# BAB I
# PENDAHULUAN

## 1.1. Latar Belakang

Dunia teknologi sekarang ini semakin berkembang. Pada teknologi khususnya *hardware* mengalami perkembangan yang begitu pesat. Salah satu contoh perkembangan tersebut adalah sebuah *hardware* yang bisa melakukan proses enkripsi dan dekripsi sekaligus. Dimana pengertian enkripsi merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaannya. Pesan asli atau yang disebut *plaintext* diubah menjadi kode-kode yang tidak dapat dimengerti atau biasa disebut *ciphertext*. Sedangkan dekripsi merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya.

Dalam hal ini, *hardware* yang menunjang adalah *hardware* berbasis FPGA. FPGA adalah singkatan dari *Field-Programmable Gate Array*. FPGA adalah komponen terpadu elektronika yang terbuat dari semikonduktor dan dirancang untuk dapat diprogram secara berulang-ulang oleh pengguna. FPGA diprogram dengan menggunakan bahasa *Hardware Description Language* (HDL). FPGA dapat melakukan proses logika dan matematika sesuai dengan *Verilog* yang ditanamkan.[1]

Dalam penelitian dikembangkan implementasi algoritma *stream cipher* Grain-128 pada FPGA Altera Cyclone IV yang dapat mengenkripsi pesan tersebut agar tetap terjaga keamanan dan kerahasiaannya dan sekaligus juga dapat melakukan proses dekripsi agar pesan tersebut bisa diterima dan dibaca oleh pihak yang berwenang. Kemudian nantinya akan dibandingkan performansi dari implentasi algoritma tersebut dengan algoritma berorientasi *hardware* lainnya sesuai dengan aspek pengujian.

## 1.2. Rumusan Masalah

Rumusan masalah dalam penelitian yang berjudul Prototipe Sistem Enkripsi dan Dekripsi Berbasis FPGA Menggunakan Algoritma Stream Cipher Grain-128 adalah seperti yang dijelaskan di bawah ini :

1. Kurangnya sistem keamanan dalam penyebaran informasi.
2. Banyaknya algoritma kriptografi berorientasi pada *hardware* yang bisa digunakan pada sistem keamanan.

## 1.3. Tujuan

Pada penelitian yang berjudul Prototipe Sistem Enkripsi dan Dekripsi Berbasis FPGA Menggunakan Algoritma Stream Cipher Grain-128, bertujuan untuk:

1. Merancang prototipe IC dan diimplementasi algoritma *stream cipher* yang bisa melakukan proses kriptografi.
2. Merancang algoritma *stream cipher* Grain-128 dengan bahasa pemrograman Verilog dan diimplementasikan pada FPGA Altera Cyclone IV.

## 1.4. Batasan Masalah

Batasan masalah pada penelitian berjudul Prototipe Sistem Enkripsi dan Dekripsi Berbasis FPGA Menggunakan Algoritma Stream Cipher Garian-128, sebagai berikut:

1. Algoritma kriptografi yang digunakan adalah algoritma *stream cipher* Grain-128.
2. Prototipe IC yang digunakan adalah FPGA Altera Cyclone IV.
3. Perancangan yang dilakukan adalah proses enkripsi dan dekripsi tanpa kompresi.
4. Desain penelitian ini dilakukan pada RTL dan gate level, tidak sampai layout level.

5. Pada simulasi dan implementasi, data inputan terpanjang adalah sepanjang 64 karakter.

## 1.5 Metodologi Penyelesaian

1. Studi Literature

   Studi literatur adalah metodolgi yang bertujuan untuk mendapatkan gambaran teori tentang penelitian yang telah dilakukan sebelumnya dan bagaimana pengerjaan penelitian tersebut, kemudian dibandingkan dengan penelitian yang akan kita lakukan. Hal tersebut dapat diperoleh melalui berbagai sumber, seperti internet dan juga jurnal atau paper yang berkaitan dengan algoritma kriptografi *stream cipher*.

2. Analisis

   Analisis yang dilakukan dalam penelitian ini adalah menganalisa proses enkripsi dan dekripsi, waktu proses enkripsi dan dekripsi, *avalanche effect, clock,* dan *area* yang dihasilkan oleh algoritma *stream cipher* Grain-128 yang diimplementasikan pada FPGA.

3. Perancangan

   Setelah menganalisa batasan masalah, maka akan dilakukan implementasi algoritma *stream cipher* Grain-128 pada FPGA Altera Cyclone IV agar bisa melakukan proses kriptografi.

4. Implementasi

   Pada tahap implementasi, algoritma *stream cipher* Grain-128 akan langsung diimplementasikan pada FPGA Altera Cyclone IV. Sehingga FPGA tersebut bisa melakukan proses enkripsi dan dekripsi sekaligus. Kemudian akan dianalisa algoritma *stream cipher* Grain-128 pada FPGA Altera Cyclone IV.

5. Pengujian

   Pada tahap pengujian akan dilakukan serangkaian pengujian hasil implementasi dari algoritma *stream cipher* Grain-128 pada FPGA Altera Cyclone IV. Parameter yang diuji.

## 1.6 Sistematika Penelitian

Sistematika penulisan Tugas Akhir ini dibagi kedalam beberapa BAB yang disusun secara sistematis yang terdiri dari :

**BAB I. PENDAHULUAN**

Bab ini berisi tentang latar belakang, rumusan masalah, tujuan masalah, batasan masalah, hipotesis dan sistematika penulisan.

**BAB II. DASAR TEORI**

Bab ini berisi tentang teori-teori dasar tentang kriptografi, algoritma kriptografi Grain-128.

**BAB III. PERANCANGAN SISTEM**

Bab ini berisi tentang dekripsi sistem kriptografi, perancangan sitem dan skenario pengujian.

**BAB IV. IMPLEMENTASI DAN PENGUJIAN**

Bab ini berisi tentang implementasi sistem dan pengujian yang dilakukan.

**BAB V. KESIMPULAN DAN SARAN**

Bab ini berisi tentang kesimpulan dari penelitian yang telah dilakukan dan saran untuk penelitian selanjutnya.