INFO TEKNIK
Volume 26 No. 2 Des 2025 (159-170)

ANALISIS KEAMANAN DATA DENGAN ALGORITMA ADVANCED ENCRYPTION STANDARDS (AES) DAN RIVEST SHAMIR ADLEMAN (RSA)

Ahmat Setiawan
Program Studi Teknik Informatika, Fakultas Teknologi Industri dan Informatika, Universitas Muhammadiyah Prof. Dr. Hamka
E-mail : ahmatsetiawanuhamka@gmail.com

ABSTRACT

In an increasingly interconnected digital era, data security has become a critical aspect across various sectors such as banking, government, and the technology industry. Threats to information, including hacking and data theft, have driven the need for encryption technology as a primary solution for data protection. This study aims to analyze the effectiveness of two widely used modern cryptographic algorithms—Advanced Encryption Standard (AES) and Rivest-Shamir-Adleman (RSA)—in safeguarding digital data. AES is a symmetric algorithm that operates on 128-bit data blocks, while RSA is an asymmetric algorithm that relies on the complexity of factoring large prime numbers. This study compares the strengths and weaknesses of both algorithms in terms of encryption efficiency, resilience against cyberattacks, and their implementation in information technology systems such as digital banking services, cloud computing, and online transactions. Through a literature review, this research seeks to provide a comprehensive understanding of the role of cryptography in addressing information security challenges in the digital age.

Keywords: Cryptography, AES, RSA, Data Security, Encryption

1. PENDAHULUAN

Dalam era digital yang semakin berkembang, keamanan data menjadi aspek krusial bagi berbagai sektor, termasuk perbankan, pemerintahan, dan industri teknologi. Ancaman terhadap keamanan informasi, seperti peretasan, pencurian data, dan serangan siber, semakin meningkat seiring dengan meningkatnya penggunaan teknologi berbasis internet. Untuk mengatasi tantangan ini, enkripsi menjadi solusi utama dalam melindungi data dari akses yang tidak sah. Saat ini, berbagai algoritma kriptografi telah dikembangkan sebagai metode untuk melindungi data. Secara umum, algoritma ini terbagi menjadi dua kategori: klasik dan modern. Algoritma klasik bekerja dengan karakter sebagai unit operasinya, sementara algoritma modern menggunakan bit dalam proses enkripsinya. Enkripsi merupakan proses yang mengubah data dari bentuk yang dapat dipahami menjadi format yang tidak dapat dibaca atau dimengerti. Dalam konteks kriptografi, enkripsi sering dikaitkan dengan istilah kode atau cipher. Beberapa isu utama yang berkaitan dengan keamanan dan kerahasiaan data meliputi privasi (kerahasiaan), integritas (keutuhan), autentikasi (keaslian), serta non-repudiation atau pembuktian yang tidak dapat disangkal (Azlin et al., 2018). Enkripsi modern berperan penting dalam melindungi keamanan dan privasi data, khususnya di tengah

lingkungan teknologi yang semakin terintegrasi dan rumit. Salah satu metode yang efektif untuk menjaga keamanan data adalah dengan menerapkan enkripsi berbasis algoritma. Saat ini mulai berkembang algoritma kriptografi dengan teknik enkripsi moderen yang sering digunakan yaitu mencakup AES (Advanced Encryption Standard) dan sistem simetris serta RSA (Rivest-Shamir-Adleman) yang bersifat asimetris. Kedua algoritma ini berperan penting dalam melindungi data dari akses yang tidak sah (Nasution et al., 2024). Keamanan algoritma RSA bergantung pada kesulitan dalam memfaktorkan bilangan besar menjadi faktor-faktor prima, yang membuatnya sulit untuk diretas. Proses pemfaktoran ini digunakan untuk mendapatkan kunci privat. Sementara itu, algoritma AES beroperasi dengan unit byte atau karakter. Dalam versi AES-128, ukuran blok yang digunakan untuk enkripsi dan pembentukan cipherteks adalah 128 bit atau setara dengan 16 byte (Laurentinus et al., 2020).

