

LAPORAN TANDA TANGAN DIGITAL

UAS Kriptografi - Implementasi RSA & SHA-256

INFORMASI DOKUMEN

Asal Dokumen:	test_sertifikat_3.pdf
Waktu Proses:	2026-01-12 19:58:04
Jenis Proses:	Pembuatan Tanda Tangan
Algoritma:	RSA-SHA256-PSS
Ukuran Kunci:	2048-bit

DETAIL TANDA TANGAN

Timestamp:	2026-01-12T19:58:04.885348
Panjang Tanda Tangan:	256 bytes
Hash Algorithm:	SHA-256
Document Hash:	28cffe9b4e7372dc66422ffad38b4100ff7398f22bee37acee1660cfaee35df1

ANALISIS KEAMANAN

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

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