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

Nama: Azkiya Zahrul Umam
NIM: 20230801187

1. Pendahuluan

Perkembangan teknologi informasi dan komunikasi menuntut sistem keamanan data yang semakin canggih untuk melindungi informasi sensitif dari ancaman siber. Berbagai aplikasi berbasis internet telah bermunculan seperti online shopping, stock trading, internet banking, dan electronic bill payment, yang semuanya memerlukan koneksi aman end-to-end. Kriptografi sebagai ilmu penyandian data menjadi fondasi utama dalam menjaga kerahasiaan, integritas, dan autentikasi informasi digital.

Dua algoritma kriptografi yang paling banyak digunakan dalam implementasi keamanan modern 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, dilakukan penelusuran literatur sistematis menggunakan portal ilmiah seperti Google Scholar, IEEE Xplore, ScienceDirect, dan jurnal nasional dengan kata kunci "RSA vs AES security comparison", "symmetric asymmetric encryption", "cryptographic algorithm vulnerability", dan "quantum computing threat".

Kriteria literatur yang digunakan:

- Diterbitkan antara 2020-2025
- Fokus pada analisis keamanan RSA dan AES
- 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, mengidentifikasi kerentanan masing-masing algoritma, serta menganalisis tren penggunaan kedua algoritma dalam implementasi keamanan data kontemporer.

2. Dasar Teori

2.1 Kriptografi dan Klasifikasi Algoritma

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" dan "keamanan dalam jaringan didasarkan pada kriptografi (kata yang berasal dari Yunani, berarti 'tulisan rahasia'), ilmu dan seni mengubah pesan untuk menjadikan mereka aman dan kebal terhadap serangan".

(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".

Algoritma kriptografi dibagi menjadi dua kategori utama: simetris (menggunakan satu kunci) dan asimetris (menggunakan sepasang kunci).(Sood & Kaur, 2023):

"Enkripsi kunci simetris adalah bentuk kriptosistem di mana enkripsi dan dekripsi dilakukan menggunakan kunci yang sama. Juga dikenal sebagai enkripsi konvensional. Enkripsi kunci asimetris adalah bentuk kriptosistem di mana enkripsi dan dekripsi dilakukan menggunakan kunci yang berbeda yaitu kunci publik dan kunci privat. Juga dikenal sebagai enkripsi kunci publik"

2.2 Algoritma RSA (Rivest-Shamir-Adleman)

RSA adalah algoritma kriptografi asimetris yang dikembangkan oleh Ron Rivest, Adi Shamir, dan Leonard Adleman pada tahun 1978. Menurut (Sood & Kaur, 2023), "RSA adalah salah satu sistem kriptografi kunci publik yang paling terkenal untuk pertukaran kunci atau tanda tangan digital atau enkripsi blok data. RSA menggunakan blok enkripsi ukuran variabel dan kunci ukuran variabel".

(Sood & Kaur, 2023)lebih lanjut menekankan bahwa "RSA memiliki banyak cacat dalam desainnya oleh karena itu tidak disukai untuk penggunaan komersial. Ketika nilai p dan q kecil untuk merancang kunci maka proses enkripsi menjadi terlalu lemah dan seseorang dapat mendekripsi data dengan menggunakan teori probabilitas acak dan serangan side channel".

2.3 Algoritma AES (Advanced Encryption Standard)

AES adalah algoritma enkripsi simetris yang diadopsi oleh NIST (National Institute of Standards and Technology) sebagai FIPS-197 pada tahun 2001. Menurut(Sood & Kaur, 2023), "Advanced Encryption Standard diadopsi oleh NIST pada tahun 2001 sebagai FIPS-197, dan menggantikan DES yang ditarik pada tahun 2005".

(Baig et al., 2024) memberikan penjelasan detail tentang AES: "Advanced Encryption Standard (AES) adalah algoritma enkripsi simetris populer yang menyediakan keamanan kuat untuk transmisi data dan penyimpanan. Dipilih oleh National Institute of Standards and Technology (NIST) untuk menggantikan Data Encryption Standard (DES) yang sudah ketinggalan zaman. AES menggunakan cipher blok untuk mengenkripsi data, yang melibatkan pembagian data menjadi blok dan kemudian mengacaknya dengan kunci rahasia. Ini mendukung ukuran kunci 128, 192, dan 256 bit, dan dianggap sebagai salah satu algoritma enkripsi paling aman yang tersedia".

(Parekh & Maru, 2025) menegaskan konsensus keamanan AES: "AES adalah cipher simetris modern yang direkomendasikan untuk data massal — aman terhadap serangan klasik yang diketahui ketika diimplementasikan dengan benar dan menggunakan ukuran kunci yang direkomendasikan".