Advance Encryption Standard (AES) juga disebut Rijndael pengganti DES, dibuat oleh seorang asal Belgia Bernama Vincent Rijmen dan John Daemen yang merupakan juara pada *Cryptographic Algorithm Contest.* AES merupakan jenis enkripsi dengan kunci simetris yang menggunakan algoritma block cipher. Dengan menggunakan kunci yang sama untuk melakukan enkripsi dan dekripsi, AES memberikan input dan output yang terdiri dari urutan data 128-bit juga disebut blok data atau plaintext (Ananda & Lukman, 2022). Rivest Shamir Adleman (RSA) adalah salah satu algoritma kriptografi dengan kunci publik yang paling populer dan banyak digunakan hingga saat ini. Algoritma ini pertama kali diperkenalkan oleh tiga ilmuwan komputer, yaitu Rivest, Shamir, dan Adleman, pada tahun 1977. Keunggulannya terletak pada keamanan yang bergantung pada kompleksitas pemfaktoran bilangan besar, sehingga sangat cocok untuk melindungi data dalam berbagai aplikasi digital (Indonesia, 2023). Keamanan algoritma RSA bergantung pada kesulitan dalam memfaktorkan bilangan besar menjadi faktor-faktor prima, yang membuatnya sulit untuk diretas. Proses pemfaktoran ini digunakan untuk mendapatkan kunci privat. Sementara itu, algoritma AES beroperasi dengan unit byte atau karakter. Dalam versi AES-128, ukuran blok yang digunakan untuk enkripsi dan pembentukan cipherteks adalah 128 bit atau setara dengan 16 byte (Laurentinus et al., 2020). Tujuan dari penelitian ini adalah untuk menganalisis efektivitas algoritma kriptografi AES dan RSA dalam menjaga keamanan data digital. Penelitian ini juga bertujuan untuk membandingkan kelebihan dan kekurangan dari kedua algoritma tersebut, baik dari segi efisiensi proses enkripsi maupun kekuatan dalam menghadapi ancaman keamanan informasi. Selain itu, penulis ingin mengidentifikasi bagaimana implementasi nyata algoritma AES dan RSA diterapkan dalam berbagai sistem teknologi informasi, seperti layanan perbankan digital, cloud computing, serta transaksi

online. Melalui kajian literatur ini, diharapkan dapat diperoleh gambaran yang komprehensif terkait tantangan, potensi, dan prospek pengembangan algoritma kriptografi sebagai solusi utama perlindungan data di era digital.

2. TINJAUAN PUSTAKA

2.1. Kriptografi dan Keamanan Data

Kriptografi merupakan cabang ilmu yang mempelajari teknik pengamanan informasi melalui proses enkripsi dan dekripsi. Tujuan utama kriptografi adalah menjaga empat aspek penting dalam keamanan informasi, yaitu kerahasiaan (confidentiality), integritas (integrity), autentikasi (authentication), dan non-repudiation (penyangkalan). Dalam konteks digital, kriptografi menjadi fondasi utama dalam melindungi data dari akses yang tidak sah, terutama pada sistem yang terhubung ke jaringan internet (Fajrin, A.M., et al. 2003)

2.2. Algoritma Advanced Encryption Standard (AES)

AES adalah algoritma kriptografi simetris yang dikembangkan sebagai pengganti Data Encryption Standard (DES). AES menggunakan blok data 128-bit dan mendukung panjang kunci 128, 192, dan 256 bit. Proses enkripsi AES terdiri dari beberapa putaran (rounds) yang melibatkan substitusi, permutasi, dan transformasi matriks untuk menghasilkan cipherteks yang aman. AES dikenal karena efisiensinya dalam perangkat lunak maupun perangkat keras, serta kecepatan proses enkripsi yang tinggi (Karim, R.M.S. 2024)

2.3. Algoritma Rivest Shamir Adleman (RSA)

RSA adalah algoritma kriptografi asimetris yang menggunakan sepasang kunci: kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Keamanan RSA bergantung pada kesulitan faktorisasi bilangan bulat besar menjadi bilangan prima, yang hingga kini belum dapat diselesaikan secara efisien oleh algoritma komputasi konvensional. RSA banyak digunakan dalam pengamanan komunikasi digital, tanda tangan digital, dan distribusi kunci.

2.4. Perbandingan AES dan RSA

Beberapa penelitian menunjukkan bahwa AES lebih unggul dalam hal kecepatan dan efisiensi karena menggunakan satu kunci untuk proses enkripsi dan

