ABSTRAK

Keamanan sistem pada jaringan GSM (*Global System for Mobile Communication)* sangat diperlukan untuk menghindari adanya pencurian informasi oleh pihak atau badan yang tidak bertanggung jawab. Keamanan sistem pada jaringan GSM diimplementasikan berupa metode kriptografi algoritma A5 yang merupakan metode penyandian suara pada saat komunikasi secara real time antara MS (*Mobile Station*) dan BS (*Base Station*).

Algoritma A5/1 merupakan algoritma A5 versi kuat pada jaringan GSM yang merupakan algoritma kriptografi simetris dengan teknik enkripsi *stream chiper* yang terdiri dari 3 buah LFSR (*Linier Feedback Shift Register*) dengan derajat 19,22, dan 23, dimana LFSR adalah register geser dengan umpan balik linier yang merupakan pembangkit deretan bilangan acak. Sedangkan TMS320VC33 ialah DSP (*Digital Signal Processor's*) Card yg mempunyai kecepatan operasi hingga 75 MIPS (*Million Instruction Operations per Second*) atau 13,34 ns per instruksi yang memungkinkan pengolahan sinyal digital secara *real time*. Tugas akhir secara khusus membahas perancangan dan implementasi kriptografi algoritma A5/1 menggunakan DSP Card TMS320VC33 dimana paramater yang dianalisis ialah *Time Processing, Avalanche Effect, Brute Forced Attack* dan *Variance.*

Dari hasil pengujian dapat disimpulkan bahwa sistem dapat direalisasikan dengan waktu proses 2,607516 ms yang dihitung berdasarkan *duty cycle*. Nilai *avalanche effect* berdasarkan perubahan 1 bit kunci mencapai 45,39473% sedangkan berdasarkan perubahan 1 bit *plaintext* atau *ciphertext* hanya 0,893%. Besarnya nilai *variance* 6,0982 sedangkan waktu untuk melakukan *brute forced attack* ialah $1{,}406791788 \times 10^{28}$ tahun.

Kata kunci : *A5/1 Algorithm, DSP Card TMS320VC33, GSM (Global System for Mobile Communication), Time Processing, Avalanche Effect, Variance, Brute Forced Attack*