Keamanan AES berdasarkan pada kompleksitas matematis dari operasi substitusi dan permutasi yang berulang melalui multiple rounds. Menurut (Mahesh et al., 2023) "sistem AES melalui 10 putaran untuk kunci 128-bit, 12 putaran untuk kunci 192-bit, dan 14 putaran untuk kunci 256-bit untuk memberikan ciphertext final atau mengambil kembali plaintext asli".

Setiap round dari AES terdiri dari empat transformasi utama:

1. SubBytes: Substitusi byte menggunakan S-box Rijndael
2. ShiftRows: Permutasi baris dengan pergeseran siklik
3. MixColumns: Perkalian matriks untuk mixing data
4. AddRoundKey: XOR dengan round key

3. Metodologi Penelusuran Literatur

Penelusuran literatur dilakukan secara sistematis melalui lima basis data ilmiah utama: Google Scholar, IEEE Xplore, ScienceDirect, PubMed Central, dan jurnal nasional terakreditasi. Tahapan seleksi meliputi:

1. Identifikasi awal sebanyak 68 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
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)	IJSRED	Literature review	AES, DES, RSA security review	AES superior untuk bulk encryption, RSA untuk key management, hybrid encryption terbaik

2	(Sood & Kaur, 2023)	SCRS Publication	Survey komparatif	Analisis keamanan AES, DES, RSA	AES fastest dan excellent security, RSA least secure
3	(Mahesh et al., 2023)	IJRAR	Hybrid encryption	RSA-AES hybrid encryption design	Hybrid RSA-AES optimal untuk security dan performance
4	(Baig et al., 2024)	MSA Journal	Studi komparatif	Perbandingan AES, RSA, 3DES	AES unggul dalam efisiensi, RSA dalam asymmetric tasks
5	(Laurentinus et al., 2020)	JTSISKOM UNDIP	Eksperimen performa	Perbandingan kinerja RSA vs AES	AES 5.8x lebih cepat dari RSA dalam enkripsi

5. Analisis dan Sintesis

5.1 Keamanan Teoretis dengan Sumber Jelas

Berdasarkan analisis literatur, AES menunjukkan kekuatan keamanan teoretis yang sangat tinggi. Menurut (Parekh & Maru, 2025):

"AES memiliki kompleksitas brute force sebesar 2^128 operasi, yang secara praktis tidak dapat dipecahkan dengan teknologi komputasi saat ini. Resistensi terhadap berbagai serangan kriptanalisis termasuk differential dan linear cryptanalysis telah terbukti"

(Sood & Kaur, 2023)melakukan perbandingan langsung: "Menurut survei literatur, telah ditemukan bahwa algoritma AES paling efisien dalam hal kecepatan, waktu, throughput dan avalanche effect".

Sebaliknya, keamanan RSA menghadapi tantangan. Menurut (Sood & Kaur, 2023),"RSA adalah algoritma yang paling tidak aman dibandingkan dengan DES dan AES". (Parekh & Maru, 2025) menambahkan: "RSA tetap penting untuk tugas kunci publik pertukaran kunci, autentikasi, tanda tangan digital tetapi tidak efisien untuk mengenkripsi payload data besar. Sebagian besar perbandingan empiris menunjukkan overhead komputasi dan memori RSA tumbuh dengan cepat dengan ukuran kunci; terlebih lagi, algoritma kuantum mengancam RSA dalam jangka panjang".

5.2 Performa dan Efisiensi Komputasi

Dari aspek performa, penelitian menunjukkan superioritas AES. (Parekh & Maru, 2025) menyatakan: "Kecepatan enkripsi: AES mengungguli DES dan jauh mengungguli RSA untuk enkripsi massal. Dokumen yang menjalankan benchmark pada file/gambar melaporkan latensi enkripsi/dekripsi AES terendah; RSA paling lambat ketika digunakan untuk melindungi data secara langsung".

Menurut (Sood & Kaur, 2023), dalam table perbandingan mereka menunjukkan bahwa "RSA memiliki kecepatan paling lambat, DES lambat, dan AES cepat". Penggunaan memori juga berbeda signifikan: "Penggunaan memori: Proses key generation dan expansion RSA memerlukan jejak memori yang lebih besar. AES menunjukkan penggunaan memori sedang dan mendapat manfaat signifikan dari dukungan hardware (AES-NI)".

5.3 Manajemen Kunci dan Distribusi

AES menghadapi tantangan fundamental dalam distribusi kunci karena sifat simetrisnya. Menurut(Sood & Kaur, 2023): "Algoritma simetris seperti DES (Data Encryption Standard) dan AES (Advanced Encryption Standard) menggunakan satu kunci rahasia untuk enkripsi dan dekripsi. Mereka efisien dengan memproses jumlah data besar, tetapi tidak efisien dengan berbagi kunci secara aman".

