BAB I
PENDAHULUAN

1.1 Latar Belakang

Komunikasi digital merupakan fondasi utama dalam ekosistem teknologi modern yang digunakan dalam berbagai konteks, mulai dari transaksi keuangan hingga kolaborasi profesional dan komunikasi sosial [1,2]. Dengan adopsi teknologi informasi yang semakin masif, tuntutan terhadap perlindungan privasi dan keamanan informasi juga meningkat [3]. Pengguna kini mengharapkan sistem komunikasi yang tidak hanya cepat dan fungsional, tetapi juga menjamin kerahasiaan dan integritas data [4]. Meskipun pemanfaatan komunikasi digital semakin meluas, hal ini turut membuka celah keamanan yang signifikan [3], seperti risiko intersepsi dan modifikasi data oleh pihak yang tidak berwenang selama proses transmisi [5].

Dusane et al. [6] mengatakan bahwa protokol seperti HTTPS telah banyak digunakan untuk mengenkripsi koneksi antara pengguna dan server. Namun, model ini hanya menjamin keamanan selama transmisi *client-server* dan tidak menyediakan enkripsi dari pengirim hingga penerima secara menyeluruh (*end-to-end encryption*). Dalam skema ini, server masih memiliki akses untuk membaca pesan karena proses dekripsi dilakukan sebelum diteruskan ke penerima. Ini menciptakan ketergantungan pada integritas penyedia layanan. Ketika terjadi kebocoran data akibat peretasan, tekanan dari otoritas eksternal seperti lembaga pemerintah atau organisasi pihak ketiga yang memiliki kepentingan terhadap data pengguna, privasi pengguna menjadi terancam. Selanjutnya, pendekatan baru seperti *End-to-End Encryption* (E2EE) semakin dibutuhkan, karena menjamin bahwa hanya pengirim dan penerima yang dapat mengakses konten pesan, bahkan tidak oleh penyedia layanan sekalipun [7,8].

Protokol pertukaran kunci *Diffie-Hellman* (DH) telah lama digunakan sebagai metode untuk menciptakan kunci rahasia di antara dua pihak melalui kanal komunikasi yang tidak aman [9,10]. Namun, DH rentan terhadap berbagai serangan, termasuk *Man-In-The-Middle* (MITM), karena ketiadaan autentikasi dua arah [10,11]. Salah satu pengembangan DH, yaitu protokol PrivateDH oleh Patgiri [12], mengintegrasikan RSA dan AES untuk memperkuat DH, namun masih menghadapi kelemahan dalam keandalannya. Kelemahan pertama adalah ketidakmampuan penerima dalam membedakan antara pengguna sah dan penyerang ketika menerima dua *ciphertext* identik dari sumber berbeda, yang dapat

menyebabkan kegagalan dalam penerapan PrivateDH. Meskipun PrivateDH memiliki mekanisme untuk mendeteksi anomali komunikasi melalui penerimaan dua *ciphertext* identik dari sumber berbeda, deteksi ini bersifat reaktif dan tidak mencegah kompromi yang mungkin sudah terjadi. Kelemahan kedua adalah adanya *overhead* komputasi yang muncul dalam proses enkripsi dan dekripsi, khususnya terkait dengan parameter DH. Dalam implementasinya, pihak pengirim harus melakukan satu kali enkripsi (*public key*) dan dua kali dekripsi (parameter *p* dan *g*), sedangkan pihak penerima melakukan dua kali enkripsi (*p* dan *g*) dan satu kali dekripsi (*public key*). Selain itu, penggunaan algoritma DH dalam protokol PrivateDH tetap menghadirkan tantangan berupa kebutuhan ukuran kunci yang besar untuk mempertahankan tingkat keamanan modern, yang pada akhirnya berdampak pada peningkatan beban komputasi dan menurunnya efisiensi protokol [13].

Untuk mengatasi kelemahan PrivateDH, penelitian ini mengintegrasikan beberapa pendekatan kriptografi modern yang dipilih secara khusus berdasarkan relevansi terhadap kelemahan yang dihadapi. Pertama, ECDHE Curve25519 dipilih sebagai pengganti DH karena Curve25519 dalam ECDHE menggunakan parameter tetap, tidak seperti DH yang membutuhkan pertukaran parameter *p* dan *g*. Ini mengurangi beban komputasi dan meningkatkan efisiensi proses pertukaran kunci. Selain itu, juga memiliki keunggulan dalam efisiensi perhitungan, ukuran kunci yang lebih kecil, dan ketahanan keamanan yang lebih baik [14,15,16]. Dibandingkan dengan ECDH biasa atau CurveP256, Curve25519 dinilai lebih stabil dan aman dalam implementasi praktis [17,18]. Kedua, RSASSA-PSS digunakan sebagai mekanisme autentikasi digital karena bersifat probabilistik dan lebih tahan terhadap serangan *padding oracle* dibandingkan skema klasik PKCS#1 v1.5, menjadikannya standar yang disarankan dalam spesifikasi kriptografi modern [19,20]. Ketiga, AES digunakan seperti dalam struktur PrivateDH, namun dengan konfigurasi AES-256 karena kemampuannya menghasilkan efek *avalanche* yang tinggi serta ketahanan terhadap *brute-force attack*, dan dinilai lebih aman dibandingkan AES-128 [21].

