signature</i> .	4

<i>Replay attack</i>	: Serangan dengan cara mengirim ulang data autentik agar sistem menganggapnya sebagai transaksi baru yang sah.	4
<i>Closed-loop</i>	: Lingkungan distribusi dokumen tertutup dimana proses penandatanganan dan verifikasi dilakukan dalam satu ekosistem internal.	4
<i>Hybrid-signature</i>	: Metode tanda tangan digital yang menggabungkan lebih dari satu algoritma kriptografi dalam satu proses penandatanganan.	5
Kunci privat (<i>Private key</i>)	: Kunci rahasia dalam kriptografi asimetris yang digunakan untuk membuat tanda tangan digital.	7
<i>Key Revocation</i>	: Mekanisme pembatalan atau pencabutan status aktif sebuah kunci kriptografi sebelum masa berlakunya habis.	10
DSRM (<i>Design Science Research Methodology</i>)	: Metodologi penelitian untuk merancang dan mengevaluasi artefak teknologi informasi secara sistematis.	11
<i>Steganography</i>	: Teknik menyembunyikan data, informasi, atau pesan rahasia di dalam suatu media digital sedemikian rupa sehingga keberadaannya tidak disadari.	18
Argon2id	: Fungsi derivasi kunci (<i>Key Derivation Function</i>) berstandar <i>memory-hard</i> yang resisten terhadap serangan <i>side-channel</i> dan akselerasi <i>brute-force</i> GPU/ASIC.	22
OOXML (<i>Office Open XML</i>)	: Format dokumen berbasis kontainer berarsip ZIP dan XML yang digunakan oleh Microsoft Office (.docx dan .xlsx).	22
PBKDF2	: Fungsi derivasi kunci linier tradisional berbasis <i>password</i> yang memiliki kerentanan matematis <i>gamma-collision</i> .	23
<i>Crypto-agility</i>	: Kemampuan sistem kriptografi untuk beradaptasi atau mengganti algoritma keamanan tanpa mengubah keseluruhan arsitektur sistem.	26

Kunci publik (<i>Public key</i>)	: Kunci dalam kriptografi asimetris yang digunakan untuk verifikasi tanda tangan digital atau enkripsi data.	27
<i>Nonce</i>	: Nilai unik yang hanya digunakan satu kali dalam proses kriptografi atau komunikasi data.	34
Serangan <i>side-channel</i>	: Serangan kriptografi yang memanfaatkan informasi tambahan dari implementasi sistem, seperti waktu eksekusi atau konsumsi daya perangkat.	35
AES-256-GCM / AEAD	: Standar enkripsi simetris terotentikasi (<i>Authenticated Encryption with Associated Data</i>) yang menjamin kerahasiaan sekaligus integritas biner melalui <i>authentication tag</i> .	36
KEK & DEK	: <i>Key Encryption Key</i> (kunci turunan <i>passphrase</i> untuk membungkus kunci privat) dan <i>Data Encryption Key</i> (kunci acak simetris untuk mengenkripsi data secara langsung).	36
Kunci asimetris	: Sistem kriptografi yang menggunakan pasangan kunci publik dan kunci privat untuk proses keamanan data.	53
<i>Metadata Embedding</i>	: Teknik penyisipan data kriptografi ke dalam metadata dokumen tanpa mengubah isi utama dokumen.	80
<i>FlateDecode</i>	: Algoritma kompresi biner standar pada struktur berkas PDF yang digunakan untuk memadatkan <i>stream</i> objek dan metadata.	92