# BAB I
# PENDAHULUAN

## 1.1 Latar Belakang

Berawal dari sebuah keamanan dalam komunikasi data yang merupakan suatu hal yang penting, karena informasi/data tersebut akan menjadi aset bagi perorangan, organisasi, dan instansi pemerintah. Apabila informasi tersebut dapat diakses secara ilegal oleh pihak tertentu maka akan dapat merugikan bagi pemilik informasi.Oleh karena itu pengiriman dan penerimaan informasi harus dilakukan secara aman dan legal serta terjamin kerahasiannya.Untuk menjaga informasi berupa data penting, salah satunya dapat dilakukan dengan menggunakan metode kriptografi.

Kriptografi adalah ilmu yang memanfaatkan fungsi matematis untuk mengubah suatu informasi yang aman melalui suatu transformasi tertentu. Terdapat beberapa algoritma yang dapat digunakan untuk melakuakan transformasi. Algoritma ini dapat diimplementasikan baik dalam bentuk software maupun hardware yang masing-masing memiliki kelebiahan dan kekurangan. Implementasi dalam bentuk hardware pada umumnya memiliki performansi yang lebih baik terutama pada kecepatan proses dibanding implementasi dalam bentuk software, namun biaya implementasi dalam bentuk hardware tentunya lebih besar dari implementasi dalam bentuk software.

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)* (*Rivest-Shamir-Adleman*). Algoritma *RSA* ini merupakan kriptografi asimetri dimana ada 2 buah kunci yang berbeda, ada *public key* pada proses enkripsi dan *private key* pada proses deskripsi. Public key dapat diketahui oleh semua orang, tetapi

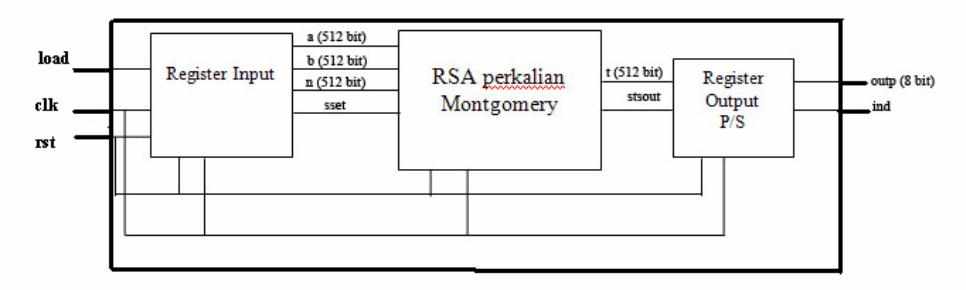
private key hanya instansi yang mengetahuinya. Sehingga algoritma ini dirasa cukup aman untuk aplikasi *e-commerce* .

Kecepatan, komputasi daya, dan tingkat keamanan adalah hal-hal yang saling berpengaruh dalam kriptosistem ini. Adalah sesuatu yang sulit untuk mencapai kecepatan yang tinggi, komputasi yang rendah, dan tingkat keamanan yang tinggi dalam suatu rancangan. Karena pada umumnya yang tercapai adalah semakin tinggi tingkat keamanan yang diinginkan maka makin tinggi pula komputasi daya yang dibutuhkan dan makin rendah kecepatan yang dihasilkan.

## 1.2 Perumusan Masalah

Dalam penulisan Tugas Akhir ini perumusan masalah akan difokuskan pada beberapa hal, yaitu:

1. Perancangan perkalian modulo *RSA* yang berbasis pada algoritma *Montgomery* dengan VHDL (*Very High Speed Integrated Circuit Hardware Language*).
2. Pengalokasian port yang diperlukan pada implementasi.
3. Sintesis perkalian modulo *Montgomery.*
4. Implementasi perkalian modulo *RSA* yang berbasis pada algoritma *Montgomery* ke devais target FPGA SPARTAN 3 seri XC3S1000 FT256-4C.




