JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 2 No: 6, Desember 2025 – Januari 2026
E-ISSN : 3046-4560

Analisis Perbandingan Algoritma Kriptografi Aes Dan Rsa Terhadap Keamanan Dan Waktu Proses Enkripsi Data Teks

Comparative Analysis of AES and RSA Cryptographic Algorithms on Security and Processing Time of Text Data Encryption

Surizky Ananda[1], Ibnu Rusydi[2], Muhammad Faruqi[3], M.Wahyu Ramadhan[4], M. N. Alfi Syahrin[5], Riko Prananda Prayugo[6], Maulana Ihsan[7]
Universitas Islam Negeri Sumatera Utara
Email: surizkyananda@gmail.com[1], ibnurusydi@uinsu.ac.id[2], muhammad0701222109@uinsu.ac.id[3], m.wahyu0701222107@uinsu.ac.id[4], iradatul22@gmail.com[5], prayugopranandariko@gmail.com[6], maulana0701221026@uinsu.ac.id[7]

Article Info

Article history :
Received : 24-12-2025
Revised : 26-12-2025
Accepted : 28-12-2025
Pulished : 30-12-2025

Abstract

Data security is a crucial aspect of digital information systems, particularly in protecting text data from unauthorized access. Cryptography plays an important role in ensuring data confidentiality through encryption algorithms. This study aims to analyze and compare the cryptographic algorithms Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) based on security level and encryption processing time for text data. The research method involves experimental testing by performing encryption and decryption processes on text data with various sizes. The AES algorithm is implemented using symmetric keys, while the RSA algorithm utilizes public and private key pairs. The evaluation parameters include encryption time, decryption time, and theoretical security characteristics of each algorithm. The experimental results show that AES has significantly faster encryption and decryption times compared to RSA, especially when processing large text data. Meanwhile, RSA provides strong security for key exchange and authentication purposes but requires higher computational cost. Based on the analysis, AES is more efficient for securing large-scale text data, whereas RSA is more suitable for key distribution and secure authentication mechanisms.

Keywords* : *Cryptography, AES, RSA

Abstrak

Keamanan data merupakan aspek penting dari sistem informasi digital, khususnya dalam melindungi data teks dari akses yang tidak sah. Kriptografi memainkan peran penting dalam memastikan kerahasiaan data melalui algoritma enkripsi. Studi ini bertujuan untuk menganalisis dan membandingkan algoritma kriptografi Advanced Encryption Standard (AES) dan Rivest Shamir Adleman (RSA) berdasarkan tingkat keamanan dan waktu pemrosesan enkripsi untuk data teks. Metode penelitian melibatkan pengujian eksperimental dengan melakukan proses enkripsi dan dekripsi pada data teks dengan berbagai ukuran. Algoritma AES diimplementasikan menggunakan kunci simetris, sedangkan algoritma RSA menggunakan pasangan kunci publik dan privat. Parameter evaluasi meliputi waktu enkripsi, waktu dekripsi, dan karakteristik keamanan teoritis dari masing-masing algoritma. Hasil eksperimen menunjukkan bahwa AES memiliki waktu enkripsi dan dekripsi yang jauh lebih cepat dibandingkan dengan RSA, terutama saat memproses data teks berukuran besar. Sementara itu, RSA memberikan keamanan yang kuat untuk pertukaran kunci dan tujuan otentikasi tetapi membutuhkan biaya komputasi yang lebih tinggi. Berdasarkan

analisis, AES lebih efisien untuk mengamankan data teks skala besar, sedangkan RSA lebih cocok untuk distribusi kunci dan mekanisme otentikasi yang aman.

Kata Kunci : Kriptografi; AES; RSA

PENDAHULUAN

Perkembangan teknologi informasi yang pesat menyebabkan peningkatan pertukaran data digital, termasuk data teks yang bersifat penting dan rahasia. Data tersebut rentan terhadap berbagai ancaman keamanan seperti pencurian, penyadapan, dan manipulasi informasi. Oleh karena itu, diperlukan mekanisme pengamanan data yang efektif untuk menjaga kerahasiaan dan integritas informasi.

