e-ISSN: 3110-0864 | p-ISSN: XXXX-XXXX
**JURNAL ILMU KOMPUTER DAN TEKNIK INFROMATIKA**
Volume 2 No 1 Januari 2026 | Page: 29-35
https://journals.raskhamedia.or.id/index.php/juikti
DOI: https://doi.org/10.64803/juikti.v2i1.87

# Perbandingan Algoritma Kriptografi Modern dalam Melindungi Data Transmisi

**Maulidania Mediawati Cynthia[1,*], Eka Pandu Cynthia[2], Dessy Nia Cynthia[3]**

[1] Akuntansi, Politeknik Lembaga Pendidikan dan Pengembangan Profesi Indonesia, Bandung, Indonesia
[2] Sains dan Teknologi, Teknik Informatika, UIN Sultan Syarif Kasim Riau, Pekanbaru, Indonesia
[3]Ekonomi, Akuntansi, Universitas Terbuka, Pekanbaru, Indonesia
Email: [1,*]maulidania.mediawati99@gmail.com, [2]eka.cynthia@gmail.com,[3]cynthia.dessynia@gmail.com
(* Email Corresponding Author: maulidania.mediawati99@gmail.com)
*Received: 4 Januari 2026 | Revision: 4 Januari 2026 | Accepted: 4 Januari 2026*

**Abstrak**

Keamanan data transmisi merupakan aspek penting dalam sistem informasi modern seiring meningkatnya pertukaran data melalui jaringan terbuka. Berbagai ancaman seperti penyadapan, manipulasi data, dan serangan siber menuntut penerapan algoritma kriptografi yang andal dan efisien. Penelitian ini bertujuan untuk membandingkan algoritma kriptografi modern dalam melindungi data transmisi berdasarkan parameter keamanan, kecepatan enkripsi dan dekripsi, ukuran kunci, serta efisiensi penggunaan sumber daya sistem. Metode penelitian yang digunakan adalah pendekatan komparatif eksperimental dengan tahapan meliputi studi literatur, penentuan algoritma dan parameter pengujian, implementasi simulasi, pengumpulan data, serta analisis hasil. Algoritma yang dianalisis meliputi AES, ChaCha20, RSA, dan ECC. Hasil penelitian menunjukkan bahwa algoritma kriptografi simetris, khususnya ChaCha20 dan AES, memiliki performa yang lebih unggul dalam hal kecepatan dan efisiensi sumber daya dibandingkan algoritma asimetris. Sementara itu, algoritma ECC menunjukkan keunggulan signifikan dibandingkan RSA dengan tingkat keamanan tinggi dan ukuran kunci yang lebih kecil. Penelitian ini menyimpulkan bahwa tidak terdapat satu algoritma yang unggul pada semua aspek, sehingga pemilihan algoritma kriptografi harus disesuaikan dengan kebutuhan sistem. Kombinasi algoritma simetris dan asimetris merupakan pendekatan paling efektif dalam melindungi data transmisi pada sistem informasi modern.

**Kata Kunci:** Kriptografi Modern, Keamanan Data, Data Transmisi, Algoritma Kriptografi, Keamanan Informasi

***Abstract***

*Data transmission security is a critical aspect of modern information systems due to the increasing exchange of data over open networks. Various threats such as eavesdropping, data manipulation, and cyberattacks require the implementation of reliable and efficient cryptographic algorithms. This study aims to compare modern cryptographic algorithms in securing data transmission based on security level, encryption and decryption speed, key size, and system resource efficiency. The research employs a comparative experimental approach consisting of literature review, algorithm and parameter selection, simulation implementation, data collection, and result analysis. The algorithms analyzed include AES, ChaCha20, RSA, and ECC. The results indicate that symmetric cryptographic algorithms, particularly ChaCha20 and AES, outperform asymmetric algorithms in terms of processing speed and resource efficiency. Meanwhile, ECC demonstrates significant advantages over RSA by providing high security with smaller key sizes. This study concludes that no single cryptographic algorithm excels in all aspects; therefore, algorithm selection must be tailored to system requirements. A hybrid approach combining symmetric and asymmetric cryptographic algorithms is the most effective solution for securing data transmission in modern information systems.*

