

ABSTRAKSI

Enkripsi menjadi hal yang vital dalam pengamanan komunikasi *wireless* yang menggunakan ruang terbuka sebagai media komunikasi. Penggunaan algoritma yang ada sekarang ini terbukti tidak efektif untuk komunikasi *wireless* karena adanya *Avalanche Effect*. *Avalanche Effect* memang dibutuhkan untuk mencegah plainteks yang mirip menghasilkan cipherteks yang mirip juga, namun hal ini menghasilkan nilai BER yang besar untuk komunikasi *wireless* karena komunikasi *wireless* melibatkan *noise*. Algoritma M-DES digunakan untuk mengurangi nilai BER yang besar pada komunikasi *wireless* tanpa harus mengorbankan tingkat keamanan pesan yang ditransmisikan.

Pada tugas akhir ini penulis merancang sistem beralgoritma M-DES dengan menggunakan software MATLAB dengan tujuan untuk mengamankan pesan yang berupa teks. Teks yang digunakan adalah teks yang diubah menjadi rangkaian biner 64-bit.

Hasil penelitian tugas akhir ini adalah sebuah sistem yang dapat mengetahui tingkat keamanan algoritma M-DES. Diharapkan, sistem ini pun dapat membuktikan bahwa algoritma M-DES merupakan algoritma yang memenuhi kriteria keamanan algoritma kriptografi.

Kata kunci: BER, DES, Keamanan Pesan, Komunikasi *Wireless* Kriptografi, M-DES