BAB 1

PENDAHULUAN

1.1 Latar Belakang

Saat ini telepon selular (*mobilephone*) merupakan sebuah alat komunikasi yang telah digunakan oleh sebagian besar orang di seluruh dunia. Telepon selular menyediakan media komunikasi yang beragam dan salah satu diantaranya adalah media SMS (*Short Message Service*). SMS merupakan suatu layanan pengiriman pesan singkat melalui telepon genggam. Walaupun merupakan bagian dari kemampuan standar GSM fase pertama, SMS masih merupakan layanan yang banyak digunakan oleh masyarakat. Penggunaan SMS menjadi popular dikalangan masyarakat dikarenakan dengan begitu mudahnya dapat saling bertukar informasi tanpa batasan jarak dan waktu dengan cepat dan biaya yang murah.

Pada saat ini perkembangan perangkat *mobile* juga telah mengalami perkembang yang sangat pesat. Perkembangan perangkat *mobile* telah membawa kemampuan yang disuguhkan oleh komputer beberapa tahun lalu ke dalam platform *mobile*. *Browsing* internet, mengirimkan email, hingga mengerjakan dokumen kerja dapat dilakukan dengan mudah melalui perangkat *mobile*, seperti *smartphone* dan tablet. Seiring dengan berkembangnya teknologi pada perangkat mobile muncul masalah yang berhubungan dengan tingkat keamanan pada perangkat *mobile* tersebut, seperti penyadapan, pencurian informasi dan yang lainnya. Hal yang riskan pada komunikasi melalui SMS adalah pesan yang dikirimkan akan disimpan di SMSC (*Short Message Service Center*), yaitu tempat dimana SMS disimpan

sebelum dikirim ke tujuan. Pesan yang sifatnya *plaintext* ini dapat disadap oleh siapa saja yang berhasil memiliki akses ke dalam SMSC. Akibatnya, informasi penting seperti *password*, nomer pin, dan lain-lain dapat diketahui oleh orang yang tidak berhak untuk mengetahuinya. Selain itu, ancaman juga bisa datang dari kondisi di sekitar, seperti saat terkadang lupa mengawasi perangkat *mobile* kita dan tanpa disadari adanya pihak yang tidak berkepentingan membaca isi pesan SMS yang terdapat pada perangkat *mobile*. Hal-hal tersebut menjadi sesuatu yang sangat merugikan jika informasi yang dicuri atau disadap adalah informasi yang bersifat pribadi atau rahasia.

Dari permasalah keamanan isi pesan SMS yang telah di jelaskan sebelumnya, muncul permasalahan bagaimana cara untuk mengatasi permasalahan tersebut. Salah satu cara untuk menaggulangi permasalahan tersebut adalah dengan melakukan enkripsi terhadap pesan SMS. Dengan semakin majunya perkembangan pada perangkat *mobile*, implementasi suatu algoritma enkripsi menjadi mungkin untuk diterapkan. Salah satu metode enkripsi yang dapat digunakan untuk permasalahan keamananan adalah dengan menerapkan enkripsi dengan metode Rabin. Teknik kriptografi Rabin merupakan varian dari RSA yang dikemukakan oleh M. Rabin. Kriptografi Rabin merupakan bagian dari kriptografi kunci publik atau *asymmetric cryptosystem* dimana kunci yang digunakan untuk proses enkripsi berbeda dengan kunci yang digunakan pada proses dekripsi.

Berbeda dengan metode enkripsi dengan metode kunci simetris atau *symmetric cryptosystem* dimana kunci yang digunakan pada proses enkripsi dan dekripsi sama. Beberapa metode kriptografi kunci publik yang popular antara lain

RSA, ElGamal dan Rabin. Perbedaan yang paling mencolok antara kriptografi RSA, ElGamal dan Rabin adalah proses kerjanya. RSA dan ElGamal bekerja dengan berbasis *exponentiation congruence*, sementara Rabin dengan berbasis *quadratic congruence*. Perbedaan ini terlihat pada proses pembangkitan kunci, sementara proses enkripsi dan dekripsinya pun juga berbeda.

