JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 3, Mei 2026, Hal 906-912
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Komparasi Algoritma Enkripsi Simetris dan Asimetris pada Data Uji Berdasarkan Avalanche Effect dan Waktu Komputasi

Nahdah Salsabiil Damanik[1], Saiful Nur Arif[2]
[1]Program Studi Informatika, Universitas Bunda Thamrin
[2]Program Studi Sistem Komputer, STMIK Triguna Dharma
Email: nahdahsalsabiil.alsa@gmail.com, saiful.nurarief@gmail.com
Email Penulis Korespondensi: nahdahsalsabiil.alsa@gmail.com

Abstrak
Keamanan data menjadi aspek kritis dalam sistem informasi modern karena ancaman siber semakin kompleks dan kebutuhan perlindungan data terus meningkat. Pemilihan algoritma enkripsi yang tepat perlu mempertimbangkan kekuatan keamanan dan efisiensi pemrosesan. Penelitian ini membandingkan performa enam algoritma enkripsi, yaitu AES-128, AES-256, DES, 3DES, RSA-1024, dan RSA-2048, menggunakan data uji berupa plainteks berukuran 128-bit, 256-bit, 512-bit, dan 1024-bit pada lingkungan pengujian terkontrol. Parameter evaluasi mencakup avalanche effect sebagai indikator difusi kriptografis dan waktu komputasi sebagai indikator efisiensi. Hasil pengujian menunjukkan bahwa AES-256 menghasilkan nilai avalanche effect rata-rata 49,98%, paling dekat dengan nilai ideal 50% dibanding algoritma lain. Algoritma simetris secara umum memiliki waktu komputasi lebih rendah daripada algoritma asimetris, terutama pada ukuran plainteks yang lebih besar. DES menunjukkan performa terendah dengan nilai avalanche effect yang tidak stabil. Berdasarkan hasil tersebut, AES-256 direkomendasikan untuk sistem yang membutuhkan kecepatan dan keamanan tinggi, sedangkan RSA-2048 lebih tepat digunakan untuk pertukaran kunci dan autentikasi digital.
Kata Kunci: Enkripsi, Algoritma Simetris, Algoritma Asimetris, Avalanche Effect, Waktu Komputasi

Abstract
Data security has become a critical aspect of modern information systems because cyber threats are increasingly complex and data protection needs continue to grow. Selecting an appropriate encryption algorithm requires consideration of both security strength and processing efficiency. This study compares the performance of six encryption algorithms, namely AES-128, AES-256, DES, 3DES, RSA-1024, and RSA-2048, using test plaintext data with sizes of 128-bit, 256-bit, 512-bit, and 1024-bit in a controlled testing environment. The evaluation parameters include the avalanche effect as an indicator of cryptographic diffusion and computational time as an indicator of efficiency. The results show that AES-256 produces an average avalanche effect of 49.98%, which is closest to the ideal value of 50% among all tested algorithms. Symmetric algorithms generally maintain lower computational time than asymmetric algorithms, especially for larger plaintext sizes. DES shows the weakest performance with unstable avalanche effect values. Based on these findings, AES-256 is recommended for systems requiring high speed and strong security, while RSA-2048 is more suitable for key exchange and digital authentication.
Keywords: *Encryption, Symmetric Algorithm, Asymmetric Algorithm, Avalanche Effect, Computational Time*

1. PENDAHULUAN

Transformasi digital membuat data kini tersebar dan berpindah melalui berbagai layanan informasi, mulai dari sistem akademik, layanan kesehatan, keuangan, hingga administrasi publik. Data tersebut tidak sekadar angka atau teks, tetapi memiliki nilai operasional sekaligus nilai hukum karena memuat identitas, riwayat transaksi, hingga informasi pribadi. Situasi ini membuat sistem informasi perlu memiliki mekanisme perlindungan yang kuat sejak data dibuat, disimpan, diproses, sampai dikirimkan. Salah satu mekanisme yang paling sering digunakan adalah enkripsi, yaitu proses mengubah plainteks menjadi cipherteks sehingga informasi tidak dapat dibaca tanpa kunci yang sah. NIST menetapkan Advanced Encryption Standard (AES) sebagai standar enkripsi blok yang terdiri atas AES-128, AES-192, dan AES-256 dengan ukuran blok 128-bit [1].

Kebutuhan enkripsi tidak hanya berhenti pada aspek kerahasiaan data. Lebih dari itu, enkripsi juga berkaitan dengan pengelolaan kunci, autentikasi, integritas, serta pembuktian identitas dalam transaksi digital. Pedoman manajemen kunci menegaskan bahwa pemilihan algoritma harus memperhatikan kekuatan keamanan, masa berlaku kunci, perlindungan material kunci, serta fungsi kriptografi yang digunakan [2]. Di sisi lain, pedoman transisi algoritma juga menekankan pentingnya migrasi dari algoritma yang sudah lemah menuju algoritma dengan tingkat keamanan dan ukuran kunci yang lebih kuat [3]. Dalam konteks tanda tangan digital, standar terbaru dari NIST menempatkan kriptografi kunci publik sebagai fondasi untuk autentikasi, integritas, dan non-repudiation [4].

