PERBANDINGAN ALGORITMA KRIPTOGRAFI SIMETRIS DAN ASIMETRIS DALAM KEAMANAN DATA DIGITAL

Muhammad Zuna, Anita Wulansari, Agung Brastama Putra
Program Studi Sistem Informasi Fakultas Ilmu Komputer
Universitas Pembangunan Nasional "VETERAN" Jawa Timur
Muhammadzuna30@gmail.com

ABSTRAK

Penelitian ini menganalisis perbandingan algoritma kriptografi simetris dan asimetris dalam menjaga keamanan data digital melalui kajian literatur terhadap tujuh jurnal terbitan 2016-2025. Hasil kajian menunjukkan bahwa algoritma simetris seperti AES dan DES unggul dari segi efisiensi dan kecepatan, namun lemah pada distribusi kunci. Sebaliknya, algoritma asimetris seperti RSA dan ECC memiliki keamanan tinggi pada pertukaran kunci, tetapi membutuhkan sumber daya dan waktu proses lebih besar. Berdasarkan sintesis literatur, penelitian ini merekomendasikan penggunaan hybrid cryptosystem yang mengombinasikan kedua pendekatan tersebut untuk mencapai keseimbangan antara efisiensi dan keamanan data digital.

Kata kunci : *Kriptografi, Simetris, Asimetris, Keamanan Data, Enkripsi.*

1. PENDAHULUAN

Perkembangan teknologi informasi masa kini sedang berkembang dengan cepat, terutama kepada pengelolaan data digital yang dapat dilihat secara nyata perkembangannya. Di sisi lain, berkembangnya pengelolaan berbanding lurus dengan risiko baru yang mungkin timbul, seprti ancaman terhadap keamanan data, seperti pencurian informasi, peretasan, serta penyalahgunaan data pribadi dan institusional [1]. Hal ini menyebabkan keamanan data menjadi salah satu isu utama yang harus diperhatikan lebih serius dalam menyambut eta sistem informasi yang lebih modern.

Salah satu yang dapat memperkuat keamanan data adalah penerapan kriptografi, yang merupakan suatu metode penyandian data yang memungkinan pesan hanya bisa diakses oleh pihak yang memiliki wewenang. Menurut [2] kriptografi memberikan jaminan empat prinsip utama keamanan informasi yang paling penting, yaitu kerahasiaan *(confidentiality*), keutuhan *(integrity)*, otentikasi *(authentication)*, dan non-penyangkalan (*non-repudiation)*. Dalam perkembangan teknologi yang lebih modern, kriptografi tidak hanya digunakan pada sistem komunikasi dan penyandian data, tetapi juga menjadi dasar bagi bermacam aplikasi teknologi seperti transaksi perbankan digital, sertifikat keamanan situs web (SSL/TLS), dan sistem identitas elektronik.

Secara umum, kriptografi dua menjadi dua pendekatan utama, yaitu kriptografi simetris dan kriptografi asimetris. Kriptografi simetris adalah metode enkripsi dengan penggunaaan satu kunci yang sama untuk proses enkripsi dan dekripsi. Sebaliknya, kriptografi asimetris menggunakan dua kunci berbeda, yaitu kunci publik dan kunci privat. Kedua metode ini memiliki karakteristik yang jelas dapat terlihat bedanya dalam hal keamanan, kecepatan, serta efisiensi komputasi. [7].

Penelitian Putri menyebutkan jika kriptografi simetris seperti AES memiliki keunggulan yang signifikan dalam kecepatan pemrosesan data dan memiliki kelemahan utama yang terletak pada distribusi kunci. Kelemahan ini dapat terjadi fatal apabila kunci tersebut diketahui oleh pihak yang tidak berwenang, karena dengan demikian pihak tersebut dapat mengakses seluruh sistem enkripsi. Sebaliknya, algoritma asimetris seperti RSA, yang dikembangkan oleh Rivest, Shamir, dan Adleman, memberikan tingkat keamanan yang lebih tinggi dalam pertukaran kunci, namun membutuhkan waktu pemrosesan yang relatif lebih lama.