Android merupakan salah satu sistem operasi *smartphone* yang baru diperkenalkan beberapa tahun belakangan ini. Namun, kehadiranya tidak dapat dianggap sebelah mata karena pengguna sistem operasi Android saat ini telah mengalamai peningkatan yang luar biasa. Hal ini diakibatkan adanya dukungan vendor *smartphone* yang mengadopsi sistem operasi baru ini dalam berbagai produk mereka. Sehingga, secara tidak langsung pengguna akan menggunakan sistem operasi Android ketika membeli *gadget* tersebut.

Android merupakan sistem operasi *mobile* yang berkembang pesat diantara sistem operasi lainya yang juga masih berkembang saat ini. Sistem operasi lainya antara lain Windows Mobile, i-Phone OS, Symbian, dan masih banyak lagi yang juga menawarkan kekayaan isi dan ke optimalan berjalan di atas perangkat *hardware* yang ada. Akan tetapi, beberapa contoh sistem operasi yang telah di sebutkan sebelumnya, berjalan dengan memprioritaskan aplikasi inti yang dibangun sendiri tanpa melihat potensi yang cukup besar dari aplikasi pihak ketiga. Oleh karena itu, adanya keterbatasan dari aplikasi pihak ketiga untuk mendapatkan data asli dari ponsel, berkomunikasi antar proses serta keterbatasan distribusi aplikasi pihak ketiga untuk platform mereka. Berbeda dengan hal tersebut, Android menawarkan sebuah lingkungan yang bersifat *open source* kepada pengembang.

Setiap aplikasi memiliki tingkatan yang sama. Android tidak membedakan antara aplikasi inti dengan aplikasi pihak ketiga. API yang disediakan menawarkan akses ke *hardware*, maupun data-data ponses sekalipun, atau data sistem sendiri. Bahkan pengguna dapat menghapus aplikasi inti dan menggantikanya dengan aplikasi pihak ketiga. Sifat open source inilah yang membuat Android memiliki tempat di antara para pengembang aplikasi saat ini.

Dari permasalahan keamanan pada SMS yang telah dijelaskan sebelumnya, tujuan dari pengerjaan Skripsi ini adalah membuat sebuah perangkat lunak yang berfungsi sebagai aplikasi SMS yang mampu melakukan proses enkripsi dan dekripsi pesan SMS pada perangkat *mobile* berbasis Android dengan menggunakan metode enkripsi RSA.

1.2 Rumusan Masalah

Berdasarkan pada permasalahan yang diangkat dalam Skripsi ini dapat disusun suatu rumusan masalah yaitu bagaimana cara melakukan perancangan Aplikasi Sms Kriptografi Dengan Metode Rsa Pada Smartphone Android agar bisa digunakan untuk mengamankan data sms, dan berapa tingkat keamanan dalam menggunakan algoritma RSA untuk mengamankan data sms.

1.3 Batasan Masalah

Permasalahan yang dibahas dalam Skripsi ini dibatasi, sebagai berikut:

1. Aplikasi ini dapat mengenkripsi dari pesan text biasa ke pesan RSA.
2. Aplikasi ini dapat mendekripsikan dari pesan RSA ke pesan text biasa.
3. Algoritma kriptografi yang digunakan adalah algoritma RSA.
4. Aplikasi yang dibuat hanya dapat dijalankan pada perangkat mobile yang mendukung aplikasi berbasis Android.
5. Implementasi menggunakan Eclipse sebagai IDE dan Android SDK sebagai emulator.
6. Aplikasi ini dapat berjalan di sistem operasi versi Android 2.3.3 .

1.4 Tujuan Penelitian

Ada beberapa maksud dan tujuan yang diharapkan bisa tercapai dari implementasi yang dilakukan, diantaranya adalah :

1. Memahami dan mengetahui bagaimana cara membuat sebuah aplikasi implementasi algoritma RSA untuk enkripsi dan dekripsi data pada smartphone android.
2. Menghasilkan sebuah aplikasi yang bisa bermanfaat untuk mengamankan data sms pada smartphone android

1.5 Manfaat Penelitian

1.5.1 Bagi Pengguna

1. Memberikan pengamanan pada data sms agar terjaga kerahasiaannya dengan menerapkan algoritma RSA untuk melakukan enkripsi.

2. Sebagai referensi bagi pengguna lain yang mempunyai minat dalam mengembangkan tentang pemrograman Android dengan memanfaatkan bidang ilmu kriptografi.