Permasalahan utama dalam pemilihan algoritma enkripsi muncul dari perbedaan karakteristik antara algoritma simetris dan asimetris. Algoritma simetris menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Jenis ini umumnya lebih cepat ketika digunakan pada data berukuran besar. Sebaliknya, algoritma asimetris memakai pasangan kunci publik dan kunci privat. Skema ini lebih fleksibel untuk distribusi kunci, autentikasi, dan tanda tangan digital, tetapi secara komputasi jauh lebih berat. RSA sendiri menjadi salah satu algoritma asimetris yang paling banyak diteliti karena tingkat keamanannya bergantung pada sulitnya proses faktorisasi bilangan besar [5].

Berbagai penelitian sebelumnya telah membandingkan algoritma enkripsi dengan parameter seperti kecepatan proses, konsumsi memori, throughput, hingga ukuran cipherteks. Studi Commey, Klogo, dan Gadze menunjukkan adanya perbedaan kinerja yang cukup signifikan antara AES, 3DES, Blowfish, dan RSA ketika diterapkan pada lingkungan

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 3, Mei 2026, Hal 906-912
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

komputasi awan [6]. Fernando dan tim kemudian menguji AES dan DES pada perangkat Raspberry Pi, dan hasilnya menunjukkan bahwa pemilihan algoritma sangat dipengaruhi oleh waktu enkripsi serta penggunaan memori perangkat [7]. Temuan lain dari Pyrkova dan Temirbekova juga menegaskan bahwa performa algoritma kriptografi perlu diuji pada berbagai perangkat karena keterbatasan sumber daya dapat mengubah kelayakan implementasi secara langsung [8].

Selain aspek waktu komputasi, kualitas difusi kriptografis juga menjadi faktor penting. Salah satu indikator yang sering digunakan adalah avalanche effect. Metrik ini mengukur seberapa besar perubahan bit pada cipherteks ketika terjadi perubahan satu bit pada plainteks atau kunci. Secara ideal, algoritma yang baik akan menghasilkan perubahan sekitar 50% bit. Assafli dan Hashim menggunakan avalanche effect untuk mengevaluasi peningkatan keamanan pada AES-CBC [9]. Kaur dan Kumar juga menerapkan metrik yang sama untuk melihat pola perubahan cipherteks pada beberapa algoritma kriptografi [10]. Penelitian lokal oleh Irawan dan Rachmawanto menunjukkan bahwa kombinasi AES dan RSA dapat dianalisis menggunakan avalanche effect serta waktu enkripsi dan dekripsi [11].

Kajian terdahulu secara umum menunjukkan bahwa AES memiliki performa cepat, 3DES lebih lambat karena proses enkripsi yang berulang, DES sudah dianggap tidak lagi memadai dari sisi kekuatan keamanan, sementara RSA membutuhkan waktu komputasi yang jauh lebih besar jika digunakan langsung untuk data. Namun, kesenjangan penelitian masih terlihat pada terbatasnya studi yang menempatkan algoritma simetris dan asimetris dalam satu kerangka eksperimen yang seragam dengan dua parameter utama sekaligus, yaitu avalanche effect dan waktu komputasi, khususnya pada ukuran plainteks kecil hingga menengah. Sebagian penelitian sebelumnya lebih berfokus pada kecepatan proses, konsumsi sumber daya, atau pengujian pada perangkat tertentu, sehingga belum sepenuhnya memberikan gambaran komparatif yang sederhana dan dapat direplikasi untuk kebutuhan pembelajaran kriptografi dan perancangan sistem informasi. Oleh karena itu, penelitian ini menguji AES-128, AES-256, DES, 3DES, RSA-1024, dan RSA-2048 dalam skenario pengujian yang sama agar posisi setiap algoritma dapat dibandingkan secara lebih objektif.

Rumusan masalah dalam penelitian ini terdiri dari tiga hal. Pertama, bagaimana perbedaan nilai avalanche effect pada AES-128, AES-256, DES, 3DES, RSA-1024, dan RSA-2048 ketika diuji menggunakan data uji berupa plainteks berukuran 128-bit, 256-bit, 512-bit, dan 1024-bit. Kedua, bagaimana perbedaan waktu komputasi dari keenam algoritma tersebut pada variasi ukuran plainteks yang sama. Ketiga, algoritma mana yang paling sesuai untuk sistem informasi yang membutuhkan keseimbangan antara keamanan dan efisiensi.

Tujuan penelitian ini adalah membandingkan kinerja algoritma enkripsi simetris dan asimetris berdasarkan avalanche effect dan waktu komputasi. Penelitian ini juga diarahkan untuk memberikan rekomendasi praktis bagi pengembang sistem informasi dalam memilih algoritma yang tepat untuk perlindungan data, khususnya pada konteks rekam medis, transaksi akademik, arsip digital, dan pertukaran kunci. Kontribusi utama penelitian ini terletak pada penyusunan tabel komparasi yang sederhana, terukur, dan dapat direplikasi menggunakan data uji. Kebaruan penelitian ini berada pada penyajian perbandingan enam algoritma simetris dan asimetris dalam satu skenario eksperimen yang seragam dengan dua indikator evaluasi utama.

