BAB I
PENDAHULUAN

1.1 Latar Belakang

Berdasarkan data yang dihimpun *eMarketer* pada tahun 2019, pengguna *Instant Messaging* mencapai 2,52 miliar orang di seluruh dunia. Di Indonesia, menurut Laporan Kementerian Komunikasi dan Informatika Republik Indonesia bertajuk *Survey Penggunaan Teknologi Informasi Tahun 2017* menyebutkan 84,76% responden menyatakan sebagai pengguna aktif *instant messenger* (IM). Hal ini menunjukkan baik penduduk di Indonesia maupun di seluruh dunia sangat aktif berkirim pesan menggunakan aplikasi media sosial.

Besarnya data pengguna *mobile instant messaging* membuka peluang kejahatan, diantaranya adalah penyabotasean pesan. Sebuah artikel di CNN Indonesia berjudul "Keamanan WhatsApp Jadi Celah Sabotase Pesan" (Tim CNN Indonesia, 2019) menyatakan perusahaan keamanan siber, Checkpoint mengungkap bagaimana sebuah alat bisa digunakan untuk mengubah teks dari sebuah pesan yang diterima, alat tersebut memungkinkan orang yang tidak bertanggung jawab untuk memanipulasi sebuah pesan. Selain itu, pada sebuah artikel dari Hindustan Times berjudul "*CERT-In asks users to update WhatsApp after MP4 video file vulnerability discovered*" (2019) mengungkap adanya celah keamanan aplikasi WhatsApp, dimana adanya kerentanan *buffer overflow* karena penguraian data berkas ".mp4" yang tidak benar, sehingga penyerang bisa mengirim berkas ".mp4" ke sistem target yang dapat mengarah pada eksekusi kode arbitrer oleh penyerang.

Agar keamanan data atau informasi saat berkomunikasi terjaga, perlu suatu metode yang tepat untuk melakukan enkripsi suatu pesan dari sebuah aplikasi *instant messaging*. Menurut Bishop (2004) terdapat tiga komponen sebagai pertimbangan dalam perancangan dan pembahasan sistem keamanan diantaranya *Confidentiality* (kerahasiaan), *Integrity* (keandalan), dan *Availability* (ketersediaan). Aspek keamanan ini dapat dipenuhi dengan mengamankan data

yang ditransmisikan dengan jalur telekomunikasi dari pencurian data, pengubahan data dan autentikasi menggunakan kriptografi (Devi, 2013). Kriptografi menyediakan layanan keamanan informasi penting seperti autentikasi, kerahasiaan, integritas, dan non-penyangkalan (Liu, dkk., 2009).

Pada dasarnya berdasarkan sistem penggunaan kunci, kriptografi diklasifikasikan menjadi dua sistem yaitu sistem kriptografi kunci simetris dan sistem kriptografi kunci asimetris (Menezes, dkk., 1997). Sistem kriptografi kunci simetris menggunakan satu kunci yang dibagikan secara rahasia untuk melakukan enkripsi dan dekripsi (Menezes, dkk., 1997). Sistem kriptografi kunci asimetris menggunakan kunci publik dan privat untuk melakukan enkripsi dan dekripsi masing-masing secara terpisah, (Menezes, dkk., 1997). Penggunaan satu kunci pada sistem kriptografi kunci simetris secara bersama-sama antar pengguna membuat rentan terjadinya serangan pada saat pertukaran pesan sehingga distribusi kunci tidak aman, namun waktu proses untuk enkripsi dan dekripsi relatif cepat karena adanya efisiensi yang terjadi pada pembangkit kunci. Penggunaan kunci publik dan privat yang berbeda pada sistem kriptografi kunci asimetris membuat tingkat kemanan pada saat pertukaran pesan lebih terjamin, namun kecepatan proses enkripsi dan dekripsi tergolong lambat.

