ABSTRAKSI

Salah satu hal yang penting dalam komunikasi data adalah sistem keamanan. Hal ini penting karena pelanggan akan merasa aman dalam berkomunikasi bila menggunakan sistem komunikasi yang aman. Sistem keamanan dengan level tinggi cocok untuk beberapa pengiriman data, misalnya *email*, *e-commerce*, dll. Sistem keamanan untuk komunikasi data lazim juga disebut kriptografi. Salah satu algoritma kriptografi yang dipakai untuk penyandian data pada *credit card* adalah algoritma *Rivest-Shamir-Adleman* (*RSA)*.

Algoritma *RSA* merupakan jenis algoritma asimetris dimana *kunci* dalam setiap prosesnya berbeda. *Public key* digunakan untuk proses enkripsi, sedangkan dalam proses deskripsi menggunakan *prívate key*. Dalam *public key RSA*, terdapat dua operasi penting yaitu proses perkalian modulo dan proses operasi eksponensiasi.

Operasi perkalian modulo merupakan inti dari algoritma *RSA*. Operasi tersebut dimplementasikan oleh algoritma *Montgomery*. *Montgomery* merupakan algoritma paling efisien dan cocok untuk diimplementasikan pada perangkat keras.Lebar data 512 bit merupakan lebar data minimal untuk Kriptografi RSA.

Perancangan dimulai dengan menerjemahkan algoritma perkalian modulo tersebut ke dalam alur komputer. Rancangan ini dimodelkan dengan menggunakan bahasa pemrograman VHDL dan disimulasikan menggunakan Modelsim SE 6.0, kemudian disintesis dan diimplementasikan menggunakan

Xilinx ISE 8.1i, sedangkan devais target menggunakan board FPGA SPARTAN 3 seri XC3S1000 FT256-4C.

Hasil implementasi rancangan tugas akhir ini dengan menggunakan target divais FPGA SPARTAN 3 seri XC3S1000 FT256-4C menunjukkan *top level entity* mampu bekerja pada frekuensi maksimum 39,469 MHz dan membutuhkan *slices* sebanyak 32% (2485 dari 7680 *slices* yang tersedia), serta membutuhkan 7% IOBs (13 dari 173 IOBs yang tersedia).

Kata Kunci: Kriptografi, *RSA*, FPGA, *Montgomery*