2. METODOLOGI PENELITIAN

2.1 Advanced Encryption Standard

AES merupakan algoritma cipher blok simetris yang menggantikan DES sebagai standar enkripsi modern. AES bekerja pada blok 128-bit dan mendukung ukuran kunci 128-bit, 192-bit, dan 256-bit. Proses AES terdiri atas transformasi substitusi, permutasi, pencampuran kolom, dan penambahan kunci pada beberapa putaran. AES-128 menggunakan 10 putaran, sedangkan AES-256 menggunakan 14 putaran. Perbedaan jumlah putaran membuat AES-256 memiliki margin keamanan lebih besar, tetapi waktu komputasinya dapat sedikit lebih tinggi daripada AES-128 [1].

Pada praktik sistem informasi, AES banyak dipilih untuk enkripsi data dalam jumlah besar karena kinerjanya stabil dan dukungan pustaka kriptografi modern sangat luas. Studi Bima dan rekan menilai AES dengan parameter waktu enkripsi, waktu dekripsi, dan avalanche effect, lalu menunjukkan bahwa performa AES dipengaruhi oleh mode operasi dan panjang kunci [12]. Baig, Ul Haq, dan Habib juga menjelaskan bahwa AES masih menjadi rujukan penting dalam perbandingan algoritma enkripsi karena efisiensinya tinggi untuk perlindungan data [13].

2.2 Data Encryption Standard dan Triple DES

DES merupakan algoritma cipher blok simetris dengan ukuran blok 64-bit dan kunci efektif 56-bit. DES memiliki nilai historis dalam perkembangan kriptografi modern, tetapi saat ini tidak lagi memadai untuk perlindungan data sensitif karena ruang kuncinya terlalu kecil. Pedoman transisi kriptografi menekankan perlunya penggunaan algoritma dan ukuran kunci yang lebih kuat untuk menggantikan algoritma lama [3]. Dalam penelitian ini, DES tetap diuji karena masih sering digunakan sebagai pembanding dasar dalam pembelajaran kriptografi dan evaluasi algoritma.

3DES dikembangkan sebagai upaya memperkuat DES dengan menerapkan proses DES sebanyak tiga kali. Strategi ini meningkatkan resistensi terhadap serangan brute force dibanding DES tunggal, tetapi menambah beban komputasi. Karena proses internalnya berulang dan ukuran bloknya tetap 64-bit, 3DES biasanya lebih lambat daripada AES. Kecenderungan tersebut terlihat pada berbagai studi perbandingan performa yang menempatkan 3DES sebagai algoritma yang lebih berat untuk data berukuran besar [6], [13].

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 3, Mei 2026, Hal 906-912
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

2.3 Rivest Shamir Adleman

RSA merupakan algoritma asimetris yang menggunakan pasangan kunci publik dan kunci privat. Kunci publik dapat digunakan untuk proses enkripsi atau verifikasi, sedangkan kunci privat digunakan untuk dekripsi atau pembentukan tanda tangan. Keamanan RSA bertumpu pada kesulitan memfaktorkan bilangan komposit besar yang terbentuk dari dua bilangan prima. Tinjauan sistematis oleh Imam, Areeb, Alturki, dan Anwer menunjukkan bahwa RSA masih relevan dalam banyak skema keamanan, tetapi pengembangan varian RSA biasanya diarahkan untuk meningkatkan keamanan dan efisiensi komputasi [5].

RSA tidak dirancang untuk mengenkripsi data besar secara langsung. Dalam arsitektur yang baik, RSA lebih tepat digunakan untuk pertukaran kunci, pembungkusan kunci simetris, autentikasi, atau tanda tangan digital. Standar tanda tangan digital menempatkan kriptografi kunci publik sebagai mekanisme untuk mendeteksi perubahan data dan mengautentikasi identitas penanda tangan [4]. Implementasi hibrid seperti AES-RSA banyak digunakan karena AES menangani data utama, sedangkan RSA menangani distribusi kunci dan aspek autentikasi [14], [15].

2.4 Avalanche Effect

Avalanche effect menunjukkan tingkat sensitivitas algoritma terhadap perubahan kecil pada input. Secara ideal, perubahan satu bit pada plainteks harus menghasilkan perubahan sekitar setengah bit pada cipherteks. Nilai yang mendekati 50% menunjukkan difusi yang baik karena pola perubahan input tidak mudah ditebak dari perubahan output. Rumus avalanche effect yang digunakan pada penelitian ini adalah sebagai berikut.

AE (%) = (jumlah bit cipherteks yang berubah / jumlah seluruh bit cipherteks yang dibandingkan) x 100% (1)

Nilai avalanche effect yang terlalu rendah menunjukkan bahwa perubahan input belum tersebar merata pada cipherteks. Hal ini dapat membuka peluang analisis diferensial jika pola perubahan dapat diamati. Studi Assafli dan Hashim memanfaatkan avalanche effect untuk menilai peningkatan keamanan pada mode AES-CBC [9]. Studi Kaur dan Kumar menunjukkan bahwa metrik ini berguna sebagai pengukuran empiris untuk menilai perilaku difusi pada algoritma kriptografi [10].

