1. Pendahuluan

1.1 Latar Belakang

Di tengah maraknya kemunculan berbagai aplikasi *instant messaging*, layanan pesan singkat *Short Message Service* (SMS) masih merupakan salah satu cara berkomunikasi yang banyak digunakan, karena SMS tidak membutuhkan koneksi internet serta SMS masih dianggap murah, cepat, dan simpel. Saat ini SMS juga digunakan untuk mengirim data-data rahasia seperti *password*, detail akun bank, informasi rahasia perusahaan, informasi rahasia negara, dsb. Namun sayangnya, media yang digunakan untuk mentransmisikan SMS tidak sepenuhnya aman dan rentan akan serangan [1]. Seperti diberitakan media pada awal tahun 2014, Dinas intelijen Amerika Serikat, NSA (*National Security Agency*), dilaporkan melakukan kegiatan pengumpulan pesan teks (SMS) per hari dari seluruh dunia [2].

Salah satu teknik yang biasa digunakan untuk memberikan keamanan adalah enkripsi. Berbagai skema enkripsi telah diterapkan pada SMS, diantaranya skema enkripsi *hybrid*, yaitu menggabungkan skema *symmetric* dan *asymmetric*. Salah satu implementasinya adalah penggunaan AES sebagai algoritma *symmetric* dan *Elliptic Curve Diffie Hellman* (ECDH) sebagai algoritma *asymmetric*-nya [3][4]. Namun protokol *Diffie-Hellman* sebagai metode pertukaran kunci tidak menyediakan otentikasi terhadap pihak yang berkomunikasi, yang mana berarti *Man-In-The-Middle (MITM) attack* memungkinkan untuk dilakukan [1].

Untuk menangani permasalahan otentikasi pertukaran kunci, kebanyakan solusi yang ada menyarankan penggunaan *third party server* [1] [5] [6]. *Third party server* bertugas sebagai media penyimpanan kunci dan sertifikat, pembangkit kunci, dan pendistribusi kunci. Namun dalam penerapan penggunaannya tidaklah mudah, karena selain dibutuhkan *hardware* tambahan yaitu *server*, dibutuhkan juga mekanisme tambahan untuk pengamanan *server*-nya. Sehingga pasti akan membutuhkan *extra cost* dalam penerapannya. Maka dicarilah metode lain untuk pengamanan pertukaran kunci ECDH yaitu dengan menerapakan *digital signature* untuk menandatangani pesan. *Digital signature* sudah pernah digunakan untuk mengamankan SMS yaitu menggunakan algoritma *Elliptic Curve Digital Signature Algorithm* (ECDSA) [7][8][9], yang mana alasan digunakannya adalah untuk mengetahui keaslian identitas pengirim pesan dan integritas data pesan.

Pada penelitian ini dirancang dan diimplementasikan skema enkripsi *hybrid peer-to-peer* yang menyediakan layanan keamanan *confidentiality*, *integrity*, *authentication*, dan *non-repudiation*, menggunakan kombinasi algoritma AES untuk enkripsinya, penanganan pertukaran kunci menggunakan ECDH, *digital signature* menggunakan ECDSA. Penelitian ini mengusulkan solusi alternatif yang menyediakan *end-to-end security*, yang diharapkan mengatasi permasalahan di atas tanpa adanya tambahan *hardware* dan tanpa adanya efek negatif pada performa perangkat *mobile phone*. Akan dilakukan pembangunan aplikasi pesan singkat SMS pada *smartphone* android. Android dipilih karena berdasarkan survei perusahaan periset pasar IT, Gartner, bahwa pada tahun 2015 android menguasai pasar *Operating System* untuk *smartphone* di seluruh dunia [10].

1.2 Perumusan masalah

Rumusan masalah pada tugas akhir ini adalah:

1. Bagaimana merancang dan menerapkan SMS terenkripsi menggunakan kombinasi algoritma ECDSA-ECDH dan AES pada aplikasi pesan teks *peer-to-peer* berbasis android.
2. Bagaimana agar aplikasi yang dibangun menerapkan proses enkripsi dan dekripsi serta menyediakan layanan keamanan *confidentiality, integrity, authentication,* dan *non-repudiation.*

1.3 Batasan Masalah

Adapun batasan masalah dalam tugas akhir ini adalah sebagai berikut:

1. Pada tugas akhir ini akan difokuskan pada penerapan *secure SMS* pada aplikasi untuk memenuhi karakteristik keamanan informasi, tidak berfokus pada *user interface* aplikasi.
2. Pada tugas akhir ini difokuskan agar data pesan dapat sampai ke penerima dengan baik, tidak dilakukan proses kompresi data.
3. Aplikasi ini dibangun untuk *smartphone* berbasis android, khususnya versi android 4.4 ke atas.
4. Proses enkipsi dan dekripsi hanya terbatas pada file text.

