BAB I
PENDAHULUAN

1.1 Latar Belakang

Ilmu tentang teknologi komunikasi dan informasi sudah dikenal sejak jaman dahulu, bahkan dari zaman prasejarah orang orang sudah melakukan kegiatan komunikasi walaupun hanya melakukan komunikasi hanya dengan gerakan atau isyarat untuk menyampaikan informasi dengan orang lain, dan jika membutuhkan jarak bisa melakukan komunikasi dengan cara menyampaikannya menggunakan media pengantar surat untuk disampaikan ke tujuan, walaupun belum tentu pesan tersebut akan sampai tepat waktu karena belum ada nya alat untuk melakukan komunikasi langsung jarak jauh.

Semakin berkembangnya teknologi komunikasi dan informasi, informasi semakin dimudahkan dengan adanya media telepon hingga internet yang semakin cepat dalam melakukan komunikasi antar manusia, maupun informasi penting ataupun tidak. Disamping itu juga berkembang nya teknologi informasi banyak juga yang melakukan pemantauan informasi secara sembunyi tanpa di ketahui pihak pengirim atau biasa di sebut penyadapan informasi oleh orang yang membutuhkan infomasi tersebut untuk kepentingan pribadi atau orang lain.

Kriptografi pada awalnya merupakan ilmu yang mempelajari penyembunyian pesan. Namun, seiring berkembangnya teknologi, kriptografi ini juga berkembang, perkembangan teknologi ini dapat dilihat dengan adanya internet yang menghubungkan komputer satu sama lain. Dengan adanya perkembangan ini kriptografi sangat dibutuhkan untuk keamanan data yang dikirim kepada komputer lain.

Kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan dan keutuhan

data. Ada empat tujuan utama dari kriptografi. Kerahasiaan (*confidentiality*) di mana kriptografi digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah disandi. Kerahasiaan dijaga dengan melakukan enkripsi (penyandian). Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak.

Fungsi kriptografi yang lain adalah autentikasi yang berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui jaringan harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain. Non-repudiation adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman dengan kata lain, terciptanya suatu informasi oleh yang mengirimkan.

Kriptografi juga dibagi atas dua: kriptografi klasik dan kriptografi modern. Yang masing-masing memiliki algoritma tersendiri. Algoritma RSA merupakan algoritma yang dikembangkan pada kriptografi modern. Algoritma ini bersifat asimetrik di mana kunci dari masing-masing algoritma ini dibangkitkan dengan menggunakan pembangkit bilangan acak dan dalam proses enkripsi dan dekripsinya menggunakan kunci yang berbeda.

Semakin berkembang pesatnya suatu teknik kriptografi pada setiap pengamanan teknologi komunikasi dan informasi dibutuhkanya sebuah pengamanan sistem informasi dan komunikasi dalam segi keefektifan salah satunya yaitu kecepatan dalam melakukan proses enkripsi dan dekripsi dari sebuah keamanan informasi dan komunikasi yaitu menggunakan kecepatan processor yang dapat komputasi secara paralel.

Komputasi paralel adalah salah satu teknik melakukan komputasi secara bersamaan dengan memanfaatkan beberapa komputer secara bersamaan. proses ini umumnya dilakukan saat kapasitas data yang diproses sangat besar, baik karena harus mengolah data dalam jumlah besar ataupun karena tuntutan proses komputasi yang banyak.

1.2 Perumusan Masalah

Konsentrasi dari penelitian ini adalah untuk mengetahui perbandingan performa algoritma *RSA* setelah di paralel kan dengan *CPU* dan *GPU* dengan menggunakan data sebagai bahan pengujian nya :

1. Bagaimana menghasilkan kunci publik dan kunci private di *RSA* dengan menggunakan komputasi paralel.
2. Bagaimana cara mengimplementasikan algoritma *RSA* dengan komputasi paralel.
3. Bagaimana cara memproses data secara paralel di algoritma *RSA*.
4. Melihat *core* yang terpakai baik menggunakan *CPU* atau *GPU* sudah paralel menggunakan profiling atau sistem monitor.

1.3 Tujuan

Tujuan dalam pembuatan Tugas Akhir ini adalah seperti yang dijelaskan di bawah ini:

1. Implementasi algoritma *RSA* pada sistem komputasi paralel dari *CPU* dan *GPU*.
2. Proses kerja dari algoritma *RSA* dalam melakukan proses enkripsi, dekripsi data dan pembangkitan kunci pada sistem komputasi paralel dari *CPU* dan *GPU*.
3. Menganalisa perbandingan performa dari waktu dan beban.