dekripsi. Sebaliknya, RSA menawarkan keunggulan dalam aspek distribusi kunci dan autentikasi karena menggunakan dua kunci yang berbeda. Dalam implementasi nyata, kombinasi keduanya sering digunakan, di mana RSA digunakan untuk mengamankan pertukaran kunci AES, dan AES digunakan untuk mengenkripsi data dalam jumlah besar.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan studi literatur (literature review), yaitu dengan mengumpulkan, menelaah, dan menganalisis berbagai sumber ilmiah yang relevan terkait algoritma kriptografi AES (Advanced Encryption Standard) dan RSA (Rivest-Shamir-Adleman) dalam konteks keamanan data digital. Metode ini dipilih karena memungkinkan penulis untuk mengevaluasi dan membandingkan efektivitas kedua algoritma berdasarkan hasil-hasil penelitian sebelumnya, tanpa melakukan eksperimen langsung. Sumber data diperoleh dari jurnal nasional dan internasional yang dipublikasikan dalam lima tahun terakhir melalui database seperti Google Scholar, Publish or Perish, dan portal jurnal universitas. Kriteria inklusi mencakup artikel yang membahas implementasi, performa, efisiensi, serta kelebihan dan kekurangan algoritma AES dan RSA dalam berbagai sistem, seperti cloud computing, transaksi online, dan sistem perbankan. Secara teoritis, penelitian ini mengacu pada konsep dasar kriptografi yang dikemukakan oleh Stallings (2017), yang menyatakan bahwa kriptografi modern bertujuan untuk menjaga kerahasiaan, integritas, dan autentikasi data melalui proses enkripsi dan dekripsi. AES dikenal sebagai algoritma simetris yang cepat dan efisien, sedangkan RSA merupakan algoritma asimetris yang unggul dalam aspek keamanan kunci publik. Sebagai penguat, penelitian (Irawan & Rachmawanto, 2021) menunjukkan bahwa kombinasi AES dan RSA dapat meningkatkan efek avalanche dan efisiensi enkripsi. Sementara itu, (Fajrin et al., 2024) membandingkan performa kedua algoritma dalam transaksi online dan menemukan bahwa keduanya memiliki tingkat keamanan tinggi, terutama saat menggunakan panjang kunci yang optimal. Dengan pendekatan ini, diharapkan penelitian dapat memberikan gambaran komprehensif mengenai efektivitas algoritma AES dan RSA dalam menjaga keamanan data digital.

4. HASIL DAN PEMBAHASAN

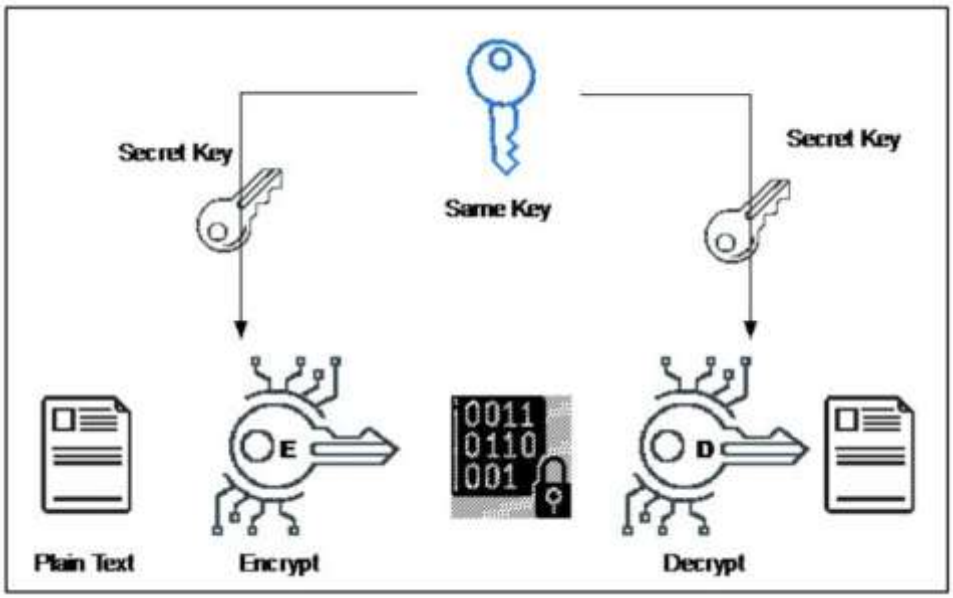
4.1 Karakteristik Algoritma AES

Algoritma Advanced Encryption Standard (AES) bekerja dengan melakukan serangkaian proses kriptografi berupa *substitusi*, *permutasi*, dan *operasi kunci* pada