1.4 Tujuan

Berdasarkan rumusan masalah, adapun tujuan yang ingin dicapai dari tugas akhir ini adalah:

1. Merancang dan menerapkan SMS terenkripsi menggunakan kombinasi ECDSA-ECDH dan AES pada aplikasi pesan teks *peer-to-peer* berbasis android
2. Menerapkan proses enkripsi dan dekripsi pada aplikasi yang dibangun, yang mana menyediakan layanan keamanan *confidentiality, integrity, Authentication,* dan *Non-repudiation.*

1.5 Metodologi Penyelesaian Masalah

a. Tahap studi literatur
   Mencari referensi yang berhubungan dengan topik tugas akhir ini, yaitu sistem enkripsi dan dekripsi AES, sistem pertukaran kunci *Elliptic Curve Diffie Hellman (ECDH),* sistem penandatanganan digital *Elliptic Curve Digital Signature (ECDSA),* penerapan sistem enkripsi pada SMS, pembuatan aplikasi Android dalam bentuk buku, jurnal, paper, dll. Selain itu, mempelajari dan memahami materi yang berhubungan dengan topik tugas akhir.
b. Tahap analisis dan perancangan kebutuhan sistem
   Menganalisis dan membuat rancangan sistem yang mencakup proses penandatanganan dan verifikasi kunci publik menggunakan ECDSA, proses pertukaran kunci publik menggunakan ECDH, proses enkripsi-dekripsi pesan menggunakan AES untuk diterapkan pada *smartphone* Android, menggunakan pendekatan *threat modelling*. Membuat rancangan antarmuka aplikasi sesuai kebutuhan sistem.
c. Tahap implementasi
   Melakukan implementasi sistem dan implementasi antarmuka pada Android yang mencakup tahap pertukaran kunci ECDSA (mulai dari membuat kunci privat dan kunci publik,

pertukaran kunci, hingga verifikasi *signature*-nya), tahap pertukaran kunci ECDH (mulai dari membuat kunci privat dan kunci publik, menandatangani kunci publik ECDH dengan kunci private ECDSA, pertukaran kunci, hingga membuat *shared secret key*), tahap enkripsi-dekripsi pesan (mulai dari mengenkripsi pesan menggunankan *shared secret key*, mengirim pesan, hingga mendekripsi pesan).

d. Tahap pengujian dan analisis
   Melakukan pengujian terhadap sistem yang dibangun. Hal yang diujikan yaitu fungsionalitas aplikasi, waktu proses enkripsi, waktu proses dekripsi, panjang pesan sebelum dan sesudah proses enkripsi, pengujian enkripsi dan dekripsi pesan, pengujian perbandingan algoritma *digital signature.* Selanjutnya melakukan analisis terhadap hal-hal yang diujikan, analisis *overhead* aplikasi, analisis karakteristik keamanan, analisis penggunaan *password.,* untuk kemudian dibuat kesimpulan dari penelitian ini.
e. Tahap pembuatan laporan
   Pada tahap ini, dilakukan penyusunan laporan akhir dan pengumpulan dokumentasi yang diperlukan, format laporan mengikuti kaidah penulisan yang benar dan yang sesuai dengan ketentuan yang ditetapkan oleh institusi.

1.6 Sistematika Penulisan

Tugas akhir ini dibagi dalam beberapa topik bahasan yang disusun secara sistematis sebagai berikut:

BAB 1 Pendahuluan

Bab ini membahas latar belakang masalah, rumusan masalah, batasan masalah, tujuan, metodologi penyelesaian masalah, sistematika penulisan.

BAB 2 Tinjauan Pustaka

Bab ini membahas prinsip dasar *Elliptic Curve Diffie Hellman*, *Elliptic Curve Digital Signature Algorithm*, dan AES. Selain itu juga membahas apa itu kriptografi secara umum, skema enkripsi *hybrid* yang merupakan penggabungan skema *asymmetric* dan *symmetric*, ulasan tentang cara kerja SMS secara umum, penjelasan mengenai sistem operasi Android, serta sedikit ulasan mengenai *library* yang digunakan dalam pembangunan aplikasi ini.

B**AB 3 Perancangan Sistem**

Bab ini menjelaskan analisis kebutuhan sistem, *threat modelling*, perancangan sistem yang diajukan, analisis kebutuhan perangkat lunak, serta bagaimana skenario pengujian terhadap sistem.

BAB 4 Pengujian dan Analisis

Bab ini membahas implementasi sistem, pembahasan kodingan aplikasi, pengujian sistem dan analisis terhadap hasil pengujian yang telah dilakukan.

BAB 5 Kesimpulan dan Saran

Bab ini membahas kesimpulan dari hasil pengujian sistem yang dibuat dan memberikan saran yang tepat sebagai bahan acuan untuk penelitian selanjutnya.