1. Pendahuluan

1.1 Latar belakang

Saat ini, seluruh aspek-aspek kehidupan telah dimasuki oleh dunia informasi. Dari urusan rumah tangga sampai dalam dunia kerja., informasi adalah sesuatu yang sangat penting dan mendasar. Seperti yang biasa digunakan untuk berkomunikasi sehari-hari yaitu handphone, merupakan suatu alat komunikasi yang tidak dapat lepas dari teknologi informasi. Dengan adanya teknologi informasi, sangat mempermudah kehidupan manusia. Teknologi informasi dapat mempersingkat waktu dan biaya yang merupakan sesuatu yang sangat berharga pada saat ini.

Ada berjuta-juta informasi dan pesan yang dikirim setiap detiknya melalui berbagai macam alat komunikasi seperti telepon, komputer, faksimili, dan lain-lain. Pada suatu komunitas yang aktif dan sangat mementingkan pertukaran informasi dalam waktu yang sangat singkat, SMS sangat dibutuhkan. Karena dengan SMS kita dapat berkirim pesan singkat dengan biaya yang murah. SMS terkadang digunakan untuk mengirimkan data rahasia seperti *social security number*, nomor rekening bank, password dan lain-lain. Tetapi, apakah saluran kita berkirim pesan aman. Aman dalam artian kerahasian pesan terjamin, keutuhan data atau pesan terjamin sampai ke penerima, data atau pesan yang dikirimkan terjamin keasliannya, dan tidak terjadi penangkalan bahwa seseorang bukan yang mengirimkan pesan. Begitu juga masalah keamanan dalam pengiriman pesan melalui SMS. SMS bukanlah pilihan terbaik untuk komunikasi yang aman. Spesifikasi dan teknologi pada SMS masih banyak terdapat celah keamanan yang menyebabkan SMS bukanlah jalur komunikasi yang aman untuk pertukaran informasi.

Oleh karena itu diperlukan aplikasi untuk memastikan bahwa pesan yang dikirim melalui SMS terjamin keamanannya. Otentifikasi dan *non-repudiation* dalam komunikasi SMS bisa didapatkan dengan mudah dari melihat pesan tersebut yang terdapat nomor pengirimnya. Enkripsi adalah salah satu cara untuk menjaga kerahasiaan suatu pesan yang dikirimkan karena dengan enkripsi, seseorang tidak dapat melihat pesan asli (plainteks) kecuali mempunyai kunci yang sesuai untuk mendekripsikannya.

Algoritma Rijndael telah terbukti merupakan algoritma yang efisien dan juga fleksibel untuk pengenkripsian. Algoritma ini mendukung panjang kunci 128, 192, dan 256 bit. Karena algoritma Rijndael mempunyai panjang kunci minimal 128 bit, maka algoritma ini tahan terhadap serangan *exhaustive key search* dengan teknologi saat ini. Dengan panjang kunci 128 bit, maka terdapat sebanyak 3.4×10^{38} kemungkinan kunci. Jika digunakan komputer tercepat yang dapat mencoba satu juta kunci setiap milidetik, maka akan dibutuhkan waktu $5{,}4 \times 10^{18}$ tahun untuk mencoba seluruh kemungkinan kunci.

Sudah banyak sekali aplikasi enkripsi yang menggunakan algoritma Rijndael karena keefisienannya dan fleksibelitasnya. Tetapi bagaimana menerapkan algoritma Rijndael untuk aplikasi enkripsi SMS pada handphone yang mempunyai

jumlah memori yang terbatas serta kerja sistem yang kecepatannya sesuai untuk penggunaan pada handphone.

Saat ini sudah banyak handphone yang mampu menjalankan aplikasi berbasis Java. Oleh karena itu, aplikasi enkripsi SMS ini dibangun dengan menggunakan teknologi Java.

1.2 Perumusan masalah

Dalam tugas akhir ini dirumuskan beberapa masalah sebagai berikut:

1. Bagaimana SMS yang dikirimkan dapat dienkripsikan dengan benar menggunakan algoritma Rijndael sesuai dengan format SMS.
2. Bagaimana cara kinerja algoritma Rijndael dalam mengenkripsikan teks pada handphone yang mendukung teknologi Java.
3. Bagaimana SMS yang telah dienkripsikan dapat dideskripsikan sesuai dengan pesan asli.

Adapula beberapa batasan masalah sebagai berikut:

1. SMS yang dikirimkan dan diterima tidak dapat disimpan (masuk *Inbox*).
2. Jumlah karakter SMS terbatas yaitu hanya bisa mengirim maksimum 300 karakter.
3. Pengenkripsian dan pendekripsian hanya bisa dilakukan jika aplikasi sedang dijalankan pada handphone.

1.3 Tujuan

Tujuan dari tugas akhir ini adalah sebagai berikut:

1. Membuat suatu aplikasi pengiriman SMS pada handphone dalam menerima maupun mengirim pesan dalam bentuk teks dengan penggunaan pengenkripsian data.
2. Menganalisis kinerja algoritma Rijndael pada handphone berdasarkan waktu respon dan jumlah karakter yang dipakai pada handphone.

1.4 Metodologi penyelesaian masalah

Metodologi penyelesaian masalah yang digunakan dalam penelitian tugas akhir ini adalah:

a. Studi Literatur
   Tahapan ini meliputi pengumpulan data yang bertujuan untuk mendapatkan deskripsi yang jelas dan dasar teori yang kuat tentang algoritma Rijndael yaitu metode yang dipakai untuk mengenkripsi SMS, MIDP yang dipakai untuk sebuah profil J2ME, dan J2ME yang dipakai untuk membangun aplikasi Enkripsi SMS ini.
b. Analisis masalah dan Perancangan pengembangan Perangkat Lunak
   Tahapan ini meliputi analisis kebutuhan untuk merancang aplikasi enkripsi SMS dengan algoritma Rijndael. Desain dari perangkat lunak yang akan dibangun dengan pendekatan berorientasi objek menggunakan metodologi RUP, bahasa pemodelan UML dan software Rational Rose.

c. Pembuatan Perangkat Lunak
   Bertujuan melakukan implementasi metode pada perangkat lunak sesuai dengan analisis perancangan yang telah dilakukan dengan menggunakan J2ME.
d. Pengujian perangkat lunak dan analisis
   Pada tahap ini akan dilakukan pengujian terhadap perangkat lunak yang telah dibangun dan sekaligus melakukan analisis terhadap hasil perangkat lunak dengan memberikan berbagai input ke dalam perangkat lunak ini. Output dari perangkat lunak ini akan dianalisis performansi dan efektifitas hasil enkripsi dari kecepatan pengenkripsian dan juga memori yang terpakai.
e. Penyusunan Laporan Tugas Akhir dan kesimpulan akhir.
   Pada tahap ini akan dilakukan penyusunan hasil laporan terhadap penelitian yang telah dilakukan, dan membuat kesimpulan dari hasil penelitian tersebut.