data biner. (Nelakuditi et al., 2024) Pada tahap substitusi (SubBytes), setiap byte dalam blok data digantikan oleh byte lain berdasarkan tabel substitusi non-linier yang disebut S-box, untuk menghasilkan keragaman dan resistansi terhadap serangan linier dan diferensial. Selanjutnya, tahap permutasi dilakukan melalui dua proses, yaitu ShiftRows dan MixColumns. ShiftRows menggeser baris-baris dalam matriks data ke kiri dengan jumlah tertentu untuk menghilangkan pola, sedangkan MixColumns mencampurkan data dalam kolom dengan operasi matematika di medan Galois guna meningkatkan difusi bit dalam blok data. Tahap terakhir pada setiap putaran disebut AddRoundKey, yaitu proses penggabungan blok data dengan kunci putaran (round key) melalui operasi XOR. Kunci ini dihasilkan melalui proses ekspansi dari kunci utama yang diberikan pengguna. Seluruh proses ini berlangsung dalam 10, 12, atau 14 putaran tergantung panjang kunci yang digunakan (128, 192, atau 256 bit). Algoritma Advanced Encryption Standard (AES) bekerja dengan memproses data dalam blok tetap berukuran 128 bit, dan mendukung tiga variasi panjang kunci yaitu 128 bit, 192 bit, dan 256 bit. Panjang kunci ini menentukan jumlah putaran (rounds) enkripsi: 10 putaran untuk AES-128, 12 putaran untuk AES-192, dan 14 putaran untuk AES-256. Semakin panjang kunci, semakin tinggi tingkat keamanannya, meskipun berdampak pada performa dan kebutuhan sumber daya (Guy-Cedric & R., 2018). AES dirancang untuk memproses blok data 128-bit dengan operasi matematis yang dapat dioptimalkan secara signifikan, baik dalam perangkat lunak maupun perangkat keras. Hal ini menjadikannya sangat ideal untuk digunakan dalam aplikasi real-time seperti komunikasi data, sistem cloud computing, hingga transaksi digital. waktu enkripsi rata-rata sebesar 12 milidetik dan waktu dekripsi sebesar 15 milidetik, jauh lebih cepat dibandingkan algoritma RSA yang mencatat waktu di atas 90 milidetik untuk enkripsi dan dekripsi (Aswandi et al., 2025). Efisiensi ini tidak hanya ditunjukkan oleh kecepatan proses, tetapi juga dalam hal konsumsi sumber daya, di mana AES tetap dapat dijalankan secara optimal pada perangkat dengan spesifikasi rendah. Kecepatan ini diperkuat oleh struktur algoritma AES yang mendukung paralelisasi proses enkripsi, sehingga memungkinkan implementasi efisien dalam arsitektur multithreaded maupun perangkat keras khusus seperti FPGA dan GPU. Selain itu, dalam lingkungan dengan lalu lintas data besar, efisiensi AES memberikan keuntungan signifikan dalam hal throughput sistem. Oleh karena itu, kombinasi antara efisiensi waktu dan pemanfaatan sumber daya yang ringan menjadikan AES sebagai salah satu algoritma yang paling banyak diadopsi dalam sistem keamanan modern (Nino, 2023).

4.2 Karakteristik Algoritma RSA

RSA (Rivest-Shamir-Adleman) merupakan algoritma kriptografi asimetris yang mendasarkan proses enkripsi dan dekripsinya pada prinsip matematika bilangan prima dan aritmatika modular. Algoritma ini menggunakan dua kunci berbeda, yaitu kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Proses pembangkitan kunci RSA melibatkan pemilihan dua bilangan prima besar, yang kemudian dikalikan untuk menghasilkan modulus (n), serta perhitungan eksponen publik dan privat berdasarkan fungsi totien Euler. Keamanan RSA sangat bergantung pada kesulitan faktorisasi bilangan besar menjadi faktor primanya, yang hingga kini belum ditemukan algoritma efisien untuk menyelesaikannya secara cepat (Arifin et al., 2009). RSA unggul dalam aspek autentikasi dan pertukaran kunci secara aman. Karena menggunakan dua kunci berbeda, RSA memungkinkan pengirim untuk mengenkripsi pesan dengan kunci publik penerima, dan hanya penerima yang dapat mendekripsi pesan tersebut



Gambar 3. 1 Proses Enkripsi RSA

menggunakan kunci privatnya. Selain itu, RSA juga digunakan dalam pembuatan tanda tangan digital, di mana pengirim mengenkripsi hash pesan dengan kunci privatnya, dan penerima dapat memverifikasi keaslian pesan menggunakan kunci publik pengirim. Hal ini menjadikan RSA sangat penting dalam protokol keamanan seperti SSL/TLS dan sistem sertifikat digital (Albert Ginting et al., 2015). Meskipun RSA sangat aman, algoritma ini memiliki kelemahan dalam hal kecepatan, terutama saat digunakan untuk mengenkripsi data dalam jumlah besar. Proses enkripsi dan dekripsi RSA melibatkan operasi eksponensial dengan bilangan besar, yang memerlukan waktu dan sumber daya komputasi yang lebih tinggi dibandingkan algoritma simetris seperti AES. Penelitian oleh Sulistiyorini dan Prihanto (2023) menunjukkan bahwa RSA membutuhkan waktu lebih lama dalam proses dekripsi dibandingkan RSA-CRT (varian RSA yang dioptimalkan), terutama saat menangani data teks berukuran besar (Sulistiyorini & Prihanto, 2020). RSA telah diimplementasikan secara luas dalam berbagai sistem keamanan digital. Algoritma ini digunakan dalam perangkat lunak komersial, sistem operasi (seperti Windows dan macOS), kartu pintar (smart card), serta protokol komunikasi aman seperti S/MIME, SSL, dan VPN. Selain itu, RSA juga digunakan oleh lembaga pemerintah dan institusi pendidikan untuk melindungi data sensitif dan menjamin integritas komunikasi. Keandalannya dalam menjaga kerahasiaan dan autentikasi menjadikan RSA sebagai salah satu algoritma kriptografi paling berpengaruh dalam sejarah keamanan informasi (Arifin et al., 2009).