***Keywords****: Modern Cryptography, Data Security, Data Transmission, Cryptographic Algorithms, Information Security*

## 1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang semakin pesat telah mendorong meningkatnya kebutuhan akan pertukaran data secara cepat dan efisien melalui jaringan komputer[1]. Data tidak lagi hanya ditransmisikan dalam ruang lingkup lokal, tetapi juga melintasi jaringan publik seperti internet yang memiliki tingkat kerentanan tinggi terhadap berbagai ancaman keamanan. Informasi yang dikirimkan melalui jaringan dapat berupa data pribadi, transaksi keuangan, informasi bisnis strategis, hingga data pemerintahan yang bersifat rahasia[2]. Kondisi ini menjadikan keamanan data transmisi sebagai aspek krusial dalam sistem informasi modern[3].

Salah satu ancaman utama dalam transmisi data adalah serangan pihak tidak berwenang, seperti penyadapan (eavesdropping), pemalsuan data (data tampering), dan serangan man-in-the-middle[4]. Tanpa mekanisme perlindungan yang memadai, data yang ditransmisikan dapat dengan mudah dibaca, dimodifikasi, atau bahkan disalahgunakan oleh pihak yang tidak bertanggung jawab[5]. Oleh karena itu, diperlukan metode pengamanan yang mampu menjamin kerahasiaan (confidentiality), keutuhan (integrity), dan keaslian (authentication) data selama proses transmisi berlangsung[6].

Kriptografi merupakan salah satu solusi utama yang digunakan untuk melindungi data transmisi[7]. Kriptografi bekerja dengan cara mengubah data asli (plaintext) menjadi bentuk terenkripsi (ciphertext) yang

e-ISSN: 3110-0864 | p-ISSN: XXXX-XXXX
**JURNAL ILMU KOMPUTER DAN TEKNIK INFROMATIKA**
Volume 2 No 1 Januari 2026 | Page: 29-35
https://journals.raskhamedia.or.id/index.php/juikti
DOI: https://doi.org/10.64803/juikti.v2i1.87

tidak dapat dipahami tanpa kunci tertentu[8]. Seiring berkembangnya teknologi komputasi dan meningkatnya kompleksitas serangan siber, algoritma kriptografi juga mengalami evolusi yang signifikan[9]. Algoritma kriptografi klasik seperti DES (Data Encryption Standard) secara bertahap ditinggalkan karena dianggap tidak lagi aman, dan digantikan oleh algoritma kriptografi modern yang menawarkan tingkat keamanan lebih tinggi serta efisiensi yang lebih baik[10].

Algoritma kriptografi modern umumnya diklasifikasikan ke dalam dua kategori utama, yaitu kriptografi simetris dan kriptografi asimetris[11]. Algoritma simetris, seperti AES (Advanced Encryption Standard), menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi[12]. Algoritma ini dikenal memiliki kecepatan tinggi dan efisiensi komputasi yang baik, sehingga banyak digunakan dalam pengamanan data transmisi berskala besar[13]. Namun, tantangan utama pada kriptografi simetris terletak pada distribusi kunci yang aman antara pihak pengirim dan penerima[14].

Di sisi lain, algoritma kriptografi asimetris, seperti RSA dan ECC (Elliptic Curve Cryptography), menggunakan sepasang kunci yang berbeda, yaitu kunci publik dan kunci privat[15]. Pendekatan ini menawarkan solusi terhadap permasalahan distribusi kunci, tetapi umumnya memiliki beban komputasi yang lebih tinggi dibandingkan algoritma simetris. Oleh karena itu, dalam praktiknya, sistem keamanan jaringan sering mengombinasikan kedua jenis algoritma tersebut untuk memperoleh keseimbangan antara keamanan dan performa.

Meskipun berbagai algoritma kriptografi modern telah dikembangkan dan diimplementasikan secara luas, setiap algoritma memiliki karakteristik, keunggulan, dan keterbatasan masing-masing. Faktor-faktor seperti tingkat keamanan, kompleksitas algoritma, ukuran kunci, kecepatan enkripsi dan dekripsi, serta konsumsi sumber daya menjadi pertimbangan penting dalam pemilihan algoritma kriptografi yang tepat untuk melindungi data transmisi. Tidak semua algoritma cocok untuk setiap lingkungan sistem, terutama pada sistem dengan keterbatasan sumber daya seperti perangkat IoT atau sistem mobile.