Pendapat tersebut juga sejalan dengan [2] yang kembali menegaskan bahwa kedua pendekatan ini memiliki keunggulan dan kelemahan masing-masing, dan pemilihan metode yang digunakan harus mempertimbangkan faktor kompleksitas komputasi dan tingkat keamanan data yang diinginkan. Berdasarkan berbagai penelitian terdahulu, muncul gagasan tentang *hybrid cryptosystem*, yaitu sistem yang menggunakan kombinasi algoritma simetris dan asimetris untuk mendapatkan keseimbangan antara efisiensi dan keamanan [3].

Berdasarkan latar belakang inilah, penelitian ini dibuat dengan berfokus pada analisis perbandingan algoritma kriptografi simetris dan asimetris dalam konteks keamanan data digital.

2. TINJAUAN PUSTAKA

2.1. Konsep Dasar Kriptogarfi

Kriptografi merupakan bidang ilmu yang berfokus pada teknik penyandian informasi agar hanya dapat diakses oleh pihak yang berwenang. Secara etimologis, istilah *kriptografi* berasal dari bahasa Yunani, yaitu *kryptos* yang berarti "rahasia" dan *graphein* yang berarti "menulis". Artinya, kriptografi dapat diartikan secara sederhana sebagai "tulisan rahasia" [2]. Dalam perkembangannya, kriptografi

tidak hanya berurusan dengan penyembunyian pesan, tetapi juga mencakup penerapan konsep matematis untuk menjaga kerahasiaan, keutuhan, serta keaslian data [1]

Pada praktiknya, kriptografi modern digunakan dalam berbagai sistem digital, mulai dari komunikasi internet yang aman, autentikasi pengguna, hingga perlindungan terhadap data sensitif. [7] menyoroti bahwa meningkatnya ancaman siber membuat penerapan kriptografi menjadi elemen penting dalam menjaga keamanan informasi berbasis jaringan. Oleh karena itu, pemahaman terhadap karakteristik dan performa algoritma kriptografi menjadi hal yang sangat dibutuhkan agar sistem yang dibangun dapat berfungsi secara optimal.

Menurut [2] kriptografi adalah ilmu sekaligus seni menjaga keamanan pesan. Pandangan ini menegaskan bahwa keberhasilan kriptografi tidak hanya bergantung pada kekuatan algoritma, tetapi juga pada manajemen kunci dan penerapannya dalam sistem yang nyata. Secara umum, proses kriptografi terdiri dari dua tahap utama, yaitu enkripsi dan dekripsi. Enkripsi mengubah pesan asli (*plaintext*) menjadi bentuk sandi (*ciphertext*), sedangkan dekripsi mengembalikannya ke bentuk semula. Proses tersebut dapat digambarkan secara matematis melalui fungsi:

$$E_k(M) = C \quad \text{dan} \quad D_k(C) = M$$

di mana E_k adalah fungsi enkripsi dengan kunci k, D_k fungsi dekripsi, M pesan asli, dan C hasil enkripsi.

Dalam sistem kriptografi modern, keamanan tidak lagi bergantung pada kerahasiaan algoritmanya, melainkan pada kunci yang digunakan. Prinsip ini dikenal sebagai *Kerckhoffs' Principle*, yang menyatakan bahwa sebuah sistem kriptografi tetap harus aman walaupun seluruh algoritmanya diketahui publik, selama kuncinya tetap rahasia [6] Prinsip ini menjadi dasar bagi pengembangan berbagai algoritma enkripsi yang digunakan hingga saat ini.

Secara umum, kriptografi dibedakan menjadi dua jenis utama berdasarkan cara penggunaan kuncinya, yaitu kriptografi simetris dan kriptografi asimetris.

2.2. Kriptografi Simetris

Kriptografi simetris menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi. Menurut [6], keunggulan utama metode ini terletak pada kecepatannya, karena operasi matematis yang digunakan relatif sederhana dan efisien. Beberapa algoritma populer yang termasuk dalam kategori ini antara lain *Data Encryption Standard* (DES), *Triple DES* (3DES), *Advanced Encryption Standard* (AES), dan *Blowfish.*

Di antara berbagai algoritma tersebut, AES menjadi standar yang paling banyak digunakan saat ini. AES memiliki keunggulan dalam menghasilkan efek *avalanche* yang ideal, yaitu perubahan besar pada hasil enkripsi akibat perubahan kecil pada input. [4]. Efek ini menunjukkan tingkat difusi yang tinggi dan menjadi indikator penting bagi kekuatan enkripsi.