4.3 Perbandingan AES dan RSA

AES (Advanced Encryption Standard) dan RSA (Rivest-Shamir-Adleman) merupakan dua algoritma kriptografi yang memiliki perbedaan fundamental dalam pendekatan dan aplikasinya. AES adalah algoritma enkripsi simetris yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi, sementara RSA adalah algoritma enkripsi asimetris yang menggunakan sepasang kunci berbeda yaitu kunci publik dan kunci privat. Perbedaan mendasar ini memberikan dampak signifikan pada kinerja dan penggunaan kedua algoritma tersebut, dimana AES menghadapi

masalah manajemen kunci simetris yang dapat diatasi dengan mengintegrasikan RSA untuk pertukaran kunci yang aman (Rath et al., 2024).

Dari segi kecepatan dan efisiensi, AES memiliki keunggulan yang sangat jelas dibandingkan RSA. AES jauh lebih cepat dalam proses enkripsi dan dekripsi dibandingkan RSA, terutama untuk enkripsi data dalam jumlah besar, serta lebih efisien secara komputasional sehingga cocok untuk perangkat dengan sumber daya terbatas. Keunggulan kecepatan AES membuatnya ideal untuk aplikasi yang memerlukan enkripsi volume data besar seperti VPN, jaringan wireless, dan solusi penyimpanan data. Sebaliknya, RSA memerlukan operasi matematika yang kompleks seperti pemfaktoran bilangan prima besar dan eksponensial modular, yang membuat prosesnya jauh lebih lambat.

Tingkat keamanan kedua algoritma bergantung pada panjang kunci yang digunakan, namun dengan pendekatan yang berbeda. AES dianggap sangat aman dan tidak ada serangan praktis yang diketahui dapat memecahkannya. ES dengan kunci 128-bit sudah dianggap sangat aman untuk sebagian besar aplikasi, sementara untuk keamanan jangka panjang dapat menggunakan kunci 256-bit. RSA memerlukan kunci yang jauh lebih panjang untuk mencapai tingkat keamanan yang setara, dimana RSA 2048-bit setara dengan AES 128-bit. AES-128 umumnya lebih cepat dibandingkan opsi bit yang lebih tinggi karena menggunakan panjang kunci yang lebih pendek, menghasilkan proses enkripsi dan dekripsi yang lebih cepat. Dalam hal manajemen kunci, kedua algoritma memiliki tantangan yang berbeda. AES menghadapi masalah distribusi kunci yang aman, karena kunci yang sama harus dimiliki oleh pengirim dan penerima tanpa diketahui pihak lain. RSA mengatasi masalah ini dengan konsep kunci publik yang dapat dibagikan secara terbuka, namun menghadapi tantangan dalam hal autentikasi kunci publik dan manajemen sertifikat digital. Kompleksitas manajemen kunci RSA memerlukan infrastruktur kunci publik (PKI) yang lebih rumit dibandingkan dengan sistem kunci simetris AES.

Dalam hal manajemen kunci, kedua algoritma memiliki tantangan yang berbeda. AES menghadapi masalah distribusi kunci yang aman, karena kunci yang sama harus dimiliki oleh pengirim dan penerima tanpa diketahui pihak lain. RSA mengatasi masalah ini dengan konsep kunci publik yang dapat dibagikan secara terbuka, namun menghadapi tantangan dalam hal autentikasi kunci publik dan manajemen sertifikat digital. Kompleksitas manajemen kunci RSA memerlukan infrastruktur kunci publik (PKI) yang lebih rumit dibandingkan dengan sistem kunci simetris AES (Fatima et al., 2022). RSA biasanya digunakan dalam tahap awal komunikasi untuk pertukaran kunci AES secara aman, kemudian AES digunakan untuk enkripsi data aktual karena kecepatannya yang superior. Pendekatan hibrida ini memanfaatkan kelebihan masing-masing algoritma sambil meminimalkan kelemahan mereka.

Perkembangan teknologi masa depan juga mempengaruhi prospek kedua algoritma ini. Ancaman komputasi kuantum telah mendorong penelitian untuk meningkatkan tingkat keberhasilan algoritma kuantum dalam menyerang sistem enkripsi RSA, menunjukkan kerentanan RSA terhadap teknologi kuantum (Mu, 2024). Sementara itu, AES masih resisten terhadap serangan yang menggunakan algoritma kuantum tertentu yang saat ini digunakan dalam komputer kuantum, meskipun penelitian masih terbatas oleh kemampuan perangkat keras saat ini.