Dari beberapa aplikasi kunci simetris, AES merupakan algoritma yang paling umum digunakan, dikarenakan ukuran memori yang dibutuhkan AES lebih kecil dibandingkan dengan kunci simetris lainnya dan AES adalah priortas tertinggi untuk digunakan dalam aplikasi yang memerlukan kerahasiaan dan integritas (Patil, dkk., 2016). Selain itu, AES dianggap sebagai teknik kriptografi terbaik yang juga menyediakan perlindungan dari berbagai serangan seperti serangan diferensial, serangan pemulihan, serangan kunci dan serangan persegi (Pancholi & Patel, 2016). Penelitian yang dilakukan Mahajan & Sachdeva (2013) dengan membandingkan tiga teknik kriptografi DES, AES dan RSA berdasarkan waktu simulasi. Hasil pada dataset yang berbeda membuktikan bahwa AES membutuhkan waktu lebih sedikit untuk enkripsi dan dekripsi. Hasil penelitian ini menunjukkan pemrosesan yang dilakukan AES dibandingkan DES dan RSA lebih cepat, sehingga data sampai lebih cepat. Salah satu penelitian yang menggunakan algoritma AES untuk

mengamankan aplikasi *instant messaging* adalah penelitian Wijaya (2015). Penelitian dilakukan pada penggunaan sistem enkripsi pada *instant messaging* menggunakan algoritma AES-128, yaitu algoritma cipher aliran yang menggunakan kunci simetris sepanjang 128-bit. Sistem ini diimplementasikan pada aplikasi *Prototype Community Messenger* berbasis sistem operasi Android yang memiliki performansi baik, terlihat dari nilai *Avalanche Effect* dengan rata-rata bernilai 0,539069. Hasilnya menunjukkan data atau informasi yang dikirim ke penerima akan lebih aman. Hal ini menunjukkan bahwa algoritma AES-128 dapat digunakan sebagai pengaman aplikasi *instant messaging*.

Pada sistem kriptografi kunci asimetris, salah satu aplikasi dari sistem kriptografi kunci asimetris yang paling umum digunakan adalah algoritma *key exchange* Diffie-Hellman. Algoritma Diffie-Hellman memiliki kelebihan dalam hal kemudahan pembuatan kunci efemeral, dan adanya autentikasi pengirim dan penerima (Roy, 2016). Ini berarti, algoritma Diffie-Hellman lebih mudah untuk membuat kunci pada setiap proses pembuatan kunci yang dibutuhkan dan pengirim dan penerima memiliki kunci yang sama. Selain kelebihan yang dimilikinya, algoritma Diffie-Hellman memiliki kelemahan yaitu adanya celah yang memungkinkan terjadinya serangan sewaktu pertukaran kunci yang disebut dengan *Man in the Middle Attack* (Stallings, 2005). Penggunaan tanda tangan digital dan sertifikat kunci publik dilakukan untuk mengatasi celah serangan pada saat pertukaran kunci (Mathur, Agarwal, & Sharma, 2015). Penelitian dengan memanfaatkan aplikasi sistem kriptografi kunci asimetris Diffie-Hellman terkait pengamanan *instant messaging* diantaranya adalah penelitian yang dilakukan Harn & Mehta (2004), dengan mengintegrasikan *key exchange* Diffie-Hellman ke dalam algoritma DSA. Hasil penelitian menujukkan bahwa algoritma Diffie-Hellman dapat digunakan sebagai *key exchange* yang terautentikasi untuk digunakan pada komunikasi interaktif dengan tujuan memberikan otentikasi, konfirmasi kunci dan pertukaran kunci *non payback* untuk komunikasi interaktif. Hasil penelitian ini menunjukkan algoritma Diffie-Hellman dapat digunakan sebagai pengaman aplikasi *instant messaging.*

Survey yang dilakukan Mathur, Agarwal, & Sharma (2015) dengan membandingkan beberapa algoritma kunci simetris dan asimetris, menemukan bahwa suatu algoritma kriptografi memberikan keamanan namun tidak menjamin keamanan 100 persen. Kriptografi hibrida (*Hybrid Cryptosystem*) adalah salah satu solusi yang digunakan untuk keamanan distribusi kunci yang lebih terjamin (Iyer, dkk., 2016). Kriptografi hibrida merupakan sebuah protokol yang menggunakan beberapa cipher dari jenis yang berbeda bersama-sama, sehingga masing-masing dapat memberikan keuntungan terbaiknya (Ramaraj, dkk., 2009). Kriptografi algoritma hibrida bertujuan mengurangi kelemahan dan menggabungkan keunggulan dari sifat algoritma kunci simetris dan asimetris. Kriptografi hibrida merupakan algoritma yang memanfaatkan dua tingkatan kunci yaitu kunci rahasia simetris dengan satu kunci (*session key*) dan enkripsi asimetris dengan sepasang kunci (*public/private key*). Kriptografi hibrida diharapkan akan memberi keamanan yang lebih baik terhadap pengiriman informasi dengan rasio ukuran dan waktu proses enkripsi yang lebih baik, sehingga *bandwith* jaringan yang digunakan relatif kecil.