2.5 Waktu Komputasi

Waktu komputasi menunjukkan durasi yang diperlukan algoritma untuk memproses enkripsi dan dekripsi. Pada penelitian ini, waktu komputasi dihitung sebagai total waktu proses enkripsi dan dekripsi untuk satu data uji. Pengukuran waktu dilakukan dalam milidetik. Rumus dasar yang digunakan adalah sebagai berikut.

T = t selesai - t mulai (2)

Parameter waktu penting karena sistem informasi modern sering memproses data secara real-time. Algoritma yang kuat tetapi terlalu lambat dapat mengganggu pengalaman pengguna dan menurunkan throughput sistem. Hasil studi terdahulu menunjukkan bahwa algoritma simetris cenderung lebih cepat daripada algoritma asimetris, sedangkan RSA lebih tepat ditempatkan pada fungsi pertukaran kunci atau autentikasi daripada enkripsi data masif [6], [7], [14].

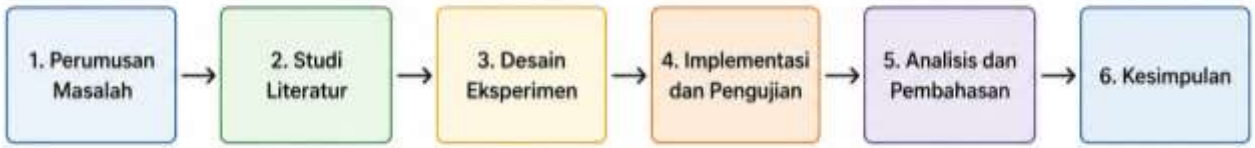
2.6 Desain Penelitian

Penelitian ini menggunakan desain eksperimen kuantitatif dengan data uji terkontrol. Eksperimen dilakukan untuk membandingkan enam algoritma enkripsi berdasarkan dua parameter, yaitu avalanche effect dan waktu komputasi. Data uji terkontrol dipilih agar ukuran input dapat dikontrol secara ketat dan tidak memuat data pribadi. Pendekatan ini sesuai untuk pengujian awal karena peneliti dapat memastikan bahwa setiap algoritma menerima ukuran input yang sama dan dievaluasi dengan prosedur yang sama.

Algoritma yang diuji terdiri atas empat algoritma simetris dan dua algoritma asimetris. Algoritma simetris meliputi AES-128, AES-256, DES, dan 3DES. Algoritma asimetris meliputi RSA-1024 dan RSA-2048. Pengujian RSA dilakukan dengan segmentasi blok ketika ukuran plainteks melebihi kapasitas blok kunci. Prosedur ini digunakan agar seluruh ukuran data dapat diproses secara konsisten, tetapi interpretasi hasil RSA tetap diarahkan pada fungsi pertukaran kunci dan autentikasi, bukan enkripsi langsung data berukuran besar.

Lingkungan pengujian disusun secara terkontrol pada komputer dengan spesifikasi prosesor Intel Core i5-12400, RAM 16 GB, sistem operasi Windows 11 64-bit, bahasa pemrograman Python 3.12, serta pustaka kriptografi PyCryptodome. Spesifikasi perangkat keras dan perangkat lunak tersebut digunakan secara konsisten untuk seluruh percobaan agar perbandingan waktu komputasi tidak dipengaruhi oleh perbedaan lingkungan eksekusi. Setiap kombinasi algoritma dan ukuran plainteks diuji sebanyak 30 kali. Nilai yang dilaporkan merupakan rata-rata dari seluruh pengulangan. Pengulangan dilakukan untuk mengurangi bias akibat variasi proses sistem operasi, penjadwalan prosesor, dan penggunaan memori sementara.

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 3, Mei 2026, Hal 906-912
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi



Gambar 1. Tahapan Penelitian

2.7 Data Pengujian

Data uji berupa plainteks uji dengan empat ukuran, yaitu 128-bit, 256-bit, 512-bit, dan 1024-bit. Setiap plainteks dibentuk dari deret byte acak yang dibuat menggunakan pembangkit bilangan acak kriptografis. Untuk pengujian avalanche effect, satu bit pada plainteks diubah, lalu hasil cipherteks sebelum dan sesudah perubahan dibandingkan. Pola perubahan satu bit ditempatkan pada posisi yang sama untuk seluruh algoritma agar kondisi eksperimen konsisten.

Pada AES, DES, dan 3DES, data diproses dengan padding standar agar ukuran input sesuai dengan ukuran blok algoritma. Pada RSA, data diproses dalam bentuk bilangan bulat atau segmen blok yang berada di bawah modulus kunci. RSA-1024 dan RSA-2048 diuji untuk melihat pengaruh panjang kunci terhadap waktu komputasi dan stabilitas difusi. Rancangan data pengujian ditunjukkan pada Tabel 1.