Kriptografi merupakan salah satu teknik yang banyak digunakan dalam pengamanan data dengan cara mengubah informasi asli menjadi bentuk yang tidak dapat dipahami tanpa kunci tertentu. Algoritma kriptografi terbagi menjadi dua jenis utama, yaitu algoritma simetris dan asimetris. Advanced Encryption Standard (AES) adalah algoritma kriptografi simetris yang dikenal memiliki kecepatan tinggi dan tingkat keamanan yang kuat. Sementara itu, Rivest Shamir Adleman (RSA) merupakan algoritma kriptografi asimetris yang banyak digunakan untuk pertukaran kunci dan autentikasi.

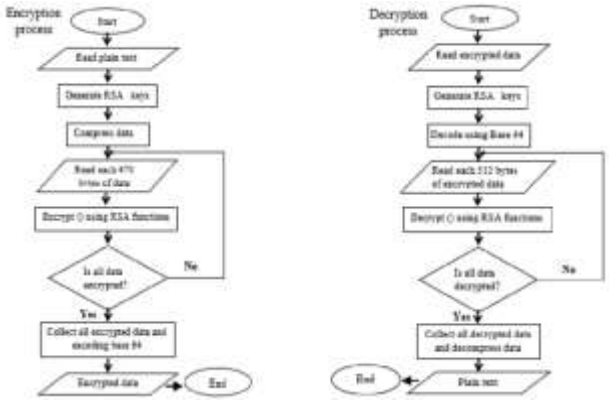
Penelitian ini bertujuan untuk menganalisis perbandingan algoritma AES dan RSA berdasarkan tingkat keamanan dan waktu proses enkripsi data teks, sehingga dapat diketahui algoritma yang paling sesuai untuk kebutuhan pengamanan data tertentu.

METODE PENELITIAN

Diagram alur di atas menggambarkan tahapan pengolahan data yang dilakukan dalam penelitian ini. Proses dimulai dengan pengunduhan dataset *unigram_freq.csv* dari platform Kaggle. Selanjutnya, dilakukan seleksi data dengan mengambil 500 kata dengan frekuensi tertinggi sebagai data uji. Data yang terpilih kemudian melalui tahap pra-pemrosesan, meliputi penggabungan kata menjadi *plaintext* dan konversi data ke format byte menggunakan encoding UTF-8.

Untuk menguji kinerja algoritma secara lebih komprehensif, *plaintext* dibagi ke dalam beberapa variasi ukuran data. Setiap variasi data selanjutnya dienkripsi menggunakan dua algoritma kriptografi, yaitu AES-128 dengan mode CBC dan RSA-2048 dengan skema padding OAEP. Pada setiap proses enkripsi dan dekripsi, dilakukan pengukuran waktu eksekusi untuk memperoleh data performa algoritma.

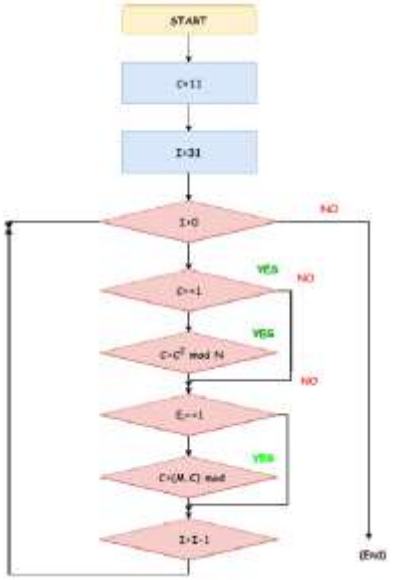
JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 2 No: 6, Desember 2025 – Januari 2026
E-ISSN : 3046-4560



Gambar 1 Diagram Alur Pengolahan Data Penelitian

Algoritma RSA

Algoritma RSA bekerja dengan memanfaatkan pasangan kunci publik dan kunci privat yang dibentuk dari dua bilangan prima besar. Proses enkripsi dilakukan menggunakan kunci publik dengan operasi perpangkatan modular, sedangkan proses dekripsi menggunakan kunci privat. Secara matematis, proses RSA dapat dirangkum dalam satu persamaan, yaitu $M = (M^e \bmod n)^d \bmod n$, yang menunjukkan bahwa data yang dienkripsi dapat dikembalikan ke bentuk semula menggunakan kunci privat yang sesuai.



