BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

Banyak fitur-fitur aplikasi yang disediakan oleh android sebagai system operasi ponsel. Dari sekian banyak fitur yang dimiliki oleh android, salah satunya yang masih banyak digunakan yaitu SMS. Namun, seringkali pengguna kurang memperhatikan system keamanan data yang ada pada ponsel tersebut khususnya keamanan informasi yang ada di pesan singkat. Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitif yang hanya boleh diketahui oleh pihak yang berhak saja.

Layanan SMS yang menggunakan aplikasi SMS bawaan ponsel bukan merupakan jalur yang aman dalam pertukaran informasi. Pesan yang dikirim menggunakan aplikasi SMS bawaan ponsel masih berupa teks terbuka yang belum terproteksi selain itu pengiriman SMS yang dilakukan tidak sampai secara langsung ke penerima, akan tetapi pengiriman SMS harus melewati *Short Message Service Center* (SMSC) yang berfungsi mencatat komunikasi yang terjadi antara pengirim dan penerima. Dengan tersimpannya SMS pada SMSC, maka seorang operator dan mungkin pihak lain yang tidak berhak mengetahui informasi tersebut dapat memperoleh informasi atau membaca SMS di dalam SMSC.

Untuk mengurangi resiko yang ditimbulkan dari celah-celah yang terdapat pada layanan SMS tersebut salah satu cara penanggulangannya adalah dengan menerapkan suatu algoritma kriptografi pada pesan yang dikirmkan. Dengan terenkripsinya pesan yang dikirim maka seseorang yang berhasil mencuri informasi pesan teks yang dikirim tersebut akan kesulitan untuk mengetahui isi dari pesan tersebut. Dengan majunya kemajuan teknologi telepon selular, di mana banyaknya bermunculan telepon selular yang memiliki memori yang cukup besar,

memungkinkan untuk melakukan implementasi enkripsi pada SMS menjadi memungkinkan.

Data-data yang dikirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Enkripsi adalah proses yang dilakukan untuk mengamankan sebuah data (*plaintext*) menjadi data yang tersembunyi (*ciphertext*). *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah. Menurut ISO 7498-2, terminologi yang lebih tepat digunakan untuk megistilahkan enkripsi adalah *"enchiper"*, sedangkan untuk dekripsi adalah *"dechiper"*.

Salah satu metode enkripsi yang dapat digunakan untuk aplikasi mobile adalah RC6 (Rivest Code 6). RC 6 merupakan pengembangan daridari algpritma sebelumnya yaitu RC5. Algoritma RC6 dilengkapi dengan beberapa parameter, sehingga dituliskan sebagai RC6-w/r/b. Parameter w merupakan ukuran kata dalam satuan bit, parameter merupakan bilangan bukan negatif yang menunjukan banyaknya iterasi selama proses enkripsi dan parameter b menunjukan ukuran kunci enkripsi dalam byte.

RC 6 dianggap cocok digunakan untuk aplikasi berbasis mobile karena selain sangat sederhana RC 6 juga mudah untuk diimplementasikan pada ponsel berbasis android, karena algoritma ini hanya membutuhkan *memory* yang kecil.

Berdasarkan pada uraian latar belakang tersebut peneliti tertarik untuk membangun aplikasi pada ponsel berbasis android untuk mengamankan data pesan singkat. Penelitian yang akan dilakukan mengambil judul **"RANCANG BANGUN APLIKASI ENKRIPSI DAN DEKRIPSI DENGAN MENGGUNAKAN ALGORITMA KRIPTOGRAFI RC-6 PADA PLATFORM ANDROID".**

.

1.2 Perumusan Masalah

Berdasarkan permasalahan yang telah diuraikan di latar belakang, maka pokok permasalahan yang akan dikaji dalam penelitian ini adalah :

> Bagaimana membangun aplikasi enskripsi dan dekripsi SMS dengan menggunakana algoritma Kriptografi RC6 pada ponsel berbasis android.

1.3 Maksud dan Tujuan

Secara umum, penelitian ini dimaksudkan untuk membangun aplikasi enskripsi dan dekripsi SMS dengan menggunakana algoritma Kriptografi RC6 pada ponsel berbasis android. Dengan demikian, penelitian ini bertujuan untuk:

> Meningkatkan keamanan pesan yang terkirim,agar tidak mudah diketahui oleh pihak yang tidak berkepentingan.

