LAPORAN TANDA TANGAN DIGITAL

UAS Kriptografi - Implementasi RSA & SHA-256

INFORMASI DOKUMEN

Asal Dokumen:	test_document_1.pdf
Waktu Proses:	2026-01-12 19:40:24
Jenis Proses:	Pembuatan Tanda Tangan
Algoritma:	RSA-SHA256-PSS
Ukuran Kunci:	2048-bit

DETAIL TANDA TANGAN

Timestamp:	2026-01-12T19:40:24.794553
Panjang Tanda Tangan:	256 bytes
Hash Algorithm:	SHA-256
Document Hash:	1cb8b92916658d9d5ee3167f748c583927234788912bbaebba3faac8d14c25d4

ANALISIS KEAMANAN

1. **RSA 2048-bit**: Tingkat keamanan tinggi, tahan terhadap serangan brute-force
2. **SHA-256**: Fungsi hash kriptografi yang kuat, resisten collision
3. **PSS Padding**: Meningkatkan keamanan terhadap serangan tertentu
4. **Timestamp**: Mencegah replay attack dengan pencatatan waktu
5. **Digital Signature**: Memberikan autentikasi, integritas, dan non-repudiasi
6. **Hash Verification**: Memastikan dokumen tidak berubah setelah ditandatangani

Kesimpulan: Sistem tanda tangan digital ini **TIDAK DAPAT** memverifikasi keaslian dokumen atau dokumen telah diubah.