Gambar 2. Flowchart algortima RSA

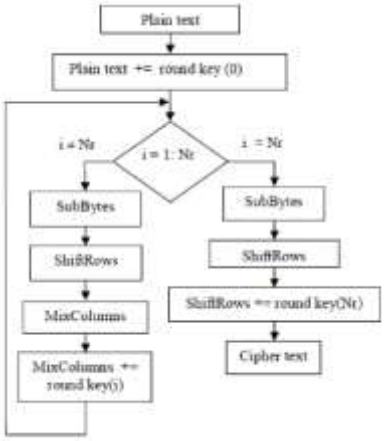
Gambar 2 menunjukkan alur kerja algoritma RSA yang diawali dengan proses pembangkitan kunci publik dan kunci privat menggunakan dua bilangan prima besar. Selanjutnya, plaintext dienkripsi menggunakan kunci publik untuk menghasilkan ciphertext. Proses dekripsi dilakukan menggunakan kunci privat sehingga ciphertext dapat dikembalikan ke bentuk plaintext semula.

Algortima AES

Algoritma Advanced Encryption Standard (AES) merupakan algoritma kriptografi kunci simetris yang memiliki tingkat keamanan tinggi serta efisiensi komputasi yang baik. Dalam penelitian ini, AES diimplementasikan menggunakan kunci 128 bit dengan mode operasi Cipher Block Chaining (CBC) untuk mengamankan data teks dari dataset *unigram_freq.csv*. Pemilihan AES-128 didasarkan pada standar keamanan yang luas digunakan serta kemampuannya dalam mengenkripsi data berukuran besar secara efisien.

Hasil pengujian menunjukkan bahwa AES memiliki kinerja enkripsi dan dekripsi yang cepat dan stabil pada berbagai ukuran data. Waktu proses meningkat secara linier seiring bertambahnya jumlah data, menandakan kompleksitas waktu yang efisien dan performa yang konsisten. Kesetaraan waktu enkripsi dan dekripsi menunjukkan bahwa AES dapat diandalkan untuk aplikasi yang membutuhkan proses kriptografi berulang, seperti penyimpanan dan transmisi data terenkripsi.

Dari sisi skalabilitas, AES mampu menangani peningkatan jumlah data tanpa mengalami lonjakan waktu yang signifikan, sehingga cocok digunakan untuk pengamanan data teks berskala besar. Ditinjau dari aspek keamanan, penggunaan kunci 128 bit dan inisialisasi vektor (IV) acak pada mode CBC efektif mencegah pola berulang pada ciphertext, sehingga meningkatkan kerahasiaan data. Seluruh hasil dekripsi berhasil dikembalikan ke bentuk plaintext semula, yang menunjukkan bahwa implementasi AES pada penelitian ini telah berjalan dengan benar dan sesuai dengan spesifikasi kriptografi.



Gambar 3. Flowchart algortima AES

Gambar 3 menunjukkan alur kerja algoritma AES yang diawali dengan proses pembangkitan round key melalui key expansion. Plaintext kemudian diproses melalui beberapa putaran enkripsi yang terdiri dari operasi substitusi, permutasi, dan transformasi matriks. Proses dekripsi dilakukan dengan operasi invers untuk mengembalikan ciphertext ke bentuk plaintext semula.

HASIL DAN PEMBAHASAN

Analisis Frekuensi Kata

Tabel 1.1

No	Kata	Frekuensi
1	the	23135851162
2	of	13151942776
3	and	12997637966
4	to	12136980858
5	a	9081174698
6	in	8469404971
7	for	5933321709
8	is	4705743816
9	on	3750423199
10	that	3400031103
11	by	3350048871
12	this	3227894564
13	with	3183110675
14	i	3086225277
15	you	2996181025

Tabel di atas menampilkan sampel data dari dataset *unigram_freq.csv* yang diperoleh dari platform Kaggle. Dataset ini berisi daftar kata bahasa Inggris beserta frekuensi kemunculannya dalam korpus teks berskala besar. Pada penelitian ini, data tersebut digunakan sebagai sumber pembentukan plaintext untuk menguji kinerja algoritma kriptografi AES dan RSA. Hanya sebagian kecil data ditampilkan sebagai representasi, sedangkan keseluruhan data digunakan dalam proses pengujian.