Meski efisien, kriptografi simetris memiliki tantangan utama pada distribusi kunci. Karena kunci yang digunakan sama, maka pengirim dan penerima harus memiliki kunci identik sebelum proses komunikasi berlangsung. Jika kunci tersebut bocor, maka seluruh sistem menjadi tidak aman [1]. Menambahkan bahwa semakin banyak pengguna dalam sistem, semakin sulit pula mengatur distribusi dan penyimpanan kunci, sehingga metode ini kurang ideal untuk sistem berskala besar.

2.3. Kriptografi Asimetris

Berbeda dengan metode simetris, kriptografi asimetris menggunakan dua kunci berbeda: kunci publik (public key) dan kunci privat (private key). Kunci publik digunakan untuk mengenkripsi pesan, sementara kunci privat dipakai untuk mendekripsi [7]. Pendekatan ini memberikan keamanan tambahan karena hanya kunci privat yang perlu dijaga kerahasiaannya oleh pemilik.

Beberapa algoritma yang umum digunakan dalam sistem asimetris adalah RSA (Rivest–Shamir–Adleman), Elliptic Curve Cryptography (ECC), Digital Signature Algorithm (DSA), dan Diffie-Hellman Key Exchange. Menurut [2]. RSA dikenal dengan tingkat kompleksitas matematis yang tinggi karena melibatkan operasi eksponensial modular pada bilangan prima besar. Keamanannya bergantung pada sulitnya proses faktorisasi bilangan tersebut. Sementara itu, ECC menawarkan keamanan setara dengan RSA tetapi menggunakan ukuran kunci yang lebih kecil, sehingga lebih efisien untuk perangkat dengan kapasitas terbatas [7].

Algoritma asimetris dikenal memiliki kinerja yang lebih lambat dibandingkan metode simetris. Penelitian Putri et al. (2021) menunjukkan bahwa proses enkripsi menggunakan RSA pada citra digital membutuhkan waktu lebih lama dibandingkan AES. Hal ini terjadi karena perhitungan matematis pada algoritma asimetris jauh lebih kompleks dan melibatkan operasi bilangan besar. Dalam penerapan nyata, karakteristik tersebut membuat kriptografi asimetris lebih cocok untuk kebutuhan autentikasi dan pertukaran kunci, sedangkan enkripsi data berukuran besar masih lebih efisien jika dilakukan dengan algoritma simetris.

3. METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan studi literatur (literature review) untuk menelaah dan membandingkan algoritma kriptografi simetris dan asimetris. Pemilihan metode ini dilakukan karena fokus penelitian bukan pada uji coba langsung, melainkan pada analisis konseptual dan teoritis yang bersumber dari berbagai publikasi ilmiah. Pendekatan semacam ini memungkinkan peneliti memahami kerangka kerja dan arah perkembangan teknologi kriptografi dari beragam perspektif.

Menurut [6], studi literatur merupakan cara untuk memperoleh pemahaman yang menyeluruh melalui

proses telaah dan sintesis terhadap berbagai sumber tertulis. Hal serupa disampaikan [7] yang menilai bahwa metode ini membantu peneliti mengidentifikasi pola, tren, dan celah penelitian yang masih terbuka.

Tahapan penelitian dilakukan melalui empat langkah utama. Pertama, tahap pengumpulan data, yaitu proses identifikasi dan seleksi literatur dari berbagai jurnal nasional maupun internasional yang membahas algoritma kriptografi. Kedua, tahap analisis kritis yang berfokus pada perbandingan variabel seperti kecepatan enkripsi, tingkat keamanan, kompleksitas komputasi, serta konteks penerapannya. Ketiga, tahap sintesis temuan, di mana hasil analisis dari masing-masing sumber digabungkan untuk membentuk gambaran menyeluruh tentang performa dua jenis kriptografi tersebut. Terakhir, tahap penyusunan hasil perbandingan, yang dituangkan dalam tabel untuk menampilkan keunggulan dan keterbatasan setiap metode secara ringkas.