4.4 Kelebihan dan Kekurangan Algoritma AES dan RSA

Algoritma AES memiliki karakteristik unggul dalam hal kecepatan pemrosesan dan efisiensi komputasi yang membuatnya sangat cocok untuk aplikasi yang membutuhkan enkripsi data dalam volume besar. Performa superior AES terlihat dari kemampuannya memproses data dengan waktu eksekusi yang relatif singkat dibandingkan algoritma enkripsi lainnya, terutama ketika diimplementasikan pada berbagai ukuran file mulai dari 1 MB hingga 50 MB Keunggulan ini menjadikan AES sebagai pilihan optimal untuk sistem yang memerlukan throughput tinggi dalam proses enkripsi dan dekripsi data. Tingkat keamanan yang ditawarkan oleh AES mencapai standar yang sangat tinggi dengan dukungan kunci hingga 256-bit, memberikan resistensi yang kuat terhadap berbagai jenis serangan kriptografi modern. Algoritma ini telah terbukti mampu mempertahankan integritas data dan confidentiality melalui struktur enkripsi yang robust, bahkan dalam menghadapi serangan differential cryptanalysis dan berbagai teknik penetrasi lainnya (Mohammed et al., 2024) Fleksibilitas AES dalam mendukung multiple block cipher modes seperti CBC, ECB, dan CTR memberikan adaptabilitas yang tinggi sesuai dengan kebutuhan spesifik aplikasi keamanan.

Meskipun memiliki keunggulan signifikan, AES menghadapi beberapa keterbatasan fundamental dalam implementasinya, terutama terkait dengan kompleksitas komputasi yang meningkat seiring dengan ukuran kunci yang digunakan. Penelitian menunjukkan bahwa peningkatan ukuran kunci dan ukuran file secara proporsional memperpanjang waktu yang diperlukan untuk proses enkripsi dan dekripsi, yang dapat menjadi bottleneck dalam sistem dengan resource terbatas. Selain itu, AES memiliki kerentanan inherent dalam hal key management, dimana kompromisnya terhadap kunci tunggal yang digunakan untuk enkripsi dan dekripsi dapat mengakibatkan total compromise terhadap keamanan sistem secara keseluruhan. Karakteristik simetris dari AES menciptakan tantangan tersendiri dalam distribusi kunci, terutama dalam environment yang tidak terpercaya atau komunikasi jarak jauh. Ketergantungan pada shared secret key membuat AES kurang optimal untuk skenario dimana pihak-pihak yang berkomunikasi tidak memiliki channel yang secure untuk pertukaran kunci awal. Hal ini membatasi implementasi AES dalam konteks public communication dan memerlukan mekanisme tambahan untuk key exchange yang dapat meningkatkan kompleksitas sistem secara keseluruhan.

RSA memberikan solusi elegant untuk masalah key distribution melalui implementasi public-key cryptography yang memungkinkan komunikasi secure tanpa memerlukan pertukaran kunci rahasia sebelumnya. Keunggulan fundamental RSA terletak pada kemampuannya memisahkan kunci public dan private, dimana pemilik private key dapat menjaga kerahasiaan kunci tersebut sementara recipient hanya perlu menggunakan public key untuk verifikasi atau enkripsi pesan (Mu, 2024). Fleksibilitas ini menjadikan RSA sangat cocok untuk aplikasi digital signature dan authentication dalam sistem terdistribusi.

Robustness RSA dalam menghadapi various cryptographic attacks telah terbukti melalui track record penggunaannya yang ekstensif dalam industri keamanan informasi selama beberapa dekade. Algoritma ini memberikan foundation yang solid untuk implementasi secure communication protocols seperti SSL/TLS dan berbagai framework keamanan lainnya. Kemampuan RSA dalam mendukung non-repudiation melalui digital signature membuatnya indispensable dalam aplikasi yang memerlukan authenticity dan integrity verification.

Performa RSA dalam hal kecepatan komputasi menjadi limitation utama yang membatasi penggunaannya untuk enkripsi data dalam volume besar. Kompleksitas mathematical operations yang involved dalam RSA, terutama operasi modular exponentiation dengan bilangan prime yang besar, mengakibatkan computational overhead yang signifikan dibandingkan dengan symmetric encryption algorithms seperti AES. Keterbatasan ini membuat RSA kurang praktis untuk real-time encryption applications atau scenarios yang memerlukan high-throughput data processing. Kebutuhan memory yang substantial untuk menyimpan kunci RSA, terutama untuk key sizes yang besar seperti 2048-bit atau 4096-bit, menciptakan tantangan dalam implementasi pada devices dengan resource constraints. Penelitian comparative menunjukkan bahwa RSA memerlukan storage space yang lebih besar dibandingkan AES, yang dapat menjadi bottleneck dalam embedded systems atau IoT devices (Mohammed et al., 2024) .Selain itu, RSA menghadapi ancaman potensial dari quantum computing, dimana algoritma quantum seperti Shor's algorithm dapat mengompromisikan keamanan RSA dengan kunci ukuran standar saat ini, meskipun threat ini masih bersifat theoretical dalam konteks practical implementation.

