BAB 1
PENDAHULUAN

1.1 Latar Belakang

Banyak fitur-fitur yang disediakan oleh Android sebagai sistem operasi telepon selular (ponsel) seperti pemutaran video, *push mail*, mengakses layanan *internet* dan sebagainya. Akan tetapi, fitur-fitur yang digunakan pada ponsel biasa lainnya yaitu seperti *Short Message Service* (SMS), *call* dan *Multimedia Message Service* (MMS) masih dapat digunakan pada perangkat android tersebut. Salah satu yang masih banyak digunakan yaitu SMS.

Layanan SMS yang menggunakan aplikasi SMS bawaan ponsel masih banyak digunakan oleh setiap orang, dan bukan merupakan jalur yang aman dalam pertukaran informasi, terlebih jika informasi yang sifatnya penting atau rahasia seperti *password*, nomor pin, atau rahasia perusahaan yang tidak boleh diketahui oleh orang yang tidak berhak. SMS pada awalnya dirancang untuk komunikasi tidak sinkron dimana pesan yang dikirimkan adalah *plaintext*. Data *plaintext* seperti ini dapat dicegat di jalan oleh siapa saja yang memiliki akses ke sistem SMS. *Short Message Service Center* (SMSC) milik operator merupakan salah satu pihak yang dapat mengambil data ini, walaupun dalam setiap perjanjian terdapat klausul tentang kerahasiaan data, akan tetapi data *plaintext* yang terkirim dan berkasnya tersimpan di berbagai tempat baik di *server* milik operator maupun milik *content provider* membawa satu potensi bahaya yang besar. Kelemahan itu dikarenakan SMS menggunakan standar pengkodingan yang *universal*, SMS dibangun dengan sistem bahasa program yang sejenis dengan bahasa program *hardware* seperti komputer dan telepon selular dapat menerjemahkan semua data dalam frekuensi tertentu yang terbuka (di udara) yang sangat rentan akan ancaman seperti penyadapan pihak yang tak bertanggung jawab. Kemudahan dalam bertukar informasi melalui SMS ini disalahgunakan oleh beberapa pihak. Beberapa orang dengan berbagai cara mencoba mencuri informasi yang bukan hak mereka. Salah satu contoh kasus penyadapan SMS tahun 2007 yang menimpa seorang wartawan

yang bernama Metta Dharmasaputra yang bukan seorang pelaku tindak pidana, teroris, dan pengedar narkotika (sesuai Nomor 36 Tahun 1999 tentang Telekomunikasi dan Peraturan Pemerintah Nomor 52 Tahun 2000) ternyata bisa disadap, itu berarti hal serupa bisa terjadi pada siapa saja. Hal ini tentunya akan sangat berbahaya untuk pengguna, terutama bagi mereka yang sering mengirimkan data dan informasi penting dan rahasia melalui SMS. Informasi penting atau rahasia yang dimaksud adalah informasi yang sifatnya positif.

Kriptografi merupakan salah satu cara dalam mengamankan pesan, karena kriptografi adalah ilmu yang mempelajari tentang penyembunyian huruf atau tulisan juga dapat disebut sebagai bahasa persandian. Dalam pembangunan aplikasi kemanan SMS ini menggunakan algoritma RSA, hal ini karena pada umumnya algoritma lain seperti *blowfish, chiper cigne* , dll. hanya menggunakan satu kunci untuk menterjemahkan isi pesan yang sudah disandikan (*chipertext*) menjadi pesan yang dapat dibaca (*plaintext*), tetapi dengan algoritma RSA proses menyandikan pesan bisa dibilang menggunakan 2 kunci dalam menyandikan atau menterjemahkan pesan yaitu *publik key* yang berfungsi sebagai menyandikan pesan dan *private key* sebagai menterjemahkan pesan yang disandikan.

Berdasarkan uraian diatas, diperlukan suatu metode dan aplikasi untuk mengamankan pesan SMS. Oleh karena itu penulis tertarik untuk membuat tugas akhir ini dengan judul **"Pembangunan Aplikasi Keamanan SMS Menggunakan Algoritma RSA Berbasis *Mobile* Pada *Platform* Android"**.

1.2 Identifikasi Masalah

Berdasarkan uraian pada latar belakang, terdapat beberapa masalah yang dialami sehingga dijadikan dasar penelitian, yaitu :

1. Bagaimana cara mengamankan data SMS *(Short Message Service)* penting atau rahasia agar pesan-pesan tersebut dapat lebih terjamin kerahasiaan dan keamanannya?
2. Bagaimana melakukan penyandian SMS menggunakan algoritma RSA?
3. Bagaimana membangun Pembangunan Aplikasi Keamanan SMS Menggunakan Algoritma RSA Berbasis *Mobile* Pada *Platform* Android?

1.3 Maksud dan Tujuan

Berdasarkan permasalahan yang diteliti, maka maksud dari penulisan tugas akhir ini adalah untuk Pembangunan Aplikasi Keamanan SMS Menggunakan Algoritma RSA Berbasis *Mobile* Pada *Platform* Android.

