BAB V
PENUTUP

5.1 KESIMPULAN

Berdasarkan hasil pengujian yang telah dilakukan, maka didapatkan kesimpulan sebagai berikut:

1) Penerapan algoritma AES-256, DES, dan IDEA pada *secure file transfer* berhasil diterapkan dan berjalan dengan baik. Sehingga dapat melakukan enkripsi, pengiriman, serta dekripsi *file* dengan baik pada masing-masing algoritmanya.
2) Ukuran *file* hasil enkripsi pada algoritma AES-256 memiliki selisih ukuran cenderung merata pada tiap *file* baik pada skenario 1,2 dan 3, dengan selisih rata-rata 42 *bytes*. Pada algoritma DES tidak terdapat peningkatan ukuran pada *file* setelah terenkripsi. Sementara pada algoritma IDEA *file* hasil enkripsi mengalami peningkatan ukuran yang besar yaitu dua kali lipat atau 100% dari ukuran aslinya. Peningkatan ukuran pada hasil enkripsi Algoritma AES dan IDEA terjadi karena ada penambahan *header* yang berisi informasi *extensi file*.
3) Kecepatan enkripsi serta dekripsi pada algoritma AES-256 lebih cepat dibanding dengan algoritma DES, dan IDEA. Hal ini dikarenakan transformasi yang digunakan oleh algoritma AES-256 lebih ringan dibanding dengan transformasi yang digunakan oleh algoritma DES maupun operasi yang digunakan algoritma IDEA.
4) Waktu yang diperlukan selama pengiriman *file* hasil enkripsi sangat bergantung pada topologi jaringan yang digunakan, besarnya ukuran *file*, serta kondisi *resource* komputer.

Pengaman yang dilakukan algoritma AES-256, DES, dan IDEA pada *secure file transfer* menggunakan *socket programming* dapat berjalan dengan baik. Yang membedakan dari masing masing-masing algoritma adalah pada performa dari ketiga algoritma tersebut. Algoritma AES-256 memiliki keunggulan pada waktu dan kecepatan enkripsi dan dekripsi yang lebih baik diantara ketiga algoritma

tersebut. Sedangkan algoritma DES memiliki keunggulan pada ukuran *file* hasil enkripsi yang tidak terdapat penambahan ukuran.

5.2 SARAN

Adapun saran yang dapat penulis berikan guna pengembangan lebih lanjut dari penelitian yang telah dilakukan diantaranya:

1) Penambahan fitur pada sistem sehingga selain sebagai *server*, *node* bertugas juga sebagai *client*. Sehingga msing-masing *node* bisa saling mengirim dan menerima *file*.
2) Penggabungan dua algoritma enkripsi pada *system*, sehingga keamanan *file* yang dikirim menjadi lebih aman.
3) Penambahan fitur login dan otentifikasi sebelum melakukan pengiriman, sehingga diketahui identitas yang mengirimkan data.