Jurnal Sains Teknologi dan Sistem Informasi
journal.yp3a.org/index.php/satesi
Vol. 6 No. 1 (2026) 46 – 51 ISSN Media Elektronik: 2807–8152

Analisis Kinerja AES dan RC6 pada File Multimedia

Sugiyatno[1*], Hafidz Maulana Rahman[2]
[1,2]Informatika, Fakultas Ilmu Komputer, Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia
Email: [1*]sugiyatno@dsn.ubharajaya.ac.id, [2]202210715069@mhs.ubharajaya.ac.id

ABSTRACT

This study aims to analyze and compare the performance of symmetric cryptographic algorithms, namely Advanced Encryption Standard (AES) and Rivest Cipher 6 (RC6), in securing multimedia files. The research employs a quantitative experimental approach using various file formats, including JPG, PNG, MP3, and MP4, with different file sizes. Performance evaluation is conducted based on three main parameters: encryption time, decryption time, and throughput. The implementation is carried out in a controlled local environment using Python to ensure consistency and accuracy of measurements. The results show that AES consistently outperforms RC6 in terms of faster encryption and decryption processes as well as higher and more stable throughput across all tested formats and file sizes. In contrast, RC6 exhibits higher computational overhead due to its complex arithmetic operations, resulting in slower processing time and less stable performance. Furthermore, the findings indicate that file size and format significantly influence algorithm performance, where larger and more complex multimedia data require higher processing time. This study contributes a comprehensive multi-format evaluation framework that provides practical insights for selecting efficient cryptographic algorithms in real-world multimedia security applications.

Keywords: AES, RC6, Multimedia Encryption, Performance Analysis, Throughput.

ABSTRAK

Penelitian ini bertujuan untuk menganalisis dan membandingkan kinerja algoritma kriptografi simetris Advanced Encryption Standard (AES) dan Rivest Cipher 6 (RC6) dalam pengamanan file multimedia. Metode yang digunakan adalah eksperimen kuantitatif dengan data uji berupa berbagai format file, yaitu JPG, PNG, MP3, dan MP4 dengan variasi ukuran. Evaluasi kinerja dilakukan berdasarkan tiga parameter utama, yaitu waktu enkripsi, waktu dekripsi, dan throughput. Implementasi dilakukan dalam lingkungan lokal terkontrol menggunakan Python untuk menjaga konsistensi hasil pengukuran. Hasil penelitian menunjukkan bahwa AES memiliki performa yang lebih unggul dibandingkan RC6, ditunjukkan oleh waktu enkripsi dan dekripsi yang lebih cepat serta nilai throughput yang lebih tinggi dan stabil pada seluruh skenario pengujian. Sebaliknya, RC6 memiliki beban komputasi yang lebih tinggi akibat penggunaan operasi aritmatika kompleks sehingga menghasilkan waktu proses yang lebih lama dan performa yang kurang stabil. Selain itu, ukuran dan jenis file terbukti berpengaruh signifikan terhadap kinerja algoritma, dimana file berukuran besar dan kompleks membutuhkan waktu pemrosesan yang lebih tinggi. Penelitian ini memberikan kontribusi berupa evaluasi komprehensif lintas format multimedia sebagai dasar dalam pemilihan algoritma kriptografi yang efisien pada implementasi nyata.

Kata Kunci: AES, RC6, Enkripsi Multimedia, Analisis Kinerja, Throughput.

1. Pendahuluan

Perkembangan teknologi digital telah meningkatkan volume pertukaran data multimedia, seperti gambar, video, dan dokumen, dalam berbagai aktivitas penyimpanan, komunikasi, dan distribusi informasi. Karakter data multimedia yang cenderung berukuran besar, mudah digandakan, dan sering ditransmisikan melalui jaringan terbuka membuat aspek kerahasiaan dan integritas data menjadi semakin penting. Dalam konteks ini, perlindungan berbasis kriptografi diperlukan agar data tidak mudah diakses, dimodifikasi, atau disalahgunakan oleh pihak yang tidak berwenang. Kebutuhan tersebut semakin relevan karena keamanan multimedia modern tidak hanya menuntut proteksi, tetapi juga efisiensi pemrosesan pada data yang heterogen dan berukuran besar [1].