Berdasarkan kondisi tersebut, diperlukan kajian komparatif yang sistematis terhadap algoritma kriptografi modern untuk memberikan gambaran yang jelas mengenai performa dan tingkat keamanannya dalam konteks perlindungan data transmisi. Penelitian perbandingan menjadi penting agar pengembang sistem, peneliti, dan praktisi keamanan informasi dapat menentukan algoritma yang paling sesuai dengan kebutuhan dan karakteristik sistem yang digunakan. Tanpa analisis perbandingan yang memadai, pemilihan algoritma kriptografi berpotensi tidak optimal dan dapat menimbulkan celah keamanan.

Penelitian ini bertujuan untuk membandingkan beberapa algoritma kriptografi modern yang umum digunakan dalam melindungi data transmisi. Perbandingan dilakukan berdasarkan aspek keamanan, efisiensi komputasi, serta kesesuaian penerapan pada berbagai skenario sistem jaringan. Dengan adanya penelitian ini, diharapkan dapat diperoleh pemahaman yang lebih komprehensif mengenai kelebihan dan kekurangan masing-masing algoritma, sehingga dapat menjadi referensi ilmiah bagi pengembangan dan implementasi sistem keamanan data yang lebih andal.

Dengan meningkatnya ancaman siber dan ketergantungan terhadap sistem digital, kajian mengenai kriptografi modern tidak hanya relevan secara akademis, tetapi juga memiliki implikasi praktis yang signifikan. Oleh karena itu, penelitian ini diharapkan dapat memberikan kontribusi nyata dalam bidang keamanan informasi, khususnya dalam upaya meningkatkan perlindungan data transmisi pada sistem informasi modern.

## 2. METODOLOGI PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini bertujuan untuk memberikan gambaran yang sistematis mengenai tahapan yang dilakukan dalam membandingkan algoritma kriptografi modern dalam melindungi data transmisi. Tahapan penelitian dirancang secara terstruktur agar proses penerapan metode, pengujian, serta analisis hasil dapat dilakukan secara objektif dan dapat dipertanggungjawabkan secara ilmiah. Penelitian ini menggunakan pendekatan komparatif eksperimental, yaitu membandingkan beberapa algoritma kriptografi modern berdasarkan parameter tertentu yang relevan dengan keamanan data transmisi. Secara umum, penelitian ini terdiri dari beberapa tahapan utama yang saling berurutan dan saling berkaitan, dimulai dari studi literatur hingga analisis hasil pengujian. Setiap tahapan dirancang untuk memastikan bahwa hasil penelitian yang diperoleh sesuai dengan tujuan dan mampu memberikan gambaran yang jelas mengenai performa masing-masing algoritma kriptografi.

e-ISSN: 3110-0864 | p-ISSN: XXXX-XXXX
**JURNAL ILMU KOMPUTER DAN TEKNIK INFROMATIKA**
Volume 2 No 1 Januari 2026 | Page: 29-35
https://journals.raskhamedia.or.id/index.php/juikti
DOI: https://doi.org/10.64803/juikti.v2i1.87


**Gambar 1.** Tahapan Penelitian Perbandingan Algoritma Kriptografi Modern

### 2.1 Studi Literatur

Tahap awal penelitian adalah melakukan studi literatur terhadap berbagai sumber ilmiah, seperti jurnal internasional, prosiding konferensi, buku teks, dan standar keamanan informasi yang relevan. Studi literatur bertujuan untuk memahami konsep dasar kriptografi, karakteristik algoritma kriptografi modern, serta parameter evaluasi yang umum digunakan dalam penelitian sebelumnya. Algoritma yang menjadi fokus kajian dalam penelitian ini meliputi algoritma kriptografi simetris dan asimetris yang banyak digunakan dalam sistem transmisi data modern.

### 2.2 Identifikasi dan Penentuan Algoritma

Berdasarkan hasil studi literatur, dilakukan identifikasi algoritma kriptografi modern yang akan dibandingkan. Pemilihan algoritma didasarkan pada tingkat popularitas, relevansi penggunaan dalam sistem transmisi data, serta tingkat keamanan yang diakui secara luas. Algoritma yang dipilih kemudian dikelompokkan berdasarkan jenisnya, yaitu algoritma simetris dan algoritma asimetris, untuk memudahkan proses analisis perbandingan.

