BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Fenomena menarik dari perkembangan dunia seluler saat ini adalah munculnya aplikasi-aplikasi baru dengan berbagai *platform* untuk mendukung pertumbuhan tingkat penggunaan telepon seluler atau ponsel di seluruh dunia. Dalam dunia teknologi *content* seluler ada beberapa *platform* yang menjadi dasar berdirinya teknologi tersebut, satu di antaranya yaitu Java. Java pada awal pertumbuhannya dibuat untuk memenuhi standar teknologi yang diakui oleh semua vendor di seluruh dunia. Java dikenal sebagai *platform* yang memiliki kebebasan *platform*. Edisi khusus dari Java untuk ponsel dinamakan dengan J2ME atau Java 2 Micro Edition yang sangat berguna untuk membangun sebuah aplikasi pada peralatan dengan kapasitas penyimpan dan kemampuan *user interface* yang terbatas seperti pada perangkat komunikasi bergerak (*mobile device*) berupa ponsel, PDA, dan sebagainya. Untuk ponsel, J2ME menyediakan profil khusus yang dinamakan dengan *Mobile Interface Device Profile* (MIDP) yang saat ini telah muncul dua versi yaitu 1.0 dan 2.0. MIDP seri 2.0 merupakan pengembangan dari seri pendahulunya. MIDP 2.0 menyediakan lebih banyak fitur khususnya dalam hal aplikasi *game* serta kemampuan untuk berinteraksi dengan dunia luar melalui teknologi-teknologi seluler saat ini seperti Bluetooth, MMS (*Multimedia Message Service*), SMS (*Short Message Service*), Video Streaming dan sebagainya.

Ponsel yang mendukung profil MIDP 2.0 dari berbagai vendor saat ini telah banyak beredar di Indonesia. Selain sebagai alat untuk berkomunikasi suara, ponsel juga menjadi alat untuk komunikasi data, baik untuk bisnis atau hiburan seperti mengirim business card melalui media transmisi SMS, infrared, Bluetooth, atau email. Jika untuk bisnis, penggunaan data bisa ditafsirkan sebagai budaya yang maju, yang lebih mementingkan akurasi, bukan dugaan atau kira-kira. Sebab data yang dikomunikasikan tidak berubah ketika mulai dikirim sampai dengan diterima oleh ponsel lain. Namun dari komunikasi data yang menggunakan media transmisi SMS terdapat hal penting yang harus diperhatikan yaitu masalah kerahasiaan informasi.

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama informasi sensitif yang hanya boleh diketahui oleh pihak yang berhak saja. Informasi yang merupakan hasil pengolahan dari data, mempunyai nilai yang berbeda bagi setiap orang. Seringkali sebuah informasi menjadi sangat berharga dan tidak semua orang diperkenankan untuk mengetahuinya. Namun selalu saja ada pihak yang berusaha untuk mengetahui informasi dengan cara-cara yang tidak semestinya bahkan bermaksud untuk merusaknya.

Berdasarkan hal di atas, perlu ada suatu pengamanan informasi pada saat pengiriman dan penerimaan informasi. Dilihat dari fitur yang dimiliki ponsel J2ME profil MIDP 2.0, maka masalah tersebut dapat dipecahkan dengan memberikan suatu sistem keamanan pada media transmisi SMS. Untuk melakukan ini ada suatu cara yang biasa disebut penyandian data. Dalam

penelitian ini penulis akan mencoba mengimplementasikan suatu cabang ilmu matematika yang disebut dengan kriptografi. Dengan kriptografi, data dapat diubah menjadi sandi-sandi yang tidak dimengerti serta mengembalikannya kembali ke semula, proses ini disebut Enkripsi dan Dekripsi data. Ada beberapa algoritma enkripsi yang sudah terbuka untuk dipelajari, seperti DES, AES, TwoFish, Blowfish, RC2, RC4, RC5. Penelitian ini membahas implementasi algoritma enkripsi RC2 (*Rivest Code 2*) pada ponsel J2ME profil MIDP 2.0 untuk mengamankan data SMS.

Berdasarkan uraian di atas maka penulis mengambil judul skripsi **Perancangan dan Implementasi Algoritma Enkripsi RC2 Guna Mengamankan Pesan SMS pada Ponsel J2ME Profil MIDP 2.0**.

1.2 Identifikasi Masalah

Berdasarkan uraian latar belakang di atas, penulis mengidentifikasi beberapa hal yang berhubungan dengan masalah komunikasi data menggunakan media transmisi SMS di antara dua ponsel J2ME profil MIDP 2.0, yaitu:

1. Rentannya keamanan data pada media transmisi SMS.
2. Adanya penyusup yang tidak diinginkan yang akan membuka isi dari pesan singkat yang ada pada ponsel.
3. Isi pesan singkat pada ponsel bisa jadi merupakan suatu informasi yang sangat penting dan berharga, sehingga informasi tersebut tidak boleh jatuh kepada orang yang tidak berhak memakainya.