Diterima Redaksi: 22-02-2026 | Selesai Revisi: 28-03-2026 | Diterbitkan Online: 15-04-2026

Pada ranah kriptografi simetris, Advanced Encryption Standard (AES) merupakan salah satu algoritma yang paling luas digunakan karena memiliki keseimbangan yang baik antara keamanan, interoperabilitas, dan efisiensi implementasi. Tinjauan mutakhir menunjukkan bahwa AES tetap menjadi fondasi penting dalam banyak aplikasi keamanan modern, mulai dari komunikasi jaringan hingga proteksi data pada sistem terdistribusi. Di sisi lain, pemilihan algoritma enkripsi dalam praktik tidak hanya dipengaruhi oleh kekuatan keamanannya, tetapi juga oleh faktor performa seperti waktu proses, efisiensi sumber daya, dan kesesuaian terhadap konteks penggunaan ([2].

Selain AES, RC6 masih relevan untuk dikaji sebagai algoritma pembanding karena memiliki struktur operasi yang berbeda, terutama melalui kombinasi rotasi bergantung data, penjumlahan modular, dan perkalian integer. Kajian yang secara khusus menelaah RC6 pada citra digital menunjukkan bahwa algoritma ini mampu menghasilkan kualitas enkripsi yang baik dan memiliki karakteristik keamanan yang layak untuk data visual. Walaupun referensi yang paling langsung mengenai RC6 pada citra yang saya temukan bersifat lebih lama, sumber tersebut tetap relevan sebagai dasar teoritis karena membahas langsung efisiensi dan evaluasi keamanan RC6 untuk objek digital image [3]

Sejumlah penelitian terdahulu telah membahas performa algoritma enkripsi pada data digital. Survei komparatif tentang teknik enkripsi data menegaskan bahwa pemilihan algoritma perlu mempertimbangkan jenis data, kebutuhan aplikasi, dan efisiensi proses. Pada konteks multimedia, studi komparatif untuk image dan video encryption menunjukkan bahwa evaluasi performa biasanya berfokus pada waktu enkripsi-dekripsi, kesesuaian untuk perangkat bergerak, dan karakteristik media yang diproses [4]. Di tingkat nasional, penelitian tentang AES-CBC pada enkripsi gambar menunjukkan bahwa AES efektif untuk objek citra, sedangkan studi lain pada file gambar dan dokumen memperlihatkan bahwa performa algoritma dapat berbeda bergantung pada jenis file dan parameter evaluasi yang digunakan [5]; [6]. Penelitian pada file video juga menunjukkan bahwa pengujian berbasis AES dapat menghasilkan performa yang baik, tetapi biasanya dibandingkan dengan pendekatan hybrid, bukan secara langsung dengan RC6 [7]. Selain itu, implementasi AES-CBC pada data multi-format menunjukkan bahwa pendekatan berbasis AES dapat diterapkan pada berbagai tipe file, termasuk dokumen, gambar, dan video, sehingga mendukung relevansi evaluasi lintas format pada penelitian ini [8].

Meskipun demikian, masih terdapat beberapa gap penelitian. Pertama, studi yang secara langsung membandingkan AES dan RC6 pada beberapa format file multimedia sekaligus masih terbatas. Kedua, banyak penelitian sebelumnya hanya berfokus pada satu jenis file, misalnya citra saja atau video saja, sehingga belum memberikan gambaran menyeluruh lintas format. Ketiga, parameter evaluasi yang digunakan sering kali belum komprehensif karena lebih banyak menekankan waktu proses atau kualitas enkripsi tertentu, tanpa menggabungkan waktu enkripsi, waktu dekripsi, throughput, dan pengaruh ukuran file dalam satu rancangan pengujian yang seragam. Keempat, studi nasional yang saya verifikasi cenderung membandingkan AES dengan Blowfish, ChaCha20, atau skema hybrid AES+RSA, bukan secara spesifik dengan RC6 pada kumpulan file multimedia yang beragam [5]; [9]; [6].

