ABSTRAKSI

Pada tugas akhir ini diimplementasikan algoritma kriptografi simetris AES (*Advanced Encryption Standard*) dengan panjang kunci 128 bit dimana proses enkripsi dan dekripsi dilakukan dalam satu *chip*/*core* yaitu pada Xilinx XC2S300E PQ208-6. Mode operasi menggunakan ECB (*Electronic Code Book*). Pemodelan rancangan menggunakan bahasa VHDL (*Very High Speed Integrated Circuit Hardware Language*). Simulasi dengan menggunakan ModelSim SE 6.0 berdasarkan KAT (*Known Answer Test*) dari pembuat algoritma, kemudian disintesis dan diimplementasikan menggunakan Xilinx ISE 7.1.03i, serta diverifikasi menggunakan Chipscope Pro 7.1.03i.

Hasil implementasi menunjukkan bahwa implementasi kriptografi AES-128 ini mampu bekerja pada frekuensi maksimum 28.771 MHz dengan *throughput* sebesar 167,395 Mbps pada frekuensi tersebut dan area yang dibutuhkan sebanyak 35.460 gate ekivalen.

Kata kunci: AES-128, Enkripsi, Dekripsi, ECB, VHDL, KAT, *Throughput*, Area.