BAB 1 PENDAHULUAN

1.1 Latar belakang

Teknologi komunikasi berkembang sangat cepat seiring dengan kebutuhan manusia akan pentingnya informasi. Hal ini didukung dengan perkembangan telepon selular sebagai media yang tidak hanya sebagai pengirim atau penerima data suara, tetapi juga data teks dan gambar. Salah satu fasilitas yang paling digemari dan mudah digunakan pada telepon selular adalah *Short Message Service* (SMS). SMS memiliki kelebihan dapat mengirimkan pesan singkat dengan cepat (Prihartini, 2006).

Dengan maraknya pemakaian SMS sebagai hasil dari inovasi teknologi mendorong banyak industri bisnis dan dunia usaha menggunakan SMS dalam berbagai bidang kehidupan dan dunia usaha. Misalnya saat ini sering kita temui aplikasi-aplikasi berbasis SMS, seperti SMS *banking,* SMS akademik, SMS *polling,* dan lainya. Layanan-layanan tersebut tentunya akan meminta data penting seperti PIN, *password,* NIM, nomor rekening, dan data penting lainya kepada pengguna untuk dapat mengaktifkan aplikasi SMS tersebut. Data-data penting tersebut dapat terbaca oleh pihak yang tidak bertanggung jawab ketika dikirimkan dan disimpan pada SMSC (*Short Message Service Center*). SMSC merupakan tempat penyimpanan SMS sebelum pesan dikirimkan ke nomor tujuan. Hal tersebut dapat menyebabkan terjadinya penyalahgunaan data yang akan merugikan pengguna (Prihartini, 2006).

Sistem nirkabel yang paling banyak digunakan pada proses pertukaran pesan SMS adalah GSM (*Global System for Mobile Communication).* Komponen-komponen yang digunakan oleh GSM antara lain *Mobile Station,* ESME (*External Short Message Entities*), BS (*Base Station*), MSC (*Mobile Switching Center*), register-register yang diantaranya adalah HLR (*Home Location Register*) dan VLR (*Visitor Location Register*), dan SMSC (*Short Message Service Center*) yang merupakan tempat dimana SMS disimpan sebelum dikirimkan ke tujuan (Prihartini, 2006).

Celah keamanan terbesar pada komunikasi SMS adalah dapat terbacanya pesan yang dikirimkan dan simpan pada SMSC ketika terjadi serangan pada SMSC. Salah satu solusi menanggulangi masalah tersebut adalah dengan melakukan penyandian pesan yang dikirimkan atau lebih dikenal dengan enkripsi. Enkripsi merupakan proses untuk mengamankan sebuah informasi (*plaintext*) menjadi informasi yang tersembunyi (*ciphertext*) dengan menggunakan kunci tertentu. *Ciphertext* merupakan sebuah informasi yang tidak dapat dibaca dengan mudah. Agar *ciphertext* dapat dibaca sebagai *plaintext* maka dilakukan proses deskripsi (Schneier, 1996)

Pengamanan pesan dengan melakukan enkripsi pada SMS diperlukan agar pesan SMS yang dikirim tidak dapat terbaca oleh pihak lain Adapun metode yang digunakan untuk melakukan enkripsi SMS dalam penelitian ini adalah dengan

menggunakan algoritma *Advanced Encryption Standard* (AES) dan Elliptic Curve Diffie-Hellman. Algoritma AES merupakan standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (*National Institute of Standard and Technology*) yang digunakan sebagai pengganti algoritma DES (*Data Encryption Standard*) yang sudah berakhir masa penggunaanya pada tahun 2001. Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendeskripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit (Kurniawan, 2007).

Metode Elliptic Curve Diffie-Hellman merupakan sebuah protokol perjanjian kunci anonim yang memungkinkan dua pihak, A dan B, untuk membangun kunci rahasia bersama (*share secret key*) melalui saluran yang tidak aman, di mana masing-masing pihak memiliki pasangan kunci public dan kunci private berbasis *elliptic curve*. *Share secret* tersebut nantinya dapat digunakan sebagai kunci untuk kriptografi kunci simetris (Hendra, 2014).