Berdasarkan gap tersebut, novelty penelitian ini terletak pada evaluasi komprehensif terhadap kinerja algoritma AES dan RC6 pada file multimedia multi-format, yaitu JPG, PNG, MP4, dan PDF, dengan pendekatan eksperimen terstruktur serta parameter pengukuran yang meliputi waktu enkripsi, waktu dekripsi, throughput, dan skalabilitas terhadap ukuran file. Dengan demikian, penelitian ini diarahkan untuk menghasilkan pembandingan yang lebih sistematis dan lebih dekat dengan kebutuhan penggunaan nyata pada pengamanan file multimedia [10]; [2].

Tujuan penelitian ini adalah menganalisis dan membandingkan kinerja AES dan RC6 pada proses enkripsi-dekripsi file multimedia, mengidentifikasi pengaruh format dan ukuran file terhadap performa kedua algoritma, serta menentukan algoritma yang lebih efisien berdasarkan parameter waktu proses dan throughput. Hasil penelitian ini diharapkan dapat menjadi referensi praktis dalam pemilihan algoritma kriptografi untuk pengamanan file multimedia pada lingkungan implementasi nyata [11]; [6]; (Ganesh et al., 2025; [12].

2. Metode Penelitian

Penelitian ini menggunakan pendekatan eksperimen kuantitatif untuk menganalisis dan membandingkan kinerja algoritma kriptografi simetris AES dan RC6 pada file multimedia. Pendekatan eksperimen dipilih karena mampu memberikan hasil yang objektif melalui pengukuran langsung terhadap parameter kinerja seperti waktu proses dan throughput dalam kondisi pengujian yang terkontrol.

2.1. Desain Eksperimen

Desain penelitian dilakukan dengan membandingkan dua algoritma, yaitu AES dan RC6, pada proses enkripsi dan dekripsi file multimedia. Pengujian dilakukan secara sistematis dengan variabel utama berupa jenis file dan ukuran file, sedangkan variabel terikat berupa waktu enkripsi, waktu dekripsi, dan throughput.

Pendekatan ini sejalan dengan penelitian evaluasi performa algoritma kriptografi yang umumnya menggunakan parameter waktu eksekusi dan throughput sebagai indikator utama kinerja [13].

DOI: 10.54259/satesi.v6i1.7523

2.2 Lingkungan Pengujian

Pengujian dilakukan pada lingkungan sistem lokal (offline) untuk memastikan konsistensi hasil tanpa dipengaruhi faktor jaringan. Implementasi algoritma dilakukan menggunakan bahasa pemrograman Python dengan spesifikasi umum perangkat sebagai berikut:

a. Prosesor: Intel Core i5 / setara
b. RAM: minimal 8 GB
c. Sistem Operasi: Windows/Linux
d. Tools: Python (library kriptografi)

Penggunaan lingkungan lokal bertujuan untuk menjaga validitas eksperimen dan menghindari variabel eksternal seperti latency jaringan yang dapat memengaruhi hasil pengukuran performa algoritma [14].

2.3 Data Uji

Data uji yang digunakan dalam penelitian ini terdiri dari beberapa format file multimedia, yaitu:

a. Gambar: JPG dan PNG
b. Video: MP4
c. Dokumen: PDF

Setiap jenis file diuji dalam beberapa ukuran yang berbeda untuk menganalisis pengaruh ukuran data terhadap performa algoritma. Penggunaan variasi ukuran file penting karena performa algoritma kriptografi sangat dipengaruhi oleh jumlah data yang diproses [15].

2.4 Parameter Pengujian

Parameter yang digunakan dalam penelitian ini meliputi:

a. Waktu Enkripsi (*Encryption Time*): Waktu yang dibutuhkan untuk mengubah plaintext menjadi ciphertext.
b. Waktu Dekripsi (*Decryption Time*): Waktu yang dibutuhkan untuk mengembalikan ciphertext menjadi plaintext.
c. Throughput: Laju data yang dapat diproses oleh algoritma per satuan waktu.

Parameter ini merupakan standar dalam penelitian performa algoritma kriptografi karena mencerminkan efisiensi komputasi dan kecepatan pemrosesan data [15].