5. KESIMPULAN

Berdasarkan analisis komprehensif yang telah dilakukan terhadap algoritma Advanced Encryption Standard (AES) dan Rivest-Shamir-Adleman (RSA), dapat disimpulkan bahwa kedua algoritma kriptografi ini memiliki karakteristik dan keunggulan yang berbeda namun saling komplementer dalam menjaga keamanan data digital. Penelitian ini mengungkapkan bahwa pemilihan algoritma yang tepat sangat bergantung pada konteks aplikasi, kebutuhan keamanan, dan sumber daya sistem yang tersedia. Algoritma AES menunjukkan superioritas dalam aspek efisiensi dan kecepatan pemrosesan data, dengan waktu enkripsi rata-rata hanya 12 milidetik dan dekripsi 15 milidetik, jauh lebih cepat dibandingkan RSA yang membutuhkan waktu di atas 90 milidetik untuk kedua proses tersebut. Keunggulan ini menjadikan AES sebagai pilihan ideal untuk aplikasi yang memerlukan enkripsi volume data besar dalam waktu real-time, seperti sistem cloud computing, komunikasi data, dan transaksi digital. Fleksibilitas AES dalam mendukung berbagai ukuran kunci (128, 192, dan 256 bit) dan multiple block cipher modes memberikan adaptabilitas tinggi untuk berbagai kebutuhan keamanan. Di sisi lain, algoritma RSA memberikan solusi fundamental untuk masalah distribusi kunci melalui implementasi public-key cryptography yang memungkinkan komunikasi aman tanpa pertukaran kunci rahasia sebelumnya. Kemampuan RSA dalam memisahkan kunci publik dan privat menjadikannya sangat cocok untuk aplikasi digital signature, autentikasi, dan non-repudiation. Robustness RSA telah terbukti melalui implementasi ekstensif dalam protokol keamanan standar industri seperti SSL/TLS dan infrastruktur kunci publik (PKI).

Perbandingan kedua algoritma menunjukkan bahwa AES unggul dalam hal kecepatan dan efisiensi komputasi, sementara RSA unggul dalam aspek manajemen kunci dan autentikasi. Namun, masing-masing algoritma juga memiliki keterbatasan yang signifikan. AES menghadapi tantangan dalam distribusi kunci yang aman dan vulnerability terhadap total compromise jika kunci tunggal terkompromisasi. Sementara itu, RSA memiliki keterbatasan dalam hal kecepatan komputasi, kebutuhan memori yang besar, dan potensi ancaman dari quantum computing di masa depan. Solusi optimal dalam implementasi praktis adalah pendekatan hibrida yang memanfaatkan kelebihan kedua algoritma secara sinergis. RSA digunakan untuk tahap awal komunikasi dalam pertukaran kunci AES secara aman, kemudian AES digunakan

untuk enkripsi data aktual karena kecepatannya yang superior. Pendekatan ini telah terbukti efektif dalam berbagai implementasi nyata, mulai dari sistem perbankan digital, cloud computing, hingga aplikasi e-government dan e-commerce. Implementasi kedua algoritma dalam konteks Indonesia menunjukkan hasil yang positif dalam berbagai sektor. Studi kasus implementasi AES dalam cloud computing perbankan dan RSA dalam sistem digital signature pemerintahan membuktikan bahwa teknologi kriptografi modern dapat diadaptasi dengan baik untuk kebutuhan spesifik Indonesia. Kombinasi RSA-AES-steganografi dalam sistem keamanan data pemerintahan dan penerapan super enkripsi dalam pengamanan data rekam medis menunjukkan evolusi signifikan dalam praktik keamanan informasi di Indonesia.

Menghadapi tantangan masa depan, kedua algoritma perlu terus dikembangkan untuk mengantisipasi ancaman teknologi quantum computing. AES menunjukkan resistensi yang lebih baik terhadap serangan quantum dibandingkan RSA, namun penelitian post-quantum cryptography tetap diperlukan untuk memastikan keamanan jangka panjang. Rekomendasi untuk penelitian selanjutnya adalah pengembangan algoritma hibrida yang lebih efisien, optimalisasi implementasi untuk IoT devices, dan pengembangan quantum-resistant cryptography. Secara keseluruhan, algoritma AES dan RSA tetap menjadi foundation penting dalam ekosistem keamanan informasi modern. Pemahaman mendalam terhadap karakteristik, kelebihan, dan keterbatasan masing-masing algoritma menjadi kunci dalam implementasi sistem keamanan yang efektif dan robust. Pendekatan hibrida yang memanfaatkan kekuatan kedua algoritma secara optimal merupakan strategi terbaik untuk menghadapi kompleksitas tantangan keamanan data di era digital saat ini dan masa depan.