Hasil Pengujian RSA dan AES

Tabel 1.2

No	Algoritma	Jumlah Kata	Ukuran (Byte)	Data Waktu (ms)	Enkripsi Waktu (ms)	Dekripsi	Validasi
1	AES-128	50	204	0.0217	0.0334		True
2	RSA-2048	50	190	0.7815	1.9138		True
3	AES-128	100	441	0.0143	0.0131		True
4	RSA-2048	100	190	0.7632	2.4004		True
5	AES-128	150	714	0.0138	0.0138		True
6	RSA-2048	150	190	0.8228	2.0711		True
7	AES-128	200	1000	0.0165	0.0145		True
8	RSA-2048	200	190	0.7505	2.2495		True

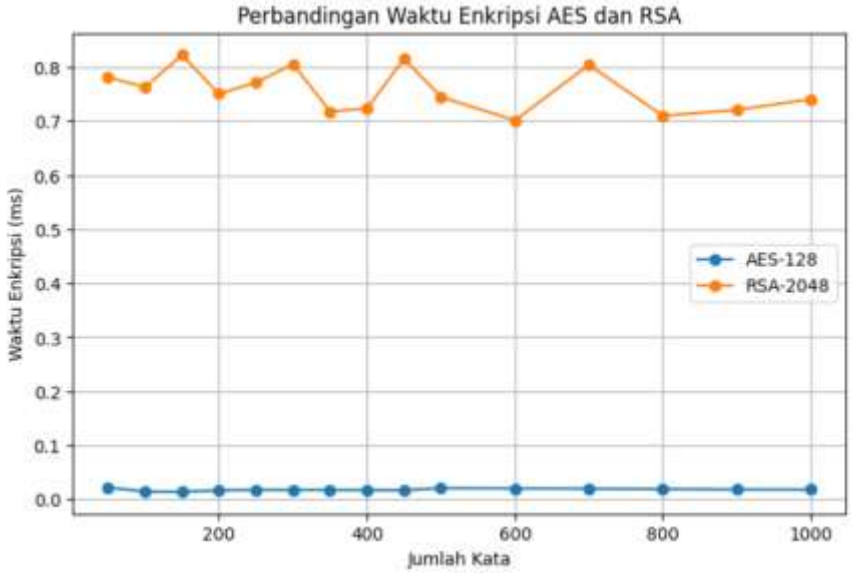
No	Algoritma	Jumlah Kata	Ukuran (Byte)	Data Waktu (ms)	Enkripsi Waktu (ms)	Dekripsi	Validasi
9	AES-128	250	1326	0.0174	0.0169		True
10	RSA-2048	250	190	0.7722	1.9860		True
11	AES-128	300	1628	0.0172	0.0157		True
12	RSA-2048	300	190	0.8056	1.9610		True
13	AES-128	350	1953	0.0174	0.0167		True
14	RSA-2048	350	190	0.7181	1.8623		True
15	AES-128	400	2281	0.0169	0.0176		True
16	RSA-2048	400	190	0.7238	1.8291		True
17	AES-128	450	2596	0.0167	0.0544		True
18	RSA-2048	450	190	0.8159	2.0075		True
19	AES-128	500	2931	0.0205	0.0179		True
20	RSA-2048	500	190	0.7448	1.8392		True
21	AES-128	600	2931	0.0200	0.0198		True
22	RSA-2048	600	190	0.7017	1.9138		True
23	AES-128	700	2931	0.0196	0.0179		True
24	RSA-2048	700	190	0.8044	1.8809		True
25	AES-128	800	2931	0.0188	0.0298		True
26	RSA-2048	800	190	0.7102	1.9209		True
27	AES-128	900	2931	0.0181	0.0184		True
28	RSA-2048	900	190	0.7212	1.8401		True
29	AES-128	1000	2931	0.0179	0.0172		True
30	RSA-2048	1000	190	0.7410	1.8575		True