2.5 Prosedur Pengujian

Prosedur eksperimen dilakukan dengan tahapan sebagai berikut:

a. Menyiapkan dataset file multimedia (JPG, PNG, MP4, PDF).
b. Menentukan ukuran file yang akan diuji.
c. Mengimplementasikan algoritma AES dan RC6 dengan kunci 128-bit.
d. Melakukan proses enkripsi pada setiap file menggunakan kedua algoritma.
e. Mengukur waktu enkripsi menggunakan timestamp sistem.
f. Melakukan proses dekripsi dan mengukur waktu dekripsi.
g. Mengulangi proses pengujian sebanyak beberapa kali untuk mendapatkan nilai rata-rata.
h. Menghitung *throughput* berdasarkan hasil pengukuran waktu enkripsi.

Pendekatan pengulangan eksperimen digunakan untuk meningkatkan reliabilitas data dan mengurangi bias hasil pengukuran [14].

2.6 Perhitungan *Throughput*

Throughput digunakan untuk mengukur efisiensi algoritma dalam memproses data dan dihitung berdasarkan ukuran data yang dienkripsi terhadap waktu yang dibutuhkan.

Secara matematis, throughput dirumuskan sebagai:

$$Throughput = \frac{Ukuran\ Data\ (Byte)}{Waktu\ Endkripsi\ (detik)} \quad (1)$$

Rumus ini banyak digunakan dalam penelitian performa kriptografi untuk mengukur kecepatan algoritma dalam memproses data dalam jumlah besar [15].

2.7 Teknik Analisis Data

Data hasil eksperimen dianalisis menggunakan pendekatan komparatif dengan langkah sebagai berikut:

a. Menghitung rata-rata waktu enkripsi dan dekripsi untuk setiap algoritma.
b. Membandingkan nilai throughput pada masing-masing algoritma.
c. Menganalisis hubungan antara ukuran file dan waktu proses.
d. Mengidentifikasi algoritma yang memiliki performa lebih baik berdasarkan parameter yang diuji.

Analisis komparatif digunakan karena sesuai untuk membandingkan performa dua algoritma dalam kondisi pengujian yang sama dan telah banyak digunakan dalam penelitian kriptografi [10].

3. Hasil dan Pembahasan

3.1. Hasil Eksperimen

Hasil eksperimen diperoleh melalui pengujian algoritma AES dan RC6 pada file multimedia dengan variasi format (JPG, PNG, MP3, MP4) dan ukuran (Small, Medium, Large). Parameter yang dianalisis meliputi waktu enkripsi, waktu dekripsi, dan throughput.

DOI: 10.54259/satesi.v6i1.7523

3.1.1 Perbandingan Kinerja AES dan RC6

Hasil perbandingan kinerja algoritma ditampilkan pada Tabel 1.

Tabel 1. Ringkasan Perbandingan AES dan RC6)

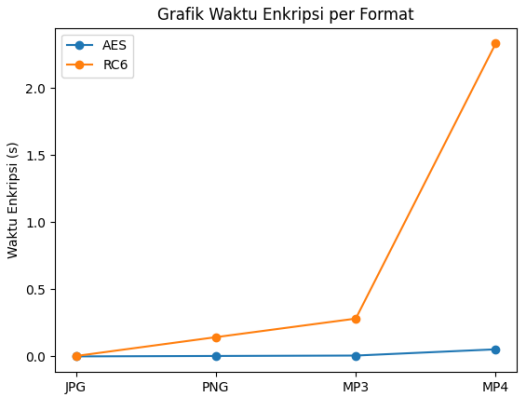
File_name	File_ type	Algo ritma	Waktu Enkripsi (s)	Waktu Dekripsi (s)	Through put (MB/s)
Album Art.jpg	JPG	AES	0.0002	0	136.515008
Album Art.jpg	JPG	RC6	0.0031	0.002	8.807419
1.png	PNG	AES	0.0034	0.0026	534.827945
1.png	PNG	RC6	0.1434	0.1399	12.680718
Franky.mp3	MP3	AES	0.0064	0.0052	552.487502
Franky.mp3	MP3	RC6	0.2817	0.2759	12.552077
VIDEO.mp4	MP4	AES	0.0529	0.037	552.084121
VIDEO.mp4	MP4	RC6	2.3303	2.238	12.532828

Berdasarkan Tabel 1, algoritma AES menunjukkan waktu enkripsi dan dekripsi yang lebih rendah dibandingkan RC6. Selain itu, throughput AES cenderung lebih tinggi, yang menunjukkan efisiensi pemrosesan data yang lebih baik.