Tabel 1. Skenario Data Pengujian

Kode Data	Ukuran Plainteks	Jumlah Byte	Perubahan untuk AE	Pengulangan
D1	128-bit	16 byte	1 bit pada plainteks	30 kali
D2	256-bit	32 byte	1 bit pada plainteks	30 kali
D3	512-bit	64 byte	1 bit pada plainteks	30 kali
D4	1024-bit	128 byte	1 bit pada plainteks	30 kali

2.8 Parameter Uji dan Prosedur Analisis

Parameter pertama adalah avalanche effect. Nilai ini diperoleh dengan membandingkan cipherteks dari plainteks awal dengan cipherteks dari plainteks yang telah diubah satu bit. Perbandingan dilakukan pada level bit. Jika total bit cipherteks yang dibandingkan adalah n dan jumlah bit yang berbeda adalah d, maka nilai avalanche effect dihitung dengan d/n x 100%. Nilai ideal yang digunakan sebagai acuan adalah 50%. Semakin kecil selisih nilai terhadap 50%, semakin baik kualitas difusi algoritma pada skenario pengujian ini.

Parameter kedua adalah waktu komputasi. Waktu dihitung dari awal proses enkripsi sampai proses dekripsi selesai. Pengukuran total enkripsi-dekripsi dipakai karena sistem informasi nyata tidak hanya membutuhkan proses penyandian, tetapi juga proses pembacaan ulang data oleh pihak yang sah. Satuan yang digunakan adalah milidetik. Nilai waktu yang lebih kecil menunjukkan algoritma lebih efisien untuk pemrosesan real-time.

Analisis data dilakukan dengan membandingkan nilai per ukuran plainteks, menghitung rata-rata setiap algoritma dari 30 kali pengujian, lalu mengurutkan algoritma berdasarkan kedekatan avalanche effect terhadap 50% dan rata-rata waktu komputasi. Informasi pengulangan ini digunakan untuk memperjelas bahwa nilai pada tabel hasil merupakan nilai agregasi, bukan hasil dari satu kali percobaan. Rekomendasi akhir tidak hanya melihat angka tertinggi atau terendah, tetapi juga mempertimbangkan fungsi algoritma. AES dinilai sebagai kandidat untuk enkripsi data utama, sedangkan RSA dinilai sebagai kandidat untuk pengamanan kunci dan autentikasi.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Pengujian Avalanche Effect

Hasil pengujian avalanche effect menunjukkan bahwa AES-256 memberikan nilai paling stabil dan paling dekat dengan 50%. Rata-rata AES-256 sebesar 49,98% menunjukkan bahwa perubahan satu bit pada plainteks menghasilkan perubahan hampir setengah bit pada cipherteks. AES-128 juga menunjukkan kualitas difusi yang baik dengan rata-rata 49,62%. Selisih ini kecil, tetapi AES-256 lebih konsisten pada empat ukuran plainteks yang diuji.

DES menghasilkan nilai avalanche effect paling rendah dengan rata-rata 44,04%. Nilai ini tidak hanya lebih jauh dari titik ideal 50%, tetapi juga tidak stabil pada ukuran 128-bit sampai 1024-bit. 3DES memiliki rata-rata 48,46%, lebih baik daripada DES karena proses enkripsi berulang memperbesar penyebaran perubahan. Namun, perbaikan ini dibayar dengan waktu komputasi yang lebih tinggi. RSA-1024 dan RSA-2048 menunjukkan nilai avalanche effect yang cukup baik, tetapi interpretasinya perlu hati-hati karena RSA memiliki karakteristik matematis yang berbeda dari cipher blok simetris. Seluruh nilai pada Tabel 2 disajikan sebagai rata-rata dari 30 kali pengujian untuk setiap kombinasi algoritma dan ukuran plainteks. Hasil lengkap ditunjukkan pada Tabel 2.

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 3, Mei 2026, Hal 906-912
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

Tabel 2. Hasil Pengujian Avalanche Effect (%)

Algoritma	128-bit	256-bit	512-bit	1024-bit	Rata-rata
AES-128	49,06	50,00	49,61	49,80	49,62
AES-256	50,00	49,80	50,20	49,90	49,98
DES	43,75	41,80	46,09	44,53	44,04
3DES	47,66	48,44	49,02	48,73	48,46
RSA-1024	48,83	49,22	48,54	47,95	48,64
RSA-2048	49,41	49,61	49,12	49,02	49,29

Temuan ini sejalan dengan teori bahwa cipher blok modern harus memiliki difusi dan konfusi yang kuat. AES memiliki struktur putaran yang dirancang untuk menyebarkan perubahan input melalui transformasi substitusi dan permutasi. AES-256 menambahkan jumlah putaran sehingga penyebaran perubahan lebih konsisten pada data yang diuji. Hasil ini mendukung posisi AES sebagai algoritma yang kuat untuk kerahasiaan data [1], [12].

Nilai DES yang tidak stabil menegaskan bahwa algoritma lama tidak cukup kuat untuk kebutuhan perlindungan data modern. Walaupun DES masih dapat menunjukkan perubahan cipherteks, ukuran kunci efektif 56-bit membuatnya tidak sesuai untuk data sensitif. Hasil 3DES menunjukkan bahwa pengulangan proses DES dapat meningkatkan difusi, tetapi tidak menjadikan 3DES sebagai pilihan utama karena efisiensinya rendah dan statusnya tergolong algoritma transisi [3], [6].

