BAB I
PENDAHULUAN

1.1 Latar Belakang

Komunikasi suara dalam sistem seluler GSM (*Global System for Mobile Communication*) merupakan suatu jenis informasi yang paling banyak diakses selain informasi data teks. Untuk informasi yang bernilai sangat penting, proses pertukarannya harus memperhatikan aspek keamanan dan kerahasiaan. Salah satu metode untuk meningkatkan keamanan informasi baik suara maupun teks adalah dengan teknik kriptografi, dimana data diolah menurut algoritma tertentu sehingga dihasilkan suatu pola data dalam bentuk yang lain sebelum dikirimkan. Pada sistem seluler GSM dibutuhkan suatu algoritma kriptografi yang mampu melakukan pemrosesan data yang cukup cepat dan juga menawarkan tingkat keamanan yang tinggi. Salah satu algoritma kriptografi yang direkomendasikan oleh vendor GSM untuk mengamankan data antara MS (*Mobile Station*) dan BS(*Base Station*) adalah algoritma A5/2.

Algoritma kriptografi A5/2 merupakan teknik kriptografi simetris dan termasuk jenis algoritma *streamchiper* yang merupakan implementasi dari LFSR (*Linear Feedback Shift Register*) dimana proses enkripsi dan deskripsi dilakukan berdasarkan posisi bit per bit dalam aliran data secara seketika (*real time*). Algoritma A5/2 terdiri dari empat LFSR, yaitu: R1, R2, R3, dan R4 dengan panjang bit setiap registernya adalah 19 bit, 22 bit, 23 bit dan 17 bit secara berurutan.

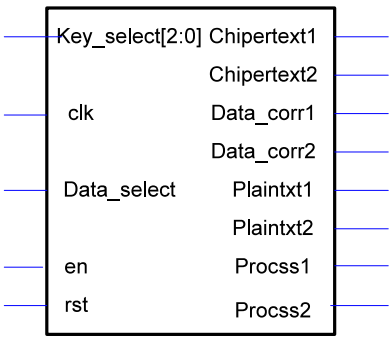
Dalam Tugas Akhir ini dilakukan perancangan dan implementasi sistem kriptografi dengan menggunakan algoritma A5/2 berbasis FPGA.

I.2 Perumusan Masalah

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

1. Perancangan kriptografi algoritma A5/2 dengan menggunakan bahasa pemrograman VHDL (*Very High Speed Integrated Circuit Hardware Description Language*).
2. Implementasi pada FPGA Virtex-4 seri XC4VLX25-10SF363C

   Secara garis besar diagram blok dari sistem yang akan diimplementasikan adalah sebagai berikut:



Gambar 1.1 Blok Sistem yang akan diimplentasikan pada FPGA.

1.3 Batasan Masalah

Dalam Tugas Akhir ini, batasan masalah yang digunakan adalah:

1. Untuk simulasi dan implementasi, kunci yang digunakan adalah data bit sepanjang 64-bit
2. Untuk simulasi dan implementasi, inputan yang digunakan adalah data bit sepanjang 114-bit
3. Pada perancangan dan implementasi tidak digunakan kode koreksi kesalahan, melainkan menggunakan pembanding sebagai cek bit hasil deskripsi.
4. Target device yang digunakan adalah FPGA Virtex-4 seri XC4VLX25-10SF363C.
5. Analisa sistem dilakukan dengan mengamati dan menyimpulkan data bit hasil keluaran sistem dengan data bit inputan dan *avalanche effect*.

1.4 Tujuan Penulisan

Tujuan dari Tugas Akhir ini adalah:

1 Melakukan perancangan algoritma A5/2 dengan bahasa pemrograman VHDL, simulasi dan merealisasikan sistem kriptografi algoritma A5/2 menggunakan board FPGA virtex-4 seri XC4VLX25-10FS363C.

2 Menganalisa sistem dalam hal analisa uji fungsional (simulasi), analisa perubahan bit, analisa frekuensi bit, analisa *avalanche effect*, analisa penggunaan *resource* dan analisa pengamatan keluaran pada FPGA dengan menggunakan *Logic Analyzer*.

1.5 Metode Penulisan

Metodologi yang 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 kriptografi A5/2 atau tentang bahasa pemrograman VHDL.

2. Perancangan Sistem

   Perancangan sistem yang sesuai dengan spesifikasi algoritma kriptografi A5/2 dengan bahasa VHDL dengan bantuan *software* Active Aldec-HDL 3.5 dan Xilinx WebPack Project Navigator 8.i. Metode perancangan yang digunakan adalah gabungan antara *top-down* dan *bottom-up.*

3. Simulasi dan implementasi sistem ke board FPGA Virtex-4 seri XC4VLX25-10SF363C

   Setelah sistem selesai dirancang maka akan dilakukan simulasi untuk mengetahui *timing diagram* apakah sesuai dengan spesifikasi dan meng-implementasikan pada board FPGA.

4. Analisa dan penarikan kesimpulan

   Analisa dilakukan dengan membagi ke dalam beberapa bagian yaitu : analisa uji fungsional (simulasi), analisa perubahan bit, analisa frekuensi bit, analisa *avalanche effect*, analisa penggunaan *resource* dan analisa pengamatan keluaran pada FPGA dengan menggunakan *Logic Analyzer.*

1.6 Sitematika Penulisan

Sistematika penulisan untuk Tugas Akhir ini adalah 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 DASAR TEORI

Membahas dasar teori yang berhubungan dengan keamanan GSM (*Global System for Mobile Communications*) menggunakan algoritma kriptografi A5/2. Teori dasar ini difokuskan pada teori-teori dasar pada mekanisme, kriptografi dan algoritma A5/2-nya sendiri.

BAB III PERANCANGAN SISTEM

Bab ini akan membahas perancangan enkripsi dan deskripsi algoritma A5/2 dengan menggunakan *software* VHDL yang siap diimplementasikan pada board FPGA.

BAB IV ANALISIS SISTEM

Bab ini akan menjelaskan tentang analisa sistem yang telah dibuat, sehingga dapat diketahui hasil yang didapat pada perancangan dan realisasi sistem.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan terhadap hasil yang diperoleh dari penelitian yang telah dilakukan serta membicarakan saran–saran untuk pengembangan sistem ini lebih lanjut