BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi telekomunikasi yang ada pada saat ini mampu menciptakan berbagai macam perangkat keras yang dapat digunakan untuk mengirim atau menerima informasi dengan cepat dan mudah. Penggunaan *handphone* sebagai *device* akses informasi telah berkembang pesat pada era ini. Terlebih lagi, banyak aplikasi *mobile* yang diciptakan, membuat informasi-informasi yang dibutuhkan mudah untuk didapat. Perangkat keras yang cukup banyak digunakan pada saat ini adalah *smartphone* android. Banyak merk dan jenis *smartphone* android beredar di pasaran. (Mangundap dan Kristiana, 2015)

Android adalah sebuah sistem operasi untuk perangkat *mobile* berbasis linux yang mencakup sistem operasi, *middleware* dan aplikasi. Android menyediakan *platform* terbuka bagi para pengembang untuk menciptakan aplikasi mereka (Haharap, 2014). .Dengan keterbukaan yang di tawarkan oleh sistem operasi android, developer dapat membuat aplikasi yang diinginkan atau dibutuhkan, misalnya membuat aplikasi SMS.

Layanan pesan singkat menggunakan aplikasi SMS pada ponsel masih banyak digunakan, namun bukan jalur yang aman untuk pertukaran informasi. Pesan yang dikirim menggunakan aplikasi SMS bawaan ponsel masih berupa teks terbuka yang belum terproteksi, selain itu proses pengiriman SMS tidak sampai ke penerima secara langsung, akan tetapi pengiriman SMS harus melewati *Short Message Service Center* (SMSC) yang berfungsi mencatat komunikasi yang terjadi antara pengirim dan penerima (Mangundap dan Kristiana, 2015).

Dengan tersimpannya isi pesan di SMSC, seorang operator dapat melihat atau membaca isi pesan. Jika isi pesan tersebut dapat dibaca oleh orang lain, maka pesan yang dikirim tidaklah aman karena isi pesan yang seharusnya bersifat rahasia menjadi dapat di lihat dan di baca oleh orang lain.

Dari masalah di atas, diperlukan suatu algoritma kriptografi yang dapat merahasiakan isi pesan dengan cara mengenkripsi oleh pengirim pesan sebelum di kirim dan di dekripsi oleh penerima pesan melalui aplikasi SMS yang berjalan di sistem operasi android. Jika pesan yang dikirim telah di enkripsi, maka tidak ada yang bisa membaca isi pesan kecuali penerima pesan. Disini penulis akan mengimplementasikan algoritma kriptografi RSA (Rivest Shamir Adleman) untuk proses enkripsi dan dekripsi pesan text.

1.2 Perumusan Masalah

Masala yang akan di selesaikan dalam penelitian ini adalah Bagaimana membuat pesan text yang akan dikirim hanya bisa dibaca oleh penerima pesan yang sudah ditentukan oleh pengirim.

1.3 Batasan Masalah

Mengingat adanya berbagai keterbatasan dan untuk menghindari kompleksitas yang mungkin timbul selama penelitian berlangsung, diberikan batasan-batasan dalam penelitian ini, yakni:

1. Pengirim dan penerima pesan harus menggunakan aplikasi yang sama untuk membaca isi pesan;
2. Hanya bisa digunakan minimal versi *Android Jelly Bean* (4.1–4.3);
3. Menggunakan Editor Andoid Studio sebagai pembuat aplikasi Androidnya.
4. Cuma 64 karakter yang bisa dikirim per 1 sms.
5. Ukuran kunci maksimum yang digunakan pada aplikasi whatmas sebesar 512 bit

1.4 Tujuan Penelitian dan Manfaat Penelitian

Tujuan penulis ialah membuat aplikasi yang dapat mengenkrip isi pesan sebelum di kirim dan mendenkrip setelah diterima dengan metode Algoritma RSA di smartphone. Ada pun manfaat nya ialah agar isi pesan kita tidak dapat dibaca oleh orang lain dengan cara menyadap ataupun di baca dari *SMS Center operator*.

