ABSTRAK

Enkripsi adalah sebuah proses yang melakukan perubahan informasi dengan algoritma tertentu sehingga menjadi sebuah kode yang tidak terbaca, hanya orang yang mempunyai kunci penerjemahnya yang bisa membacanya. Proses enkripsi dan dekripsi membutuhkan kemampuan komputasi yang tinggi, hal ini berpengaruh pada kecepatan dan berbagai aspek performansi. Jika diterapkan dalam prosesor, masalah yang diangkat dalam penelitian ini adalah algoritma enkripsi mana yang paling tepat digunakan untuk enkripsi data.

Untuk bisa mengetahui algoritma mana yang lebih efisien, diimplementasikan algoritma *Data Encyption Standard* (DES) dan *Advanced Encryption Standard* (AES) pada aplikasi Cygwin. Aplikasi Cygwin berfungsi untuk meng*compile* program. Pengujian dilakukan dengan membuat program enkripsi untuk AES 128 dan DES dengan bahasa assembly x86. Penelitian ini membandingkan hasil enkripsi untuk parameter komposisi instruksi dan kecepatan komputasi enkripsi pada kedua program.

Hasil pengujian diperoleh algoritma AES membutuhkan lebih sedikit instruksi. Dengan hasil 1537 instruksi pada skenario enkripsi data input dan output terpisah, dan 1487 instruksi pada skenario enkripsi data overwrite. Dengan jenis instruksi yang paling banyak dipakai kedua algoritma adalah Data Transfer. Serta algoritma AES membutuhkan waktu lebih cepat dibandingkan DES. Dengan hasil rata-rata waktu komputasi pada skenario data input dan output terpisah, waktu yang dibutuhkan adalah 0.0544653 detik. Sedangkan pada skenario overwrite data, waktu yang dibutuhkan adalah 0.0520902 detik

Kata kunci : *Enkripsi, AES-128, DES, x86*