ABSTRAK

Standar internasional keamanan sistem komunikasi *mobile* 3G ditetapkan dalam UMTS (Universal Mobile Telecommunication System). Sistem keamanan pada jaringan 3G sendiri memiliki banyak sekali algoritma dalam penentuan kriptografi yang akan digunakan dalam jaringan tersebut. Algoritma kriptografi yang digunakan pada jaringan 3G adalah algoritma f8 dan f9, yang digunakan untuk menjaga keamanan pada sistem jaringan antara *UE (User Equipment)* dan *RNC (Radio Network Controller).* Algoritma f8 dan f9 merupakan algoritma yang dibuat berdasarkan algoritma A5/3 (Kasumi) yang merupakan algoritma jenis algoritma simetris dengan bagian enkripsi dan dekripsi sama memiliki blok cipher 64-bit dan ukuran kunci sebesar 128-bit.

Tugas akhir ini secara khusus membahas pada perancangan dan implementasi algoritma A5/3 (Kasumi) tersebut menggunakan *DSP Card TMS320VC33*. *TMS320VC33* merupakan *DSP(Digital Signal Processing*) *card* yang mempunyai kecepatan operasi hingga 150 MFLOPS (*Million Floating Point Operations per Second*) atau sama dengan 75 MIPS (*Million Instruction Operations per Second*) yang mampu melakukan pengolahan sinyal digital secara *real time.* Perancangan dan pengimplementasian dilakukan dengan membuat program berdasar algoritma dengan menggunakan bahasa assembly yang kemudian diimplementasikan pada *TMS320VC33*. Hasil keluaran pada enkripsi menggunakan algoritma A5/3 (Kasumi) dianalisa performansinya dengan menghitung *time processing*, *avalanche effect*, dan kehandalan tehadap *brute force attack*.

Dari hasil analisa pengujian terhadap perancangan dan pengimplementasian algoritma kriptografi A5/3 (Kasumi) dapat disimpulkan bahwa sistem dapat direalisasikan dengan waktu proses 2,97 x 10^{-2} ms yang dihitung berdasarkan *duty cycle*. Nilai *avalanche effect* berdasarkan perubahan 1 bit kunci mencapai 48,88 % sedangkan berdasarkan perubahan 1 bit *plaintext* yaitu 49,66 %, dan perubahan 1 bit *ciphertext* adalah 50,15 %. Waktu untuk melakukan *brute force attack* ialah $1{,}60x\ 10^{26}$ tahun.

Kata kunci: algoritma f8 ,f9, A5/3 (Kasumi), *DSP Card TMS, avalanche effect, time processing brute force attack*