Dalam penelitian ini dilakukan analisis perbandingan antar algoritma AES 128 bit, 192 bit, serta 256 bit. Analisis perbandingan diperlukan agar kita dapat mengetahui perbandingan waktu proses enkripsi dan dekripsi serta tingkat keamanan dari masing-masing AES 128 bit, AES 192 bit serta AES 256 bit. Dari penelitian ini diharapkan kita dapat mengetahui perbandingan waktu proses dari algoritma AES untuk enkripsi perpesanan.

1.2 Rumusan masalah

Berdasarkan uraian latar belakang masalah, maka dapat dirumuskan permasalahan yang dibahas dalam penelitian ini adalah:

1. Bagaimana analisis perbandingan performansi algoritma AES 128 bit, AES 192 bit serta AES 256 bit untuk enkripsi SMS berbasis android?

1.3 Tujuan

Tujuan yang ingin dicapai dalam penelitian ini adalah:

1. Untuk mengetahui analisis perbandingan performansi algoritma AES 128 bit, AES 192 bit serta AES 256 bit untuk enkripsi SMS berbasis android.
2. Untuk mengetahui analisis varians dari performansi algoritma AES 128 bit, AES 192 bit serta AES 256 bit untuk enkripsi SMS berbasis android?

1.4 Manfaat

a. Manfaat bagi penulis
b. Penulis dapat mengetahui perbandingan performansi serta analisa variansi dari AES 128 bit, AES 192 bit dan AES 256 bit untuk enkripsi SMS berbasis Android.
c. Manfaat bagi pembaca

Sebagai tambahan informasi dan bahan masukan untuk mempertimbangkan pemakaian algoritma AES dan ECDH untuk enkripsi SMS pada telepon seluler berbasis android.

1.5 Batasan masalah

Batasan masalah dalam skripsi ini adalah sebagai berikut:

a. Dalam penelitian ini tidak memperhatikan besar biaya pengiriman SMS
b. Dalam penelitian ini tidak membahas mengenai proses pengiriman paket data SMS dalam jaringan telepon selular.
c. Algoritma enkripsi-deskripsi pada aplikasi menggunakan algoritma *Advanced Ecryption Standard* (AES) dengan panjang kunci 128 bit.
d. Metode pertukaran kunci rahasia menggunakan algoritma Elliptic Curve Diffie-Hellman.

1.6 Sistematika pembahasan

Adapun sistematika pembahasan dari skripsi ini disusun secara garis besar adalah:

BAB I Pendahuluan

Bab ini menguraikan latar belakang masalah, rumusan masalah, batasan masalah, tujuan, manfat dan sistematika pembahasan

BAB II Tinjauan Pustaka

Bab ini membahas mengenai kajian pustaka dan teori-teori yang diperlukan untuk enkripsi SMS pada telepon seluler berbasis android dengan menggunakan metode ECDH dan AES yang terdiri dari teori mengenai kriptografi, AES, ECDH, SMS serta Android.

BAB III Metodologi Penelitian

Bab ini menjelaskan mengenai metode yang digunakan dalam melakukan proses enkripsi SMS pada telepon seluler berbasis android dengan metode ECDH dan algoritma AES

BAB IV Perancangan

Bab ini membahas tentang perancangan proses algoritma serta perancangan sistem yang akan dibuat.

BAB V Implementasi

Bab ini membahas tentang teknis implementasi beserta algoritma operasi yang digunakan dalam pengembangan sistem.

BAB VI Pengujian dan Analisis

Bab ini berisi teknik pengujian, hasil pengujian dan analisis hasil pengujian dari perangkat lunak yang telah dibangun serta algoritma yang digunakan.

BAB VII Penutup

Bab ini berisi kesimpulan dan saran yang merupakan penutup dari penelitian ini.