Tabel berikut memperlihatkan hasil perbandingan antara kriptografi simetris dan asimetris berdasarkan hasil sintesis literatur:

Tabel 1. Perbandingan Kriptografi

Aspek	Kriptografi Simetris	Kriptografi Asimetris
Jumlah kunci	Menggunakan satu kunci yang sama untuk enkripsi dan dekripsi.	Menggunakan dua kunci berbeda (publik dan privat).
Kecepatan proses	Lebih cepat dan efisien karena algoritma matematis sederhana (Rahmaniah et al., 2023).	Lebih lambat akibat perhitungan eksponensial besar (Putri et al., 2021)
Keamanan distribusi kunci	Lemah karena kunci harus dibagikan kepada pihak penerima (Basri, 2020)	Sangat kuat, karena kunci publik dapat disebarkan tanpa mengancam keamanan kunci privat (Saputro et al., 2020)
Kompleksitas komputasi	Rendah, cocok untuk perangkat dengan kapasitas terbatas (Prabowo & Anwar, 2025)	Tinggi, membutuhkan daya pemrosesan besar (Basri, 2020)
Konteks penggunaan	Cocok untuk enkripsi data besar (file, backup, sistem penyimpanan).	Cocok untuk autentikasi, tanda tangan digital, dan pertukaran kunci (Amalya et al., 2023)
Contoh algoritma	AES, DES, Blowfish, 3DES.	RSA, ECC, DSA, Diffie–Hellman.

Hasil analisis menunjukkan bahwa tidak ada satu metode kriptografi yang benar-benar unggul di semua aspek. Pemilihan algoritma bergantung pada kebutuhan sistem serta kondisi operasionalnya. [6] menyebut bahwa sistem yang menuntut kecepatan tinggi lebih sesuai menggunakan algoritma simetris seperti AES. Sebaliknya, algoritma asimetris seperti RSA atau ECC lebih efektif ketika keamanan pertukaran kunci menjadi prioritas utama.

Perbandingan dua pendekatan ini sebaiknya dilihat dari keseimbangan antara efisiensi dan tingkat keamanan [1]. Konsep *hybrid cryptosystem* yang diusulkan [3] berupaya menjembatani kedua kebutuhan tersebut. Dalam pendekatan ini, algoritma simetris digunakan untuk mengenkripsi data utama, sedangkan algoritma asimetris bertugas melindungi kunci simetris. Kombinasi ini menghasilkan sistem yang lebih efisien sekaligus tetap aman, dan telah menjadi dasar bagi berbagai protokol keamanan modern seperti HTTPS serta SSL/TLS.

Metodologi penelitian ini diharapkan mampu memberikan gambaran objektif mengenai performa dua jenis kriptografi tersebut. Selain menjadi acuan teoritis, hasilnya juga dapat dimanfaatkan sebagai pijakan bagi penelitian lanjutan maupun penerapan nyata dalam bidang keamanan siber.Metodologi ini secara keseluruhan bertujuan menghasilkan kajian yang objektif, komprehensif, dan berbasis bukti literatur, sehingga dapat dijadikan dasar untuk penelitian lanjutan maupun implementasi praktis di bidang keamanan siber.

4. HASIL DAN PEMBAHSAN

4.1. Analisis Umum Kriptografi Simetris dan Asimetris

Kajian literatur menunjukkan bahwa kriptografi simetris dan asimetris memiliki tujuan serupa, yakni melindungi data digital melalui proses enkripsi dan dekripsi. Keduanya berbeda dalam hal efisiensi, tingkat keamanan, serta kompleksitas komputasi yang dibutuhkan.

Algoritma simetris menggunakan satu kunci untuk proses enkripsi dan dekripsi, sehingga strukturnya relatif sederhana dan lebih cepat dalam memproses data [2]. Karakter ini membuatnya banyak digunakan pada sistem yang membutuhkan respons tinggi seperti penyimpanan data berukuran besar atau komunikasi real-time. Di sisi lain, kriptografi asimetris bekerja dengan dua kunci yang saling berkaitan secara matematis, yaitu kunci publik dan privat. Pendekatan ini mampu meningkatkan keamanan pertukaran data, meskipun memerlukan daya komputasi yang lebih besar.