1.5.2 Bagi Penulis

1. Sebagai syarat kelulusan program strata 1 pada Sekolah Tinggi Manajemen Informatika dan Komputer STMIK ''Amikom'' Yogyakarta.
2. Membantu pemahaman tentang kriptografi terutama mengenai algoritma RSA untuk enkripsi dan dekripsi data.
3. Menambah pengalaman, memperluas wawasan penulis tentang pemrograman Android dengan memanfaatkan algoritma RSA dan untuk enkripsi dan dekripsi data.
4. Mengembangkan opini penulis untuk selalu percaya diri dengan kemampuan diri sendiri dalam penulisan Skripsi.

1.6 Metode Penelitian

Metodologi yang digunakan untuk menyelesaikan skripsi ini adalah sebagai berikut:

1. Studi Pustaka

   adalah teknik pengumpulan data dengan menghimpun dan menganalisis dokumen. Dokumen-dokumen yang termasuk didalamnya yaitu penelitian-penelitian terdahulu, buku, artikel dan jurnal yang berkaitan dengan objek penelitian.

2. Studi Literatur

Melakukan studi perbandingan dan analisis antara aplikasi yang pernah dibuat oleh seseorang dengan aplikasi yang penulis buat. Termasuk kelebihan dan kekurangan aplikasi yang telah di buat.

3. Analisis dan Desain

Setelah melewati tahapan studi literatur, tahapan selanjutnya adalah analisis dan desain. Analisis dilakukan untuk mengetahui kebutuhan perangkat lunak berdasarkan domain permasalahan. Hasil analisis tadi akan dilanjutkan menjadi bahan untuk mendesain fungsionalitas apa saja yang nantinya akan digunakan dalam perangkat lunak nantinya.

4. Implementasi

Pada tahap ini dimulai proses untuk membangun perangkat lunak. Dimulai dari menyiapkan *class* yang diperlukan dan yang terakhir adalah *user interface*.

5. Uji Coba dan Evaluasi

Setelah perangkat lunak selesai dibangun, selanjutnya akan dilakukan uji coba dengan beberapa skenario yang meliputi beberapa parameter dan mengacu pada domain permasalahan. Dari sini dapat dilakukan evaluasi jika metode yang digunakan masih belum bisa sepenuhnya menyelesaikan domain permasalahan. Untuk selanjutnya dilakukan identifikasi masalah dan perbaikan.

6. Penyusunan Laporan

Tahap ini dilakukan untuk menyusun dokumentasi tertulis berupa laporan dari semua dasar teori, metode yang digunakan serta hasil-hasil yang diperoleh selama pengerjaan.

1.7 Ruang Lingkup

Penulis membatasi ruang lingkup pembahasan Aplikasi SMS Kriptografi Dengan Metode RSA Pada Smartphone Android agar tidak keluar jauh dari pokok permasalahan yang akan di bicarakan.

1.8 Sistematika Penulisan

Penulis memberikan sistematika berdasarkan bab-bab yang berurutan berdasarkan pokok-pokok permasalahanya untuk mempermudah penyusunan dalam penulisan Skripsi yaitu sebagai berikut :

BAB I : Pendahuluan

Bab ini berisi pengantar terhadap masalah-masalah yang akan dibahas seperti latar belakang masalah, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat, metode pengumpulan data dan sistematika penulisan.

BAB II : Landasan Teori

Bab ini berisi tinjauan pustaka yang mengulas penelitian yang sebelumnya yang berkaitan dengan penelitian tugas akhir ini. Bab ini juga menguraikan teori-teori yang mendasari pembahasan secara detail tentang konsep dasar dalam pembuatan aplikasi dan *software* yang digunakan.

BAB III : Analisis dan Perancangan

Bab ini membahas tentang pengumpulan kebutuhan, analisis dan perancangan perangkat lunak, perancangan antarmuka serta penjelasan tentang perancangan perangkat lunak yang dibangun.

BAB IV : Implementasi dan Pembahasan

Bab ini berisi implementasi dan perancangan sistem aplikasi yang diinginkan.

BAB V : Penutup

Bab ini membahas tentang kesimpulan dan saran yang penulis ambil dari penulisan tugas akhir ini.