

# KONTRAK DIGITAL UAS KRIPTOGRAFI

---

## PERJANJIAN TANDA TANGAN DIGITAL

Pihak Pertama: Mahasiswa

Pihak Kedua: Sistem Tanda Tangan Digital

### PASAL 1 - KETENTUAN UMUM

1. Dokumen ini digunakan untuk keperluan UAS Kriptografi
2. Tanda tangan digital menggunakan algoritma RSA 2048-bit
3. Hash dokumen menggunakan SHA-256

### PASAL 2 - VERIFIKASI

1. Tanda tangan dapat diverifikasi kapan saja
2. Integritas dokumen terjamin melalui hash
3. Non-repudiasi tercapai melalui kriptografi asimetris

Dibuat pada: 12 January 2026

# DIGITAL SIGNATURE VERIFICATION PAGE

---

## Document Information:

Original File: test\_kontrak\_2.pdf

Signing Time: 2026-01-12T19:58:04.440044

Algorithm: RSA-SHA256-PSS

## Signature Information:

Key Size: 2048-bit RSA

Hash Algorithm: SHA-256

Signature Length: 256 bytes

## Document Hash (SHA-256):

d68acb2e934367f4338b6c78eba18f76827fdff86eb9eb503214d1005f282c23

## 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