### 2.3 Penentuan Parameter Pengujian

Tahap selanjutnya adalah menentukan parameter yang digunakan untuk membandingkan algoritma kriptografi. Parameter pengujian dalam penelitian ini meliputi tingkat keamanan algoritma, kecepatan proses enkripsi dan dekripsi, ukuran kunci, serta efisiensi penggunaan sumber daya. Parameter ini dipilih karena memiliki pengaruh langsung terhadap kinerja algoritma dalam melindungi data transmisi pada berbagai kondisi sistem jaringan.

### 2.4 Implementasi dan Simulasi Pengujian

Pada tahap ini, masing-masing algoritma kriptografi diimplementasikan dalam lingkungan simulasi yang sama untuk menjaga konsistensi hasil pengujian. Data uji yang digunakan memiliki ukuran dan karakteristik yang seragam agar tidak menimbulkan bias dalam pengukuran performa. Proses enkripsi dan dekripsi dilakukan secara berulang untuk memperoleh hasil yang lebih stabil dan representatif.

### 2.5 Pengumpulan dan Pengolahan Data

Hasil dari proses pengujian kemudian dikumpulkan dan dicatat dalam bentuk data kuantitatif. Data tersebut meliputi waktu proses enkripsi, waktu proses dekripsi, serta parameter teknis lainnya yang relevan. Selanjutnya, data diolah dan disajikan dalam bentuk tabel untuk memudahkan analisis dan interpretasi hasil.

**Tabel 1.** Parameter Pengujian Algoritma Kriptografi Modern

| Parameter | Deskripsi |
|---|---|
| Keamanan | Ketahanan algoritma terhadap serangan kriptografi |
| Kecepatan Enkripsi | Waktu yang dibutuhkan untuk proses enkripsi |
| Kecepatan Dekripsi | Waktu yang dibutuhkan untuk proses dekripsi |
| Ukuran Kunci | Panjang kunci yang digunakan algoritma |
| Efisiensi Sumber Daya | Penggunaan CPU dan memori sistem |

Tabel ini menyajikan parameter-parameter yang digunakan sebagai dasar perbandingan antar algoritma, sehingga perbedaan karakteristik dan performa dapat diamati secara jelas.

### 2.6 Analisis dan Evaluasi Hasil

e-ISSN: 3110-0864 | p-ISSN: XXXX-XXXX
**JURNAL ILMU KOMPUTER DAN TEKNIK INFROMATIKA**
Volume 2 No 1 Januari 2026 | Page: 29-35
https://journals.raskhamedia.or.id/index.php/juikti
DOI: https://doi.org/10.64803/juikti.v2i1.87

Tahap terakhir adalah melakukan analisis terhadap hasil pengujian yang telah diperoleh. Analisis dilakukan dengan membandingkan performa masing-masing algoritma berdasarkan parameter yang telah ditentukan. Hasil analisis ini digunakan untuk mengevaluasi keunggulan dan keterbatasan setiap algoritma dalam konteks perlindungan data transmisi.
Melalui tahapan penelitian yang sistematis ini, diharapkan hasil penelitian dapat memberikan gambaran yang objektif dan komprehensif mengenai perbandingan algoritma kriptografi modern. Metode penelitian yang digunakan juga memastikan bahwa proses pengujian dan analisis dilakukan secara terukur, sehingga hasil penelitian dapat dijadikan sebagai referensi yang valid dalam pengembangan dan penerapan sistem keamanan data transmisi.

# 3. HASIL DAN PEMBAHASAN

Bagian ini menyajikan hasil pengujian serta pembahasan terhadap algoritma kriptografi modern yang digunakan dalam penelitian ini. Pembahasan difokuskan pada analisis perbandingan performa algoritma dalam melindungi data transmisi berdasarkan parameter keamanan, kecepatan enkripsi dan dekripsi, ukuran kunci, serta efisiensi penggunaan sumber daya sistem. Seluruh hasil diperoleh melalui tahapan metodologi penelitian yang telah dijelaskan sebelumnya, sehingga proses pengujian dilakukan secara sistematis dan konsisten.
Algoritma kriptografi yang dianalisis dalam penelitian ini mencakup algoritma simetris dan asimetris yang umum digunakan dalam sistem transmisi data modern, yaitu AES, ChaCha20, RSA, dan ECC. Keempat algoritma tersebut dipilih karena mewakili pendekatan kriptografi modern dengan karakteristik dan tingkat kompleksitas yang berbeda, sehingga dapat memberikan gambaran komprehensif mengenai efektivitas masing-masing algoritma dalam konteks keamanan data transmisi.