1.3 Batasan Masalah

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

1. Algoritma enkripsi yang digunakan adalah *RC2 (Rivest Code 2)*.
2. Informasi yang akan dienkripsi hanya pesan singkat (SMS) pada ponsel dengan ukuran pesan maksimal adalah dua pesan SMS.
3. Panjang kunci maksimal yang digunakan 128 bit atau 16 karakter.
4. Software developer untuk implementasi dan pengujian adalah Sony Ericsson Java MIDP SDK Release 2.2.
5. Ponsel untuk implementasi dan pengujian adalah ponsel dengan dukungan teknologi J2ME profile MIDP 2.0.

1.4 Maksud dan Tujuan

Maksud dari penulisan Tugas Akhir ini adalah untuk merancang dan mengimplementasikan aplikasi algoritma enkripsi RC2 pada ponsel berbasis J2ME profil MIDP 2.0.

Tujuan dari penulisan Tugas Akhir ini adalah untuk mengamankan isi pesan SMS pada ponsel J2ME profil MIDP 2.0 sehingga kerahasiaan informasinya terjaga.

1.5 Metodologi Penelitian

Metodologi penelitian merupakan tahapan-tahapan yang dilalui dalam sebuah penelitian, mulai dari perumusan masalah, perancangan, analisis,

implementasi, sampai dengan penarikan kesimpulan yang membentuk sebuah alur yang sistematis. Metodologi penelitian ini digunakan sebagai pedoman peneliti dalam pelaksanaan penelitian agar hasil yang dicapai tidak menyimpang dari tujuan yang sudah ditetapkan.

1.5.1 Metode Penelitian

1. Studi Pustaka

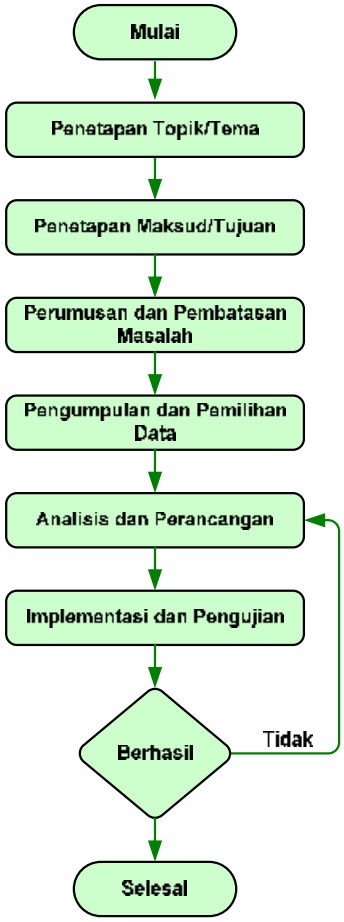
   Studi yang bisa dijadikan sebagai bahan untuk mengumpulkan dan mengkaji data dengan membaca berbagai literatur seperti buku, skripsi, jurnal maupun bentuk tulisan lainnya yang isinya berkaitan erat dengan masalah yang akan diteliti sebagai bahan referensi tertulis.

2. 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 Diagram Alir Penelitian

Untuk memberikan panduan dalam melaksanakan proses penelitian serta memberikan gambaran secara umum, maka penulis membuat suatu diagram alir penelitian, seperti pada gambar 1.1.



Gambar 1.1 Diagram alir penelitian

1.6 Tempat dan Waktu Penelitian

Tempat dan waktu penelitian dilakukan di Jurusan Teknik Informatika UNIKOM, dimulai dari bulan Oktober 2005 sampai dengan bulan Januari 2006.

1.7 Sistematika Penulisan

Sistematika penulisan yang digunakan dalam menyusun skripsi ini, adalah sebagai berikut:

BAB I. PENDAHULUAN

Bab ini memuat uraian-uraian tentang latar belakang, perumusan masalah, batasan masalah yang akan dibahas, maksud dan tujuan penelitian, langkah-langkah metodologi penelitian dan sistematika penulisan.

BAB II. TINJAUAN PUSTAKA

Bab ini akan mengulas masalah keamanan data, pengertian kriptografi, kelompok enkripsi, mekanisme kriptografi, keamanan sistem kriptografi, sekilas tentang Java, dan software developer MIDP yang digunakan.

BAB III. ANALISA DAN PERANCANGAN SISTEM

Bab ini berisi model perancangan perangkat lunak, analisa kebutuhan sistem, perancangan sistem, perancangan antarmuka perangkat lunak, algoritma enkripsi RC2 dan analisa perhitungannya.

BAB IV. IMPLEMENTASI DAN PENGUJIAN

Bab ini berisi tentang implementasi desain sistem dan pengujian dari program yang dibuat berdasarkan kriteria pengujian panjang kunci yang dilakukan pada emulator Sony Ericsson Java MIDP SDK Release 2.2 dan perangkat keras berupa ponsel Sony Ericsson K300i.

BAB V. KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dan saran-saran yang dapat memberikan masukan bagi pembaca dan merupakan penutup dari tugas akhir ini.