BAB I

PENDAHULUAN

1.1 Latar Belakang

File dokumen umumnya berisi informasi penting milik individu maupun perusahaan, seperti laporan rahasia, strategi bisnis, data administrasi, serta arsip organisasi. Dokumen yang tidak dilindungi dengan baik berpotensi dicuri, diakses oleh pihak tidak berwenang, dimodifikasi, ataupun disalahgunakan sehingga dapat menimbulkan kerugian bagi pemilik data (Prameshwari & Sastra, 2023). Selain itu, pertukaran dokumen digital khususnya dalam format *Portable Document Format* (PDF) semakin banyak digunakan pada sektor pendidikan, pemerintahan, bisnis, dan layanan publik karena format PDF mampu mempertahankan konsistensi tampilan dokumen pada berbagai perangkat dan sistem operasi. Meningkatnya penggunaan dokumen digital tersebut menyebabkan kebutuhan terhadap keamanan data menjadi semakin penting untuk menjaga kerahasiaan, integritas, dan autentikasi informasi dari berbagai ancaman siber (Timur et al., 2025).

Perkembangan transformasi digital juga mendorong meningkatnya kebutuhan terhadap mekanisme keamanan yang tidak hanya kuat secara kriptografis, tetapi juga efisien dalam performa sistem, khususnya pada proses pengolahan dokumen digital berukuran besar (Patria & Andriati, 2025). Dalam implementasi modern, algoritma berbasis *Authenticated Encryption with Associated Data* (AEAD) menjadi salah satu solusi utama

karena mampu menyediakan fungsi enkripsi sekaligus autentikasi data dalam satu proses. Dua algoritma AEAD yang saat ini banyak digunakan adalah AES-GCM dan ChaCha20-Poly1305. AES-GCM merupakan mode operasi AES yang memiliki performa sangat tinggi pada perangkat yang mendukung AES *New Instructions* (AES-NI), yaitu instruksi khusus pada prosesor yang dirancang untuk mempercepat proses komputasi AES berbasis *hardware*. Sementara itu, ChaCha20-Poly1305 dirancang sebagai algoritma berbasis *software* yang mampu bekerja secara efisien tanpa bergantung pada akselerasi perangkat keras khusus.

Beberapa penelitian sebelumnya telah membandingkan performa AES-GCM dan ChaCha20-Poly1305 dalam berbagai skenario pengujian. Penelitian oleh Patria dan Andriati tahun 2025 menunjukkan bahwa AES-GCM memiliki performa lebih cepat dan stabil dibandingkan ChaCha20-Poly1305 pada proses enkripsi dokumen PDF menggunakan parameter waktu eksekusi dan *throughput* (Patria & Andriati, 2025). Penelitian lain oleh Bagus et al. membandingkan algoritma AES dan ChaCha20 pada *file* dokumen dan citra dengan menambahkan parameter *CPU Usage* dan *Memory Usage*, di mana ChaCha20 menunjukkan efisiensi penggunaan *resource* yang lebih efisein pada beberapa kondisi pengujian (Timur et al., 2025). Selain itu, menurut penelitian Hendrawan (2025) menunjukkan bahwa ChaCha20-Poly1305 mampu memberikan performa yang lebih efisein dibandingkan AES-GCM pada lingkungan tanpa dukungan akselerasi perangkat keras AES. Hasil tersebut menunjukkan bahwa

performa kedua algoritma sangat dipengaruhi oleh kondisi perangkat keras dan dukungan akselerasi perangkat keras yang digunakan selama proses komputasi (Hendrawan, 2025).

Berdasarkan karakteristik kedua algoritma tersebut, dapat diperkirakan bahwa AES-GCM akan menunjukkan performa terbaik pada sistem yang mendukung AES-NI karena memperoleh akselerasi langsung dari perangkat keras(Dworkin, 2007). Sebaliknya, ChaCha20-Poly1305 diperkirakan memiliki performa yang lebih stabil pada kondisi tanpa AES-NI karena tidak bergantung pada instruksi kriptografi khusus. Oleh sebab itu, penelitian ini membandingkan kedua algoritma pada kondisi AES-NI aktif dan nonaktif untuk mengevaluasi pengaruh akselerasi perangkat keras terhadap waktu enkripsi, waktu dekripsi, *throughput*, *CPU Usage*, dan *Memory Usage* (Nir et al., 2018).

