ABSTRAK

Pengiriman informasi melalui *socket programming* pada dasarnya tidak dilengkapi dengan keamanan yang mempuni, sehingga rentan terjadi penyadapan, maupun pencurian data oleh pihak yang tidak bertanggung jawab. Untuk mengatasi hal ini, dibutuhkan suatu metode kriptografi untuk menjamin kemanan data yang akan dikirimkan. Ada beberapa metode kriptografi diantaranya *Advanced Encryption System* (AES-256), *Data Encryption Standart* (DES), dan *International Data Encryption Algorithm* (IDEA). Ketiga metode kriptografi tersebut merupakan algoritma simetris yang memiliki keunggunalan dalam hal efisiensi enkripsi dan pengiriman pesan, dibandingkan dengan kriptografi asimetris. Namun, berdasarkan studi yang telah dilakukan, belum diketahui performansi dari ketiga algoritma tersebut jika diterapkan pada *socket programming*. Untuk menjawab hal tersebut maka dalam penelitian ini dilakukan percobaan penerapan ketiga algoritma tersebut pada *socket programming*. Untuk mengetahui performa dari masing-masing algoritma, maka dilakukan percobaan pengiriman file dengan format Txt, Docx, Pdf, Rar, Jpg, Mp3, dan MP4, yang dienkripsi menggunakan algoritma AES-256, DES, dan IDEA. Dari hasil pengujian didapatkan bahwa algoritma AES-256 memiliki performansi paling baik dalam kecepatan melakukan enkripsi serta dekripsi, sehingga waktu yang diperlukan lebih singkat. Sedangkan algoritma DES memiliki keunggulan pada ukuran *file* hasil enkripsi yang tidak terdapat penambahan ukuran.

Kata Kunci : AES-256, DES, IDEA, *Socket Programming*.