Temuan ini konsisten dengan penelitian oleh [10] yang menyatakan bahwa AES memiliki performa yang lebih optimal dibandingkan algoritma kriptografi simetris lainnya dalam hal efisiensi komputasi dan kecepatan pemrosesan data multimedia.

Perbedaan performa ini disebabkan oleh struktur algoritma AES yang berbasis substitusi-permutasi yang efisien, sedangkan RC6 menggunakan operasi aritmatika kompleks seperti rotasi bergantung data dan perkalian modular yang meningkatkan waktu komputasi [3].

Untuk memperjelas perbandingan kinerja algoritma, visualisasi waktu enkripsi ditampilkan pada Gambar 1.



Gambar 1. Grafik Waktu Enkripsi AES vs RC6 per Format

Grafik menunjukkan bahwa AES secara konsisten memiliki waktu enkripsi lebih rendah pada semua format file dibandingkan RC6.

3.1.2 Analisis Berdasarkan Format File

Hasil pengujian berdasarkan format file ditampilkan pada Tabel 2.

Tabel 2. Hasil Pengujian Berdasarkan Format File

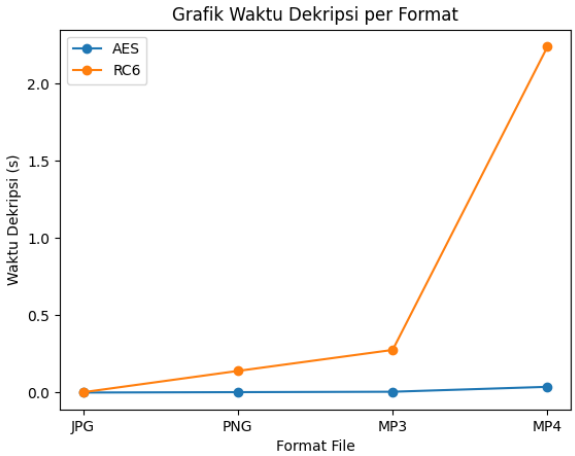
File_ name	For mat	Size (MB)	AES Enc	AES Dec	AES Thr	RC6 Enc	RC6 Dec	RC6 Thr
Album Art.jpg	JPG	0.0273 03	0.000 2	0	136.51500 8	0.003 1	0.00 2	8.8074 19
1.png	PNG	1.8184 15	0.003 4	0.00 26	534.82794 5	0.143 4	0.139 9	12.6807 18
Franky.mp3	MP3	3.535 92	0.006 4	0.00 52	552.48750 2	0.281 7	0.275 9	12.5520 77
VIDEO.mp4	MP4	29.2052 5	0.052 9	0.03 7	552.08412 1	2.330 3	2.23 8	12.5328 28

Berdasarkan Tabel 2, diperoleh bahwa:

a. Format JPG dan PNG memiliki waktu enkripsi yang relatif lebih rendah
b. Format MP3 menunjukkan peningkatan waktu proses
c. Format MP4 memiliki waktu enkripsi dan dekripsi tertinggi

Hal ini disebabkan oleh kompleksitas struktur data multimedia, dimana file video memiliki ukuran lebih besar dan struktur encoding yang lebih kompleks dibandingkan file gambar dan audio.

Untuk memperjelas analisis ini, visualisasi waktu dekripsi ditampilkan pada Gambar 2.



Gambar 2. Grafik Waktu Dekripsi Berdasarkan Format File

Grafik menunjukkan pola yang konsisten dengan waktu enkripsi, dimana RC6 memiliki waktu dekripsi yang lebih tinggi dibandingkan AES pada seluruh format.