Namun demikian, sebagian besar penelitian (Bagus et al, 2025), (Patria & Andriati, 2025) (Hendrawan, 2025) masih berfokus pada perbandingan umum performa algoritma tanpa melakukan pengujian secara khusus terhadap pengaruh kondisi AES-NI aktif dan AES-NI non-aktif. Padahal, AES-GCM diketahui sangat bergantung pada dukungan AES-NI untuk meningkatkan efisiensi komputasi, sedangkan ChaCha20-Poly1305 dirancang agar tetap optimal pada sistem tanpa dukungan akselerasi perangkat keras AES. Selain itu, masih sedikit penelitian yang membandingkan kedua algoritma menggunakan skenario pengujian variasi ukuran *file* PDF dengan parameter pengukuran yang mencakup waktu

enkripsi, waktu dekripsi, *throughput*, *CPU Usage*, dan *Memory Usage* secara bersamaan. Menurut penelitian (Hernandez et al, 2018), menjelaskan bahwa prosesor *modern* telah mengintegrasikan ekstensi instruksi kriptografi seperti AES-NI dan SHA-NI untuk meningkatkan efisiensi eksekusi algoritma keamanan. Hasil evaluasi yang dilakukan menunjukkan bahwa pemanfaatan instruksi kriptografi mampu menurunkan waktu komputasi berbagai operasi kriptografi, termasuk pengurangan waktu eksekusi sebesar 12% pada proses CBC *decryption* dan 7% pada CTR *encryption* dibandingkan implementasi sebelumnya. Temuan tersebut menunjukkan bahwa dukungan instruksi perangkat keras memiliki pengaruh yang signifikan terhadap performa algoritma kriptografi yang dijalankan pada sistem modern (Hernandez et al., 2018).

Dari penelitian terdahulu yang telah sebelumnya disebutkan telah menunjukkan bahwa AES-NI mampu meningkatkan performa algoritma berbasis AES, kajian mengenai pengaruh aktivasi dan deaktivasi AES-NI terhadap algoritma AEAD (*Authenticated Encryption with Associated Data*) masih relatif terbatas. Padahal, AES-GCM merupakan algoritma yang secara langsung memanfaatkan operasi AES sehingga berpotensi memperoleh peningkatan performa yang signifikan ketika AES-NI diaktifkan. Sebaliknya, ChaCha20-Poly1305 dibangun menggunakan operasi ARX (Addition, Rotation, XOR) dan tidak bergantung pada instruksi AES-NI. Perbedaan karakteristik tersebut menimbulkan pertanyaan mengenai sejauh mana AES-NI memengaruhi waktu eksekusi,

throughput, serta penggunaan *resource* sistem pada kedua algoritma tersebut. Oleh karena itu, diperlukan penelitian yang secara khusus mengevaluasi pengaruh AES-NI terhadap performa AES-GCM dan ChaCha20-Poly1305 melalui pengujian waktu enkripsi, waktu dekripsi, *throughput*, *CPU Usage*, *Memory Usage*, dan *scalability* pada berbagai ukuran *file* PDF

Berdasarkan celah penelitian tersebut, diperlukan suatu penelitian yang secara khusus mengevaluasi performa AES-GCM dan ChaCha20-Poly1305 pada kondisi AES-NI aktif dan AES-NI non-aktif menggunakan skenario eksperimen yang terkontrol. Penelitian ini menggunakan *file* PDF berukuran 10 MB hingga 100 MB dengan interval pengujian bertahap untuk mengamati pengaruh akselerasi perangkat keras terhadap performa kedua algoritma. Parameter yang digunakan meliputi waktu enkripsi, waktu dekripsi, *throughput*, *CPU Usage* , dan *Memory Usage* sehingga hasil pengujian dapat memberikan gambaran yang lebih komprehensif mengenai karakteristik performa masing-masing algoritma.

Dengan demikian, kebaruan penelitian ini terletak pada evaluasi terkontrol terhadap pengaruh AES-NI aktif dan nonaktif terhadap performa dua algoritma AEAD, yaitu AES-GCM dan ChaCha20-Poly1305, pada variasi ukuran *file* PDF. Berbeda dari penelitian sebelumnya yang hanya membandingkan performa algoritma secara umum, penelitian ini memisahkan skenario berbasis dukungan akselerasi perangkat keras

sehingga mampu memberikan rekomendasi pemilihan algoritma berdasarkan kondisi *hardware* yang digunakan.

