ABSTRAK

Keamanan komunikasi suara dalam jaringan internet belum terjamin. Padahal penggunaan komunikasi suara telah banyak digunakan. Tugas Akhir ini akan membahas tentang solusi pengamanan pesan suara dengan menggunakan enkripsi. Enkripsi berarti melakukan pengkodean pesan suara agar pihak yang tidak berhak tidak dapat memahaminya.

Algoritma enkripsi yang digunakan pada Tugas Akhir ini adalah algoritma enkripsi cipher blok Mars. Algoritma cipher blok akan menimbulkan delay yang lebih besar daripada algoritma cipher aliran. Oleh karena itu, penerapan algoritma Mars harus disesuaikan agar delay yang ditimbulkan kecil. Pada makalah ini, perubahan tersebut dilakukan dengan menggunakan mode operasi counter yang dikatakan dapat merubah efisiensi cipher blok menjadi menyerupai cipher aliran.

Analisa subsistem security dilakukan berdasarkan beberapa parameter yaitu *time processing,* perbandingan *file input* dan *output*, *avallanche effect*, *brute force attack*, variance , perbandingan dengan algoritma yang lain dan MOS.

Dari hasil pengujian dapat disimpulkan sistem dapat direalisasikan dengan menghasilkan waktu delay antar blok adalah 0,5716 ms, perbandingan *file input* dan *output* sama. Nilai *avalanche effect* berdasarkan perubahan 1 bit kunci mencapai 51,25 % sedangkan berdasarkan perubahan 1 bit plainteks besarnya 0.781 %. Waktu untuk melakukan *bruce force attack* adalah 2.24×10^{25} tahun dan untuk penilaian MOS tergolong *excellent* untuk data hasil enkripsi dan *fine* untuk data hasil dekripsi.

Kata Kunci : *Enkripsi, Cipher Block, Mars, time processing, file input* dan *output, avallanche effect, brute force attack,* MOS