Penelitian oleh [16] menunjukkan bahwa kompleksitas struktur data multimedia berpengaruh langsung terhadap waktu enkripsi, terutama pada file dengan ukuran besar dan struktur kompleks.

3.1.3 Analisis Berdasarkan Ukuran File

Hasil pengujian berdasarkan ukuran file ditampilkan pada Tabel 3.

DOI: 10.54259/satesi.v6i1.7523

Tabel 3. Hasil Pengujian Berdasarkan Ukuran File

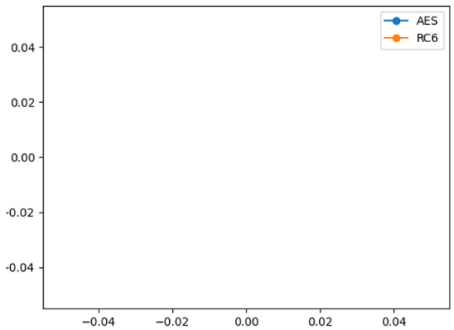
File_ name	file_ type	Size	AES Enc	AES Thr	RC6 Enc	RC6 Thr
Album Art.jpg	JPG	Small	0.0002	136. 515008	0.0031	8. 807419
1.png	PNG	Medium	0.0034	534. 827945	0.1434	12. 680718
Franky. mp3	MP3	Medium	0.0064	552. 487502	0.2817	12. 552077
VIDEO. mp4	MP4	Large	0.0529	552. 084121	2.3303	12. 532828

Berdasarkan Tabel 3, terlihat bahwa:

a. Waktu enkripsi meningkat seiring dengan ukuran file
b. Throughput menurun pada file berukuran besar

Fenomena ini sesuai dengan karakteristik algoritma block cipher yang memproses data dalam blok tetap, sehingga jumlah blok meningkat seiring ukuran file.

Visualisasi hubungan antara ukuran file dan throughput ditampilkan pada Gambar 3.



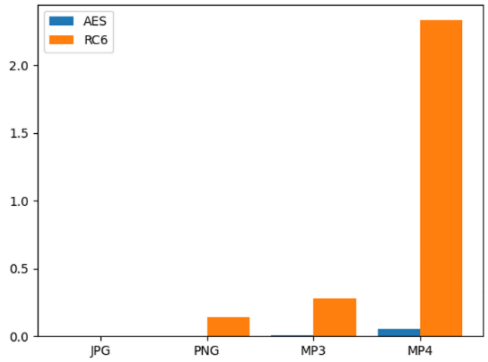
Gambar 3. Grafik Throughput Berdasarkan Ukuran File

Grafik menunjukkan bahwa AES memiliki throughput yang lebih stabil dibandingkan RC6 pada semua kategori ukuran.

Temuan ini sejalan dengan penelitian oleh Chen (2024) yang menunjukkan bahwa performa AES lebih stabil terhadap variasi ukuran data dibandingkan algoritma block cipher lainnya.

3.1.4 Analisis Perbandingan Visual AES vs RC6

Untuk memberikan perbandingan yang lebih jelas, digunakan visualisasi bar chart yang ditampilkan pada Gambar 4.



Gambar 4. Bar Chart Perbandingan AES dan RC6)

Grafik ini menunjukkan perbedaan yang signifikan antara waktu enkripsi AES dan RC6, dimana RC6 memiliki waktu yang jauh lebih tinggi pada semua format file.

3.1.5 Analisis Statistik

Analisis statistik dilakukan untuk mengevaluasi stabilitas performa algoritma.

Hasil menunjukkan bahwa:

a. AES memiliki nilai rata-rata waktu enkripsi yang rendah dengan deviasi standar kecil
b. RC6 memiliki rata-rata yang lebih tinggi dengan deviasi standar besar

Hal ini menunjukkan bahwa AES memiliki performa yang lebih stabil dan konsisten dibandingkan RC6.

Dalam konteks kriptografi, stabilitas performa merupakan faktor penting dalam aplikasi real-time, dimana variasi waktu komputasi harus diminimalkan [15].

3.2 Pembahasan

3.2.1 Efisiensi Komputasi

AES lebih efisien karena struktur algoritma yang lebih sederhana dan telah dioptimalkan secara luas pada berbagai platform.

