ABSTRAK

Algoritma DES dikembangkan di IBM (International Business Machines) dibawah pimpinan W.L. Tuchman pada tahun 1972. Algoritma ini didasarkan pada algoritma Lucifer yang dibuat oleh Horst Fiestel. Algoritma DES awal mempunyai panjang kunci 56 bit. Dengan panjang kunci 56 bit, DES lemah terhadap *exhaustive key search* attack atau dengan cara mencoba semua kemungkinan kunci.

Pada proyek akhir telah dikembangkan algoritma DES dengan ekspansi kunci sepanjang 112 bit. Pengembangan yang dilakukan adalah dengan menambahkan jaringan fiestel menjadi 4 blok yang sebelumnya hanya 2 blok.

Hasil analisa menunjukkan bahwa DES termodifikasi dengan panjang kunci 112 bit mempunyai waktu *exhaustive key search* 256 kali DES semula dengan panjang kunci 56 bit. Hasil demonstrasi menunjukkan bahwa DES termodifikasi memenuhi dua prinsip penyandian Shannon yaitu confussion dan diffusion.

Kata Kunci: *Cipher* Block, DES, dekripsi, enkripsi