BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi komunikasi digital telah mendorong peningkatan signifikan dalam pertukaran data, mulai dari pesan teks hingga *file* multimedia seperti gambar, audio, dan video yang dikirimkan secara *real-time* melalui jaringan internet. Data yang dipertukarkan sering kali bersifat sensitif, seperti informasi pribadi, finansial, maupun dokumen penting, sehingga menimbulkan risiko keamanan yang tinggi apabila tidak dilindungi dengan mekanisme yang memadai. Berbagai penelitian menunjukkan bahwa komunikasi pada jaringan terbuka sangat rentan terhadap serangan seperti *eavesdropping*, modifikasi data, dan akses tidak sah (Ananya Mishra et al., 2024). Untuk mengatasi permasalahan tersebut, pendekatan *end-to-end encryption* (E2EE) telah umum digunakan dalam sistem komunikasi modern. E2EE memastikan bahwa hanya pihak pengirim dan penerima yang dapat mengakses isi pesan, dengan menjamin aspek *confidentiality, integrity, authenticity*, dan *forward secrecy* (Knodel et al., 2024).

Dalam implementasinya, sistem E2EE umumnya menggunakan kombinasi algoritma kriptografi simetris seperti Advanced Encryption Standard (AES) dan algoritma pertukaran kunci seperti Diffie-Hellman atau turunannya (Alatawi & Saxena, 2023). Namun demikian, penggunaan AES dalam mode *Galois/Counter Mode* (GCM) memiliki kelemahan mendasar, yaitu sensitivitas ekstrem terhadap penggunaan ulang *nonce* (*nonce reuse*). Apabila *nonce* yang sama digunakan dua kali dengan kunci yang sama, *keystream* yang dihasilkan menjadi identik, sehingga

penyerang dapat melakukan operasi XOR antara dua *ciphertext* untuk mengeliminasi *keystream* dan merekonstruksi informasi *plaintext* secara langsung. Lebih jauh, kondisi ini juga membocorkan kunci autentikasi internal AES-GCM, yang memungkinkan penyerang memalsukan tag autentikasi pada pesan-pesan berikutnya sehingga seluruh jaminan integritas sistem runtuh seketika (Mattsson, 2024).

Risiko *nonce reuse* bukan sekadar skenario teoretis dalam lingkungan aplikasi *chatting real-time*. Kondisi ini dapat terjadi secara nyata akibat kesalahan implementasi, *race condition* pada sistem konkuren, atau kegagalan *random number generator* pada perangkat klien. Sebagai solusi terhadap kelemahan tersebut, dikembangkan varian AES-GCM-SIV yang secara khusus dirancang untuk memiliki ketahanan terhadap kesalahan pengelolaan *nonce* (*nonce-misuse resistance*) (Gueron & Lindell, 2015). Berbeda dengan AES-GCM yang menggunakan *nonce* eksternal secara langsung sebagai *initialization vector* (IV), AES-GCM-SIV menghitung IV secara deterministik sebagai fungsi kriptografis dari kunci, *nonce*, pesan, dan *associated data* mekanisme inilah yang disebut *Synthetic Initialization Vector* (SIV). Dengan pendekatan ini, meskipun *nonce* yang sama digunakan ulang, IV sintetis yang dihasilkan tetap berbeda selama *plaintext*-nya berbeda, sehingga *keystream* tidak pernah berulang. Satu-satunya konsekuensi dari *nonce reuse* pada AES-GCM-SIV adalah terungkapnya fakta bahwa dua pesan identik telah dikirimkan sebuah kebocoran yang jauh lebih dapat ditoleransi dibandingkan runtuhnya kerahasiaan sistem secara menyeluruh seperti pada AES-GCM (Gueron et al., 2019).

