

Abstrak

Saat ini, telah banyak algoritma kriptografi yang telah diciptakan baik yang diaplikasikan pada perangkat lunak maupun perangkat keras. Dari yang sederhana hingga yang kompleks. Masing-masing algoritma mempunyai kelebihan masing-masing. Kelebihan dari segi kecepatan dalam proses enkripsi / proses dekripsi ataupun dari kebutuhan memori. Kelebihan-kelebihan ini dapat menjadi bahan pertimbangan dalam pemilihan algoritma kriptografi dalam merahasiakan data.

Pada tugas akhir ini terdapat dua algoritma kriptografi yang diimplementasikan yaitu DECIM dan Grain. Keduanya merupakan *stream cipher*. Kemudian akan dilakukan perbandingan terhadap kedua algoritma tersebut. Perbandingan dilakukan terhadap waktu yang dibutuhkan untuk melakukan proses enkripsi / proses dekripsi, besarnya memori yang dibutuhkan dan *avalanche effect*.

Berdasarkan implementasi dan analisis yang telah dilakukan, dapat disimpulkan bahwa algoritma kriptografi Grain membutuhkan waktu yang lebih singkat dan memori yang lebih sedikit dibandingkan dengan algoritma DECIM. Algoritma Grain juga memiliki nilai *avalanche effect* yang lebih tinggi dibandingkan dengan algoritma DECIM.

Kata kunci: Kriptografi, DECIM, Grain, Enkripsi, Dekripsi