3.2.2 Pengaruh Kompleksitas Data

Performa algoritma dipengaruhi oleh kompleksitas struktur file, terutama pada file video yang memiliki ukuran besar.

3.2.3 Stabilitas Algoritma

AES menunjukkan stabilitas performa yang lebih baik dibandingkan RC6, yang terlihat dari nilai deviasi standar yang lebih kecil.

3.2.4 Implikasi Praktis

a. AES cocok untuk sistem real-time (IoT, multimedia streaming)
b. RC6 dapat digunakan untuk studi akademik dan eksplorasi algoritma

3.2.5 Keterbatasan

a. Jumlah sampel terbatas
b. Variasi dataset belum luas
c. Pengujian pada satu lingkungan sistem

4. Kesimpulan

Berdasarkan hasil penelitian yang telah dilakukan mengenai perbandingan kinerja algoritma Advanced Encryption Standard (AES) dan Rivest Cipher 6 (RC6) pada proses enkripsi dan dekripsi file multimedia,

DOI: 10.54259/satesi.v6i1.7523

dapat disimpulkan bahwa kedua algoritma memiliki karakteristik dan performa yang berbeda dalam pengolahan data digital, khususnya pada file dengan format JPG, PNG, MP3, dan MP4.

Hasil eksperimen menunjukkan bahwa algoritma AES memiliki keunggulan utama dalam hal efisiensi waktu, di mana waktu enkripsi dan dekripsi yang dihasilkan relatif lebih cepat dibandingkan RC6 pada seluruh skenario pengujian. Selain itu, AES juga menunjukkan nilai throughput yang lebih stabil pada berbagai ukuran file, baik pada kategori small, medium, maupun large. Hal ini menunjukkan bahwa AES memiliki kemampuan pemrosesan data yang lebih konsisten dan efisien untuk kebutuhan aplikasi yang membutuhkan kecepatan tinggi, seperti sistem real-time dan pengamanan data multimedia.

Di sisi lain, algoritma RC6 memiliki performa yang lebih fluktuatif, yang ditunjukkan oleh nilai waktu enkripsi dan dekripsi yang lebih tinggi serta variasi throughput yang lebih besar. Kondisi ini dipengaruhi oleh struktur algoritma RC6 yang menggunakan operasi aritmatika kompleks seperti rotasi bergantung data dan perkalian modular, sehingga meningkatkan beban komputasi, terutama pada file berukuran besar. Meskipun demikian, RC6 tetap memiliki keunggulan dalam aspek desain kriptografis yang kuat dan fleksibel untuk pengembangan lebih lanjut.

Pengujian juga menunjukkan bahwa ukuran dan jenis file multimedia memiliki pengaruh signifikan terhadap kinerja kedua algoritma. Semakin besar ukuran file, maka waktu enkripsi dan dekripsi akan meningkat, sementara throughput cenderung menurun. Hal ini menegaskan bahwa kompleksitas data multimedia menjadi faktor penting dalam menentukan performa algoritma kriptografi.

Secara keseluruhan, dapat disimpulkan bahwa algoritma AES merupakan pilihan yang lebih optimal untuk digunakan dalam pengamanan data multimedia, terutama pada sistem yang membutuhkan efisiensi tinggi, stabilitas performa, dan kecepatan pemrosesan. Sementara itu, RC6 dapat dipertimbangkan sebagai alternatif pada kebutuhan tertentu yang memerlukan fleksibilitas algoritma atau eksplorasi pengembangan kriptografi lebih lanjut.

Sebagai pengembangan penelitian selanjutnya, disarankan untuk melakukan pengujian dengan jumlah dataset yang lebih besar, variasi format file yang lebih luas, serta mempertimbangkan parameter tambahan seperti penggunaan sumber daya sistem dan analisis keamanan lanjutan, sehingga diperoleh hasil yang lebih komprehensif dalam mengevaluasi kinerja algoritma kriptografi pada berbagai kondisi nyata.

Ucapan Terimakasih

Kami ucapkan terima kasih banyak kepada Universitas Bhayangkara Jakarta Raya yang telah memberikan kesempatan kepada kami, sehingga jurnal ini dapat diselesaikan dengan baik.