Berdasarkan hasil pengujian yang disajikan pada Tabel 1.2, algoritma AES-128 menunjukkan kinerja enkripsi dan dekripsi yang sangat cepat dan stabil pada seluruh variasi jumlah kata yang diuji. Waktu enkripsi dan dekripsi AES berada pada kisaran yang relatif rendah dan meningkat secara linier seiring bertambahnya ukuran data. Hal ini menunjukkan bahwa algoritma AES memiliki kompleksitas komputasi yang efisien dan mampu menangani data teks berukuran besar tanpa mengalami penurunan performa yang signifikan.

Sebaliknya, algoritma RSA-2048 menunjukkan waktu proses yang lebih tinggi, khususnya pada tahap dekripsi. Waktu enkripsi RSA berada pada kisaran yang lebih besar dibandingkan AES, sedangkan waktu dekripsinya menunjukkan nilai yang paling dominan akibat kompleksitas operasi eksponensiasi modular dengan kunci privat. Selain itu, meskipun jumlah kata yang diuji meningkat, ukuran data yang diproses oleh RSA relatif konstan karena keterbatasan panjang *plaintext* pada algoritma kriptografi kunci asimetris, sehingga RSA kurang efisien untuk pengamanan data teks berukuran besar secara langsung.

JICN: Jurnal Intelek dan Cendikiawan Nusantara
https://jicnusantara.com/index.php/jicn
Vol : 2 No: 6, Desember 2025 – Januari 2026
E-ISSN : 3046-4560

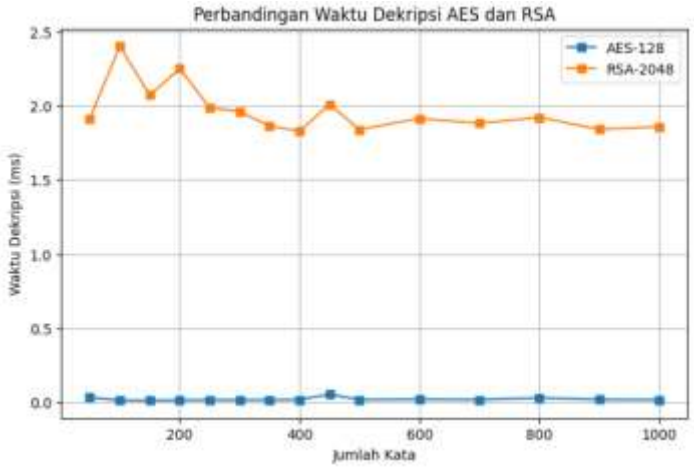
Seluruh pengujian menghasilkan nilai validasi dekripsi bernilai *True*, yang menandakan bahwa kedua algoritma berhasil mengembalikan *plaintext* ke bentuk semula tanpa kehilangan data. Berdasarkan hasil tersebut, dapat disimpulkan bahwa AES-128 lebih unggul dari sisi efisiensi dan skalabilitas dalam pengamanan data teks, sedangkan RSA-2048 lebih sesuai digunakan untuk pengamanan data berukuran kecil atau sebagai mekanisme pertukaran kunci dalam sistem keamanan hybrid.



Gambar 3. Pengujian Enkripsi

Gambar 3 menunjukkan perbandingan waktu enkripsi antara algoritma AES-128 dan RSA-2048 terhadap variasi jumlah kata pada data teks. Berdasarkan grafik, terlihat bahwa waktu enkripsi AES-128 berada pada nilai yang sangat rendah dan relatif konstan meskipun jumlah kata meningkat hingga 1000 kata. Hal ini mengindikasikan bahwa proses enkripsi AES memiliki kompleksitas yang efisien dan mampu menangani peningkatan ukuran data secara linear tanpa penurunan performa yang signifikan.