RSA memberikan solusi elegant. (Parekh & Maru, 2025)menjelaskan: "Fitur asimetris: pertukaran kunci yang aman & tanda tangan. RSA digunakan untuk mengenkripsi kunci simetris sehingga komunikasi diamankan. Algoritma asimetris seperti RSA mengenkripsi kunci simetris sehingga komunikasi diamankan".

5.4 Implementasi Hybrid Encryption

Penelitian terkini menunjukkan tren penggunaan hybrid encryption.(Parekh & Maru, 2025):

"Hybrid AES+RSA tetap menjadi standar praktis. Model hybrid yang menggabungkan keunggulan simetris dan asimetris sangat penting dalam mengamankan komunikasi di kondisi yang tidak aman seperti Internet of Things (IoT), di mana daya pemrosesan dan penyimpanan dalam perangkat biasanya kurang"

(Mahesh et al., 2023) menekankan: "Hybrid encryption menggunakan AES dan RSA menawarkan pendekatan yang kuat dan fleksibel untuk enkripsi data. Kombinasi enkripsi simetris AES dan enkripsi asimetris RSA memberikan manfaat dari kedua teknik, termasuk enkripsi dan dekripsi kecepatan tinggi, keamanan kuat, dan fleksibilitas dalam manajemen kunci".

(Parekh & Maru, 2025) memberikan rekomendasi spesifik:

"Berdasarkan literatur yang ditinjau, AES-256 direkomendasikan untuk enkripsi payload, idealnya dengan AES-GCM untuk integritas dan autentisitas. Kunci sesi AES harus diangkut dengan aman menggunakan RSA-2048/3072 atau ECC (misalnya, secp256r1), dengan ECC menjadi diinginkan di lingkungan terbatas sumber daya. Hybrid AES + RSA/ECC adalah praktik saat ini terbaik untuk enkripsi file dan gambar yang aman"

6. Arah Peluang Penelitian

Beberapa peluang penelitian yang masih terbuka antara lain:

1. Post-Quantum Cryptography: Pengembangan algoritma pengganti RSA yang tahan terhadap serangan kuantum
2. Standardized Benchmarking: Pembentukan suite benchmarking yang konsisten untuk perbandingan algoritma kriptografi
3. Energy-Efficient Cryptography: Kriptografi yang cocok untuk perangkat IoT dengan keterbatasan sumber daya

4. Integration with AI/ML: Penelitian tentang dampak enkripsi terhadap sistem AI/ML
5. Key Management: Pengembangan sistem manajemen kunci yang usable dan aman

7. Kesimpulan

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

1. AES unggul dalam keamanan dan performa: Menurut(Parekh & Maru, 2025), "AES adalah cipher simetris modern yang direkomendasikan untuk data massal karena keamanan kuat dan performa tinggi". (Sood & Kaur, 2023)menegaskan "algoritma AES paling efisien dalam hal kecepatan, waktu, throughput dan avalanche effect".
2. RSA lebih cocok untuk manajemen kunci: (Parekh & Maru, 2025)mengidentifikasi bahwa "RSA tetap fundamental untuk tugas asimetris (pertukaran kunci, tanda tangan) namun tidak praktis untuk mengenkripsi payload besar besar". (Sood & Kaur, 2023)menambahkan bahwa "RSA memiliki banyak cacat dalam desainnya oleh karena itu tidak disukai untuk penggunaan komersial".
3. Hybrid encryption sebagai solusi optimal: Menurut Batta & Kumar (2023), "hybrid encryption menggunakan AES dan RSA menawarkan pendekatan yang kuat dan fleksibel untuk enkripsi data yang dapat digunakan dalam berbagai skenario di mana keamanan adalah kekhawatiran, termasuk transaksi online, transfer file dan komunikasi email".
4. Kebutuhan transisi ke post-quantum cryptography: (Parekh & Maru, 2025)merekomendasikan "pekerjaan masa depan harus mengatasi standardisasi benchmarking, migrasi post-kuantum, dan kriptografi yang efisien energi untuk IoT".

Dengan demikian, AES menunjukkan superioritas keamanan jangka panjang dibandingkan RSA, terutama untuk enkripsi data dalam jumlah besar. Namun, RSA tetap memiliki nilai strategis dalam manajemen kunci hingga algoritma post-quantum matang untuk implementasi komersial. Kombinasi hybrid RSA-AES merupakan praktik best practice saat ini yang mengoptimalkan kedua algoritma.

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