1. Pendahuluan

1.1 Latar belakang

Keamanan suatu data merupakan suatu prioritas tertinggi bagi seseorang user yang datanya tidak ingin diketahui oleh orang lain tanpa ijin atau sepengetahuan orang yang memiliki data tersebut. Oleh karena itu, banyak orang berusaha untuk membuat suatu sistem keamanan data yang lebih baik lagi, sehingga sampai saat ini sangat banyak produk yang dihasilkan dalam mengamankan datanya. Apalagi, pada aplikasi seperti SMS yang digunakan pada teknologi GSM dan CDMA sangat rawan akan pencurian data oleh orang yang paham akan spesifikasi dan teknologi dasar SMS, Sehingga diperlukan adanya suatu pengamanan atau kerahasiaan pesan.

Salah satu metode yang digunakan untuk menjaga kerahasiaan data adalah kriptografi. Kriptografi merupakan seni atau ilmu untuk menjaga kerahasiaan pesan[5,6,7]. Di dalam kriptografi, terdapat proses enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu data asli (*plaintext*) ke dalam bentuk yang tidak dapat dibaca (*ciphertext*) dengan menggunakan suatu kunci. Dekripsi adalah proses mengubah data yang sudah dalam bentuk yang tidak dapat dibaca (*ciphertext*) menjadi dapat dibaca (*plaintext*) dengan menggunakan suatu kunci. Untuk dapat melakukan enkripsi dan dekripsi, dibutuhkan algoritma (*cipher*) dan kunci. Algoritma atau Chiper adalah suatu fungsi matematika dan kunci adalah sederetan bit, dimana keduanya digunakan untuk proses enkripsi dan dekripsi. Untuk kunci pun ada 2 tipe, yaitu: kunci simetri yang menggunakan sebuah kunci rahasia yang sama untuk melakukan proses enkripsi dan dekripsinya; dan kunci asimetri yang menggunakan sepasang kunci yang berbeda (publik dan pribadi) untuk melakukan proses enkripsi dan dekripsinya [5,6,[7].

Algoritma kriptografi yang akan digunakan dalam tugas akhir ini yakni algoritma RSA. Algoritma RSA dijabarkan pada tahun 1977 oleh Ron Rivest, Adi Shamir dan Len Adleman dari Massachusetts Institute of Technology, huruf **RSA** itu sendiri juga berasal dari inisial nama mereka (**R**ivest—**S**hamir—**A**dleman) [2,5,7]. Algoritma RSA merupakan algoritma kunci asimetri yang memungkinkan tingkat sekuritasnya tinggi karena Algoritma RSA mempunyai *public key* yang dapat diketahui secara umum dan private key yang hanya diketahui oleh user yang mengenkripsi serta tingkat kesulitan pemfaktoran bilangan non prima menjadi faktor primanya [2,5,7].

Pada tugas akhir ini dikembangkan aplikasi untuk mengamankan data yang akan dikirim melalui handphone dengan menambahkan fasilitas pengiriman data text (SMS) yang dienkripsi menggunakan algoritma RSA dengan menggunakan teknologi Java 2 Micro Edition (J2ME). J2ME merupakan salah satu teknologi Java yang memungkinkan mobile user dapat mengakses dan berinteraksi dengan informasi serta layanan-layanan aplikasi wireless, antara lain fasilitas security tambahan misalnya dengan cara mengenkripsi terhadap pesan yang akan dikirimkan sehingga diharapkan akan didapat suatu aplikasi pengiriman pesan terenkripsi yang cepat, lebih aman dan mudah untuk digunakan

sehingga data penting yang bersifat rahasia hanya dapat dibaca oleh orang yang dituju.

1.2 Perumusan masalah

Dalam tugas akhir ini dirumuskan beberapa masalah sebagai berikut:

1. Bagaimana membuat suatu aplikasi enkripsi data SMS menggunakan algoritma RSA yang dapat digunakan pada handphone yang mensupport teknologi Java 2 Micro Edition (J2ME) .
2. Pemilihan algoritma RSA pada aplikasi enkripsi SMS karena menggunakan public key dan private key serta adanya tingkat sekuritas yang tinggi karena tingkat kesulitan pemfaktoran bilangan non prima menjadi faktor primanya untuk mendapatkan private key.

Ruang lingkup yang menjadi batasan masalah pada penelitian tugas akhir ini antara lain:

1. Antara pengirim dan penerima sms sudah mengetahui private key atau *bit key* yang digunakan dan berhak mengubahnya.
2. Pengenkripsian dan pendekripsian hanya bisa dilakukan jika aplikasi sedang dijalankan pada handphone.
3. Data yang akan dienkripsi dan didekripsi dititik beratkan pada masalah tingkat keamanan sms sehingga tidak mempermasalahkan masalah biaya yang dikenakan.

1.3 Tujuan

Tujuan dari penelitian tugas akhir ini adalah :

1. Mengimplementasikan algoritma kriptografi RSA ke dalam sebuah handphone yakni aplikasi SMS pada handphone dalam menerima maupun mengirim pesan dalam bentuk teks dengan penggunaan pengenkripsian data.
2. Menganalisa performansi (kecepatan, penggunaan memori, keamanan) algoritma kriptografi RSA terhadap aplikasi SMS yang dibangun pada handphone.

1.4 Metodologi penyelesaian masalah

Metodologi pembahasan yang digunakan dalam penelitian Tugas Akhir ini adalah:

1. Studi pustaka :
   a. Pencarian referensi
      Mencari referensi yang berhubungan dengan Kriptografi terutama untuk Algoritma RSA dan hal-hal yang berkaitan dengan arsitektur SMS (sistem kerja, format sms, dll) serta J2ME.
   b. Pendalaman materi
      Mempelajari dan memahami proses enkripsi dan deskripsi algoritma RSA, arsitektur sms pada handphone, serta bahasa pemrograman yang digunakan.

2. Perancangan Perangkat Lunak
   Perancangan Perangkat Lunak dengan menggunakan konsep analisis dan desain yang berorientasikan objek. Dalam hal ini, pemodelan yang akan digunakan adalah UML (*Unified Modeling Language*).
3. Pembangunan aplikasi
   Implementasi apliklasi yakni dengan menggunakan J2ME untuk pembangunan aplikasi sms baik enkripsi maupun deskripsi berdasarkan algoritma RSA dengan memperhatikan spesifikasi yang ingin dibuat.
4. Analisis hasil aplikasi
   Aplikasi yang telah dibangun akan dilakukan pengujian atau testing yakni berdasarkan penggunaan memori, kecepatan, keamanan. Setelah diuji, akan di analisis berdasarkan tingkat keamanan aplikasi sms tersebut .
5. Penyusunan laporan tugas akhir dan kesimpulan akhir.