1.5 Metodologi Penelitian

Metode yang digunakan dalam penelitian ini adalah sebagai berikut.

1. Jenis Penelitian

   Jenis penelitian yang digunakan pada penelitian ini adalah penelitian Eksperimen dimana peneliti akan mencoba membuat aplikasi untuk mengirim pesan *text* yang telah di enkripsi dengan algoritma kriptografi RSA berbasis android dengan menggunakan *phonegap* sebagai editornya.

2. Waktu Penelitian

   Dikarenakan adanya keterbatasan waktu maka penelitian akan dilakukan selama 6 bulan.

3. Alat dan Bahan

   Dalam pembuatan sistem ini, alat dan bahan yang akan digunakan yaitu meliputi *hardware*, *software* serta bahan-bahan lain yang menunjang.

   a. Perangkat Keras (*Hardware*)

      Perangkat keras yang akan digunakan adalah laptop dengan spesifikasi sebagai berikut :

      1. *Laptop Asus* X450JNo
      2. *Intel core* i7-4710HQ
      3. *RAM* 8GB
      4. *Hardisk* 1TB

   b. Perangkat Lunak (*Software*)

      Perangkat Lunak yang digunakan dalam pembuatan sistem ini adalah Sistem Operasi *Windows* 10, Eclipse *Indigo*.

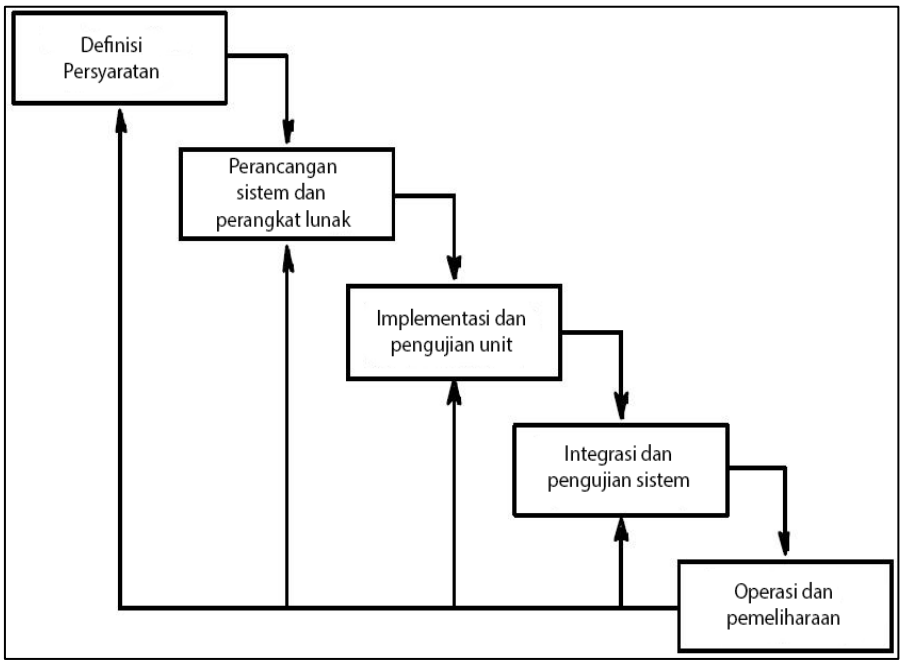
4. Metode Pengumpulan Data

   a. Studi Pustaka

      Mencari teori dan informasi yang berhubungan dengan topik yang akan dibuat. Pencarian teori dan informasi akan di cari melalui buku-buku,internet,dan hasil penelitian maupun karya ilmiah.

5. Metode Pengembangan Sistem

   Metode yang digunakan dalam pengembangan sistem ini menggunakan model air terjun (*waterfall*). Model ini di ilustrasikan pada gambar 1.



Gambar 1.1 Model *Waterfall* (Sommerville, 2003)

Berikut penjelasan mengenai fase-fase tersebut menurut Sommerville (Sommerville, 2003).

a. Analisis dan Definisi Persyaratan

Pelayanan, batasan dan tujuan sistem ditentukan melalui konsultasi dengan *user* sistem. Persyaratan ini kemudian didefinisikan secara rinci dan berfungsi sebagai spesifikasi sistem.