Di sisi pertukaran kunci, sistem E2EE memerlukan mekanisme yang memungkinkan dua pihak membangun *shared secret* secara aman tanpa harus mengirimkan kunci rahasia melalui jaringan. Algoritma Diffie-Hellman (DH) klasik berbasis logaritma diskrit pada bilangan prima telah lama digunakan untuk tujuan ini, namun memerlukan ukuran kunci yang sangat besar (2048–4096 bit) untuk mencapai tingkat keamanan yang memadai, sehingga menimbulkan beban komputasi dan konsumsi memori yang signifikan. Alternatif berbasis RSA juga bukan pilihan optimal karena RSA dirancang sebagai algoritma enkripsi asimetris, bukan protokol pertukaran kunci, sehingga penggunaannya untuk pembentukan *session key* menimbulkan kompleksitas implementasi yang lebih tinggi. Elliptic Curve Diffie-Hellman (ECDH) hadir sebagai solusi yang lebih efisien, dimana keamanan ECDH bertumpu pada kesulitan Elliptic Curve Discrete Logarithm Problem (ECDLP), yang memungkinkan tingkat keamanan setara RSA 3072-bit dicapai hanya dengan kunci 256-bit (Dar et al., 2021). Keunggulan ini menjadikan ECDH sangat sesuai untuk aplikasi yang membutuhkan pertukaran kunci yang cepat dengan *overhead* komputasi minimal. Dalam penelitian ini, digunakan kurva Curve25519 yang telah terstandarisasi melalui RFC 7748, dirancang secara khusus untuk meminimalkan risiko kesalahan implementasi, dan terbukti tahan terhadap berbagai serangan *side-channel* (Hafeez et al., 2025).

Di sisi derivasi kunci, *shared secret* yang dihasilkan oleh protokol ECDH tidak dapat langsung digunakan sebagai kunci enkripsi simetris AES. Nilai tersebut memiliki struktur aljabar bawaan dari operasi perkalian skalar pada kurva eliptik dan tidak memiliki sifat *pseudorandomness* yang disyaratkan untuk kunci

kriptografi tingkat aplikasi; penggunaannya secara langsung membuka risiko kebocoran informasi struktural lintas sesi apabila pasangan kunci ECDH yang sama digunakan lebih dari sekali (Krawczyk & Eronen, 2010). Untuk mengatasi permasalahan ini, diperlukan sebuah *Key Derivation* Function (KDF) yang mampu mengubah material kunci mentah menjadi kunci simetris yang seragam dan terisolasi secara kriptografis. Beberapa KDF yang relevan telah tersedia, antara lain PBKDF2 (RFC 8018), CONCAT KDF (NIST SP 800-56C), dan KDF1/KDF2 berbasis *hash*. Namun PBKDF2 dirancang untuk skenario password-based dengan iterasi tinggi untuk memperlambat serangan *brute-force*, sehingga tidak sesuai untuk derivasi kunci high-entropy seperti *shared secret* ECDH; CONCAT KDF tidak menyediakan mekanisme pemisahan fungsi ekstraksi dan perluasan secara eksplisit; sementara KDF1/KDF2 tidak memiliki dukungan salt formal yang menjamin isolasi antar sesi. HKDF (RFC 5869) dirancang secara spesifik untuk skenario ini melalui paradigma *extract-then-expand* dua tahap, tahap HKDF-Extract menormalkan entropi dari material kunci mentah menjadi *pseudorandom* key (PRK), sedangkan tahap HKDF-Expand menurunkan satu atau lebih kunci operasional dengan isolasi konteks melalui parameter info yang berbeda per tujuan penggunaan. Analisis formal menunjukkan bahwa HKDF memenuhi definisi KDF yang aman selama HMAC memenuhi asumsi PRF yang wajar, dan HKDF telah diadopsi pada protokol keamanan utama seperti TLS 1.3 dan Signal Protocol (Krawczyk & Eronen, 2010). Dalam penelitian ini, SHA-256 dipilih sebagai fungsi *hash* yang mendasari HKDF karena merupakan standar yang telah terbukti secara

luas dan memberikan output 256-bit yang sesuai dengan panjang kunci AES-256-GCM-SIV yang digunakan.

