# Implementasi kriptografi kurva eliptik pada pengiriman SMS melalui telepon selular dengan teknologi J2ME

Yusri, author



---

Abstrak

Tugas akhir ini bertujuan untuk mengimplementasikan kriptografi kurva eliptik pada pengiriman SMS melalui telepon selular agar kerahasiaan dan integritas SMS terjaga. Tugas akhir ini menelaah kurva eliptik, metode dasar enkripsi-dekripsi kriptografi kurva eliptik, dan mengimplementasikan sistem kriptografi kurva eliptik pada pengiriman SMS melalui telepon selular dengan menggunakan teknologi J2ME dari Sun Microsystem. Sebuah SMS yang terenkripsi memiliki tingkat kerahasiaan yang tinggi karena selama perjalanan, SMS berada dalam bentuk ciphertext yang tidak dapat dibuka dan dibaca oleh pihak-pihak lain. SMS tersebut juga memiliki integritas data yang cukup tinggi karena perubahan kecil pada sebuah ciphertext dapat terdeteksi dengan mudah. Pengujian dilakukan pada komputer dengan prosesor AMD Duron 800 dan SDRAM 320 MB. Sistem operasi yang digunakan adalah Microsoft Windows XP dan MIDlet dijalankan pada perangkat emulator DefaultColorPhone yang disediakan di J2ME WTK versi 2.0 dari Sun Microsystem. Emulator mengemulasikan prosesor telepon selular dengan kecepatan 4000 bytecodes/millisekon. Parameter-parameter domain yang digunakan adalah secp128r1 dari Certicom. Hasil pengujian menunjukkan rata-rata waktu yang digunakan untuk melakukan enkripsi adalah sekitar 10 detik untuk setiap 15 karakter. Rata-rata waktu yang dibutuhkan untuk melakukan dekripsi adalah setengah dari waktu enkripsi yaitu sekitar 5 detik untuk setiap 15 karakter.