ABSTRAK

ANALISIS PERBANDINGAN KOMPLEKSITAS WAKTU ALGORITMA KRIPTOGRAFI ASIMETRIS (RSA, ECC, DAN ELGAMAL) DALAM PROSES ENKRIPSI, DEKRIPSI, DAN TANDATANGAN DIGITAL

Oleh
Melinda Utami
17102133

Perkembangan digitalisasi yang terjadi saat ini membuat adanya pergeseran perilaku masyarakat dalam melakukan kegiatan sehari-hari menjadi *online* atau digital. Semakin banyaknya kegiatan yang dilakukan secara *online*, maka semakin banyak pula data yang diunggah dan ditransmisikan melalui internet. Hal ini dapat menyebabkan timbulnya kejahatan digital seperti peretasan, pencurian data, penggunaan data pribadi secara ilegal, dan lain-lain. Untuk menghindari berbagai jenis kejahatan digital, solusi yang dapat digunakan adalah dengan mengimplementasikan sistem keamanan menggunakan kriptografi. Penelitian membandingkan waktu enkripsi, dekripsi data dan tandatangan digital serta nilai kompleksitas waktu pada algoritma kriptografi asimetris RSA, ECC, dan ElGamal. Parameter yang digunakan dalam penelitian ini adalah waktu pembangkitan kunci, waktu enkripsi, waktu dekripsi, waktu pembangkitan kunci untuk tandatangan digital, serta waktu pembuatan tandatangan digital. Sistem yang digunakan dalam penelitian dibangun menggunakan Bahasa C++ dengan library NTL *(Number Theory Library)*. Data yang diperoleh berupa data waktu yang selanjutnya dibandingkan dari setiap algoritma. Nilai kompleksitas waktu diperoleh dari penjumlahan kompleksitas setiap langkah yang terdapat dalam *pseudocode* dari setiap algoritma. Hasil perbandingan waktu menunjukan bahwa algoritma RSA lebih baik dari algoritma ECC dan Elgamal dalam waktu enkripsi, dekripsi, dan tandatangan digital serta memiliki pertumbuhan waktu yang konstan dan tidak mengalami kenaikan yang terlalu besar. Algoritma RSA memiliki nilai kompleksitas tertinggi dengan nilai $O(n \log n^2)$ yang menunjukan bahwa pertumbuhan waktu bernilai lanjar dikali logaritmik. Nilai kompleksitas terendah adalah ElGamal dengan nilai $O(\log n)$ yang menunjukan bahwa pertumbuhan waktu bernilai logaritmik.

Kata kunci: Kriptografi, RSA, ECC, ElGamal, Kompleksitas Waktu.