1.4 Batasan Masalah

Dalam penulisan tugas akhir ini penulis akan membatasi masalah pada beberapa hal berikut ini :

1. Metoda Kriptografi yang digunakan yaitu Algoritma Kriptografi RC-6 simetris.
2. Informasi yang akan di enkripsi hanya pesan singkat pada ponsel yang berbasis android
3. Implementasi metode enkripsi dan dekripsi hanya dilakukan pada aplikasi SMS.
4. Aplikasi yang dibangun tidak menangani pengiriman kunci enkripsi ataupun
   dekripsi .
5. Aplikasi ini berjalan minimal meggunakan OS android Versi 2.3 (Gingerbread).
6. Perangkat lunak yang digunakan yaitu *eclipse* dan *framework* Android SDK.

1.5 Metodologi Penelitian

1.5.1 Metodologi penelitian yang digunakan.

a. Studi Literatur

Studi yang bisa dijadikan sebagai bahan untuk mengumpulkan dan mengkaji data dengan membaca berbagai literatur yang ada kaitannya dengan masalah yang akan dibahas seperti buku, skripsi, jurnal maupun bentuk tulisan lainnya yang isinya berkaitan erat dengan masalah yang akan diteliti sebagai bahan referensi tertulis.

b. Eksperimen

Eksperimen dilakukan dengan cara melakukan perancangan, implementasi sistem untuk membuat gambaran yang jelas dari masalah yang dihadapi dengan pembuatan simulasi program aplikasi, selain itu dilakukan uji coba dan analisis implementasi yang dibuat.

1.5.2 Metode Pembangunan Perangkat Lunak

Metode pengembangan perangkat lunak yang digunakan untuk membangun aplikasi e-learning untuk pemrograman berorientasi objek ini menggunakan paradigma model waterfall (Ian Sommerville, 2010), yang meliputi beberapa proses diantaranya:

1. *Requirements analysis and definition*

   Tahap ini mengumpulkan kebutuhan secara lengkap kemudian dianalisis dan didefinisikan kebutuhan yang harus dipenuhi oleh program yang akan dibangun. Tahap ini harus dikerjakan secara lengkap untuk bisa menghasilkan desain yang lengkap.

2. *System and software design*

   Tahap ini merupakan kegiatan mengumpulkan kebutuhan secara lengkap kemudian dianalisis dan didefinisikan kebutuhan yang harus dipenuhi oleh aplikasi yang akan dibangun. Tahap ini

harus dikerjakan secara lengkap untuk bisa menghasilkan desain yang lengkap.

3. *Implementation and unit testing*

   Desain program diterjemahkan ke dalam kode-kode dengan menggunakan bahasa pemrograman yang sudah ditentukan. Program yang dibangun langsung diuji baik secara unit.

4. *Integration and system testing*

   Penyatuan unit-unit program kemudian diuji secara keseluruhan (system testing).

5. *Operation and maintenance*

   Mengoperasikan program dilingkungannya dan melakukan pemeliharaan, seperti penyesuaian atau perubahan karena adaptasi dengan situasi sebenarnya.

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini bertujuan untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan ini diatur dalam lima bab, yaitu :

BAB 1 PENDAHULUAN

Bab ini menguraikan secara umum tentang latar belakang masalah, identifikasi masalah, maksud dan tujuan, batasan masalah, yang kemudian diikuti dengan metodologi yang digunakan, serta sistematika penulisan penelitian sebagai ringkasan materi dari masing-masing bab.

BAB 2 TINJAUAN PUSTAKA

Membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan serta tinjauan terhadap hasil penelitian tentang keamanan pesan singkat pada ponsel.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Bab ini akan menjelaskan mengenai analisa dan perancangan simulasi, pemilihan *software* yang digunakan, dan analisis perhitungan algoritma kriptografi simetris. serta model matematis untuk analisisnya.

BAB 4 IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini merupakan tahapan percobaan dan sekaligus pengujian terhadap program yang dibuat yang diimplementasikan pada ponsel yang berbasis Android

BAB 5 KESIMPULAN DAN SARAN

Pada bab ini akan dibahas mengenai kesimpulan dari keseluruhan masalah yang telah dibahas pada bab sebelumnya dan dilengkapi dengan saran-saran yang dapat dijadikan masukan untuk kemudian dapat dikembangkan dan disempurnakan pada perangkat lunak ini.