Meskipun berbagai penelitian terkait telah dilakukan, masih terdapat beberapa celah penelitian yang signifikan dan belum terjawab oleh literatur yang ada. Pertama, berdasarkan kajian literatur pada Tabel 2.1 dan Tabel 2.2, belum ditemukan penelitian yang mengintegrasikan AES-GCM-SIV secara penuh dalam skenario komunikasi *chat* dua arah secara *real-time* yang sekaligus mencakup pesan teks dan *file* media dalam satu sistem penelitian yang menggunakan AES-GCM-SIV seperti (Asgap Putra Zulian et al., 2026) masih terbatas pada pengamanan berkas statis, sementara penelitian yang membangun aplikasi *chat* seperti (Perkasa et al., 2025) dan (Alkhyeli et al., 2023) masih menggunakan AES-GCM standar yang rentan terhadap *nonce reuse*. Kedua, belum ditemukan penelitian yang menggabungkan ECDH dan AES-GCM-SIV dalam satu skema E2EE terpadu sekaligus menguji ketahanannya terhadap skenario *nonce reuse* secara eksplisit dan terukur melalui pendekatan eksperimen kuantitatif komparatif. Ketiga, pengukuran performa yang komprehensif di sisi klien (*client-side*) mencakup waktu enkripsi, waktu dekripsi, *throughput*, konsumsi memori, dan *overhead* ukuran data untuk skema AES-GCM-SIV pada konteks *chat real-time* juga belum ditemukan dalam literatur yang dikaji. Keempat, meskipun ketiga komponen kriptografi tersebut, yaitu ECDH, HKDF, dan AES-GCM-SIV, masing-masing telah dikaji secara individual dalam literatur, belum ditemukan penelitian yang secara empiris membuktikan kontribusi masing-masing komponen terhadap keamanan dan performa sistem ketika ketiganya diintegrasikan dalam satu *pipeline* E2EE yang

sama. Tanpa evaluasi semacam ini, tidak dapat dipastikan apakah setiap komponen benar-benar memberikan kontribusi yang tidak tergantikan, ataukah satu atau lebih komponen dapat dieliminasi tanpa mengorbankan jaminan keamanan sistem secara keseluruhan. Ketidakhadiran bukti empiris tersebut menjadi celah metodologis yang perlu diisi melalui pendekatan *ablation study* terhadap setiap komponen secara terpisah dalam kondisi eksperimen yang terkontrol.

Mengingat ruang lingkup penelitian yang berfokus pada evaluasi kuantitatif algoritma kriptografi dan bukan pada rekayasa perangkat lunak komunikasi secara menyeluruh, pendekatan simulasi dipilih sebagai kerangka implementasi yang paling sesuai. Pembangunan aplikasi komunikasi penuh yang mencakup infrastruktur server relay, antarmuka pengguna, dan pengelolaan koneksi jaringan secara nyata akan menambahkan variabel eksternal yang tidak terkontrol—seperti latensi jaringan, *overhead* protokol transportasi, dan fragmentasi paket—sehingga hasil pengukuran tidak lagi secara murni mencerminkan karakteristik algoritma kriptografi itu sendiri. Sebaliknya, lingkungan simulasi memungkinkan seluruh variabel kontrol dijaga konsisten, setiap iterasi pengujian dapat direproduksi secara deterministik, dan pengukuran performa maupun keamanan dilakukan langsung pada lapisan kriptografi tanpa noise dari lapisan sistem lainnya. Pendekatan ini sejalan dengan metodologi yang digunakan dalam penelitian-penelitian evaluasi algoritma kriptografi terdahulu seperti (Dungog, 2025) dan (Serrano et al., 2022), yang membuktikan bahwa simulasi terkontrol merupakan cara yang valid dan ilmiah untuk menghasilkan data empiris yang dapat diperbandingkan secara adil antar algoritma.

