LAPORAN UAS KRIPTOGRAFI
IMPLEMENTASI TANDA TANGAN DIGITAL

INFORMASI MAHASISWA

Nama:	Aldi Satriya
NIM:	312310759
Mata Kuliah:	Kriptografi
Dosen:	Hemdani Rahendra Herlianto, S.Kom., M.T.I
Tanggal:	12 January 2026

1. PENDAHULUAN

Laporan ini merupakan hasil implementasi sistem tanda tangan digital untuk UAS Kriptografi. Sistem ini mengimplementasikan algoritma RSA dengan fungsi hash SHA-256 untuk memberikan jaminan keamanan terhadap dokumen digital dalam hal:
- **Autentikasi**: Memverifikasi identitas penandatangan
- **Integritas**: Memastikan dokumen tidak berubah
- **Non-repudiasi**: Mencegah penyangkalan tanda tangan

2. IMPLEMENTASI ALGORITMA

2.1 **RSA (Rivest-Shamir-Adleman)**
- Key Size: 2048-bit
- Public Exponent: 65537
- Padding Scheme: PSS dengan MGF1

2.2 **SHA-256 (Secure Hash Algorithm)**
- Output: 256-bit hash value
- Collision resistant
- One-way function

3. HASIL IMPLEMENTASI

Total Aktivitas Sistem: 2
Fitur yang berhasil diimplementasikan:
- Pembuatan tanda tangan digital
- Verifikasi tanda tangan
- Pembuatan dokumen test
- Analisis keamanan
- Laporan otomatis
- Export hasil lengkap

4. ANALISIS KEAMANAN

4.1 **Kekuatan Sistem**
- RSA 2048-bit memberikan keamanan yang memadai

- SHA-256 menjamin integritas data
- Timestamp mencegah replay attack

4.2 **Kelemahan dan Perbaikan**

- Private key harus disimpan dengan aman
- Perlu implementasi sertifikat digital
- Dapat dikembangkan dengan blockchain

5. KESIMPULAN

Sistem tanda tangan digital berhasil diimplementasikan dengan baik.
Semua persyaratan UAS terpenuhi termasuk:

- File PDF asli dan bertanda tangan
- File tanda tangan digital
- Hasil verifikasi
- Source code program
- Laporan lengkap

Sistem ini dapat digunakan untuk menjamin keaslian dokumen digital
dalam berbagai aplikasi seperti kontrak, sertifikat, dan dokumen penting lainnya.