Contoh penelitian yang menggabungkan sistem kriptografi kunci simetris dan asimetris adalah penelitian You, dkk (2018). Pada penelitian ini dilakukan studi mendalam tentang ECC dan algoritma enkripsi AES sebagai standar enkripsi, yang dikombinasikan dengan *key exchange* Diffie-Hellman. Kombinasi ketiga algoritma menghasilkan desain sistem campuran kriptografi dengan keamanan komunikasi lebih terjamin, mudah diterapkan, kecepatan operasi cepat dan biaya rendah.

Salah satu algoritma yang merupakan pengembangan dari ECC adalah ECDSA. ECDSA adalah varian dari DSA yang menggunakan ECC (Vijayakumar, dkk., 2014). ECDSA memiliki ukuran kunci yang lebih kecil, yang menyebabkan waktu komputasi dan pengurangan pemrosesan yang lebih cepat daya, ruang penyimpanan, dan *bandwidth*. Ini membuat ECDSA ideal untuk perangkat yang dibatasi seperti pager, *mobile instant*, dan *smart card* (Khalique, dkk., 2010). Penelitian yang dilakukan Hutter, Feldhofer, & Wolkerstorfer (2011) dengan menggabungkan pembuatan tanda tangan digital menggunakan ECDSA dan

menggunakan AES sebagai layanan enkripsi / dekripsi pada prosesor perangkat keras bersumber daya rendah. Penelitian menunjukkan kinerja AES hanya membutuhkan 2387 GE dan SHA-1 membutuhkan 889 GE. Hasil penelitian ini menunjukkan bahwa penggunaan ECDSA sebagai tanda tangan digital dapat meningkatkan efisiensi kerja AES dan hanya memerlukan sedikit memori.

Berdasarkan permasalahan, literatur, dan hasil penelitian yang telah diungkapkan sebelumnya, menunjukkan sistem kriptografi hibrida dapat lebih menjamin keamanan informasi, juga algoritma AES, algoritma Diffie-Hellman, dan algoritma ECDSA masing-masing dapat digunakan sebagai pengaman aplikasi *instant messaging*. Oleh karena itu, maka peneliti mencoba membuat aplikasi pengaman *instant messaging* dengan sistem kriptografi hibrida dengan menggabungkan algoritma AES-128, algoritma Diffie-Hellman, dan ECDSA. Aplikasi *instant messaging* digunakan pada perangkat *mobile* yang memiliki jumlah memori terbatas, maka diperlukan algoritma pengamanan yang menggunakan memori minimal tetapi memiliki performa yang maksimum, sehingga dalam penelitian ini sebagai kunci simetris dipilih algoritma AES-128 karena kecepatan proses enkripsi algoritma AES-128 lebih cepat dan memakan memori paling kecil dibandingkan jenis algoritma AES lainnya (NIST & PUBS.F, 2001; Rayarikar, dkk., 2012), serta Diffie-Hellman sebagai kunci asimetris. Untuk mengatasi serangan pada algoritma Diffie-Hellman saat pertukaran kunci, maka digunakan algoritma tanda tangan digital ECDSA. ECDSA dipilih sebagai algoritma tanda tangan digital, karena memiliki keunggulan dibandingkan dengan DSA dan RSA dalam hal waktu eksekusi dan jumlah penyimpanan yang digunakan lebih kecil (Levy, 2015).

Penelitian akan menggunakan skema sistem kriptografi hibrida yang diadaptasi dari Gutub & Khan (2012) dimana algoritma Diffie-Hellman digunakan sebagai *key exchange* untuk mengenkripsi pesan, algoritma AES-128 digunakan sebagai pengamanan isi pesan, serta algoritma ECDSA digunakan sebagai autentikasi pengirim pesan. Kombinasi dari ketiga algoritma ini diharapkan, berpengaruh terhadap kerahasiaan, integritas, autentikasi, dan non-penyangkalan.