Berdasarkan permasalahan dan celah penelitian tersebut, penelitian ini bertujuan untuk mengintegrasikan dan mengevaluasi skema *end-to-end encryption* yang menggabungkan algoritma AES-GCM-SIV dan Elliptic Curve Diffie-Hellman (ECDH) dengan kurva Curve25519, serta HKDF-SHA256 sebagai fungsi derivasi kunci, untuk mengamankan pertukaran pesan teks dan file media secara terukur dan dapat direproduksi. Selain itu, penelitian ini juga mengevaluasi tingkat keamanan sistem terhadap berbagai skenario serangan termasuk *eavesdropping*, *tampering*, *replay attack*, *nonce reuse*, dan *Man-in-the-Middle* serta menganalisis dan membandingkan performa algoritma secara komprehensif berdasarkan parameter waktu enkripsi, waktu dekripsi, *throughput*, dan penggunaan sumber daya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, permasalahan inti dalam penelitian ini berpusat pada belum ditemukannya dalam kajian literatur yang dilakukan simulasi skema E2EE berbasis AES-GCM-SIV dan ECDH yang mencakup pertukaran pesan teks dan file media secara terpadu, serta belum tersedianya data empiris mengenai performa dan ketahanan keamanan skema tersebut yang dapat diukur secara kuantitatif. Secara spesifik, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana mengintegrasikan algoritma AES-GCM-SIV sebagai mekanisme enkripsi, Elliptic Curve Diffie-Hellman (ECDH) dengan kurva Curve25519 sebagai protokol pertukaran kunci, dan HKDF-SHA256 sebagai fungsi derivasi kunci sesi ke dalam satu skema *end-to-end encryption* yang mampu mengamankan pertukaran pesan teks dan file media secara terukur?

2. Bagaimana mengevaluasi dan membuktikan kemampuan skema yang diusulkan dalam menjamin aspek keamanan *confidentiality*, *integrity*, *authenticity*, dan *forward secrecy*, serta menganalisis ketahanannya terhadap skenario *nonce reuse* dan serangan *Man-in-the-Middle* berdasarkan hasil pengujian terhadap data terenkripsi yang dapat diverifikasi secara kuantitatif?
3. Bagaimana menganalisis kinerja algoritma AES-GCM-SIV dalam simulasi sistem berdasarkan parameter waktu enkripsi (ms), waktu dekripsi (ms), *throughput* (MB/s), konsumsi memori (MB), dan *overhead* ukuran data (%) pada berbagai jenis dan ukuran data uji secara terukur?
4. Bagaimana mengevaluasi kontribusi masing-masing komponen kriptografi (ECDH, HKDF, dan AES-GCM-SIV) terhadap keamanan dan performa sistem melalui *ablation study*, serta membandingkan hasil pengukuran skema yang diusulkan dengan *baseline* AES-GCM secara kuantitatif dalam aspek ketahanan terhadap *nonce reuse* dan efisiensi kriptografi?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah diuraikan, tujuan dari penelitian ini diantaranya sebagai berikut:

1. Merancang skema *end-to-end encryption* (E2EE) yang mengintegrasikan algoritma AES-GCM-SIV sebagai mekanisme enkripsi, Elliptic Curve Diffie-Hellman (ECDH) dengan kurva Curve25519 sebagai protokol pertukaran kunci, dan HKDF-SHA256 sebagai fungsi derivasi kunci sesi untuk mengamankan pertukaran pesan teks dan file media.

2. Mengevaluasi kemampuan skema yang diusulkan dalam menjamin aspek keamanan, meliputi *confidentiality*, *integrity*, *authenticity*, dan *forward secrecy*, serta menguji ketahanannya terhadap skenario *nonce reuse* dalam komunikasi data.
3. Menganalisis kinerja algoritma AES-GCM-SIV dalam simulasi sistem berdasarkan parameter waktu enkripsi, waktu dekripsi, *throughput*, konsumsi memori, dan *overhead* ukuran data pada berbagai jenis dan ukuran data uji secara terukur.
4. Mengevaluasi kontribusi masing-masing komponen kriptografi (ECDH, HKDF, dan AES-GCM-SIV) terhadap keamanan dan performa sistem melalui *ablation study*, serta membandingkan performa dan tingkat keamanan skema yang diusulkan dengan *baseline* AES-GCM khususnya dalam aspek ketahanan terhadap *nonce reuse* dan efisiensi kriptografi.

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Secara ilmiah penelitian ini diharapkan dapat memberikan kontribusi berupa bukti empiris mengenai karakteristik keamanan dan kinerja algoritma AES-GCM-SIV dalam skema *end-to-end encryption* yang diintegrasikan dengan ECDH Curve25519 dan HKDF-SHA256. Hasil simulasi dan evaluasi yang dilakukan diharapkan dapat memperkaya literatur kriptografi terapan, khususnya terkait ketahanan skema terhadap skenario *nonce reuse* serta analisis perbandingan efisiensi kriptografi antara AES-GCM-SIV dan AES-GCM sebagai *baseline*.

