ABSTRAK

Keamanan suatu informasi menjadi hal yang sangat penting saat ini. Banyak orang kemudian berusaha untuk mencari cara bagaimana mengamankan informasi dalam melakukan pertukaran informasi. Salah satu caranya adalah dengan metode enkripsi menggunakan algoritma simetri. Namun terdapat kendala dalam penggunaan kunci untuk tipe algoritma simetri, dimana kunci yang digunakan untuk enkripsi dan dekripsi harus sama, sedangkan jika kunci untuk dekripsi dikirimkan terpisah akan menyebabkan kunci dapat diketahui dengan mudah oleh penyadap.

Maka untuk mengatasi permasalahan tersebut, dalam tugas akhir ini dirancang suatu aplikasi enkripsi dan dekripsi *file* menggunakan algoritma Blowfish serta mengimplementasikannya pada jaringan LAN. Kunci yang digunakan untuk enkripsi dan dekripsi akan disamarkan dan disisipkan bersama dengan data yang telah dienkripsi, hal ini dilakukan agar informasi kunci tidak dapat diketahui dengan mudah oleh penyadap. Setelah data yang telah dienkripsi dan dikirimkan sampai pada penerima, kunci yang telah disamarkan dan disisipkan akan diambil kembali dari data dan akan digunakan untuk proses dekripsi. Pengujian terhadap sistem akan dilakukan dengan mengukur kinerja dari algoritma blowfish dari segi waktu enkripsi, waktu dekripsi, waktu pemecahan kunci, dan *avalanche effect*. Kemudian akan dilakukan perbandingan kinerja dari algoritma Blowfish terhadap algoritma DES, sehingga dapat diketahui algoritma manakah yang paling efektif untuk diterapkan pada sistem keamanan *file.*

Hasil implementasi dari sistem ini adalah data yang dikirim telah terenkripsi saat berada dalam jaringan dan kunci yang telah disisipkan tidak terlihat karena telah disamarkan, kemudian data yang sampai di penerima didekripsi secara otomatis menggunakan kunci yang telah disisipkan. Pada akhirnya sistem ini dapat mengatasi kelemahan pada konsep algoritma simetri dalam hal pengiriman data.

Kata Kunci : *Kriptografi, Algoritma Blowfish, Enkripsi, Dekripsi, Cipher Block.*