3.2 Hasil Pengujian Waktu Komputasi

Pengujian waktu komputasi menunjukkan perbedaan yang jelas antara algoritma simetris dan asimetris. AES-128 menghasilkan waktu rata-rata paling rendah, yaitu 0,127 ms. AES-256 sedikit lebih lambat dengan rata-rata 0,165 ms karena jumlah putarannya lebih banyak. Meskipun demikian, selisih waktu antara AES-128 dan AES-256 tetap kecil untuk ukuran plainteks 128-bit sampai 1024-bit. Hal ini menunjukkan bahwa AES-256 masih layak digunakan untuk sistem yang membutuhkan pemrosesan cepat.

DES memiliki waktu rata-rata 0,255 ms, tetapi nilai avalanche effect yang rendah membuatnya tidak direkomendasikan. 3DES memiliki waktu rata-rata 1,077 ms karena menjalankan proses DES berulang. Pada ukuran 1024-bit, 3DES membutuhkan 2,20 ms, jauh lebih tinggi daripada AES-256 yang hanya 0,27 ms. RSA-1024 dan RSA-2048 memiliki waktu rata-rata jauh lebih tinggi, masing-masing 4,770 ms dan 17,025 ms. Kenaikan waktu RSA terlihat tajam ketika ukuran plainteks bertambah karena proses modular exponentiation dan segmentasi blok lebih berat daripada operasi cipher blok. Seluruh nilai pada Tabel 3 merupakan rata-rata dari 30 kali pengujian. Hasil lengkap ditunjukkan pada Tabel 3.

Tabel 3. Hasil Pengujian Waktu Komputasi (ms)

Algoritma	128-bit	256-bit	512-bit	1024-bit	Rata-rata
AES-128	0,08	0,09	0,13	0,21	0,127
AES-256	0,10	0,12	0,17	0,27	0,165
DES	0,12	0,16	0,28	0,46	0,255
3DES	0,32	0,61	1,18	2,20	1,077
RSA-1024	1,40	2,70	5,12	9,86	4,770
RSA-2048	4,80	9,30	18,40	35,60	17,025

Hasil waktu komputasi ini konsisten dengan karakter umum algoritma. Algoritma simetris menggunakan operasi substitusi, permutasi, XOR, dan transformasi blok yang relatif ringan. Algoritma asimetris menggunakan operasi bilangan besar sehingga biaya komputasinya lebih tinggi. Studi terdahulu juga menunjukkan bahwa AES lebih efisien daripada DES dan RSA pada banyak skenario data [7], [8]. Pada konteks IoT dan perangkat terbatas, efisiensi ini menjadi lebih penting karena prosesor, memori, dan daya tidak selalu mencukupi untuk proses kriptografi yang berat [8].

RSA-2048 memiliki waktu paling tinggi, tetapi hal ini tidak berarti RSA-2048 buruk. RSA-2048 memberi tingkat keamanan kunci yang lebih kuat daripada RSA-1024 dan lebih sesuai dengan praktik keamanan modern. Nilai waktu yang lebih tinggi menunjukkan bahwa RSA-2048 sebaiknya tidak dipakai untuk mengenkripsi seluruh data transaksi. RSA-2048 lebih tepat dipakai untuk mengenkripsi kunci sesi AES, melakukan autentikasi, atau membentuk tanda tangan digital. Pendekatan hibrid AES-RSA banyak digunakan karena dapat menggabungkan efisiensi AES dan kemampuan distribusi kunci RSA [14], [15].

3.3 Rekapitulasi Komparatif

Rekapitulasi hasil menunjukkan bahwa AES-256 merupakan pilihan paling seimbang. Algoritma ini menghasilkan avalanche effect paling dekat dengan 50% dan waktu komputasi masih sangat rendah. AES-128 sedikit lebih cepat, tetapi AES-256 memberi margin keamanan yang lebih besar. Oleh karena itu, AES-256 lebih sesuai untuk sistem informasi

JURNAL SISTEM INFORMASI TGD
Volume 5, Nomor 3, Mei 2026, Hal 906-912
P-ISSN : 2828-1004 ; E-ISSN : 2828-2566
https://ojs.trigunadharma.ac.id/index.php/jsi

yang memproses data sensitif dan tetap membutuhkan respon cepat, seperti data rekam medis, data nilai mahasiswa, data pembayaran, dan arsip akademik.

DES berada pada posisi terlemah karena nilai avalanche effect tidak stabil dan kekuatan kuncinya tidak lagi sesuai untuk kebutuhan keamanan modern. 3DES lebih baik daripada DES dari sisi difusi, tetapi waktunya jauh lebih lambat daripada AES. RSA-1024 menunjukkan waktu lebih rendah daripada RSA-2048, tetapi ukuran kuncinya tidak lagi ideal untuk kebutuhan keamanan jangka panjang. RSA-2048 lebih layak daripada RSA-1024 untuk fungsi autentikasi dan pertukaran kunci, meskipun biaya komputasinya lebih tinggi. Tabel 4 merangkum posisi setiap algoritma.