Membandingkan beberapa algoritma simetris seperti AES, DES, 3DES, dan Blowfish [6]. Hasilnya menunjukkan bahwa AES memiliki kinerja paling efisien dengan waktu enkripsi yang lebih singkat. Struktur Substitution-Permutation Network (SPN) yang kompleks membuat AES tetap unggul dari sisi keamanan, walau proses distribusi kunci masih menjadi tantangan tersendiri.

Keunggulan algoritma asimetris seperti RSA dan ECC. RSA mengandalkan kesulitan faktorisasi bilangan prima besar, sedangkan ECC memanfaatkan

kompleksitas kurva eliptik [7]. Menariknya, ECC dapat mencapai tingkat keamanan yang setara dengan RSA meski menggunakan panjang kunci yang lebih pendek, sehingga lebih efisien untuk perangkat dengan sumber daya terbatas seperti ponsel pintar atau sistem IoT.

4.2. Analisis Kinerja dan Kompleksitas Komputasi

Kinerja algoritma kriptografi biasanya dinilai dari kecepatan enkripsi-dekripsi dan penggunaan sumber daya sistem. [4] mengukur kinerja ini dengan efek avalanche, yaitu sejauh mana perubahan kecil pada input memengaruhi hasil enkripsi. Mereka menemukan bahwa AES-128 memiliki efek avalanche mendekati 50%, menandakan perubahan 1 bit pada plaintext dapat memengaruhi ciphertext secara signifikan. Hal ini menunjukkan kemampuan difusi yang baik dalam melindungi data dari serangan statistik.

Dari segi kompleksitas, [2] menyoroti bahwa algoritma asimetris seperti RSA memerlukan waktu proses lebih lama karena melibatkan perhitungan eksponensial modular. Panjang kunci berpengaruh langsung terhadap keamanan sekaligus waktu komputasi. Ia menulis bahwa meskipun prosesnya lebih kompleks, metode asimetris mampu memberikan tingkat keamanan yang lebih baik.

Hasil serupa disampaikan oleh Putri et al. (2021) yang membandingkan AES dan RSA untuk enkripsi citra digital. AES terbukti jauh lebih cepat dan efisien, sedangkan RSA unggul dalam keamanan pertukaran kunci serta autentikasi. Temuan tersebut menunjukkan adanya hubungan terbalik antara efisiensi dan keamanan maka semakin tinggi tingkat keamanan, semakin besar beban komputasi yang dibutuhkan.

4.3. Analisis Aspek Keamanan

Aspek keamanan dalam kriptografi mencakup empat elemen utama: kerahasiaan, keutuhan, autentikasi, dan non-penyangkalan [1]. Pada sistem simetris, perlindungan data bergantung pada satu kunci yang digunakan bersama antara pengirim dan penerima. Jika kunci tersebut bocor, seluruh pesan terenkripsi dapat diakses oleh pihak tidak berwenang, menjadikan distribusi kunci sebagai titik paling rentan dalam metode ini.

Pendekatan asimetris menawarkan mekanisme yang lebih aman karena menggunakan dua kunci yang berbeda. Kunci publik bisa dibagikan secara bebas tanpa menurunkan tingkat keamanan, sebab proses dekripsi hanya dapat dilakukan dengan kunci privat. [7] menjelaskan bahwa karakteristik ini memungkinkan penggunaan tanda tangan digital yang dapat memastikan integritas dan keaslian pesan.

Dalam praktik tanda tangan digital berbasis RSA, hash pesan dienkripsi menggunakan kunci privat pengirim, lalu diverifikasi oleh penerima melalui kunci publik. Langkah ini memastikan pesan tidak diubah selama proses pengiriman sekaligus membuktikan identitas pengirim. Sistem hybrid yang dikemukakan oleh [3] mampu meningkatkan keamanan tanpa mengorbankan kecepatan. Pada model tersebut, data utama dienkripsi dengan algoritma simetris seperti AES, sedangkan kunci AES itu sendiri diamankan menggunakan RSA. Hanya pihak yang memiliki kunci privat RSA yang dapat membuka akses ke data. Pendekatan ini efektif dalam mencegah serangan seperti man-in-the-middle atau pencurian kunci.

