Abstrak

Perkembangan teknologi informasi yang semakin cepat membuat kebutuhan akan informasi semakin penting. Hal inilah yang mengilhami suatu bank untuk mengimplementasikan suatu layanan transaksi yang sering disebut dengan sms-banking. Namun, sms-banking yang diimplementasikan saat ini tidak menjamin data keamanan para nasabahnya. Ancaman keamanan tersebut meliputi pihak ketiga yang ingin menyadap transkasi antara nasabah dengan bank. Salah satu cara mengatasi celah keamanan tersebut adalah dengan mengimplementasikan suatu algoritma kriptografi. Metode yang digunakan adalah ECDSA untuk tanda tangan digital dan suatu algoritma ECC yaitu ECIES untuk enkripsi pesan. ECDSA dan ECIES merupakan salah satu algoritma kunci publik yang berbasis kurva elips. Aplikasi ini akan diimplementasikan pada bahasa pemrograman java yang terdiri dari klien yang menggunakan J2ME dan server yang menggunakan J2EE.

Tugas akhir ini akan menganalisis parameter waktu performansi dari tiap domain parameter yang direkomendasikan NIST, parameter keamanan, dan parameter kriptografi(autentikasi,non repudiasi,integritas, dan *confidentiality*). Berdasarkan hasil penelitian didapatkan kesimpulan bahwa Perpaduan algoritma ECDSA dan ECIES dapat menjamin terpenuhinya semua aspek keamanan kriptografi yaitu aspek autentikasi,non repudiasi, integritas data dan *confidentiality*. Dalam penelitian ini juga didapatkan bahwa *domain parameter* yang paling cocok diterapkan pada telepon seluler adalah NIST 163.

Kata Kunci : ECDSA,ECIES, domain parameter, enkripsi, tanda tangan digital