BAB I

PENDAHULUAN

1.1 Latar Belakang

Sistem komputer terdistribusi merupakan sebuah sistem yang memungkinkan aplikasi komputer beroperasi secara terintegrasi pada lebih dari satu lingkungan yang terpisah secara fisis. Ciri khas sistem komputer terdistribusi adalah heterogenitas dalam berbagai hal: perangkat keras, sistem operasi, dan bahasa pemrograman (Lukito Eddi Nugroho, 2004).

Sistem komputer terdistribusi terdiri dari dua tipe aplikasi yaitu komputasi paralel (*parallel computing*) dan komputasi terdistribusi (*distributed computing*). Dalam komputasi paralel, suatu proses dibagi-bagi menjadi beberapa proses yang saling bebas. Proses ini didistribusikan dan dieksekusi pada banyak komputer untuk mendapatkan performa yang tinggi. Sedangkan dalam komputasi terdistribusi, kumpulan komputer yang terkoneksi dalam suatu jaringan bekerja secara kolektif untuk menyelesaikan suatu tugas terdistribusi (*distributed job*) (Iis Haryono, 2004).

Java, adalah sebuah bahasa pemrograman yang tidak hanya digunakan untuk membangun sebuah sistem *standalone*,

tetapi juga bisa digunakan untuk membangun sebuah sistem terdistribusi. Selain *Java CORBA*, *Java* juga memiliki teknologi eksklusif yang digunakan untuk membangun sebuah sistem terdistribusi yaitu *Java Remote Method Invocation (Java RMI).*

Berbeda dengan *CORBA* yang mampu bekerja dengan berbagai macam bahasa pemrograman, *Java RMI* hanya akan berjalan optimal untuk aplikasi berskala *enterprise* yang murni berbasis *Java*. Namun demikian, *Java RMI* terintegrasi penuh dengan model obyek yang dikembangkan oleh *Java* dan mudah untuk dikembangkan.

Kriptografi Hill Cipher adalah suatu bentuk algoritma kriptografi yang menerapkan operasi matriks pada proses enkripsi maupun dekripsinya. Idenya adalah menentukan sebuah matriks *A* berukuran *n* x *n*, kemudian plainteks dipecah menjadi matriks kolom *n* x 1. Setiap matriks kolom tersebut dikalikan dengan matriks *A.* Hasil perkalian yang diperoleh selanjutnya dikonversikan kembali ke dalam bentuk abjad menggunakan aturan modulo aritmatika. Hasil inilah yang dijadikan cipherteks. Sedangkan untuk dapat membaca cipherteks, penerima harus mengkonversi cipherteks ke plainteks dengan algoritma yang sama tetapi matriks yang digunakan adalah A^{-1} (invers) (Dony Ariyus, 2004).

Oleh karena proses enkripsi dan dekripsi kriptografi Hill Cipher merupakan sebuah proses mandiri yang tidak tergantung dengan proses lain, maka algoritma kriptografi ini dapat diselesaikan menggunakan komputasi terdistribusi. Keuntungan menggunakan sistem terdistribusi pada algoritma Hill Cipher adalah waktu proses eksekusi yang semakin singkat karena proses enkripsi dan dekripsi kriptografi Hill Cipher didistribusikan ke banyak mesin untuk dieksekusi.

1.2 Rumusan Masalah

Permasalahan skripsi ini adalah bagaimana mendistribusikan proses enkripsi dan dekripsi di kriptografi Hill Cipher ke beberapa mesin terpisah untuk dieksekusi selanjutnya dikembalikan ke mesin pengirim dalam bentuk yang diinginkan. Plainteks atau cipherteks awalnya dibagi sesuai sejumlah *server* kemudian dikirim bersama dengan kunci untuk dieksekusi di mesin *server* sebelum dikembalikan ke dalam bentuk cipherteks atau plainteks ke komputer pengirim. Pada proses dekripsi, kunci matriks diinvers terlebih dahulu sebelum dikirim ke *server*. Untuk menghubungkan antara mesin pengirim dan mesin *server* digunakan teknologi *Java*, yaitu *Java RMI* yang ditanam di *client* dan di *server*.

1.3 Ruang Lingkup

Kasus yang akan diambil pada skripsi ini berupa permasalahan kriptografi Hill Cipher, yaitu:

a. Sistem komputer terdistribusi dibangun menggunakan *Java RMI* dengan sebuah komputer sebagai komputer *client* dan dua komputer sebagai komputer *server*.
b. Kunci yang digunakan adalah matriks berbesaran maksimal 50 x 50.
c. Data yang dienkripsi dan didekripsi berupa teks.

1.4 Tujuan Penulisan

Penelitian ini bertujuan mengimplementasikan sistem komputer terdistribusi menggunakan teknologi *Java RMI* untuk membantu menyelesaikan permasalahan kriptografi Hill Cipher khususnya kasus kriptografi Hill Cipher dengan karakter plainteks dan cipherteks yang panjang serta kunci berupa matriks berordo besar.