

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Kemajuan dan perkembangan teknologi telekomunikasi yang begitu pesat dan besar manfaatnya terhadap kebutuhan masyarakat luas. Salah satunya yang menjadi kebutuhan utama masyarakat yaitu keamanan pada data. Keamanan pada data merupakan aspek terpenting dari sebuah sistem informasi. Namun kenyataannya masalah keamanan sering kali hal yang dianggap kurang penting atau bahkan sering diabaikan oleh banyak perusahaan-perusahaan besar[1].

Pada dasarnya manusia tidak lepas dari hal yang disebut komunikasi. Salah satunya pada telepon seluler yang berupa pesan singkat atau SMS (*Short Message Service*). Telepon seluler dapat menerjemahkan semua data dalam frekuensi tertentu yang terbuka (di udara) yang sangat rentan akan ancaman seperti penyadapan oleh pihak yang tidak bertanggung jawab[2]. Sebab, SMS merupakan media komunikasi yang bukan point-to-point, tentu pesan yang dikirimkan tidak langsung sampai pada tujuan.

Dalam hal ini penulis mencoba meneliti sebuah komunikasi berupa pesan singkat melalui piranti bergerak atau *mobile* pada *smartphone* berbasis android di PT. Time Excelindo yang merupakan sebuah perusahaan yang bergerak dibidang usaha Penyedia Jasa Layanan Internet (ISP), *Online System*, *Telecommunication*, *Data Communication*, *Software Development* serta pembangunan dan

pemeliharaan jaringan komputer maupun jaringan telekomunikasi. Dalam berkomunikasi atau saling bertukar informasi yang pada saat ini masih bersifat umum untuk penggunaan smartphone atau melalui ponsel, dan apabila mengirimkan sebuah pesan yang bersifat rahasia atau penting menggunakan sebuah aplikasi SMS pada sebuah komputer khusus yang nantinya mampu membroadcast pesan kepada nomor tujuan yang hendak dikirim. Namun dari kedua mode pengiriman pesan ini, informasi yang dikirimkan itu belumlah begitu aman atau pesan yang dienkripsi. Pesan yang dikirimkan masih berbentuk teks biasa.

Oleh karena itu penulis mencoba merancang sebuah aplikasi SMS sederhana dengan penerapan algoritma kriptografi RC6 pada android yang memberikan keamanan dengan enkripsi pada sebuah teks berupa pesan singkat atau SMS. Dan bisa dibaca oleh penerima pesan dengan menggunakan aplikasi dan kunci yang sama untuk membaca pesan tersebut dengan kata lain yaitu dekripsi pada pesan rahasia yang telah dienkripsi oleh pengirim.

1.2 Rumusan Masalah

Untuk mempermudah dalam penyusunan karya tulis dan perancangan sebuah aplikasi SMS berbasis android maka dirumuskan masalah sebagai berikut:

1. Bagaimana cara melakukan penyandian pesan menggunakan eclipse?
2. Bagaimana merancang dan menerapkan algoritma kriptografi RC6 pada aplikasi SMS yang dibuat?

1.3 Batasan Masalah

Batasan masalah pada penelitian ini adalah:

1. Aplikasi SMS ini hanya digunakan untuk enkripsi dan dekripsi pada teks berbasis android dengan menggunakan software Eclipse.
2. Algoritma yang digunakan untuk enkripsi dan dekripsi pada teks berupa pesan singkat adalah algoritma kriptografi RC6.
3. Penggunaan kunci yang sama pada saat proses enkripsi maupun dekripsi.
4. Pembangkit sub kunci algoritma RC6 memiliki maksimal panjang tipe data string 128 bit.
5. Pendistribusian kunci yang digunakan secara manual.

1.4 Tujuan Penelitian

Dalam penelitian ini ada beberapa tujuan yang hendak penulis capai yaitu :

1. Untuk mempermudah dalam penyandian teks pada aplikasi SMS berbasis android yang dibuat dengan software Eclipse.
2. Menciptakan aplikasi keamanan yang sederhana dan efisien pada teks berupa pesan singkat bagi pengguna.

1.5 Manfaat Penelitian

Adapun manfaat yang diperoleh dari penelitian ini adalah :

1. Memberikan keamanan bagi pengguna aplikasi SMS pesan rahasia pada smartphone berbasis android dalam bentuk *chipertext*.
2. Memberikan kemudahan bagi pengguna dalam menyandikan sebuah pesan pada smartphone berbasis android.

1.6 Metodologi Penelitian

Adapun metode penelitian yang digunakan untuk memperoleh informasi tentang perancangan dan permasalahan penelitian ini adalah :

1. Pengumpulan Data

a. Metode Literatur

Metode pengambilan data menggunakan berbagai macam literatur yaitu mencari informasi diberbagai website yang memiliki konten-konten yang berkaitan dengan ilmu kriptografi modern.

b. Metode Kepustakaan

Metode kepustakaan dengan membaca buku-buku literatur, dokumen, catatan kuliah dan bacaan lainnya sebagai referensi yang berhubungan dengan permasalahan.

2. Analisis Sistem

Analisis pada sistem dilakukan untuk mengetahui kebutuhan yang diperlukan oleh sistem. Model analisis yang digunakan penulis adalah SWOT untuk mengetahui kelemahan pada sistem. Sedangkan analisis kebutuhan pada sistem penulis menggunakan analisiskebutuhan fungsional dan non fungsional.

3. Perancangan Aplikasi

Metode yang digunakan untuk mempersiapkan proses atau cara dengan menggambarkan alur dari sebuah sistem dan algoritma kriptografi yang diterapkan dalam aplikasi SMS berbasis android. Dalam hal ini penulis menggunakan perancangan model UML.

4. Pembuatan Program

Metode ini dilakukan untuk implementasi dari hasil perancangan aplikasi. Program dibuat dengan menggunakan bahasa pemrograman java berbasis android pada interface.

5. Metode Testing

Metode testing merupakan suatu cara yang digunakan untuk pengujian aplikasi yang dibuat dengan menggunakan software testing. Pada penelitian ini penulis menggunakan software testing yaitu *Black-box testing*.

1.7 Sistematika Penulisan

Adapun sistematika penulisan dalam penulisan skripsi ini terbagi dalam beberapa pokok bahasan yaitu :

BAB I PENDAHULUAN

Pada bab ini akan diuraikan mengenai latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini mengenai ulasan teori-teori pada tinjauan pustaka yang mendukung judul dan pembahasan penelitian secara rinci baik itu berupa defenisi-defenisi pada permasalahan maupun model yang berkaitan dengan ilmu yang akan diteliti oleh penulis.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini merupakan pembahasan bab yang berkaitan dengan tahapan-tahapan pada proses pembuatan aplikasi pesan rahasia seperti kebutuhan apa saja yang dibutuhkan pada saat pembuatan aplikasi, analisa penerapan algoritma yang digunakan dalam enkripsi SMS, Implementasi antar muka, UML dan lain-lain.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini akan dibahas dan diuraikan secara rinci tentang tahapan-tahapan pada perancangan, cara kerja sistem dan implementasi algoritma RC6 serta pengujian aplikasi pesan rahasia.

BAB V PENUTUP

Pada bab ini berisikan sebuah kesimpulan dari hasil penelitian serta adanya masukan berupa saran-saran dari penulis yang bersangkutan pada pihak yang terkait bahwa perlu adanya suatu pengembangan dari aplikasi yang telah dibuatA