KRIPTOGRAFI SMS PADA APLIKASI JAVA DENGAN MENGGUNAKAN ECC

Wahyu Widagdo Purnomo[1], Rendy Munadi [2], Yudha Purwanto[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Teknologi telepon selular saat ini sebagai alat komunikasi bergerak yang tidak dapat dipisahkan dari kehidupan sehari-hari karena memberikan banyak kemudahan bagi penggunanya. Setiap informasi, baik berupa text, suara, maupun gambar, dapat dikirimkan atau diterima melalui telepon selular. Salah satu fasilitas yang paling penting dan mudah digunakan yaitu pengiriman data berupa text atau pesan yang dikenal dengan nama SMS.

SMS (Short Message Service) adalah layanan yang digunakan secara luas sebagai salah satu alat komunikasi. Umumnya data yang dikirim menggunakan layanan SMS kerahasiaannya masih bersifat terbuka. Artinya seseorang dengan privilege dan kemampuan yang cukup, dapat dengan mudah membaca informasi yang kita kirimkan.

SMS (Short Message Service) adalah layanan yang digunakan secara luas sebagai salah satu alat komunikasi. Umumnya data yang dikirim menggunakan layanan SMS kerahasiaannya masih bersifat terbuka. Artinya seseorang dengan privilege dan kemampuan yang cukup, dapat dengan mudah membaca informasi yang kita kirimkan.

Dalam Tugas Akhir ini, diimplementasikan suatu aplikasi pengenkripsian data SMS dengan menggunakan ECC (Elliptic Curve Cryptography) yang ditulis dengan dalam bahasa Java. Aplikasi ini berfungsi mengirim dan menerima sms dan kunci publik yang terenkripsi.

Telepon selular yang berbasis Java merupakan dasar yang sesuai dalam pembuatan aplikasi ini karena semua ponsel sekarang sudah mendukung teknologi ini. Teknologi Java juga mendukung fasilitas keamanan tambahan misalnya dengan cara melakukan enkripsi terhadap pesan yang akan dikirimkan sehingga dapat diperoleh suatu aplikasi pengiriman pesan terenkripsi yang cepat, aman, dan mudah untuk digunakan.

Kata Kunci : ECC, J2ME, SMS, Asymmetric, Kriptografi, Kunci publik

Abstract

Phone cellular technology in this time as a means of inseparable mobile communications of daily life because giving many amenity to its consumer. Each information, as text, voice, and also picture, can be delivered or received to a cellular phone. One of the easiest and useful service used these day is delivery of data in the form of message or plain text known as SMS.

Phone cellular technology in this time as a means of inseparable mobile communications of daily life because giving many amenity to its consumer. Each information, as text, voice, and also picture, can be delivered or received to a cellular phone. One of the easiest and useful service used these day is delivery of data in the form of message or plain text known as SMS.

Cellular phone based on Java represent appropriate base in making of this application because all cellular phone now have supported this technology. Java technology also supports addition security facility for example by doing message encryption before delivered so that can be obtained encrypted message delivery application which fast, secure, and ease to be used.

Keywords : ECC, J2ME, SMS, Asymmetric, Cryptography, Public key

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.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Beberapa kesimpulan yang dapat diambil dari pembangunan Aplikasi Kriptografi SMS ini adalah:

1. Sistem dapat berjalan dengan baik di emulator maupun di perangkat teleponseluler dan dapat melakukan pengenkripsian dan pendekripsian data SMS.
2. Jumlah karakter yang diketik berdampak pada biaya yang akan dikeluarkan. Hal ini dikarenakan jumlah karakter SMS normal maksimum 160 karakter untuk satu *fragment* SMS. Jika SMS yang diketikkan dan setelah dienkripsi menjadi lebih besar dari 160 karakter, maka akan dikenakan biaya sebanyak *fragment* SMS tersebut. Agar *user* dapat memakai genap satu *fragment* SMS maka *user* harus mengetikkan karakter sejumlah maksimal 80 karakter. Hal ini menyebabkan pemakaian aplikasi ini menjadi terbatas.
3. Penggunaan memori penyimpanan pada telepon seluler memang harus seefektif mungkin. Spesifikasi pada ponsel sangatlah terbatas. Untuk menghemat penggunaan memori, sebelum kelas-kelas java aplikasi ini di *package*, terlebih dahulu dilakukan *obfuscating* agar kelas-kelas java yang tidak dipakai dalam aplikasi ini tidak diikutkan dalam *package*. Besar file hasil *packaging* sebesar 118 KB.
4. Waktu enkripsi dan dekripsi antara PC dan ponsel berbeda jauh. Hal ini dikarenakan perangkat PC lebih memakan *resource* yang memang untuk *development* aplikasi java membutuhkan *resource* yang banyak. Sehingga waktu proses yang dihasilkan tidak normal.

5.2 Saran

Saran dan pengembangan untuk penelitian yang akan datang:

1. Adanya perbandingan dengan metode kriptografi yang lain sehingga dapat dibandingkan performansi antara metode yang satu dengan yang lain.
2. Diperlukan suatu teknik kompresi data sebelum dikirimkan ke penerima untuk menghemat biaya yang dikeluarkan.
3. *User Interface* dapat diujikan pada telepon seluler yang berbeda sehingga dapat diketahui hasilnya pada beberapa telepon seluler yang lain.
4. Pengembangan lebih lanjut dengan fungsi yang sama pada format media yang berbeda, misal: MMS.

DAFTAR PUSTAKA

Bouncy Castle. Bouncy castle crypto package. http://www.bouncycastle.org. Light-weight API, release 1.35.

Forum-Nokia. September 2003. A brief introduction to secure sms messaging in midp. Appendix B.

Brute Force Attack on cryptographic key. http://www.cl.cam.ac.uk/~rnc1/brute.html

Hankerson, Darrel, Alfred Menezes, Scott Vanstone. 2004. Guide to Elliptic Curve Cryptography. Springer Verlag, Inc. New York.

Hartanto, Antonius Aditya. 2004. Pemrograman Mobile Java dengan MIDP 2.0. ANDI OFFSET, Yogyakarta.

Solution, Network Security. 2006. SMS Vulnerabilities and XMS Technology White Paper. http://www.mynetsec.com.

White, James, David Hemphill. 2002. Java 2 Micro Edition: Java in a Small Thing. Manning Publication Co.

Wicaksono, Ady. 2002. Pemrograman Aplikasi Wireless dengan Java. PT Elexmedia Komputindo, Jakarta.