ABSTRAK

Algoritma DES (Data Encryption Standard) dan Algoritma International Data Encryption Algorithm (IDEA) adalah algoritma kriptografi simetris dengan kategori cipher blok. Kedua algoritma ini beroperasi dalam bentuk blok bit, dengan ukuran blok sebesar 64 bit. Kedua algoritma ini juga dikenal sangat tangguh dalam mengamankan informasi. analisis dan perbandingan *Data Encryption Standard (DES)* dengan *International Data Encryption Algorithm (IDEA)*. DES merupakan salah satu algoritma kriptografi cipher block dengan ukuran blok 64 bit dan ukuran kuncinya 56 bit. Algoritma DES dibuat di IBM, dan merupakan modifikasi daripada algoritma terdahulu yang bernama *Lucifer*. *Lucifer* merupakan algoritma cipher block yang beroperasi pada blok masukan 64 bit dan kuncinya berukuran 128 bit. IDEA adalah algoritma kriptografi simetri yang beroperasi dalam bentuk blok 64 bit. Dalam sejarah aloritma DES . *Lucifer* beroperasi pada blok input 64 bit dan menggunakan key sepanjang 128 bit. Lama kelamaan *Lucifer* semakin dikembangkan agar bisa lebih kebal terhadap serangan analisis cypher tetapi panjang kuncinya dikurangi menjadi 56 bit dengan maksud supaya dapat masuk pada satu chip.

Kemudian akan dibahas pula proses cara melakukan dekripsi kembali untuk mengembalikan plaintext hasil enkripsi menjadi seperti sedia kala dengan menggunakan algoritma DES. Dalam studi ini juga akan dianalisis mengenai kelebihan dan kelemahan dari algoritma DES itu sendiri.

Algoritma DES yang akan dibahas dalam studi ini juga akan dibandingkan dengan algoritma IDEA. Studi ini akan membandingkan performansi masing-masing algoritma dalam mengenkripsi dan mendekripsi berbagai jenis file dalam berbagai ukuran. Sebuah perangkat lunak bernama Netbeans akan digunakan untuk membandingkan antara algoritma DES dengan algoritma IDEA. Perangkat lunak inilah yang digunakan untuk membandingkan performansi algoritma DES dengan IDEA.

Kata kunci:
Data Encryption Standard, International Data Encryption Algorithm, plaintext, chipertext, Netbeans, dekripsi, enkripsi.