LAPORAN TANDA TANGAN DIGITAL

UAS Kriptografi - Implementasi RSA & SHA-256

INFORMASI DOKUMEN

Asal Dokumen:	20260112_123113_Ini adalah percobaan testing pertama 1.pdf
Waktu Proses:	2026-01-12 12:31:17
Jenis Proses:	Pembuatan Tanda Tangan
Algoritma:	RSA-SHA256-PSS
Ukuran Kunci:	2048-bit

DETAIL TANDA TANGAN

Timestamp:	2026-01-12T12:31:17.636904
Panjang Tanda Tangan:	256 bytes
Hash Algorithm:	SHA-256
Document Hash:	c86e3e4e2a177c513a41940934f25a2e1f9e3c8a8acbe0f3a47a6fb2b9782685

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.

DIGITAL SIGNATURE VERIFICATION PAGE

Document Information:

Original File: verification_report.pdf

Signing Time: 2026-01-12T20:35:32.186188

Algorithm: RSA-SHA256-PSS

Signature Information:

Key Size: 2048-bit RSA

Hash Algorithm: SHA-256

Signature Length: 256 bytes

Document Hash (SHA-256):

`d333d7946322e807ecf718af7152c883b530bc2f3d8d35764d30ad98bc1362d8`

Verification Instructions:

1. Hash dokumen asli menggunakan SHA-256
2. Dekripsi tanda tangan menggunakan public key
3. Bandingkan hash yang didekripsi dengan hash dokumen
4. Jika sama, tanda tangan VALID
5. Jika berbeda, tanda tangan INVALID atau dokumen berubah