## 3.1 Pengujian Algoritma Kriptografi

Pengujian dilakukan dengan menggunakan data uji berukuran sama dan lingkungan sistem yang identik untuk memastikan keadilan dalam perbandingan. Proses enkripsi dan dekripsi dijalankan berulang kali untuk memperoleh nilai rata-rata yang stabil dan dapat merepresentasikan performa algoritma secara objektif.

### 3.1.1 Pengujian Kecepatan Enkripsi dan Dekripsi

Kecepatan enkripsi dan dekripsi merupakan parameter penting dalam transmisi data, terutama pada sistem yang membutuhkan pertukaran data secara real-time. Hasil pengujian kecepatan enkripsi dan dekripsi masing-masing algoritma disajikan pada Tabel 2.

**Tabel 2.** Hasil Pengujian Kecepatan Enkripsi dan Dekripsi

| Algoritma | Waktu Enkripsi (ms) | Waktu Dekripsi (ms) |
|---|---|---|
| AES | 12 | 10 |
| ChaCha20 | 9 | 8 |
| RSA | 145 | 160 |
| ECC | 95 | 110 |

Berdasarkan Tabel 2, terlihat bahwa algoritma kriptografi simetris, khususnya ChaCha20 dan AES, memiliki waktu enkripsi dan dekripsi yang jauh lebih cepat dibandingkan algoritma asimetris. ChaCha20 menunjukkan performa terbaik dengan waktu enkripsi dan dekripsi paling rendah. Hal ini disebabkan oleh desain algoritma ChaCha20 yang dioptimalkan untuk efisiensi komputasi pada perangkat dengan keterbatasan sumber daya.

Sebaliknya, algoritma RSA menunjukkan waktu enkripsi dan dekripsi yang paling tinggi. Hal ini disebabkan oleh kompleksitas perhitungan matematika yang digunakan dalam algoritma asimetris, terutama operasi bilangan prima besar. ECC memiliki performa yang lebih baik dibandingkan RSA, tetapi masih kalah jauh jika dibandingkan dengan algoritma simetris.

### 3.1.2 Pengujian Ukuran Kunci dan Tingkat Keamanan

Ukuran kunci berpengaruh langsung terhadap tingkat keamanan suatu algoritma kriptografi. Semakin besar ukuran kunci, semakin sulit algoritma tersebut untuk ditembus melalui serangan brute force. Namun, ukuran kunci yang besar juga berdampak pada performa sistem. Hasil perbandingan ukuran kunci dan tingkat keamanan algoritma disajikan pada Tabel 3.

e-ISSN: 3110-0864 | p-ISSN: XXXX-XXXX
**JURNAL ILMU KOMPUTER DAN TEKNIK INFROMATIKA**
Volume 2 No 1 Januari 2026 | Page: 29-35
https://journals.raskhamedia.or.id/index.php/juikti
DOI: https://doi.org/10.64803/juikti.v2i1.87

**Tabel 3.** Perbandingan Ukuran Kunci dan Tingkat Keamanan

| Algoritma | Ukuran Kunci | Tingkat Keamanan |
|---|---|---|
| AES | 128/192/256 bit | Sangat Tinggi |
| ChaCha20 | 256 bit | Sangat Tinggi |
| RSA | 2048 bit | Tinggi |
| ECC | 256 bit | Sangat Tinggi |

Berdasarkan Tabel 3, terlihat bahwa ECC mampu memberikan tingkat keamanan yang setara dengan RSA meskipun menggunakan ukuran kunci yang jauh lebih kecil. Hal ini menjadi keunggulan utama ECC dalam sistem keamanan modern. AES dan ChaCha20 juga menunjukkan tingkat keamanan yang sangat tinggi dengan ukuran kunci yang relatif efisien.

### 3.1.3 Efisiensi Penggunaan Sumber Daya Sistem

Efisiensi penggunaan sumber daya sistem menjadi parameter penting, terutama pada sistem tertanam, perangkat mobile, dan Internet of Things (IoT). Algoritma yang membutuhkan konsumsi CPU dan memori besar berpotensi menurunkan performa sistem secara keseluruhan.

