BAB I
PENDAHULUAN

1.1 Latar Belakang

Algoritma RSA (Rivest-Shamir-Adleman) digunakan secara luas dalam bidang keamanan internet. Beberapa contoh penggunaaannya antara lain untuk tanda tangan digital dan pada komunikasi transaksi kartu kredit. Meskipun memiliki keamanan yang baik, RSA memerlukan kebutuhan komputasi yang kompleks. Kompleksitas perhitungan pada algoritma RSA bergantung kepada dua jenis operasi matematika, yaitu operasi modular dan operasi perpangkatan. Operasi perpangkatan memerlukan waktu yang banyak dan kompleksitas yang tinggi. Salah satu metode untuk mempercepat operasi pada RSA adalah *Chinese Remainder Theorem* (CRT). *Chinese Remainder Theorem* membagi satu operasi perpangkatan besar menjadi dua operasi perpangkatan yang lebih kecil. Saat ini algoritma RSA CRT sudah berhasil diterapkan pada komputer, namun terbatas pada perhitungan berbasis perangkat lunak.

Dari permasalahan di atas penulis mengajukan sebuah penelitian untuk membuat sebuah sistem yang dapat melakukan operasi algoritma RSA CRT berbasis perangkat keras yaitu *Field Programmable Gate Array* (FPGA). Sistem berbasis perangkat keras mampu menawarkan kecepatan proses yang lebih tinggi dibandingkan dengan perangkat lunak.

Dengan dibuatnya sistem ini diharapkan dapat membantu mempercepat operasi bilangan pada RSA dengan algoritma RSA CRT. Operasi perpangkatan dapat dilakukan dengan lebih optimal sehingga mengurangi total waktu yang diperlukan untuk proses dekripsi.

1.2 Maksud dan Tujuan

Maksud yang ingin dicapai adalah membangun sistem yang dapat melakukan perhitungan algoritma RSA dengan metode *Chinese Remainder Theorem* (CRT).

Tujuan yang ingin dicapai dalam perancangan ini adalah sebagai berikut:

1. Melakukan perancangan algoritma RSA CRT dengan bahasa VHDL.

1.3 Batasan Masalah

Batasan masalah dalam pembuatan sistem ini adalah sebagai berikut:

1. Pembahasan difokuskan pada perancangan dan implementasi menggunakan algoritma *Chinese Remainder Theorem*.
2. Input yang digunakan dalam perancangan dan implementasi menggunakan lebar data 512 bit.
3. *Target device* yang digunakan adalah FPGA Altera DE2 seri Cyclone II 2C35.
4. Analisis pada sistem dilakukan dengan mengamati dan menyimpulkan data keluaran sistem dengan masukan sistem serta melakukan verifikasi rancangan.

1.4 Metode Penelitian

Metode penelitian yang dilakukan dalam penyusunan skripsi ini adalah sebagai berikut:

1. Studi Literatur

   Pencarian dan pengumpulan literatur yang berkaitan dengan masalah yang ada pada skripsi ini baik mengenai algoritma kriptografi RSA atau tentang bahasa VHDL.
2. Perancangan Sistem

   Perancangan sistem yang sesuai dengan spesifikasi algoritma kriptografi RSA dengan bahasa VHDL dengan bantuan *software* Altera Quartus 13.0. Metode perancangan yang digunakan adalah *top-bottom*.
3. Simulasi dan Implementasi Sistem ke Board FPGA

   Setelah sistem selesai dirancang maka akan dilakukan simulasi pada ModelSim 10.1 untuk mengetahui *timing diagram* apakah sesuai dengan spesifikasi untuk kemudian dilakukan implementasi pada board FPGA.

4. Analisis

   Analisis dilakukan dalam beberapa bagian yaitu: analisis uji fungsional (simulasi), verifikasi perancangan, dan analisis penggunaan *resources*.

1.5 Sistematika Penulisan

Sistematika penulisan ini disusun untuk mengetahui gambaran umum tentang penelitian yang dilakukan. Sistematika penulisan ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini menjelaskan secara singkat tentang latar belakang, maksud dan tujuan, batasan masalah, metode penelitian dan sistematika penulisan.

BAB II DASAR TEORI

Bab ini membahas mengenai dasar-dasar teori, rujukan dan metode yang berhubungan dengan judul penelitian.

BAB III PERANCANGAN SISTEM

Bab ini berisi tentang deskripsi sistem dan perancangan sistem kriptografi RSA CRT.

BAB IV PENGUJIAN DAN ANALISIS

Bab ini berisi implementasi dari perancangan yang telah dilakukan beserta hasil pengujian, sehingga dapat diketahui apakah sistem yang dibangun sudah sesuai dengan spesifikasi.

BAB V KESIMPULAN DAN SARAN

Bab ini membahas kesimpulan dan saran yang bermanfaat bagi perbaikan dan perkembangan dalam perancangan sistem kriptografi RSA pada FPGA.