Putri menilai konsep hybrid sebagai solusi paling seimbang, karena mampu memadukan kecepatan metode simetris dengan tingkat keamanan yang dimiliki sistem asimetris [2].

4.4. Analisis Implementasi dalam Sistem Keamanan Digital

Kriptografi simetris dan asimetris banyak diterapkan dalam sistem keamanan digital modern. Salah satu contoh yang paling umum adalah protokol HTTPS. Dalam mekanisme ini, proses pertukaran kunci awal menggunakan algoritma asimetris seperti RSA atau ECC, sedangkan enkripsi data selanjutnya menggunakan algoritma simetris seperti AES atau ChaCha20. Kombinasi ini memberikan keseimbangan antara kecepatan dan keamanan [7].

Menekankan peran penting kriptografi dalam menjaga integritas data organisasi, terutama menghadapi ancaman seperti malware, sniffing, dan ransomware. Penerapannya tidak terbatas pada komunikasi data, tetapi juga meluas ke penyimpanan cloud, transaksi keuangan digital, hingga perangkat IoT [1].

Pemilihan algoritma mempertimbangkan kebutuhan sistem. Untuk aplikasi yang memerlukan kecepatan tinggi, metode simetris lebih tepat, sedangkan asimetris lebih efektif untuk autentikasi dan distribusi kunci [6]. [4] juga menyoroti aspek efisiensi energi, terutama untuk perangkat bergerak. Mereka menemukan bahwa AES-128 memerlukan daya pemrosesan lebih rendah dibanding algoritma lain, sehingga cocok digunakan pada konteks mobile computing. Atas dasar hal ini lah, sistem hybrid kembali dipandang sebagai solusi paling realistis untuk menjaga keseimbangan performa dan keamanan

4.5. Proses Enkripsi AES

Proses enkripsi algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns dan AddRoundKey. Pada awal proses enkripsi, input yang telah dicopykan ke dalam state akan mengalami transformasi byte AddRoundKey.Setelah itu state akan mengalami transformasi SubBytes, ShiftRows MixColumns, dan AddRoundKey secara berulang-ulang sebanyak [8]. Proses ini dalam algoritma AES disebut sebagai round function. Round yang terakhir agak berbeda dengan round-round sebelumnya dimana pada round terakhir, state tidak mengalami transformasi MixColumns :

a. SubBytes
   Prinsip dari SubBytes adalah menukar isi matriks/tabel yang ada dengan matriks/tabel lain yang disebut dengan Rijndael S-Box.
b. ShiftRows
   ShiftRows seperti namanya adalah sebuah proses yang melakukan shift atau pergeseran pada setiap elemen blok/tabel yang dilakukan perbarisnya
c. Mixcolumns
   Yang terjadi saat MixColumns adalah mengalikan tiap elemen dari blok chiper dengan matriks dengan pengalian dilakukan seperti perkalian matriks biasa yaitu menggunakan dot product.
d. AddRoundKey
   Add Round Key pada dasarnya adalah mengkombinasikan chiper teks ya n g sudah ada dengan chiperkey yang chiper key dengan hubungan XOR

4.6. Proses Deskripsi RSA

Dekripsi digunakan untuk mengubah pesan hasil enkripsi (chipertext) menjadi pesan asli (plaintext) yaitu dengan menggunakan rumus untuk dekripsi RSA sebagai berikut [9] :

P = Cd mod n.

a. Ambil pesan (cipherteks) yang telah diterima.
b. Kemudian ambil kunci rahasia d dan modulus n atau (d,n)
c. Potong pesan menjadi blok-blok pesan c1, c2, c3, ... dengan nilai setiap bloknya adalah $0 \leq c \leq n-1$
d. Hitung mi = cid mod n.
e. Susun nilai m hasil dekripsi dengan susunan m1, m2, m3,.mn sehingga diperoleh plainteks (pesan asli) dari cipherteks yang diterima.

