ABSTRAKSI

Sejalan dengan perkembangan teknologi informasi, media komunikasi yang digunakan dan sistem aliran data yang dipakai juga semakin beragam. Perkembangan ini memberikan kemudahan dalam berkomunikasi. Namun, perkembangan ini juga menimbulkan permasalahan baru dibidang keamanan informasi.

Salah satu metode pengamanan data adalah kriptografi. Dengan metode ini, data disamarkan terlebih dahulu sebelum dikirimkan pada media transmisi. Salah satu jenis algoritma kriptografi yang digunakan adalah A5 yang digunakan dalam sistem komunikasi *Global System for Mobile communication* (GSM). Algoritma A5 dibedakan menjadi 3 jenis yaitu A5/1, A5/2, dan yang terbaru yaitu A5/3.

Pada tugas akhir ini, dilakukan perancangan algoritma A5/1 dengan menggunakan bahasa VHDL dan diimplementasikan pada board *Field Programmable Gate Array* (FPGA) Virtex-4 seri XC4VLX25-10SF363C. Dilakukan analisa pada keluaran sistem untuk mengetahui nilai *avalanche effect*, dan frekuensi keluaran dan frekuensi perubahan bit dari informasi yang tersamar. Simulasi dari perancangan dilakukan dengan menggunakan software Aldec-Active HDL 3.5. Sedangkan hasil implementasi akan diamati pada *logic analyzer* LA-2124A.

Hasil analisa perancangan menunjukkan sistem memiliki *avalanche effect* dan frekuensi bit *ciphertext* yang mendekati 50% dengan frekuensi keluaran bit dan perubahan bit yang mendekati 50%. Hasil *synthesis* pada bagian enkripsi memerlukan *Slices* sebanyak 1%, *Slice Flip Flops* sebanyak 0%, *4 input LUTs* sebanyak 1%, *bonded IOBs* sebanyak 3%, dan *GCLKs* sebanyak 3% dari *resource* yang tersedia pada *device*, dengan frekuensi *clock* maksimum sebesar 126,173 Mhz. Sedangkan hasil synthesis bagian enkripsi memerlukan *Slices* sebanyak 1%, *Slice Flip Flops* sebanyak 0%, *4 input LUTs* sebanyak 0%, *bonded IOBs* sebanyak 2%, dan *GCLKs* sebanyak 3% dari yang tersedia pada *device*, dengan frekuensi *clock* maksimum sebesar 125,796 Mhz.