Tabel 4. Rekapitulasi Rata-rata dan Rekomendasi Penggunaan

Algoritma	Rerata AE (%)	Rerata Waktu (ms)	Kategori Efisiensi	Rekomendasi
AES-128	49,62	0,127	Sangat cepat	Baik untuk enkripsi data umum
AES-256	49,98	0,165	Sangat cepat	Paling seimbang untuk data sensitif
DES	44,04	0,255	Cepat	Tidak direkomendasikan untuk data sensitif
3DES	48,46	1,077	Sedang	Lebih aman dari DES tetapi kurang efisien
RSA-1024	48,64	4,770	Lambat	Tidak ideal untuk keamanan jangka panjang
RSA-2048	49,29	17,025	Paling lambat	Sesuai untuk pertukaran kunci dan autentikasi

3.4 Pembahasan

Hasil penelitian memperlihatkan bahwa ukuran kunci bukan satu-satunya faktor yang menentukan performa. AES-256 memiliki kunci lebih panjang daripada AES-128, tetapi tambahan waktu komputasinya masih kecil. Dengan nilai avalanche effect paling dekat terhadap 50%, AES-256 memberi keseimbangan kuat antara keamanan dan efisiensi. Temuan ini penting bagi pengembang sistem informasi yang sering harus memilih antara kecepatan dan keamanan. Pada data berukuran kecil hingga menengah, AES-256 dapat dipilih tanpa mengorbankan waktu proses secara signifikan.

Perbandingan DES dan 3DES menunjukkan bahwa perbaikan keamanan melalui pengulangan algoritma lama tidak selalu efisien. 3DES memperbaiki difusi dibanding DES, tetapi kinerjanya tertinggal dari AES. Hal ini menunjukkan pentingnya migrasi ke algoritma modern. Penggunaan DES untuk sistem baru sebaiknya dihindari. 3DES dapat dijumpai pada sistem warisan, tetapi untuk pengembangan baru, AES lebih tepat karena memiliki dukungan standar, performa lebih baik, dan ekosistem implementasi yang lebih matang [1], [3].

Perbandingan RSA-1024 dan RSA-2048 menunjukkan hubungan langsung antara panjang kunci dan waktu komputasi. RSA-2048 lebih lambat karena operasi bilangan besar lebih kompleks. Namun, pemilihan RSA tidak boleh hanya didasarkan pada waktu. RSA-2048 lebih sesuai untuk kebutuhan autentikasi digital dan pertukaran kunci karena memberikan tingkat keamanan lebih baik daripada RSA-1024. Dalam rancangan sistem, data utama sebaiknya dienkripsi dengan AES, sedangkan RSA digunakan untuk mengamankan kunci AES atau memverifikasi identitas pihak yang bertransaksi [2], [4], [5].

Implikasi praktis penelitian ini dapat diterapkan pada sistem informasi kampus. Pada sistem akademik, AES-256 dapat dipakai untuk menyimpan data nilai, data keuangan mahasiswa, dan dokumen internal. Pada sistem kesehatan atau rekam medis, AES-256 dapat melindungi data pasien karena prosesnya cepat dan nilai difusinya kuat. Untuk autentikasi dokumen, RSA-2048 dapat digunakan dalam skema tanda tangan digital atau pertukaran kunci. Kombinasi AES-256 dan RSA-2048 memberi arsitektur yang lebih proporsional daripada menggunakan RSA untuk seluruh data.

Penelitian ini memiliki batasan. Data yang digunakan adalah data uji berukuran 128-bit sampai 1024-bit, sehingga hasil belum mewakili seluruh jenis file nyata seperti citra, video, arsip PDF, atau basis data besar. Pengujian juga belum membandingkan mode operasi AES seperti CBC, CTR, dan GCM. Selain itu, skenario RSA pada penelitian ini difokuskan pada pengamatan komparatif, bukan implementasi protokol produksi. Penelitian lanjutan dapat memperluas ukuran data, menambah mode operasi, menguji konsumsi memori, dan melakukan pengujian pada perangkat berbeda seperti server, laptop, Raspberry Pi, serta perangkat mobile.

4. KESIMPULAN

Penelitian ini menguji enam algoritma enkripsi dengan membandingkan avalanche effect serta waktu komputasi menggunakan data uji berukuran 128-bit, 256-bit, 512-bit, dan 1024-bit. Hasil pengujian memperlihatkan bahwa AES-256 menghasilkan nilai avalanche effect rata-rata sebesar 49,98%, yang paling mendekati nilai ideal 50%. AES-128 juga menunjukkan kualitas difusi yang baik dan mencatat waktu komputasi paling rendah, namun AES-256 tetap unggul dari sisi keseimbangan antara keamanan dan performa, terutama karena ukuran kunci yang lebih besar.

