BAB I
PENDAHULUAN

1.1 Latar Belakang

Masalah s*ecurity* dalam komunikasi merupakan hal yang sangat penting karena informasi merupakan barang yang sangat berharga bagi setiap individu atau kelompok. Apabila informasi tersebut berhasil didapatkan oleh pihak tertentu secara *illegal* maka akan dapat menimbulkan kerugian. Karena itu, perlu diterapkan suatu cara untuk menjamin keamanan dan legalitas dari pengiriman dan penerimaan informasi.

Semua sistem komunikasi yang ada pada masa sekarang, baik untuk keperluan data, suara, atau multimedia, dituntut untuk menyediakan kemampuan mengacak dalam proses transmisi untuk menghindari pencurian informasi. Tuntutan keamanan ini menyebabkan berkembangnya jenis-jenis algoritma yang digunakan dalam proses pengkodean dengan tujuan menciptakan suatu sistem komunikasi yang aman. Untuk menjaga informasi berupa percakapan atau data penting, salah satu cara yang dilakukan adalah dengan metode kriptografi.

Kriptografi dapat diartikan sebagai suatu metode untuk menyamarkan informasi sehingga tidak mudah diketahui atau dibaca selain pengirim dan penerima yang dituju. Kriptografi telah diterapkan pada banyak hal yang memerlukan tingkat keamanan tinggi untuk pengiriman informasi dalam sistem komunikasi.

Seiring perkembangan teknologi sistem komunikasi, informasi yang dikirimkan pada saluran memiliki karakteristik yang beragam. Sehingga algoritma yang digunakan untuk keperluan keamanan informasi semakin berkembang sesuai dengan karakteristik sistem yang digunakan.

Salah satu jenis algoritma yang dikembangkan dalam komunikasi adalah A5. Algoritma ini dirancang untuk mengamankan transmisi data dalam sistem GSM. Terdapat 3 jenis algoritma A5 yaitu A5/1, A5/2, dan A5/3.

Dalam tugas akhir ini, akan dilakukan perancangan dan implementasi dari algoritma A5/1 pada FPGA dimana proses enkripsi dan dekripsi dibatasi hanya untuk satu arah untuk mengetahui parameter-parameter pada *core* sistem.

1.2 Tujuan

Tujuan dari perancangan sistem yang dilakukan adalah :

1. Melakukan perancangan algoritma A5/1 dengan menggunakan bahasa pemrograman *VHSIC Hardware Description Language* (VHDL).
2. Melakukan *synthesis* dan *implement* terhadap sistem yang dirancang.
3. Mengimplementasikan hasil perancangan kedalam perangkat *Field Programmable Gate Array* (FPGA).
4. Melakukan analisa terhadap kinerja sistem.

1.3 Perumusan Masalah

Permasalahan yang akan dipecahkan dalam tugas akhir ini:

1. Pemodelan algoritma A5/1 dengan menggunakan bahasa pemrograman *VHSIC Hardware Description Language* (VHDL).
2. Jumlah *resource* yang digunakan dalam pengimplementasian pada FPGA.
3. Performansi hasil perancangan dan implementasi pada bagian enkripsi dan deskripsi.

1.4 Batasan Masalah

Pembahasan yang dilakukan dalam tugas akhir ini dibatasi pada:

1. Sistem yang dirancang adalah bagian *stream cipher* dengan menerapkan aturan-aturan sesuai dengan yang terdapat pada algoritma A5/1.
2. Perancangan dilakukan pada bagian enkripsi dan deskripsi.
3. Perancangan dilakukan dengan menggunakan bahasa pemrograman VHDL.
4. Implementasi dilakukan dengan menggunakan FPGA Virtex-4 seri XC4VLX25-10SF363C sebagai devais sasaran.
5. Simulasi dan implementasi menggunakan nilai konstan sebagai kunci.
6. Masukan yang digunakan berbentuk data yang dibangkitkan pada FPGA.
7. Perancangan tidak membahas tentang *smart card* yang diterapkan pada sistem GSM.

1.5 Metodologi

Metode yang dilakukan dalam penyusunan tugas akhir ini adalah:

1. Studi literatur

   Studi literatur mengenai hal-hal yang berhubungan dengan pembahasan algoritma A5/1 dan bahasa pemrograman *VHSIC Hardware Description Language* (VHDL) yang digunakan sebagai bahan referensi.

2. Perancangan dan simulasi

   Perancangan dan simulasi dari tugas akhir ini dilakukan dengan menggunakan software Aldec Active-HDL 3.5.

3. Implementasi

   Implementasi dilakukan pada *board* FPGA Virtex-4 seri XC4VLX25-10SF363C dan kemudian dilakukan pengujian serta analisis kinerja sistem.

1.6 Sistematika Pembahasan

Pembahasan pada perancangan ini akan dibagi menjadi 5 (lima) bab, dengan urutan 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 algoritma kriptografi A5/1 dan penerapannya. Bab ini difokuskan pada teori-teori dasar yang terdapat pada pada mekanisme, kriptografi, algoritma A5/1, dan pengantar dari perangkat yang digunakan.

BAB III : PERANCANGAN SISTEM

Bab ini akan membahas tentang alur perancangan enkripsi dan dekripsi algoritma A5/1 dengan menggunakan *software* VHDL (*Very High Speed Integrated Circuit Hardware Description Language*), dan deskripsi tentang sistem dan sub-sistem yang dirancang.

BAB IV : IMPLEMENTASI DAN ANALISIS

Bab ini menjelaskan tentang pengujian yang dilakukan terhadap sistem kriptografi A5/1 dan menganalisis hasil implementasi tersebut.

BAB V : PENUTUP

Bab ini berisi kesimpulan dan saran dari hasil-hasil yang diperoleh pada perancangan yang telah dilaksanakan dan mengemukakan saran-saran yang berguna bagi pengembangan sistem kedepannya.