**Gambar 1.1** Blok Sistem yang akan diimplementasikan pada FPGA

## 1.3 Batasan Masalah

Dalam Tugas Akhir ini, batasan masalah yang digunakan adalah:

1. Pembahasan difokuskan pada perancangan dan implementasi menggunakan algoritma perkalian modulo *Montgomery*.
2. Input yang digunakan dalam perancangan & implementasi menggunakan lebar data 512 bit.
3. Tidak mengimplementasikan dalam bentuk *smartcard.*
4. Target device yang digunakan adalah FPGA SPARTAN 3 seri XC3S1000 FT256-4C.
5. Analisa sistem dilakukan dengan mengamati dan menyimpulkan data data keluaran sistem (512 bit) dengan masukan sistem (512 bit ) serta melakukan verifikasi rancangan.

## 1.4 Tujuan Penulisan

Tujuan dari Tugas Akhir ini adalah:

1. Melakukan perancangan dan simulasi perkalian modulo *RSA* 512 bit yang berbasis pada algoritma Montgomery menggunakan bahasa pemrograman VHDL.
2. Mengimplementasikan perkalian modulo *RSA* 512 bit yang berbasis pada algoritma Montgomery ke board FPGA Spartan 3 seri XC3S1000 FT256 –4C.
3. Menganalisa sistem dalam hal analisa perancangan (simulasi), verifikasi perancangan, dan analisa penggunaan resources.

## 1.5 Metode penulisan

Metode yang akan dilakukan dalam penyusunan Tugas Akhir ini adalah:

1. Studi literatur

   Pencarian dan pengumpulan literatur yang langsung berkaitan dengan masalah-masalah yang ada pada Tugas Akhir ini baik mengenai algoritma perkalian modulo *Montgomery* atau tentang bahasa pemrograman VHDL, serta dari Tugas Akhir Mahasiswa ITTelkom dan perguruan tinggi lain, yang mendukung Tugas Akhir ini.

2. Perancangan dan Simulasi

   Perancangan sistem yang sesuai dengan spesifikasi algoritma kriptografi A5/2 dengan bahasa VHDL dengan bantuan *software* Modelsim 6.0 dan Xilinx WebPack Project Navigator 8.1i. Metode perancangan yang digunakan adalah gabungan antara *top-down* dan *bottom-up.*

3. Analisa

   Analisa sistem dalam hal analisa perancangan (simulasi), verifikasi perancangan, dan analisa penggunaan resources.

4. Implementasi

   Desain yang telah berhasil dijalankan pada software simulasi, kemudian akan disintesis & diimplementasikan pada FPGA SPARTAN 3 Seri XC3S1000 FT256-4C , dan diuji serta dianalisis kinerjanya

## 1.6 Sistematika Penulisan

Laporan Tugas Akhir akan dirancang dengan sistematika sebagai berikut :

BAB I : Pendahuluan

Bab ini membahas tentang latar belakang, maksud dan tujuan, batasan masalah, rumusan masalah, serta sistematika pembahasan dari perancangan sistem.

BAB II : Landasan Teori

Membahas landasan teori yang berhubungan dengan keamanan algoritma kriptografi *RSA*. Teori dasar ini difokuskan pada teori-teori dasar pada mekanisme, kriptografi dan algoritma perkalian *Montgomery*.

BAB III : Perancangan Sistem

Bab ini akan membahas perancangan algoritma Perkalian *Montgomery* dengan menggunakan *software* VHDL Model sim 6.0, simulasi, dan analisa hasil simulasi.

BAB IV : Analisa Sistem

Bab ini berisi analisa hasil perancangan, analisa hasil sintesis, dan akan diimplementasikan sistem hasil simulasi di model sim 6.0 ke devais target board FPGA SPARTAN 3 seri XC3S1000 FT256-4C.

BAB V : Kesimpulan & Saran

Bab ini berisi kesimpulan mengenai tugas akhir ini dan saran untuk pengembangan TA ini selanjutnya.