Perbandingan yang dilakukan pada penelitian ini dengan cara mengeksekusi dan menerapkan kedua algoritma kriptografi simetris dan asimteris yaitu AES yang tergolong kedalam simetris dan RSA yang asimetris, perbandingan dilakukan untuk mencari tau waktu eksekusi dan menghitung pendeskripsian waktu dari kedua algoritma [10].

5. KESIMPULAN DAN SARAN

Hasil kajian literatur menunjukkan bahwa algoritma kriptografi simetris dan asimetris saling melengkapi dalam menjaga keamanan data digital. Algoritma simetris seperti AES unggul dalam kecepatan dan efisiensi, sehingga sesuai untuk pemrosesan data besar. Namun, kelemahan utamanya terletak pada distribusi kunci yang rawan kebocoran

Sebaliknya, algoritma asimetris seperti RSA dan ECC menawarkan keamanan tinggi pada autentikasi dan pertukaran kunci , meski membutuhkan waktu komputasi lebih panjang. Beberapa penelitian membuktikan bahwa sistem hybrid yang menggabungkan kedua pendekatan dapat menyeimbangkan efisiensi dan keamanan dengan baik.

Menguji performa algoritma simetris dan asimetris secara eksperimental pada data besar dan perangkat bergerak. Mengembangkan sistem *hybrid* adaptif yang mampu menyesuaikan jenis enkripsi dengan kebutuhan performa dan keamanan. Mengeksplorasi potensi kriptografi kuantum sebagai alternatif jangka panjang dalam menghadapi tantangan komputasi modern.

DAFTAR PUSTAKA

[1] Amalya, N., Silalahi, S. M. S., Silalahi, S., Nasution, D. F., Sari, M., & Gunawaan, I. (2023). Kriptografi dan Penerapannya Dalam Sistem Keamanan Data. *Jurnal Media Informatika*, *4*, 90–93.

[2] Basri. (2020). Kriptografi simetris dan asimetris dalam perspektif keamanan data dan kompleksitas komputasi. *Jurnal Ilmiah Ilmu Komputer*, *2*(2).

[3] Jamaludin. (2021). Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem. *Jurnal Sinkron*, *2*(April 2018).

[4] Prabowo, W., & Anwar, N. (2025). Pengujian Model Simulasi Efek Avalanche Kriptografi Simetris Algoritma AES 128-bit , Mode ECB dan CBC. *Jurnal Ikrath*, *9*(1), 178–186.

[5] jam, G. G., Styorini, W., & Rahayani, R. D. (2021). Pendahuluan Dengan berkembang pesatnya teknologi , menjadikan internet sebagai wadah utama dalam Landasan Teori Kriptografi Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara Algoritm Kriptografi Algoritma kriptografi disebut jug. *Jurnal Penelitian Dan Pengabdian Masyarakat*, 197–207.

[6] Rahmaniah, R., Aditya, M. F., Arfanda, W., Purnama, V. N., & Dara, C. (2023). Studi Algoritma Kriptografi Kunci Simteris Pada Keamanan Data dengan Metode Komparasi. *Jurnal Siteba*, *2*(1), 7–14.

[7] Saputro, T. H., Hidayati, N., & Ujianto, E. I. . (2020). Survei tentang algoritma kriptografi asimetris. *Jurnal Informatika Polinema*, 67–72.

[8] Tulloh et al., "Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen Cryptography Advanced Encryption Standard (AES) for File Document Encryption," J. Mat. UNISBA, vol. Vol 2, no. 1, pp. 1–8, 2024

[9] Sari, H. D. Purnomo, and I. Sembiring, "Review: Algoritma Kriptografi Sistem Keamanan SMS di Android," J. Inf. Technol., vol. 2, no. 1, pp. 11–15, 2 022 , doi: 10.46229/jifotech.v2i1.292

[10] Sulistiyorini and A. Prihanto, "Perbandingan Efisiensi Algoritma RSA dan RSA-CRT Dengan Data Teks Berukuran Besar," J. Informatics Comput. Sci., v ol. 1, no. 02, pp. 84–90, 2020, doi: 10.26740/jinacs.v1n02.p84-90