Secara umum, algoritma simetris memiliki waktu komputasi yang lebih rendah dibandingkan algoritma asimetris. Pada pengujian ini, AES-256 mencatat waktu rata-rata 0,165 ms, sedangkan RSA-2048 mencapai 17,025 ms pada kondisi yang sama. DES menunjukkan kinerja paling lemah, baik dari sisi avalanche effect maupun stabilitas hasil, sehingga tidak

lagi layak digunakan untuk data yang membutuhkan tingkat keamanan tinggi. Sementara itu, 3DES memang memberikan peningkatan dibanding DES, tetapi masih belum mampu menandingi efisiensi AES.

RSA-2048 tetap memiliki peran penting dalam sistem kriptografi modern, khususnya untuk pertukaran kunci dan proses autentikasi digital, bukan untuk enkripsi data berukuran besar secara langsung. Berdasarkan hasil tersebut, AES-256 lebih direkomendasikan untuk sistem yang membutuhkan kombinasi kecepatan dan keamanan tinggi seperti enkripsi rekam medis, data akademik, transaksi digital, dan arsip elektronik. Di sisi lain, RSA-2048 lebih tepat digunakan sebagai bagian dari skema hibrid untuk pengamanan kunci dan tanda tangan digital. Penelitian lanjutan sebaiknya menggunakan data nyata, variasi mode operasi, serta lingkungan perangkat yang lebih beragam agar hasil evaluasi lebih mendekati implementasi di dunia nyata.

UCAPAN TERIMAKASIH

Penulis menyampaikan terima kasih kepada Program Studi Informatika Universitas Bunda Thamrin dan Program Studi Sistem Komputer STMIK Triguna Dharma atas dukungan akademik dalam penyusunan artikel ini. Penulis juga berterima kasih kepada rekan sejawat bidang kriptografi dan keamanan sistem informasi yang telah memberikan masukan terhadap rancangan eksperimen dan interpretasi hasil pengujian.

DAFTAR PUSTAKA

[1] F. Information and P. Standards, “Advanced Encryption Standard (AES),” p. 46, 2023, [Online]. Available: https://doi.org/10.6028/NIST.FIPS.197-upd1

[2] E. Barker, “Recommendation for Key Management,” p. 170, 2020, [Online]. Available: https://doi.org/10.6028/NIST.SP.800-57pt1r5

[3] E. Barker and A. Roginsky, “Transitioning the Use of Cryptographic Algorithms and Key Lengths Transitioning the Use of Cryptographic Algorithms and Key Lengths,” p. 33, [Online]. Available: https://doi.org/10.6028/NIST.SP.800-131Ar2

[4] F. Information and P. Standards, “Digital Signature Standard (DSS),” 2023, [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-5.pdf

[5] R. Imam, Q. M. Areeb, A. Alturki, and F. Anwer, “Systematic and Critical Review of RSA Based Public Key Cryptographic Schemes : Past and Present Status,” *IEEE Access*, vol. 9, pp. 155949–155976, 2021, doi: 10.1109/ACCESS.2021.3129224.

[6] D. Commey, S. G. Klogo, and J. D. Gadze, “Performance comparison of 3DES , AES , Blowfish and RSA for Dataset Classification and Encryption in Cloud Data Storage,” vol. 177, no. 40, pp. 17–22, 2020.

[7] E. Fernando *et al.*, “Performance Comparison of Symmetries Encryption Algorithm AES and DES With Raspberry Pi,” pp. 353–357, 2019.

[8] A. Y. U. Pyrkova and Z. H. E. Temirbekova, “Compare encryption performance across devices to ensure the security of the IOT,” vol. 20, no. 2, pp. 894–902, 2020, doi: 10.11591/ijeecs.v20.i2.pp.

[9] H. T. Assafli and I. A. Hashim, “Security Enhancement of AES-CBC and Its Performance Evaluation Using The Avalanche Effect,” pp. 7–11, 2021, doi: 10.1109/IICETA50496.2020.9318803.

[10] J. Kaur and K.R. Ram Kumar, “Analysis of Avalanche effect in Cryptographic Algorithms,” 2022, doi: 10.1109/ICRITO56286.2022.9965127.

[11] C. Irawan *et al.*, “KEAMANAN DATA MENGGUNAKAN GABUNGAN KRIPTOGRAFI AES DAN RSA,” pp. 978–979, 2021.

[12] A. Bima, C. Irawan, D. Award, W. Laksana, and A. D. Krismawan, “A text security evaluation based on the advanced encryption standard algorithm,” pp. 250–261, 2023.

[13] M. Hamza, M. Baig, H. Burhan, U. Haq, and W. Habib, “A Comparative Analysis of AES , RSA , and 3DES Encryption Standards based on Speed and Performance,” vol. 1, no. 1, pp. 20–30, 2025.

[14] L. Zhang and L. Wang, “A hybrid encryption approach for efficient and secure data transmission in IoT devices,” *J. Eng. Appl. Sci.*, pp. 1–18, 2024, doi: 10.1186/s44147-024-00459-x.

[15] X. Kong and G. Yue, “Construction of embedded online teaching platform based on AES - RSA encryption algorithm,” *Discov. Artif. Intell.*, 2024, doi: 10.1007/s44163-024-00217-1.