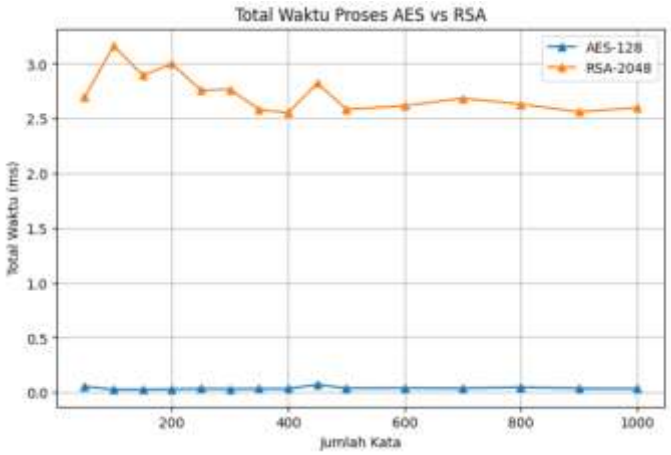
Sebaliknya, waktu enkripsi RSA-2048 berada pada nilai yang jauh lebih tinggi dibandingkan AES dan menunjukkan fluktuasi ringan pada setiap variasi jumlah kata. Kondisi ini disebabkan oleh karakteristik RSA sebagai algoritma kriptografi kunci asimetris yang menggunakan operasi matematika kompleks berbasis eksponensiasi modular. Meskipun ukuran data teks bertambah, waktu enkripsi RSA relatif tidak terpengaruh secara signifikan karena panjang *plaintext* yang diproses dibatasi oleh ukuran kunci.



Gambar 4. Pengujian Deskripsi

Gambar 4 memperlihatkan perbandingan waktu dekripsi antara algoritma AES-128 dan RSA-2048. Hasil pengujian menunjukkan bahwa waktu dekripsi AES tetap rendah dan stabil pada seluruh variasi jumlah kata. Nilai waktu dekripsi yang hampir sebanding dengan waktu enkripsi menunjukkan bahwa AES memiliki beban komputasi yang seimbang antara proses enkripsi dan dekripsi, sesuai dengan karakteristik algoritma kriptografi kunci simetris.

Berbeda dengan AES, algoritma RSA-2048 menunjukkan waktu dekripsi yang paling tinggi dibandingkan seluruh proses lainnya. Waktu dekripsi RSA secara konsisten berada di atas waktu enkripsi karena proses ini melibatkan penggunaan kunci privat dengan perhitungan matematika yang lebih kompleks. Hasil ini menegaskan bahwa RSA memiliki keterbatasan performa pada tahap dekripsi dan kurang efisien jika digunakan untuk pengamanan data teks dalam jumlah besar.



Gambar 5. Pengujian Waktu Proses AES dan RSA

Gambar 5 menunjukkan total waktu proses yang merupakan akumulasi dari waktu enkripsi dan dekripsi pada algoritma AES-128 dan RSA-2048. Dari grafik terlihat bahwa total waktu proses AES tetap berada pada nilai yang sangat rendah dan meningkat secara bertahap seiring

bertambahnya jumlah kata. Hal ini menandakan bahwa AES memiliki efisiensi komputasi yang tinggi dan sangat cocok untuk aplikasi yang membutuhkan pengamanan data teks secara berkelanjutan.

KESIMPULAN

Berdasarkan hasil pengujian dan analisis yang telah dilakukan terhadap algoritma kriptografi AES-128 dan RSA-2048 dalam pengamanan data teks, dapat disimpulkan bahwa kedua algoritma mampu melakukan proses enkripsi dan dekripsi dengan baik, yang ditunjukkan oleh hasil validasi dekripsi bernilai *True* pada seluruh data uji. Hal ini menandakan bahwa implementasi algoritma pada penelitian ini berjalan sesuai dengan prinsip kriptografi yang digunakan.

Algoritma AES-128 menunjukkan kinerja yang sangat efisien dengan waktu enkripsi dan dekripsi yang relatif cepat dan stabil pada seluruh variasi ukuran data. Peningkatan jumlah kata tidak menyebabkan lonjakan waktu proses yang signifikan, sehingga AES terbukti memiliki skalabilitas yang baik dan sangat sesuai untuk pengamanan data teks dalam jumlah besar. Keunggulan ini menjadikan AES sebagai pilihan yang tepat untuk diterapkan pada sistem informasi yang memerlukan proses enkripsi dan dekripsi secara berkelanjutan.