Pada tahapan ini dilakukan dengan mencari tahu apakah sistem ini dibutuhkan sebagai dasar pembuatan sistem ini.

b. Perancangan Sistem dan Perangkat Lunak

Proses perancangan sistem membagi persyaratan dalam sistem perangkat keras atau perangkat lunak. Kegiatan ini menentukan arsitektur sistem secara keseluruhan. Perancangan perangkat lunak melibatkan identifikasi dan deskripsi abstraksi sistem perangkat lunak yang mendasar dan hubungan-hubungannya.

Pada tahapan ini dilakukan dengan melakukan desain rangkaian dari komponen-komponen yang ada sehingga dapat digunakan.

c. Implementasi dan Pengujian Unit

Perancangan perangkat lunak direalisasikan sebagai serangkaian program atau unit program. Pengujian unit melibatkan verifikasi bahwa setiap unit telah memenuhi spesifikasinya

Pada tahapan ini dilakukan dengan merealisasikan desain yang ada menjadi sebuah *prototype* sehingga bisa dijalankan.

d. Integrasi dan Pengujian sistem

Unit program atau program individual diintegrasikan dan diuji sebagai sistem yang lengkap untuk menjamin bahwa persyaratan sistem telah dipenuhi. Setelah pengujian sistem, perangkat lunak dikirim kepada pelanggan.

Pada tahapan ini dilakukan dengan melakukan pengujian *blackbox* dan pengujian *whitebox* terhadap sistem. Setelah dilakukan pengujian, perbaikan akan dilakukan jika diperlukan dan atau ditemukannya *error*.

e. Operasi dan pemeliharaan

Biasanya (walaupun tidak seharusnya), ini merupakan fase siklus hidup yang paling lama. Sistem di *install* dan dipakai. Pemeliharaan mencakup koreksi dari berbagai *error* yang tidak ditemukan pada tahap-tahap terdahulu, perbaikan atas implementasi unit sistem dan pengembangan pelayanan sistem, sementara persyaratan-persyaratan baru ditambahkan.

Pada tahapan ini tidak akan dilakukan karena sistem tidak dilakukan secara langsung pada publik sehingga tidak akan terjadi perubahan dan tidak membutuhkan proses pemeliharaan.

Pemilihan metode *waterfall* dalam pengembangan sistem ini dikarenakan metode ini dirasa cocok yang di dasari oleh berbagai pertimbangan, salah satunya karena metode ini sering dibahas dan digunakan dalam berbagai penelitian dapat dijadikan referensi.

1.6 Sistematika Penulisan

Pembahasan skripsi ini dibagi menjadi lima bab, masing-masing bab terdiri dari sub bab yang disusun secara sistematis. Secara garis besar, isi dari masing-masing bab adalah sebagai berikut.

BAB I PENDAHULUAN

Bab ini berisi latar belakang permasalahan, perumusan masalah, batasan masalah, tujuan dan manfaat penelitian, metodologi penelitian serta sistematika penulisan.

BAB II LANDASAN TEORI

Bab ini berisi penjelasan mengenai landasan teori serta referensi yang dijadikan sarana pendukung oleh penulis dalam mengimplementasikan Algoritma kriptografi RSA untuk keamanan data pesan teks berbasis android.

BAB III ANALISIS DAN PERANCANGAN

Pada bab ini akan dibahas mengenai desain sistem menggunakan *Unifild Modeling Language* (UML), serta rancangan antarmuka sistem yang akan dibangun.

BAB IV IMPLEMENTASI DAN PENGUJIAN

Pada bab ini dibahas mengenai proses pembuatan perangkat lunak, tampilan perangkat lunak yang dibuat, dan hasil pengujian perangkat lunak.

BAB V PENUTUP

Bab ini berisi kesimpulan secara umum serta saran-saran yang dapat digunakan dalam pengembangkan lebih lanjut di masa mendatang