Abstraksi

Metoda kriptografi yang digunakan untuk meningkatkan keamanan informasi baik suara maupun teks pada sistem telepon seluler GSM (*Global System for Mobile Communication*) adalah dengan menggunakan algoritma kriptografi A5. Algoritma A5 merupakan jenis algoritma simetri dimana kunci yang dipakai untuk proses enkripsi dan dekripsi sama. Algoritma A5 dibagi menjadi A5/1, A5/2, dan Versi terbarunya yaitu A5/3.

Tugas akhir ini merepresentasikan rancangan algoritma A5/2 yang dapat melakukan proses enkripsi dan deskripsi dalam satu sistem. Rancangan ini menggunakan mode operasi LFSR *(Liniear Feedback Shift Register*) yang digunakan untuk pembangkit deretan bilangan acak, dan akan dimodelkan dengan menggunakan bahasa VHDL (*Very High Speed Integrated Circuit Hardware Language*). Rancangan ini akan disimulasikan menggunakan Aldec Active HDL 3.5 serta disintesis menggunakan Xilinx ISE 8.1i,dan devais target menggunakan FPGA Virtex-4 seri XC4VLX25-10SF363C

Hasil implementasi rancangan tugas akhir ini dengan menggunakan target divais FPGA Virtex-4 seri XC4VLX25-10SF363C menunjukkan *top level entity* mampu bekerja pada frekuensi maksimum 198,159 MHz dan membutuhkan *slices* sebanyak 2% (292 dari10752 *slices* yang tersedia), serta membutuhkan 6% IOBs (15 dari 240 IOB yang tersedia).

Kata kunci : *Cryptography, GSM (Global System for Mobile Communications, A5, A5/2,* LFSR *(Liniear Feedback Shift Register*), FPGA.