Systematic Literature Review (SLR): Perbandingan Keamanan Algoritma RSA dan Advanced Encryption Standard (AES) untuk Implementasi Tanda Tangan Digital

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi menuntut sistem keamanan yang andal untuk memastikan keaslian, integritas, dan non-repudiasi dokumen digital. Berbagai aplikasi yang memerlukan verifikasi identitas dan otentikasi dokumen seperti kontrak elektronik, sertifikat digital, surat resmi elektronik, dan transaksi hukum digital memerlukan mekanisme tanda tangan yang aman. Kriptografi sebagai ilmu penyandian data menjadi fondasi utama dalam menjaga autentikasi, integritas, dan keabsahan hukum dari dokumen digital.

Dua algoritma kriptografi yang paling banyak digunakan dalam implementasi tanda tangan digital adalah RSA (Rivest-Shamir-Adleman) dan AES (Advanced Encryption Standard), yang masing-masing mewakili paradigma enkripsi asimetris dan simetris. Menurut (Sood & Kaur, 2023), *"dengan evolusi kecerdasan manusia, seni kriptografi menjadi lebih kompleks agar informasi lebih aman"* dan berbagai algoritma enkripsi diperlukan untuk melindungi informasi.

Untuk memahami karakteristik keamanan kedua algoritma tersebut dalam konteks tanda tangan digital, dilakukan penelusuran literatur sistematis menggunakan portal ilmiah seperti Google Scholar, IEEE Xplore, ScienceDirect, dan jurnal nasional dengan kata kunci "RSA digital signature", "AES in digital signature", "symmetric asymmetric signature", "cryptographic algorithm vulnerability", dan "quantum computing threat".

Kriteria literatur yang digunakan:

- Diterbitkan antara 2020–2025
- Fokus pada analisis keamanan RSA dan AES dalam konteks tanda tangan digital
- Berasal dari jurnal terindeks atau publikasi resmi
- Memuat data eksperimen atau kajian teoretis mendalam terkait keamanan kriptografi

Tujuan utama dari SLR ini adalah memberikan pemahaman mendalam terhadap perbandingan keamanan RSA dan AES dalam implementasi tanda tangan digital, mengidentifikasi kerentanan masing-masing algoritma, serta menganalisis tren penggunaan kedua algoritma dalam sistem otentikasi dokumen kontemporer.

2. Dasar Teori

2.1 Kriptografi dan Tanda Tangan Digital

Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematis untuk menjaga kerahasiaan, integritas, dan autentikasi data melalui proses penyandian. Menurut (Sood & Kaur, 2023), *"keamanan adalah mekanisme yang melindungi informasi dan layanan dari akses yang tidak disengaja atau tidak sah"*.

Dalam konteks tanda tangan digital, kriptografi digunakan untuk:

- Memastikan integritas dokumen
- Memberikan autentikasi identitas
- Menjamin non-repudiasi

(Parekh & Maru, 2025) menambahkan bahwa *"di era digital saat ini, melindungi kerahasiaan, integritas, dan keamanan data adalah kekhawatiran utama. Kriptografi adalah metode komunikasi informasi dan perlindungan data yang aman"*.

2.2 Algoritma RSA dalam Tanda Tangan Digital

RSA adalah algoritma kriptografi asimetris yang digunakan untuk **tanda tangan digital** dengan memanfaatkan pasangan kunci publik dan privat. Menurut (Sood & Kaur, 2023), *"RSA adalah salah satu sistem kriptografi kunci publik yang paling terkenal untuk pertukaran kunci atau tanda tangan digital"*.

Namun, (Sood & Kaur, 2023) juga menekankan bahwa *"RSA memiliki banyak cacat dalam desainnya... Ketika nilai p dan q kecil untuk merancang kunci maka proses enkripsi menjadi terlalu lemah"*.

2.3 Peran AES dalam Sistem Tanda Tangan Digital

AES adalah algoritma enkripsi simetris yang diadopsi oleh NIST sebagai FIPS-197 pada tahun 2001. Meskipun tidak digunakan langsung untuk tanda tangan, AES berperan dalam mengenkripsi dokumen sebelum proses penandatanganan atau melindungi kunci sesi.

(Baig et al., 2024) menjelaskan: *"Advanced Encryption Standard (AES) adalah algoritma enkripsi simetris populer yang menyediakan keamanan kuat untuk transmisi data dan penyimpanan"*.

(Parekh & Maru, 2025) menegaskan: *"AES adalah cipher simetris modern yang direkomendasikan untuk data massal — aman terhadap serangan klasik yang diketahui"*.

3. Metodologi Penelusuran Literatur

Penelusuran literatur dilakukan secara sistematis melalui lima basis data ilmiah utama: Google Scholardan jurnal nasional terakreditasi. Tahapan seleksi meliputi:

1. Identifikasi awal sebanyak 10 artikel yang relevan berdasarkan kata kunci yang telah ditentukan
2. Penyaringan inklusi berdasarkan tahun penerbitan (2020–2025) dan fokus pada keamanan algoritma RSA dan AES dalam konteks tanda tangan digital
3. Penyaringan eksklusi terhadap artikel non-ilmiah, laporan tanpa data empiris, atau tulisan yang hanya membahas implementasi tanpa analisis keamanan

Setelah tahap seleksi, 5 artikel utama dipilih karena memenuhi seluruh kriteria kelayakan dan memiliki data empiris yang dapat dibandingkan secara objektif dengan pembahasan mendalam tentang keamanan RSA dan AES.