Protokol PrivateDH masih memiliki kelemahan yang relevan dalam konteks kebutuhan komunikasi modern, seperti tidak adanya autentikasi yang memadai, kerentanan terhadap serangan manipulatif karena *ciphertext* identik, dan keterbatasan efisiensi akibat penggunaan DH klasik juga tidak mendukung *forward secrecy* secara optimal. Sebagai kontribusi terhadap peningkatan aspek keamanan dan efisiensi protokol PrivateDH, penelitian ini mengusulkan integrasi dua pendekatan utama. RSA dan AES tetap dipertahankan sebagai bagian dari struktur awal protokol. Sementara itu, pendekatan baru meliputi: (1) ECDHE Curve25519 untuk menggantikan peran DH dalam menghasilkan

kunci sesi sementara yang lebih aman dan efisien, dan (2) RSASSA-PSS sebagai mekanisme autentikasi digital guna mengatasi kegagalan identifikasi pengguna sah saat *ciphertext* identik diterima dari sumber berbeda. Sejauh penelusuran yang dilakukan, belum banyak penelitian yang secara eksplisit mengintegrasikannya secara terpadu dalam satu protokol komunikasi *end-to-end*, terutama sebagai peningkatan dari PrivateDH. Pendekatan ini diharapkan dapat meningkatkan protokol PrivateDH dalam mendukung komunikasi *end-to-end* yang aman dan efisien.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana integrasi ECDHE Curve25519 dapat menggantikan DH dalam menghasilkan kunci sesi yang aman dan efisien pada protokol PrivateDH?
2. Bagaimana RSASSA-PSS dapat digunakan untuk mengautentikasi pengguna dan mencegah kegagalan identifikasi saat *ciphertext* yang identik diterima dari sumber berbeda?

1.3 Tujuan

Tujuan dari penelitian ini adalah sebagai berikut:

1. Mengintegrasikan ECDHE Curve25519 sebagai pengganti DH untuk menghasilkan kunci sesi yang lebih aman dan efisien dalam protokol PrivateDH.
2. Menerapkan RSASSA-PSS sebagai mekanisme autentikasi digital guna membedakan pengguna sah dari penyerang saat *ciphertext* yang identik diterima.

1.4 Manfaat

Penelitian ini diharapkan mampu memberikan manfaat sebagai berikut:

1. Memberikan kontribusi dalam pengembangan protokol pertukaran kunci yang aman dan efisien di bidang komunikasi digital.
2. Menawarkan solusi teknis untuk meningkatkan keamanan pertukaran kunci melalui pendekatan autentikasi dan efisiensi perhitungan.
3. Menyediakan landasan ilmiah dan teknis bagi akademisi maupun praktisi dalam mengembangkan protokol kriptografi dan sistem komunikasi yang lebih kuat terhadap serangan dan kebocoran data.

1.5 Ruang Lingkup

Ruang lingkup penelitian ini mencakup integrasi algoritma ECDHE Curve25519 untuk menghasilkan kunci sesi sementara, RSASSA-PSS untuk autentikasi digital terhadap pesan, dan AES-256 sebagai algoritma enkripsi dalam komunikasi yang terenkripsi secara *end-to-end*. Evaluasi dilakukan dalam lingkungan tertutup dan terkontrol untuk menguji aspek keamanan dan performa protokol pertukaran kunci. Penelitian ini tidak mencakup pengembangan aplikasi komunikasi lengkap atau fitur tambahan seperti pengiriman file besar, komunikasi grup, atau integrasi dengan layanan *cloud*. Dalam penelitian ini, diasumsikan bahwa *public key* RSA dari pengirim dan penerima telah tervalidasi dan tersedia secara sah. Selain itu, keandalan pihak ketiga tepercaya (*trusted third party*) untuk distribusi *public key* juga dianggap valid dan tidak menjadi fokus pengujian. Oleh karena itu, aspek seperti verifikasi sertifikat digital, manajemen kepercayaan, dan otoritas sertifikasi berada di luar cakupan penelitian ini.