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang, dapat dirumuskan masalah pada penelitian ini, yaitu:

a. Bagaimana performa algoritma AES-GCM dan ChaCha20-Poly1305 pada proses enkripsi dan dekripsi variasi ukuran *file* PDF 10 MB hingga 100 MB pada kondisi AES-NI aktif dan AES-NI non-aktif?
b. Bagaimana pengaruh aktivasi dan deaktivasi AES-NI terhadap waktu eksekusi, *throughput*, *CPU Usage* dan *Memory Usage* pada algoritma AES-GCM dan ChaCha20-Poly1305?

1.3 Tujuan Penelitian

Dari uraian masalah yang sudah dirumuskan, didapat tujuan penelitian sebagai berikut:

a. Menganalisis performa algoritma AES-GCM dan ChaCha20-Poly1305 dalam proses enkripsi dan dekripsi serta *throughput* pada kondisi AES-NI aktif dan AES-NI non-aktif pada *File* PDF dengan variasi ukuran 10 MB hingga 100 MB.
b. Mengevaluasi pengaruh aktivasi dan deaktivasi AES-NI terhadap waktu eksekusi, *throughput*, *CPU Usage* dan *Memory Usage* pada algoritma AES-GCM dan ChaCha20-Poly1305.

1.4 Manfaat Penelitian

Adapun beberapa manfaat yang didapatkan dari penelitian ini, sebagai berikut:

a. Diharapkan dapat memperkaya kajian ilmiah di bidang kriptografi, khususnya terkait evaluasi performa algoritma a*uthenticated encryption modern* pada pengamanan *file* digital berukuran besar.
b. Memberikan rekomendasi algoritma yang lebih efisien berdasarkan hasil pengukuran waktu enkripsi, dekripsi, dan *throughput* dan penggunaan *resource.*
c. Memberikan rekomendasi teknis mengenai pemilihan algoritma *authenticated encryption* yang optimal untuk implementasi pengamanan dokumen digital, khususnya pada lingkungan komputasi dengan keterbatasan sumber daya.

1.5 Kontribusi penelitian

Adapun beberapa manfaat yang didapatkan dari penelitian ini, sebagai berikut:

a. Memberikan bukti empiris mengenai perbandingan performa algoritma AES-GCM dan ChaCha20-Poly1305 berdasarkan parameter waktu enkripsi, waktu dekripsi, *throughput*, *CPU Usage*, dan *Memory Usage* pada *file* PDF dengan variasi ukuran 10 MB hingga 100 MB dalam kondisi AES-NI aktif dan nonaktif.
b. Menyajikan hasil evaluasi mengenai pengaruh dukungan akselerasi perangkat keras AES terhadap performa kedua algoritma, sehingga dapat memberikan gambaran karakteristik masing-masing algoritma pada lingkungan pengujian yang digunakan.

c. Menyusun rekomendasi pemilihan algoritma berdasarkan hasil pengujian pada lingkungan penelitian, yaitu AES-GCM lebih sesuai digunakan pada sistem yang mendukung AES-NI, sedangkan ChaCha20-Poly1305 memberikan performa yang lebih baik pada kondisi pengujian tanpa dukungan akselerasi AES.

1.6 Batasan Penelitian

Berikut merupakan batasan masalah yang terdapat pada penelitian ini:

a. Penelitian hanya membandingkan algoritma AES-GCM dan ChaCha20-Poly1305.
b. Objek pengujian yang digunakan dalam penelitian ini berupa *file* dengan format PDF.
c. Implementasi dilakukan pada proses enkripsi dan dekripsi *file*, bukan pada komunikasi jaringan atau sistem *real-time*.
d. Variasi ukuran *file* PDF yang digunakan dalam pengujian dibatasi pada ukuran 10 MB, 20 MB, 30 MB, 40 MB, 50 MB, 60 MB, 70 MB, 80 MB, 90 MB hingga 100 MB.
e. Parameter performa yang dianalisis dalam penelitian ini meliputi waktu enkripsi, waktu dekripsi, *throughput*, *CPU Usage*, dan *Memory Usage*.
f. Implementasi algoritma menggunakan *library* kriptografi standar tanpa melakukan modifikasi terhadap struktur internal algoritma dan bukan membangun algoritma dari nol.
g. Seluruh proses pengujian dilakukan pada lingkungan perangkat keras dan sistem operasi yang sama untuk menjaga konsistensi hasil.