4. Hasil Studi Literatur

No	Penulis & Tahun	Sumber	Metode	Fokus Penelitian	Temuan Utama
1	(Parekh & Maru, 2025)	USRED	Literature review	AES, DES, RSA security review	AES superior untuk enkripsi dokumen, RSA untuk tanda tangan digital, hybrid encryption terbaik
2	(Sood & Kaur, 2023)	SCRS Publication	Survey komparatif	Analisis keamanan AES, DES, RSA	AES fastest dan excellent security, RSA least secure untuk enkripsi massal

No	Penulis & Tahun	Sumber	Metode	Fokus Penelitian	Temuan Utama
3	(Mahesh et al., 2023)	URSAR	Hybrid encryption	RSA-AES hybrid encryption design	Hybrid RSA-AES optimal untuk keamanan dan performa sistem tanda tangan
4	(Baig et al., 2024)	MSA Journal	Studi komparatif	Perbandingan AES, RSA, 3DES	AES unggul dalam efisiensi, RSA dalam tugas asimetris seperti tanda tangan
5	(Laurentinus et al., 2020)	JTSISKOM UNDIP	Eksperimen performa	Perbandingan kinerja RSA vs AES	AES 5.8x lebih cepat dari RSA dalam enkripsi dokumen

5. Analisis dan Sintesis

5.1 Keamanan Teoretis untuk Tanda Tangan Digital

Berdasarkan analisis literatur, **RSA** menunjukkan kekuatan dalam **tanda tangan digital** karena sifat asimetrisnya. Namun, (Parekh & Maru, 2025) memperingatkan: *"RSA tetap penting untuk tugas kunci publik pertukaran kunci, autentikasi, tanda tangan digital tetapi tidak efisien untuk mengenkripsi payload data besar"*.

AES tidak digunakan langsung untuk tanda tangan, tetapi berperan dalam **melindungi integritas dokumen** yang akan ditandatangani.

5.2 Performa dalam Sistem Tanda Tangan

(Laurentinus et al., 2020) menemukan bahwa **AES 5.8x lebih cepat daripada RSA** dalam enkripsi dokumen. Namun, untuk proses tanda tangan, **RSA** tetap diperlukan untuk memastikan non-repudiasi.

5.3 Implementasi Hybrid untuk Tanda Tangan Digital

(Mahesh et al., 2023) menekankan: *"Hybrid encryption menggunakan AES dan RSA menawarkan pendekatan yang kuat dan fleksibel untuk enkripsi data dan tanda tangan digital"*.

(Parekh & Maru, 2025) memberikan rekomendasi spesifik:
"Berdasarkan literatur yang ditinjau, AES-256 direkomendasikan untuk enkripsi dokumen, idealnya dengan AES-GCM untuk integritas dan autentisitas. Tanda tangan digital harus dilakukan menggunakan RSA-2048/3072 atau ECC".

6. Arah Peluang Penelitian

Beberapa peluang penelitian yang masih terbuka antara lain:

1. Membuat website untuk digital signature
2. Standardized Benchmarking untuk Tanda Tangan Digital
3. Energy-Efficient Cryptography untuk Perangkat Mobile
4. Integration with laravel untuk Sertifikasi Dokumen
5. Key Management System untuk Sertifikat Digital

7. Kesimpulan

Berdasarkan hasil penelusuran literatur sistematis terhadap 5 sumber kredibel, dapat disimpulkan bahwa:

1. **RSA lebih cocok untuk tanda tangan digital** karena sifat asimetrisnya yang mendukung non-repudiasi dan autentikasi
2. **AES unggul dalam enkripsi dokumen** yang akan ditandatangani, menjamin kecepatan dan kerahasiaan
3. **Kombinasi hybrid RSA-AES** merupakan praktik terbaik untuk sistem tanda tangan digital yang aman dan efisien
4. **Perlunya transisi menuju algoritma pasca-kuantum** untuk menjamin keamanan jangka panjang

Daftar Pustaka

Baig, M. H. M., Ul Haq, H. B., & Habib, W. (2024). A Comparative Analysis of AES, RSA, and 3DES Encryption Standards based on Speed and Performance. *Management Science Advances*, *1*(1), 20–30. https://doi.org/10.31181/msa1120244

Laurentinus, L., Pradana, H. A., Sylfania, D. Y., & Juniawan, F. P. (2020). Performance comparison of RSA and AES to SMS messages compression using Huffman algorithm. *Jurnal Teknologi Dan Sistem Komputer*, *8*(3), 171–177. https://doi.org/10.14710/jtsiskom.2020.13468

Mahesh, V., Batta, B., & Suresh Kumar, L. K. (2023). "RSA-AES Hybrid Encryption: Combining The Strengths Of Two Powerful Algorithms For Enhanced Security." *International Journal of Research and Analytical Reviews*, *10*(2), 992–998. www.ijrar.org

Parekh, S., & Maru, J. (2025). *AES, DES, and RSA in Data Security: A Review*. *8*(5).

Sood, R., & Kaur, H. (2023). A Literature Review on RSA, DES and AES Encryption Algorithms. *Emerging Trends in Engineering and Management*, 57–63. https://doi.org/10.56155/978-81-955020-3-5-07