1.4 Batasan Masalah

Batasan masalah pada tugas akhir ini seperti yang dijelaskan di bawah ini :

1. Program ini hanya berjalan pada sistem operasi Linux.
2. Data yang digunakan hanya plain teks.

3. Panjang kunci yang di gunakan pada *RSA* tidak melebihi 512 bit.
4. Program ini hanya membahas tentang pengukuran performa proses kunci, enkripsi dan dekripsi setelah di paralel dengan *CPU* atau *GPU.*
5. Pengujian menggunakan personal desktop dengan kartu grafis nvidia tanpa menggunakan *SLI* dan *CPU* intel 4 *core.*

1.5 Metode Penelitian

Metode yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Studi Literatur

   Bertujuan untuk mengumpulkan, mempelajari dan memahami materi-materi dasar dan literatur-literatur yang berkaitan dengan *GPU,Cuda paralel*, *CPU*, *Openmp Paralel*, Algoritma RSA dan materi-materi yang digunakan dalam penelitian ini yang bersumber dari berbagai sumber pustaka berupa karya ilmiah, jurnal, *paper*, maupun media elektronik.

2. Analisis dan Perancangan Kebutuhan Sistem

   Merancang sistem yang dibuat, yaitu Enkripsi dan dekripsi data yang menggunakan algoritma RSA yang akan di implementasikan secara paralel pada *GPU* yang menggunakan *Cuda* Paralel dan *CPU* yg menggunakan *Openmp*.

3. Implementasi Sistem

   Pada tahap implemetasi ini, program yg dapat menghasilkan kunci publik dan kunci private yang akan digunakan untuk enkripsi dan dekripsi menggunakan algoritma RSA akan di implementasi menggunakan *Openmp* Paralel untuk menjalankan *multithread* pada *CPU* sedangkan perbandingannya menggunakan *Cuda* Paralel untuk menjalankan *multithread* pada *GPU.*

4. Pengujian Sistem

   Pada tahap pengujian sistem ini dilakukan pengujian terhadap sistem yang telah dibangun. Hal yang diujikan antara lain yaitu pengujian proses *thread* dan *core* yg berjalan saat mengeksekusi enksipsi maupun dekripsi menggunakan sistem monitor pada ubuntu dan pengujian

resource yang berjalan pada saat mengeksekusi enkripsi maupun dekripsi menggunakan *nvidia profiler*.

5. Analisis Hasil Pengujian

   Analisa dari pengujian ini berdasarkan kemampuan sebuah *CPU* dan *GPU* yg berjalan secara paralel dalam mengeksekusi sebuah algoritma *RSA*.

6. Penyusunan Laporan Tugas Akhir

   Menyusun laporan penelitian tugas akhir sebagai syarat sidang penelitian.

1.6 Sistematik Penulisan

Penulisan Tugas Akhir ini disusun berdasarkan sistematika sebagai berikut:

BAB I PENDAHULUAN

Pada bab ini berisi tentang latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, metode penelitian dan sistematika penelitian.

BAB II DASAR TEORI

Pada Bab ini berisi penjelasan tentang Perangkat yang digunakan yaitu *Desktop PC* yg di dukung kartu grafis nvidia dan *intel cpu*, dan menjelaskan tentang Cuda C dan C programming beserta arsitekturnya dan tentang cara kerja komputasi paralel pada *GPU* dan *CPU*.

BAB III PERANCANGAN DAN IMPLEMENTASI SISTEM

Pada bab ini berisi tentang perancangan sistem, kebutuhan sistem, implementasi *RSA* pada *Openmp* pada *CPU* dan *GPU* dari segi perangkat keras maupun kode pemrograman serta.

BAB IV PENGUJIAN DAN ANALISIS

Pada bab ini pengujian dan analisis yang dilakukan pada penelitian ini adalah menguji dan menganalisa proses *thread* dan *core* yg berjalan saat mengeksekusi enksipsi maupun dekripsi menggunakan sistem monitor pada

ubuntu dan pengujian dan analisa proses *grid* dan *block* yang berjalan pada saat mengeksekusi enkripsi maupun dekripsi menggunakan *nvidia profiler*.

BAB V KESIMPULAN DAN SARAN

Pada bab ini disampaikan kesimpulan dari penelitian ini dan saran saran untuk penelitian selanjutnya yang merujuk pada penelitian ini.