BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Salah satu perkembangan teknologi informasi yang paling mutakhir adalah penggunaan teknologi nirkabel (*wireless*) untuk menyajikan informasi. Telepon selular (ponsel) banyak digunakan sebagai media yang tidak hanya sebagai pengirim atau penerima data suara tetapi juga berupa text atau gambar. Salah satu fasilitas yang paling penting dan mudah digunakan yaitu pengiriman data berupa text atau pesan yang dikenal dengan nama SMS.

Pengiriman SMS biasanya digunakan sebagai pertukaran data yang rahasia seperti nomor akun bank, *password*, dan lain-lain. Ketidaksengajaan pengiriman pesan seperti ini ke nomor tujuan yang salah dapat menjadi suatu masalah apabila dibaca oleh penerima yang tidak bertanggung jawab. Umumnya setiap operator selular menyandikan semua data komunikasi selular, termasuk pesan SMS. Tetapi kadang kala, meskipun telah disandikan data masih dapat dibaca oleh operator. Hal inilah yang mendasari pengembangan aplikasi tambahan untuk dapat menyandikan SMS yang akan dikirimkan, jadi hanya orang-orang tertentu saja yang dapat membacanya.

Tujuan dari pembuatan Tugas Akhir ini adalah mengembangkan sebuah aplikasi yang dapat digunakan pada ponsel untuk mengenkripsi pesan yang akan dikirim. Pendekripsian pesan yang telah dienkripsi juga termasuk didalam aplikasi ini. Enkripsi dan dekripsi disandikan dengan sebuat kunci rahasia. Teknik pengenkripsian berdasarkan pada ECC (*Elliptic Curve Cryptography*) yang disebutkan sebagai generasi selanjutnya dari kriptografi kunci publik.

Penggunaan ECC merupakan solusi terkini dalam pengenkripsian pada perangkat kecil atau *embedded system* seperti telepon selular. Pengenkripsian dengan menggunakan elliptic curve memungkinkan performansi yang terbaik dan hanya membutuhkan sedikit kapasitas memori. Dalam tugas akhir ini akan

dibandingkan hasil yang didapat dari percobaan yang diterapkan pada *emulator* dan pada *device* yang sebenarnya.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas maka dirancang suatu perangkat lunak yang mencakup permasalahan-permasalahan berikut:

1. Bagaimana membuat suatu aplikasi enkripsi data SMS menggunakan kriptografi *Elliptic Curve* yang dapat digunakan pada ponsel yang mendukung teknologi java.
2. Bagaimana performansi dalam pengenkripsian dan pendekripsian data sms yang didapat dari hasil pengujian.

1.3 Batasan Masalah

Dalam perancangan perangkat lunak pada tugas akhir ini perlu ditentukan batasan atau ruang lingkup dari permasalahan yang akan dipecahkan. Adapun batasan masalahnya adalah sebagai berikut:

1. Aplikasi ini menggunakan teknologi J2ME, sehingga aplikasi ini dapat digunakan pada perangkat telepon seluler dengan dukungan MIDP 2.0.
2. Aplikasi ini diaplikasikan pada *emulator Java Wireless Toolkit* 2.2 dan sebuah perangkat telepon selular.
3. Algoritma yang dipakai dalam aplikasi ini menerapkan ECC berdasar skema Diffie-Hellman.
4. Banyak karakter text maksimal yang dapat dienkripsi 200 karakter karena keterbatasan perangkat.
5. Tidak membahas algoritma kriptografi yang lain.
6. Tidak membahas proses pengiriman dan penerimaan SMS yang terjadi diluar aplikasi ini.

1.4 Tujuan Tugas Akhir

Tujuan dari tugas akhir ini adalah:

1. Membuat suatu aplikasi pengiriman SMS pada ponsel, menerima maupun mengirim pesan dalam bentuk text terenkripsi dengan aman.
2. Mengukur dan menganalisis performansi dari aplikasi ini.

1.5 Metode Penelitian

Metodologi yang digunakan dalam penyelesaian tugas akhir ini adalah :

1. Studi literatur, dengan mempelajari bahan-bahan materi yang mendukung.
2. Analisis dan perancangan perangkat lunak.
3. Pembuatan perangkat lunak.
4. Pengujian perangkat lunak dan menganalisanya.
5. Pengambilan kesimpulan dan penyusunan laporan.

1.6 Sistematika Penulisan

Adapun sistematika yang digunakan untuk penulisan laporan hasil penelitian tugas akhir ini adalah sebagai berikut :

BAB I Pendahuluan

Pada bab ini membahas mengenai : latar belakang masalah, perumusan masalah dan batasan masalah, tujuan, metodologi penelitian, serta sistematika penulisan dari kegiatan penelitian tugas akhir ini.

BAB II Landasan Teori

Pada bab ini dibahas mengenai teori dasar yang berhubungan dengan aplikasi yang dibangun.

BAB III Analisa dan Perancangan Sistem

Bab ini berisi analisa terhadap seluruh sistem yang dibuat untuk menentukan kebutuhan apa saja yang harus dipenuhi dan pengembangannya disesuaikan dengan keterbatasan yang dimiliki oleh sumber daya telepon selular.

BAB IV Implementasi dan Analisa Hasil Sistem

Pada bab ini dibahas tentang implementasi dan pengujian terhadap aplikasi yang dikembangkan, serta analisa aplikasi.

BAB V Kesimpulan dan Saran

Pada bab ini berisi kesimpulan dan saran dari seluruh kegiatan penelitian tugas akhir ini yang bisa digunakan sebagai masukan untuk pengembangan lebih lanjut.