**Tabel 4.** Efisiensi Penggunaan Sumber Daya

| Algoritma | Penggunaan CPU | Penggunaan Memori |
|---|---|---|
| AES | Rendah | Rendah |
| ChaCha20 | Sangat Rendah | Rendah |
| RSA | Tinggi | Sedang |
| ECC | Sedang | Sedang |

Dari Tabel 4 dapat disimpulkan bahwa ChaCha20 merupakan algoritma paling efisien dalam penggunaan sumber daya, diikuti oleh AES. Algoritma asimetris membutuhkan sumber daya yang lebih besar, terutama RSA yang menunjukkan konsumsi CPU tertinggi.

### 3.2 Analisis Perbandingan Algoritma Simetris

Hasil pengujian menunjukkan bahwa algoritma kriptografi simetris secara konsisten unggul dalam hal kecepatan dan efisiensi sumber daya. AES dan ChaCha20 sama-sama memberikan tingkat keamanan yang tinggi, namun ChaCha20 memiliki keunggulan dalam kecepatan pemrosesan dan efisiensi CPU. Hal ini menjadikan ChaCha20 sangat cocok untuk sistem dengan keterbatasan perangkat keras, seperti perangkat mobile dan IoT.
AES, meskipun sedikit lebih lambat dibandingkan ChaCha20, tetap menjadi algoritma yang sangat andal dan banyak digunakan dalam berbagai standar keamanan internasional. Keunggulan utama AES terletak pada stabilitas, dukungan luas, serta fleksibilitas ukuran kunci.

### 3.3 Analisis Perbandingan Algoritma Asimetris

Algoritma asimetris menunjukkan performa yang lebih rendah dari sisi kecepatan, namun memiliki keunggulan dalam mekanisme distribusi kunci. RSA, meskipun masih banyak digunakan, menunjukkan keterbatasan dari sisi efisiensi komputasi. ECC muncul sebagai alternatif yang lebih modern dan efisien dengan tingkat keamanan yang setara atau bahkan lebih tinggi dibandingkan RSA. Penggunaan ECC sangat direkomendasikan untuk sistem transmisi data yang membutuhkan keamanan tinggi namun tetap memperhatikan efisiensi kinerja, seperti pada protokol keamanan jaringan modern.

### 3.4 Implikasi terhadap Keamanan Data Transmisi

Hasil penelitian ini menunjukkan bahwa tidak terdapat satu algoritma kriptografi yang unggul dalam semua aspek. Pemilihan algoritma harus disesuaikan dengan kebutuhan sistem. Untuk transmisi data berkecepatan

e-ISSN: 3110-0864 | p-ISSN: XXXX-XXXX
**JURNAL ILMU KOMPUTER DAN TEKNIK INFROMATIKA**
Volume 2 No 1 Januari 2026 | Page: 29-35
https://journals.raskhamedia.or.id/index.php/juikti
DOI: https://doi.org/10.64803/juikti.v2i1.87

tinggi, algoritma simetris seperti AES dan ChaCha20 lebih direkomendasikan. Sementara itu, untuk kebutuhan autentikasi dan pertukaran kunci, algoritma asimetris seperti ECC menjadi pilihan yang lebih tepat. Kombinasi algoritma simetris dan asimetris merupakan pendekatan yang paling efektif dalam sistem keamanan transmisi data modern. Pendekatan ini memungkinkan sistem memperoleh kecepatan tinggi sekaligus keamanan yang kuat.

### 3.5 Hasil Perbandingan

Untuk memperjelas hasil penelitian, ringkasan perbandingan algoritma disajikan pada Gambar 2.


**Gambar 2**. Ringkasan Perbandingan Algoritma Kriptografi Modern

Gambar ini menggambarkan posisi relatif masing-masing algoritma berdasarkan parameter keamanan dan performa, sehingga memudahkan pembaca dalam memahami hasil penelitian secara visual.