SUMBER RUJUKAN
Referensi

[1] M. A. Jimale *et al.*, “Authenticated encryption schemes: A systematic review,” *IEEE Access*, vol. 10, pp. 14739–14766, 2022, doi: 10.1109/ACCESS.2022.3147201.
[2] S. Balli and M. Yilmaz, “Multi-criteria usability evaluation of symmetric data encryption algorithms in fuzzy environment,” *SN Appl. Sci.*, vol. 2, p. 1393, 2020, doi: 10.1007/s42452-020-3170-9.
[3] X. Zhang, Y. Liu, and Z. Wang, “Improved RC6 block cipher,” *Comput. Mater. Contin.*, vol. 70, no. 1, pp. 1123–1137, 2021.
[4] H. Kaur and M. Singh, “Performance evaluation of symmetric encryption algorithms for multimedia data,” *Int. J. Comput. Appl.*, vol. 183, no. 4, pp. 1–6, 2021.
[5] S. Gafur and E. Aribowo, “Studi Pendekatan Quality \& Differential Analysis terhadap Kinerja Algoritma {AES}-{CBC} pada Enkripsi Gambar,” *J. Teknol. Inf. dan Ilmu Komput.*, vol. 12, no. 5, pp. 1115–1122, 2025.
[6] M. B. B. Timur, Royansyah, and D. Kusumaningsih, “Comparison of Efficiency and Security of {AES}, Blowfish, and ChaCha20 Cryptographic Algorithms on Image and Document Files,” *Innov. Res. Informatics*, vol. 7, no. 2, pp. 96–102, 2025, doi: 10.37058/innovatics.v7i2.15748.
[7] S. Basu, S. Roy, and A. Mukherjee, “Multimedia data encryption using symmetric cryptography: A performance perspective,” *Multimed. Tools Appl.*, vol. 82, pp. 21435–21458, 2023.
[8] W. Gondowarsito, “Multi-Format Data Encryption and Decryption with {AES} Cipher Block Chaining in Python,” *Crossroad Res. J.*, vol. 2, no. 2, pp. 56–65, 2025, doi: 10.61402/crj.v2i2.348.
[9] A. F. Pranata, A. F. Saragih, R. Fikri, K. Rahmadani, and N. P. Aulia, “Analisis Perbandingan Enkripsi dan Dekripsi Menggunakan Algoritma Simetris {AES} dan Hybrid ({AES} + {RSA}) Pada File Video,” *JIKUM J. Ilmu Komput.*, vol. 2, no. 1, pp. 102–107, 2026, doi: 10.62671/jikum.v2i1.143.
[10] R. B. Alothman, I. I. Saada, and B. S. B. Al-Brge, “A Performance-Based Comparative Encryption and Decryption Technique for Image and Video for Mobile Computing,” *J. Cases Inf. Technol.*, vol. 24, no. 2, pp. 1–18, 2022, doi: 10.4018/JCIT.20220101.oa1.
[11] A. Arifin and M. Rizal, “Implementasi Sistem Otomatisasi Perawatan Tanaman indoor berbasis Internet of Things (IoT),” *remik*, vol. 7, no. 2, pp. 935–945, 2023, doi: 10.33395/remik.v7i2.12277.
[12] P. Matta, “A comparative survey on data encryption techniques: Big data perspective,” *Mater. Today Proc.*, vol. 51, pp. 776–779, 2021, doi: 10.1016/j.matpr.2021.05.415.
[13] R. B. Alothman, “A performance-based comparative study of symmetric encryption algorithms,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 6, pp. 3275–3285, 2022.
[14] M. A. Khan, A. U. Rehman, and M. K. Khan, “Performance evaluation of AES for secure multimedia communication,” *IEEE Access*, vol. 10, pp. 84567–84580, 2022.
[15] R. B. Alothman, “A performance-based comparative encryption analysis,” *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 6, pp. 3275–3285, 2022.
[16] A. P. U. Siahaan, “Secure image encryption using AES,” in *Information Technology Conference*, 2024.

DOI: 10.54259/satesi.v6i1.7523