ABSTRAK

Kerahasiaan data sudah menjadi suatu bahan penelitian yang banyak dikembangkan dalam proses pengiriman informasi. Namun, kerahasiaan dalam komunikasi suara sekarang ini masih belum terjamin. Oleh karena itu, diperlukan metoda yang sesuai agar pengiriman informasi saat ini dapat lebih aman digunakan. Banyak teknologi yang menggunakan enkripsi sebagai teknologi pengiriman informasi saat ini.

Pada tugas akhir ini membahas tentang solusi pengaman pesan suara dengan menggunakan enkripsi. Enkripsi berarti proses pengamanan data (pesan suara) agar pihak yang tidak berkepentingan tidak dapat memahami pesan suara tersebut. Algoritma enkripsi yang di gunakan pada tugas akhir ini adalah Algoritma enkripsi shared-key cipher blok MARS. Algoritma cipher blok ini akan menimbulkan delay yang lebih besar daripada algoritma cipher aliran. Oleh karena itu, penerapan algoritma MARS harus disesuaikan agar delay yang ditimbulkan kecil dan property real time terjaga.

Pada Tugas Akhir ini, perubahan tersebut dilakukan dengan mengubah mode operasi MARS menjadi mode operasi counter yang dikatakan dapat merubah efisiensi cipher blok menjadi menyerupai cipher aliran dan melakukan pemisahan kunci pada sub-band.

Dari hasil pengujian dapat disimpulkan sistem dapat direalisasikan dengan menghasilkan waktu delay adalah 0,155053 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 2.28×10^{25} tahun.

Kata Kunci : *Enkripsi, Cipher Block, MARS,sub-band.*