

ABSTRAK

Kriptografi menjadi suatu bagian yang tidak dapat dipisahkan dari sistem keamanan jaringan pada era informasi global. Terdapat banyak parameter pada sistem kriptografi, sebagai contoh : tingkat keamanan algoritma, *flexibility*, distribusi frekuensi kemunculan karakter, variansi distribusi, *avalanche effect*, *brute force attack* dan waktu eksekusi data. Parameter tersebut dapat menjadi panduan bagi pengguna untuk menyesuaikan algoritma terhadap tingkat kebutuhan sistem kriptografi.

Algoritma *Advanced Encryption Standard* (AES) dan *Camellia* merupakan contoh algoritma kriptografi berbasis blok *cipher* dimana pada kedua algoritma tersebut terdapat beberapa kesamaan yaitu, jenis kunci adalah kunci simetris, ukuran blok data senilai 128 bit dan panjang kunci dengan nilai 128, 192 dan 256 bit.

Pada tugas akhir ini dilakukan pengukuran dan analisa perbandingan performansi algoritma AES dan *Camellia* dengan menggunakan perangkat lunak simulasi proses kriptografi dari kedua algoritma tersebut. Parameter performansi yang diukur meliputi waktu proses, pengaruh mode operasi, *avalanche effect*, dan *brute force attack*. Simulasi yang dibangun pada tugas akhir ini menggunakan bahasa pemrograman Java.

Kata kunci : *Camellia*, *Advanced Encryption Standard*, kriptografi, blok *cipher*, *avalanche effect*, *brute force attack*.