BAB I
PENDAHULUAN

1.1 Latar Belakang

Dewasa ini kemanan informasi menjadi sebuah permasalahan penting. Terdapat berbagai cara untuk mengamankan sebuah informasi salah satu caranya menggunakan kriptografi. Pada teknik kriptografi *plaintext* atau teks pesan asli dilakukan pengacakan dengan aturan tertentu sehingga menghasilkan *ciphertext* atau pesan yang sudah berubah, sehingga tidak bisa dibaca oleh orang yang tidak berhak menerima pesan tersebut. Untuk membaca kembali *ciphertext* tersebut di butuhkan *key* atau aturan yang digunakan untuk mengubah kembali *ciphertext* menjadi *plaintext* agar bisa dibaca (Arifin 2009). Salah satu algoritma kriptografi yang bagus saat ini dan sering digunakan pada beberapa protokol kemanan adalah algoritma Rivest Shamir Aldeman (RSA) (Frederico 2003).

Algoritma Rivest Shamir Aldeman (RSA) ditemukan pada tahun 1997 oleh Ron Rivest, Adi Shamir, dan Len Aldeman dari *Massachusetts Institute of Technology* (MIT). Pada algoritma RSA kunci untuk melakukan enkripsi pesan dengan kunci untuk dekripsi pesan berbeda. Letak kemanan pada algoritma ini yaitu pada pembuatan kunci menggunakan angka prima serta tingginya pemfaktoran yang di lakukan sehingga sulit untuk dilakukan *bruteforce* dan juga sulitnya untuk mendapatkan kunci untuk mengubah data yang ada (Arifin, Zainal 2009). Walaupun Algoritma RSA merupakan salah satu algoritma kriptografi yang aman tetapi algoritma ini memiliki kelemahan yaitu waktu pemrosesanya yang memerlukan waktu yang relatif lebih lama dibandingkan algoritma kriptografi lainnya. Menurut Sachdeva, Abishek dan Mahajan, Prerna 2013 menyebutkan pada jurnalnya yang berjudul *A Study of Encryption Algorithms AES, DES, and RSA for Security* menyebutkan bahwa algoritma RSA tidak cocok untuk perangkat kecil seperti perangkat mobile, karena algoritma asimetris

memiliki 1000 kali waktu komputasi lebih lama dibandingkan algoritma kriptografi simetris.

Komputasi paralel adalah sebuah teknologi pengeksekusian proses pengoperasian aritmatik atau logik yang sejenis secara bersama-sama. Sebuah masalah komputasi yang kompleks akan dipecah menjadi bagian-bagian yang kecil dan sederhana dan dijalankan dibeberapa prosesor secara bersamaan sehingga keseluruhan proses dapat diselesaikan dengan lebih cepat (Barney & Lawrence Livermore National Laboratory 2016) . Salah penerapan komputasi paralel adalah pada *cluster* komputer. *Cluster* komputer adalah kumpulan beberapa komputer yang terpusat pada suatu geografis yang dapat beroperasi secara mandiri. *Cluster beowulf* adalah sebuah tipe *cluster* komputer yang menggunakan komponen – komponen komputer *consumer-grade* dengan harga yang murah, seperti contoh adalah komponen komputer yang sudah bekas pakai. Sehingga untuk melakukan komputasi paralel dengan tipe *cluster* b*eowulf* dapat menghemat biaya untuk pembuatan sebuah komputer dalam melakukan komputasi paralel (Sterling et al. 1998).

Adapun penelitian yang serupa adalah penelitian oleh Deguang Le dkk tahun 2014 dengan judul "*Parallel AES Algorithm for Fast Data Encryption on GPU",* hasil penelitian tersebut algoritma paralel AES menghasilkan 7x lebih cepat daripada penggunaan algoritma AES pada sebuah komputer. Penelitian oleh Vandan Pendli dkk tahun 2016 dengan judul *"Improvising performance of Advanced Encryption Standard Algorithm",* hasil penelitian tersebut adalah penggunaan pemerosesan paralel pada algoritma AES dapat mempercepat 40-45% dari pada penggunaan pemerosesan serial. Penelitian oleh Tejal Mahajan dkk dengan judul *"Enhancing Blowfish File Encryption Algorithm through Parallel Computing on GPU"* tahun 2015 hasil penelitian tersebut adalah penggunaan pemerosesan paralel pada algoritma blowfish dapat menurunkan waktu proses enkripsi dan dekripsi. Penggunaan GPU memberikan peforma yang lebih baik dibandingkan implementasian menggunakan CPU. Serta penelitian oleh Abu Asaduzzaman dkk dengan judul *"A Promising Parallel Algorithm to Manage the*