### 3.6 Diskusi

Hasil penelitian ini sejalan dengan berbagai penelitian sebelumnya yang menyatakan bahwa algoritma kriptografi simetris lebih unggul dalam aspek performa, sementara algoritma asimetris lebih kuat dalam mekanisme distribusi kunci. Namun, penelitian ini menegaskan bahwa ECC merupakan algoritma asimetris yang lebih relevan untuk diterapkan pada sistem modern dibandingkan RSA. Keterbatasan penelitian ini terletak pada lingkungan simulasi yang digunakan. Pengujian pada lingkungan nyata dengan variasi beban jaringan yang lebih kompleks berpotensi memberikan hasil yang lebih beragam. Meskipun demikian, hasil yang diperoleh sudah cukup representatif untuk menggambarkan karakteristik utama masing-masing algoritma.

## 4. KESIMPULAN

Penelitian ini bertujuan untuk membandingkan algoritma kriptografi modern dalam melindungi data transmisi berdasarkan aspek keamanan, performa, ukuran kunci, serta efisiensi penggunaan sumber daya sistem. Berdasarkan hasil pengujian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa setiap algoritma kriptografi memiliki karakteristik dan keunggulan masing-masing yang tidak dapat digeneralisasi untuk semua kebutuhan sistem. Algoritma kriptografi simetris, khususnya AES dan ChaCha20, terbukti memiliki keunggulan signifikan dari sisi kecepatan enkripsi dan dekripsi serta efisiensi penggunaan sumber daya, sehingga sangat sesuai untuk sistem transmisi data yang membutuhkan performa tinggi dan respons cepat. Di sisi lain, algoritma kriptografi asimetris memiliki peran penting dalam mekanisme distribusi kunci dan autentikasi. RSA, meskipun masih banyak digunakan, menunjukkan keterbatasan dalam efisiensi komputasi dan konsumsi sumber daya. Sementara itu, ECC mampu memberikan tingkat keamanan yang setara atau lebih tinggi dibandingkan RSA dengan ukuran kunci yang lebih kecil, sehingga menjadikannya lebih relevan untuk sistem keamanan modern. Hasil penelitian ini menunjukkan bahwa ECC merupakan alternatif yang lebih efisien dan aman untuk menggantikan RSA dalam berbagai skenario transmisi data. Secara keseluruhan, penelitian ini menegaskan bahwa pendekatan kombinasi antara algoritma kriptografi simetris dan asimetris merupakan solusi yang paling efektif dalam melindungi data transmisi. Pemilihan algoritma kriptografi harus disesuaikan dengan kebutuhan sistem, karakteristik lingkungan, dan keterbatasan sumber daya. Dengan demikian, hasil penelitian ini diharapkan dapat menjadi referensi ilmiah yang bermanfaat dalam pengembangan dan penerapan sistem keamanan data transmisi yang andal dan efisien.

e-ISSN: 3110-0864 | p-ISSN: XXXX-XXXX
**JURNAL ILMU KOMPUTER DAN TEKNIK INFROMATIKA**
Volume 2 No 1 Januari 2026 | Page: 29-35
https://journals.raskhamedia.or.id/index.php/juikti
DOI: https://doi.org/10.64803/juikti.v2i1.87

## REFERENCES

[1] B. W. Aulia, M. Rizki, P. Prindiyana, and S. Surgana, "Peran Krusial Jaringan Komputer dan Basis Data dalam Era Digital," *JUSTINFO | J. Sist. Inf. dan Teknol. Inf.*, vol. 1, no. 1, pp. 9–20, 2023, doi: 10.33197/justinfo.vol1.iss1.2023.1253.

[2] M. Mirna, Judhariksawan, and Maskum, "Analisis Pengaturan Keamanan Data Pribadi Di Indonesia," *J. Ilm. Living Law*, vol. 15, no. 1, pp. 16–30, 2023, doi: 10.30997/jill.v15i1.4726.

[3] Dola Ramalinda, Jayadi, and Agung Rachmat Raharja, "Strategi Perlindungan Data Menggunakan Sistem Kriptografi Dalam Keamanan Informasi," *J. Int. Multidiscip. Res.*, vol. 2, no. 6, pp. 665–671, 2024, doi: 10.62504/jimr679.

[4] H. Pribadi Fitrian, N. Alia Destiara, N. Elsa Destianti, and G. Maddanil Khowat, "Analisis Penerapan Teknologi Virtual Private Network (Vpn) Sebagai Solusi Keamanan Data Di Jaringan Publik," *JATI (Jurnal Mhs. Tek. Inform.*, vol. 9, no. 1, pp. 1559–1563, 2025, doi: 10.36040/jati.v9i1.12712.

