Universitas Indonesia Library >> UI - Skripsi Membership

Analisa dan perbandingan unjuk kerja algoritma enkripsi asimetrik antara RSA dan ECC pada aplikasi komunikasi data real-time

Adhitya P., author

Deskripsi Lengkap: https://lib.ui.ac.id/detail?id=20242446&lokasi=lokal

---

Abstrak

Semakin meningkamya kemampuan komputasi dari prosesor sebuah komputer pada saat ini, membuat pemecahan kunci publik dari suatu algoritma enkripsi asimetrik semakin mudah. Akibatnya data yang beredar dalam jaringan komputer memerlukan enkripsi yang lebih baik Iagi. Agar kunci publik sulit untuk dipecahkan, salah satu caranya adalah dengan memperbesar jumlah bit yang digunakan untuk enkripsi (misalnya, RSA 1024 bit). Akan tetapi, cara ini menjadi tidak efektif apabila diterapkan pada sistem yang memiliki kapasitas memori yang kecil seperti Smart Card.

Algoritma Elliptic Curve C13/Cryptography (ECC) dikembangkan untuk mengatasi masalah di atas. Secara teori, ECC 160 bit memiliki tingkat keamanan yang sama dengan RSA 1024 bit. Akan tetapi, ECC masih menghadapi kendala dalam standarisasi.

Skripsi ini dibuat dengan tujuan untuk membuktikan teori tasebut di atas. Pembuktian dilakukan dengan membandingkan ketepatan proses enkripsi-dekripsi pada komunikasi data real-time dan waktu yang dibutuhkan untuk memecahkan kunci publik antara RSA dan ECC. Deugan asumsi bahwa semakin lama waktu yang dibutuhkan umuk memecahkan kunci publik maka tingkat keamanan kunci tersebut makin tinggi, dari uji coba yang dilakukan diperoleh hasil sebagai berikut:
Ukuran kunci publik 96 bit:
RSA = 0.22 detik
ECC = 1.08 detik
Ukuran kuuci public 112 bit:
RSA = 1.12 detik
ECC = 14.59 detik