RSA Decryption Complexity", hasil penelitian tersebut adalah pengguna workstation memiliki performa yang lebih baik dari pada PC dan Laptop karena workstation memiliki jumlah core lebih banyak dibandingkan dengan PC dan Laptop dimana dapat menangani lebih banyak thread sehingga terjadi pengingkatan kinerja RSA dalam proses dekripsi dan sebagian dari proses enkripsi.

Berdasarkan permasalahan dan beberapa teori pendukung yang telah diuraikan sebelumnya maka dilakukanlah sebulah penelitian dengan judul "**Implementasi Pemrosesan Paralel Pada Algoritma Rivest Shamir Aldeman (RSA) Menggunakan Cluster Beowulf".** Diharapkan dari penelitian ini dapat mengatasi masalah waktu komputasi lama pada algoritma RSA dengan menggunakan komputasi paralel dengan metode .

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan diatas maka adapun rumusan masalah pada penelitian ini antara lain:

1. Bagaimana cara membuat komputasi paralel pada *cluster beowulf*?
2. Bagaimana cara membuat aplikasi kriptografi menggunakan algoritma RSA pada sistem komputer paralel ?
3. Bagaimana pengaruh pengaruh waktu proses aplikasi setelah melakukan enkripsi dan dekripsi menggunakan komputasi paralel pada cluster komputer?

1.3 Batasan Masalah

Agar hasil penelitian optimal maka dibutuhkan ruang lingkup untuk membatasi cangkupan penelitian. Adapun batasan masalah sebgai berikut :

1. Pada penelitian ini jumlah komputer yang digunakan untuk komputasi paralel adalah 6 buah unit komputer sebagai node dengan 1 buah komputer sebagai *head node*.
2. Data yang digunakan pada proses kriptografi berupa text

1.4 Tujuan Penelitian

Adapun tujuan penelitian ini adalah :

1. Menerapkan metode komputasi paralel menggunakan *Cluster Beowulf* pada proses kriptografi menggunakan algoritma Rivest Shamir Aldeman (RSA).
2. Mengetahui kemampuan komputasi paralel menggunakan *Cluster Beowulf* yang telah di buat pada program kriptografi Rivest Shamir Aldeman (RSA), adapun kriteria yang digunakan dalam proses prngukuran antaralain :
    a. Mengukur waktu kecepatan proses enkripsi dan dekripsi pesan secara serial pada satu buah node.
    b. Mengukur waktu kecepatan proses enkripsi dan dekripsi pesan secara paralel dengan jumlah node yang digunakan berbeda-beda pada setiap percobaan.

1.5 Sistematika Penulisan

Penulisan penelitian ini akan terdiri dari 6 Bab yang masing-masing bab dirincikan sebagai berikut :

Bab I Pendahuluan

Berisi tentang deskripsi umum penelitian yang mencakup latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, dan sistematika penulisan

Bab II Landasan Teori

Berisi penjelasan mengenai penjelasan teori-teori komputasi paralel, jaringan, algoritma kriptografi Rivest Shamir Aldeman (RSA), *ClusterBeowulf* dan beberapa penelitian yang dijadikan kajian pustaka dalam penyusunan penelitian ini.

Bab III Metodologi Penelitian

Berisi tentang metodologi penelitian, identifikasi masalah, analisa algoritma, dan alat pendukung penelitian

Bab IV Analisa dan Pembahasan

Berisi tentang analisa algortima RSA dan analisa proses komputasi paralel menggunakan .

Bab V Implementasi dan Pengujian

Berisi implementasi komputasi paralel dan algoritma enkripsi Rivest Shamir Aldeman (RSA) menggunakan .

Bab VI Penutup

Berisi kesimpulan hasil penelitian dan saran demi kemajuan penelitian ini