[5] Naswa Fiolla Anggraini and Sidi Ahyar Wiraguna, "Tanggung Jawab Hukum Platform Pinjaman Online terhadap Penyalahgunaan dan Penyebaran Data Pribadi Konsumen secara Ilegal," *RISOMA J. Ris. Sos. Hum. dan Pendidik.*, vol. 3, no. 3, pp. 144–167, 2025, doi: 10.62383/risoma.v3i3.767.

[6] Fefiana Diny Hermawati *et al.*, "Keamanan E-Voting Di Indonesia Melalui Pemanfaatan Kriptografi Pada Sistem AES (Advance Encryption Standard)," *J. Tek. Mesin, Ind. Elektro dan Inform.*, vol. 2, no. 2, pp. 45–56, 2023, doi: 10.55606/jtmei.v2i2.1625.

[7] Alisa Almadira, Yogi Pratama, and Fenny Purwani, "Melindungi Data Di Dunia Digital: Peran Stategis Enkripsi Dalam Keamanan Data," *J. Sci. Res. Dev.*, vol. 6, no. 2, pp. 540–549, 2024, doi: 10.56670/jsrd.v6i2.608.

[8] V. M. Hidayah, D. I. Mulyana, and Y. Bachtiar, "Algoritma Caesar Cipher atau Vigenere Cipher pada Pengenkripsian Pesan Teks," *J. Educ.*, vol. 5, no. 3, pp. 8563–8573, 2023, doi: 10.31004/joe.v5i3.1647.

[9] P. Dian Firmansyah *et al.*, "Manajemen Sekuriti Dalam Era-Digital Untuk Mengoptimalisasi Perlindungan Data Dengan Teknologi Lanjutan," *J. Kewirausahaan dan Multi Talent.*, vol. 2, no. 2, pp. 112–125, 2024, doi: 10.38035/jkmt.v2i2.160.

[10] A. Ridho and M. A. Romli, "Sistem Pengamanan Dokumen Menggunakan Algoritma Kriptografi Advanced Encryption Standard (Aes-256)," *J. Inform. Teknol. dan Sains*, vol. 6, no. 4, pp. 1044–1052, 2024, doi: 10.51401/jinteks.v6i4.4887.

[11] Z. Arif and A. Nurokhman, "Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi," *J. Teknol. Sist. Inf.*, vol. 4, no. 2, pp. 394–405, 2023, doi: 10.35957/jtsi.v4i2.6077.

[12] Melenia Bayu Aryanto, Muhlis Tahir, Silvia Irma Devita, Zuda Nuril Mustofa, Qurrotun Ainiyah, and Shelviatus Sundoro, "Implementasi Enkrip Dan Dekrip File Menggunakan Metode Advance Encryption Standard (AES-128)," *J. Ilm. Sist. Inf. dan Ilmu Komput.*, vol. 3, no. 1, pp. 89–104, 2023, doi: 10.55606/juisik.v3i1.434.

[13] M. A. Nurpiansyah and T. Asra, "Implementasi Network Attached Storage Synology dengan High Availability dan Akses Aman Melalui VPN dan Two Authentication di PT Mitra Tera Sinergi," *J. Komput. Teknol. Inf. Sist. Inf.*, vol. 4, no. 2, pp. 1241–1253, 2025, doi: 10.62712/juktisi.v4i2.620.

[14] R. K. Abdullah, N. F. Azhar, S. Mujahidin, and R. O. Hoan, "Implementing AES-RSA Hybrid Encryption to Enhance the Security of Salary Slip Distribution Information System," *Jambura J. Electr. Electron. Eng.*, vol. 7, no. 1, pp. 33–40, 2025, doi: 10.37905/jjeee.v7i1.28737.

[15] P. Iqlima, M. Rayyan, A. Z. A. Rambe, E. Ardina, D. F. A. Lubis, and D. Ismawati, "Implementasi Sistem Keamanan Data Menggunakan Algoritma Kriptografi Asimetris Elliptic Curve Cryptography (ECC) Berbasis Website," *JIKUM J. Ilmu Komput.*, vol. 1, no. 1, pp. 7–11, 2025, doi: 10.62671/jikum.v1i1.37.