Sebaliknya, algoritma RSA-2048 memiliki waktu proses yang lebih tinggi, khususnya pada tahap dekripsi, akibat kompleksitas perhitungan matematika yang lebih besar. Meskipun demikian, RSA tetap memiliki peran penting dalam sistem keamanan, terutama untuk pengamanan data berukuran kecil dan mekanisme pertukaran kunci. Dengan demikian, hasil penelitian ini menegaskan bahwa penggunaan AES untuk enkripsi data utama dan RSA sebagai pendukung pertukaran kunci merupakan pendekatan yang efektif dalam sistem keamanan data modern.

DAFTAR PUSTAKA

AlgoTRIC. (2024). Symmetric and asymmetric encryption algorithms in AI era. *arXiv*. https://arxiv.org/abs/2412.15237

Anwar, S., Nugroho, A., & Lestari, D. (2024). Komparatif performance model keamanan menggunakan AES 256 dan RSA. *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*. https://jurnal.iaii.or.id/index.php/RESTI/article/view/606

Hadi, A., Prasetyo, B., & Kurniawan, R. (2025). Performance analysis of RSA and AES algorithms in digital image encryption. *JTINFO: Jurnal Teknik Informatika, 4*(1), 197–207. https://journal.unisnu.ac.id/JTINFO/article/view/1049

Haque, M., Rahman, S., & Islam, T. (2024). A comparative analysis of AES, RSA, and 3DES encryption standards. *Management Science Advances*. https://msa-journal.org

International Journal of Research Publication and Reviews. (2022). Comparative study of AES, DES, and RSA for file encryption. *IJRPR*. https://ijrpr.com/uploads/V6ISSUE10/IJRPR53678.pdf

Journal of Computer Science and Information Technology. (2025). Hybrid AES and RSA encryption analysis. *Journal of Computer Science and Information Technology, 1*(2). https://ejournal.publine.or.id

Lingga, A., Sembiring, R., & Hutagalung, T. (2025). Advance encryption standard (AES) dalam mengamankan data aplikasi e-pariwisata. *sudo Jurnal Teknik Informatika*. https://jurnal.ilmubersama.com/index.php/sudo/article/view/923

Nawawi, M., Rahman, A., & Putra, D. (2025). Comparison of AES and RSA encryption performance. *G-Tech: Jurnal Teknologi Terapan*. https://ejournal.uniramalang.ac.id/index.php/gtech

Oktaviani, S., Rizky, F., & Gunawan, I. (2023). Analisis keamanan data dengan algoritma AES. *Jurnal Media Informatika, 4*(2), 97–101. https://ejournal.sisfokomtek.org/index.php/jumin/article/view/435

Olutola, A., & Olumuyiwa, M. (2023). Comparative analysis of encryption algorithms (AES vs RSA). *European Journal of Technology, 7*(1), 1–9. https://ajpojournals.org/journals/EJT/article/view/1312

Permana, R., Siregar, M., & Putri, N. (2024). Mengamankan file rahasia menggunakan hybrid AES dan RSA. *Jurnal Review Pendidikan dan Pengajaran, 7*(1), 2449–2460. https://journal.universitaspahlawan.ac.id/index.php/jrpp/article/view/26156

Prashant, K., Sharma, R., & Verma, S. (2024). Comparative analysis of AES and RSA with other encryption for secure communication. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10*(2). https://ijsrcseit.com

Sholikhatin, S. A., Kuncoro, A. P., Munawaroh, A. L., & Setiawan, G. A. (2022). Comparative study of RSA asymmetric algorithm and AES algorithm for data security. *Edu Komputika Journal, 9*(1), 60–67. https://journal.unnes.ac.id/sju/index.php/edukom/article/view/57389

Tuo, J. (2023). A comparative analysis of AES and RSA algorithms and their integrated application. *ResearchGate*. https://www.researchgate.net/publication/376680083

Zulfikar, M., Hasan, A., & Ramadhan, D. (2023). Analisis kompleksitas waktu dan keamanan RSA, DES, dan AES. *JURNAL SITEBA, 2*(2). https://journal.iteba.ac.id/index.php/jurnalsiteba/article/view/153