Adapun tujuan yang ingin dicapai dari Pembangunan Aplikasi Kemanan SMS Menggunakan Algoritma RSA Berbasis *Mobile* Pada *Platform* Android adalah sebagai berikut:

1. Mengamankan SMS *(Short Message Service)* penting atau rahasia yang agar pesan-pesan tersebut dapat lebih terjamin kerahasiaan dan keamannya.
2. Melakukan penyandian SMS menggunakan algoritma RSA.
3. Pembangunan Aplikasi Keamanan SMS Menggunakan Algoritma RSA Berbasis *Mobile* Pada *Platform* Android.

1.4 Batasan Masalah

Adapun batasan masalah dari Pembangunan Aplikasi Keamanan SMS Menggunakan Algoritma RSA Berbasis *Mobile* Pada *Platform* Android adalah :

1. Pesan yang dikirim maupun diterima berupa pesan SMS.
2. Spesifikasi SMS (panjang 1 pesan SMS) disesuaikan dengan standar teknologi *Global System for Mobile Communication* (GSM).
3. Dua belah pihak yang mengirim dan yang menerima SMS harus sama-sama menggunakan aplikasi ini.
4. Aplikasi yang dibangun menggunakan kriptografi asimetrik RSA.
5. Generate *key* untuk menghasilkan *private key* dan *public key* dilakukan di dalam aplikasi.
6. Aplikasi yang akan dibangun menggunakan bahasa pemrograman Java Android.
7. Pengujian aplikasi menggunakan 2 *smartphone* android.
8. Aplikasi yang akan dibangun merupakan aplikasi yang diterapkan pada telepon selular yang bersistem oprasi android minimal menggunakan android versi 2.2 Froyo *(Frozen Yogurt).*

1.5 Metodologi Penelitian

Metode pembangunan perangkat lunak ini menggunakan metode *waterfall* seperti pada gambar I.1 yang terdiri dari beberapa tahap, yaitu [12]:

1. *Requirement*

   Requirement merupakan tahapan analisis terhadap apa saja yang dibutuhkan oleh *system* yang akan dibangun. Analisis yang dilakukan meliputi analisis *user* dan kebutuhan *system*.

2. *Design*

   Design merupakan tahap melakukan perancangan terhadap keseluruhan *system*. Perancangan yang dilakukan yaitu perancangan antarmuka dari *system* yang dibangun.

3. *Implementation*

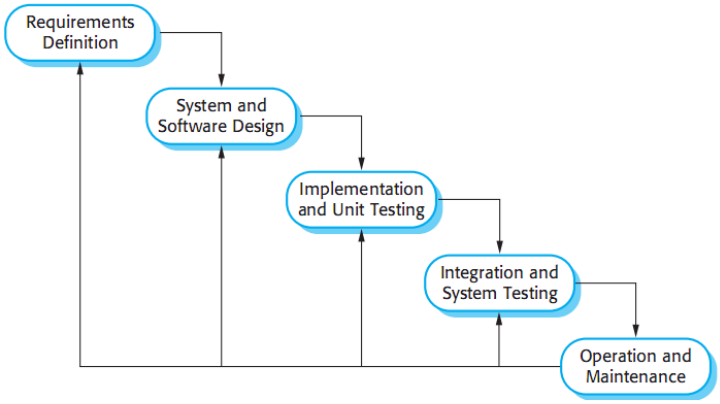
   Implementation merupakan tahap merubah perancangan dan analisis yang dilakukan sebelumnya kedalam kode pemrograman yang digunakan. Tahap ini juga dilakukan *unit testing* untuk mengetahui apakah telah sesuai dengan kebutuhan *system*.

4. *Testing*

   Testing merupakan tahap dimana *system* yang telah dikodekan dilakukan pengujian. Pengujian ini dilakukan untuk mengetahui apakah terdapat kesalahan pada *system* yang telah dikodekan pada tahap *implementation* atau tidak.

5. *Maintenance*

   Maintenance merupakan tahap perawatan jika terjadi kesalahan pada *system*. Perawatan yang dilakukan yaitu mengkoreksi jika terjadi kesalahan, menambah fungsionalitas dan *requirement system*.



Gambar 1.1 Metode Waterfall

1.6 Sistematika Penulisan

Sistematika penulisan proposal penelitian ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini menerangkan secara umum mengenai latar belakang, perumusan masalah, menentukan maksud dan tujuan, batasan masalah, metodologi penelitian serta sistematika penulisan tugas akhir.

BAB II LANDASAN TEORI

Pada bab ini membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan untuk mendukung analisis dan perancangan.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini berisi tentang analisis sistem yang meliputi gambaran umum permasalahan yang dihadapi, ususlan pemecahan tersebut serta kebutuhan dan rancangan sistem yang disusulkan.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Bab ini menjelaskan implementasi dari perangkat lunak yang dibangun. Implementasi perangkat lunak dilakukan berdasarkan kebutuhan analisis dan perancangan perangkat lunak yang sudah dilakukan.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dan saran yang sudah diperoleh dari hasil penulisan tugas akhir.