2. Secara praktis penelitian ini diharapkan dapat menjadi referensi teknis bagi pengembang perangkat lunak yang ingin mengimplementasikan skema E2EE pada sistem komunikasi digital, khususnya yang membutuhkan ketahanan terhadap kesalahan pengelolaan *nonce*. Data kuantitatif yang dihasilkan dari simulasi komunikasi antara dua entitas mencakup waktu enkripsi, *throughput*, konsumsi memori, dan *overhead* ukuran data dapat digunakan sebagai acuan dalam pengambilan keputusan pemilihan algoritma enkripsi pada sistem komunikasi digital secara umum.
3. Bagi pengembangan ilmu penelitian ini diharapkan dapat menjadi landasan bagi penelitian lanjutan di bidang kriptografi terapan, khususnya dalam pengembangan dan evaluasi skema E2EE yang lebih tahan terhadap kesalahan implementasi. Metodologi simulasi dan *ablation study* yang digunakan dalam penelitian ini juga diharapkan dapat diadopsi sebagai pendekatan evaluasi algoritma kriptografi yang sistematis dan terukur pada penelitian-penelitian berikutnya.

1.5 Batasan Penelitian

Untuk menjaga fokus penelitian dan memastikan penyelesaian yang optimal, penulis membatasi ruang lingkup pembahasan pada bidang keamanan sistem dan pengembangan aplikasi. Batasan masalah dalam penelitian ini dirumuskan sebagai berikut:

1. Penelitian ini berfokus pada implementasi dan evaluasi pipeline kriptografi E2EE antara tiga entitas (Alice, Bob, dan Server) yang berjalan sebagai proses terpisah pada tiga VPS yang saling terhubung melalui jaringan internet publik,

dan tidak mencakup pembangunan aplikasi komunikasi penuh dengan antarmuka pengguna, manajemen akun, maupun basis data pesan.

2. Algoritma enkripsi yang disimulasikan dan dievaluasi adalah AES-256-GCM-SIV dengan algoritma pembanding (*baseline*) AES-256-GCM, menggunakan Elliptic Curve Diffie-Hellman (ECDH) dengan kurva Curve25519 untuk pertukaran kunci dan HKDF-SHA256 sebagai fungsi derivasi kunci sesi.
3. Simulasi mencakup dua jenis data uji, yaitu pesan teks dan file media (gambar, audio, dan video), dengan variasi ukuran data yang telah ditentukan untuk setiap kategori pengujian.
4. Setiap skenario pengujian dilakukan sebanyak 30 iterasi pada kondisi lingkungan yang terkontrol untuk memastikan validitas dan konsistensi data hasil pengukuran.
5. Parameter kinerja yang diukur meliputi waktu enkripsi (µs), waktu dekripsi (µs), *throughput* (MB/s), konsumsi memori (MB), dan *overhead* ukuran data (%), yang seluruhnya diukur secara lokal pada masing-masing entitas sehingga mencerminkan performa kriptografi murni, terlepas dari adanya transmisi jaringan fisik yang menghubungkan ketiga entitas tersebut.
6. Pengujian keamanan dilakukan melalui lima skenario serangan, yaitu *eavesdropping*, *tampering*, *replay attack*, *nonce reuse*, dan *Man-in-the-Middle*, yang dimodelkan berdasarkan *threat model* Dolev-Yao dengan Server berperan ganda sebagai relay pesan sekaligus simulasi penyerang (Eve) pada kanal komunikasi nyata antar VPS.

7. *Ablation study* dilakukan dengan mengevaluasi kontribusi masing-masing komponen kriptografi (AES-GCM-SIV, ECDH, dan HKDF) secara kumulatif melalui empat konfigurasi bertingkat (AES-GCM sebagai *baseline*, AES-GCM-SIV, AES-GCM-SIV+ECDH, dan AES-GCM-SIV+ECDH+HKDF) untuk mengukur pengaruh penambahan setiap komponen terhadap keamanan dan performa sistem secara keseluruhan.