DAFTAR PUSTAKA

Albert Ginting, R. Rizal Isnanto, & Ike Pertiwi Windasari. (2015). Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. *Jurnal Teknologi Dan Sistem Komputer*, *3*(2), 253–258. https://jtsiskom.undip.ac.id/article/view/12009

Ananda, S. P., & Lukman, S. (2022). Analisa Metode Kriptografi Modern Advance Encryption Standard (AES) 128 Bit dalam Mengenkripsi dan Mendekripsi File Dokumen Digital. *Jurnal Ilmiah Komputasi*, *21*(3), 333–344. https://doi.org/10.32409/jikstik.21.3.2973

Arifin, Z., kunci, K., Rsa, A., Privat, K., & Publik, K. (2009). Studi Kasus Penggunaan Algoritma RSA Sebagai Algoritma Kriptografi yang Aman. *Jurnal Informatika Mulawarman Program Studi Ilmu Komputer Universitas Mulawarman*, *4*(3), 7–14.

Aswandi, A. S., Pradipta, A., Informasi, S., Sembilanbelas, U., & Kolaka, N. (2025). *Analisis performa dan keamanan implementasi kriptografi aes untuk penyandian dokumen berbasis web*. *8*(1), 24–32.

Azlin, Musadat, F., & Nur, J. (2018). Aplikasi Kriptografi Keamanan Data Menggunakan Algoritma Base64. *Jurnal Informatika*, *7*(2), 1–5.

Fajrin, A. M., Kelvin, C., Owen, B., & Aji, B. (2024). *Perbandingan Performa dari Algoritma AES dan RSA dalam Keamanan Transaksi*. *5*(2), 696–705.

Fatima, S., Rehman, T., Fatima, M., Khan, S., & Ali, M. A. (2022). Comparative Analysis of Aes and Rsa Algorithms for Data Security in Cloud Computing †. *Engineering Proceedings*, *20*(1). https://doi.org/10.3390/engproc2022020014

Guy-Cedric, T. B. I., & R., S. (2018). A Comparative Study on AES 128 BIT AND AES 256 BIT. *International Journal of Scientific Research in Computer Science and Engineering*,

6(4), 30–33. https://doi.org/10.26438/ijsrcse/v6i4.3033

Indonesia, U. P. (2023). *Machine Translated by Google Jurnal Ilmu Komputer Indonesia Machine Translated by Google*. *7286*(127), 2401–2413.

Irawan, C., & Rachmawanto, E. H. (2021). Keamanan Data Menggunakan Gabungan Kriptografi AES dan RSA. *Proceeding SENDIU*, *l*(2), 978–979.

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

Mohammed, Z. A., Gheni, H. Q., Hussein, Z. J., & Al-Qurabat, A. K. M. (2024). Advancing Cloud Image Security via AES Algorithm Enhancement Techniques. *Engineering, Technology and Applied Science Research*, *14*(1), 12694–12701. https://doi.org/10.48084/etasr.6601

Mu, C. (2024). Application of optimizing advanced encryption standard encryption algorithm in secure communication of vehicle controller area network bus. *Frontiers in Mechanical Engineering*, *10*(July), 1–11. https://doi.org/10.3389/fmech.2024.1407665

Nasution, A. N., Syahfitri, A., Indra, Z., Studi, P., Komputer, I., Medan, N., Medan, K., Utara, P. S., & Nasution, A. N. (2024). *Implementasi Algoritma Kriptografi Modern melalui Google Colab : Studi Kasus AES dan RSA*. *2*(2), 841–845.

Nelakuditi, N. C., Namburi, N. K., Sayyad, J., Rudraraju, D. V., Govindan, R., & Rao, P. V. (2024). Secure File Operations: Using Advanced Encryption Standard for Strong Data Protection. *International Journal of Safety and Security Engineering*, *14*(3), 1007–1014. https://doi.org/10.18280/ijsse.140330

Nino, B. E. (2023). Perbandingan Performa Algoritma AES dan Twofish Menggunakan Metode Strict Avalanche Criterion pada Nomor Induk Kependudukan Indonesia. *Jurnal Teknologi Informasi*, *9*(1), 19–29. https://doi.org/10.52643/jti.v9i1.2994

Rath, S., Priyadarshini, S. B. B., Patel, D. K., & Sahu, P. K. (2024). *INTELLIGENT SYSTEMS AND APPLICATIONS IN AES-RSA : An Innovative Hybrid Security Framework for File Authentication , Integrity , and Data Secrecy Model*. *12*, 303–312.

Sulistiyorini, S., & Prihanto, A. (2020). Perbandingan Efisiensi Algoritma RSA dan RSA-CRT Dengan Data Teks Berukuran Besar. *Journal of Informatics and Computer Science (JINACS)*, *1*(02), 84–90. https://doi.org/10.26740/jinacs.v1n02.p84-90

Halaman ini sengaja dikosongkan