Pada penelitian ini akan dibahas mengenai cara penggabungan algoritma Diffie-Hellman, AES-128 dan ECDSA pada pengamanan aplikasi *instant messaging*, pengaruh penggabungan algoritma Diffie-Hellman, AES-128 dan ECDSA terhadap pengamanan aplikasi *instant messaging*, dan berapa banyak data yang dapat diproses (*throughput*) dalam waktu bit/detik untuk mengukur performa gabungan algoritma Diffie-Hellman, AES-128 dan ECDSA.

1.2 Rumusan Masalah

Dari penjelasan pada bagian latar belakang, maka rumusan masalah dalam penelitian ini adalah:

1. Bagaimana cara menggabungkan algoritma Diffie-Hellman, AES-128, dan ECDSA pada proses pengenkripsian dan pendekripsian pesan pada *mobile instant messaging*?
2. Bagaimana pengaruh penggabungan algoritma Diffie-Hellman, AES-128, dan ECDSA pada sistem keamanan pesan *mobile instant mesaging* terhadap kerahasiaan, integritas data, autentikasi dan non-penyangkalan?
3. Bagaimana hasil pengujian terhadap waktu proses enkripsi dan dekripsi dari penggabungan algoritma Diffie-Hellman, AES-128, dan ECDSA pada berbagai ukuran *plaintext* dan *ciphertext*?

1.3 Tujuan Penelitian

Adapun tujuan dari penelitian ini sebagai berikut:

1. Menerapkan penggabungan algoritma Diffie-Hellman, AES-128, dan ECDSA pada proses pengenkripsian dan pendekripsian pesan pada *mobile instant messaging*.
2. Mengkaji pengaruh penggabungan algoritma Diffie-Hellman, AES-128, dan ECDSA terhadap kerahasiaan, integritas data, autentikasi dan non-penyangkalan.
3. Mendapatkan lama waktu proses enkripsi dan dekripsi dari hasil penggabungan algoritma Diffie-Hellman, AES-128, dan ECDSA pada berbagai ukuran *plaintext* dan *ciphertext*.

1.4 Batasan Masalah

Dalam penelitian ini dilakukan pembatasan masalah antara lain adalah:

1. Pesan pada mobile *instant messaging* yang digunakan untuk enkripsi maupun dekripsi hanya berupa pesan berbentuk teks.
2. Ukuran *plaintext* dan *ciphertext* pada penelitian ini menggunakan format ASCII (*American Standart Code for Information Interchange*).
3. Penulisan pesan hanya sampai 150 karakter
4. Algoritma AES yang digunakan menggunakan kunci sepanjang 128 bit

1.5 Sistematika Penulisan

Adapun sistematika penulisan skripsi ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah yang melandasi dilakukannya penelitian mengenai sistem keamanan pada *mobile instant mesaging* menggunakan algoritma Diffie-Hellman, AES-128, dan ECDSA. Kemudian memaparkan solusi yang penulis tawarkan serta harapan penulis terhadap penelitian ini. Selain itu**,** pada bab ini akan diuraikan mengenai rumusan masalah, tujuan penelitian, batasan masalah serta sistematika penulisan.

BAB II TINJAUAN PUSTAKA

Bab ini berisi penjelasan tentang teori-teori keamanan data dan informasi, kriptografi, perhitungan konversi heksadesimal, algoritma Diffie-Hellman, algoritma AES-128, dan algoritma ECDSA yang digunakan dalam penelitian.

BAB III METODE PENELITIAN

Bab ini berisi penjelasan langkah-langkah yang akan dilakukan dalam penelitian.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini membahas mengenai hal-hal yang dilakukan selama penelitian berlangsung, mulai dari pembangunan perangkat lunak, hingga pengujian sistem keamanan *mobile instant messaging* menggunakan algoritma Diffie-Hellman, algoritma

AES-128, dan algoritma ECDSA yang akan digunakan untuk menjawab apa yang sudah dirumuskan dalam rumusan masalah.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dari keseluruhan penelitian yang telah dilakukan, serta saran dari penulis untuk kegiatan penelitian selanjutnya terkait dengan topik yang sedang dibahas.