BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Socket programming merupakan teknik menghubungkan node *client* dan *server* melalui jaringan untuk berkomunikasi satu sama lain. Untuk menghubungkan *client* dan *server* setiap *node* harus diberikan alamat *socket* yang unik (sama) sebagai indentifikasi. Alamat *socket* terdiri dari alamat IP dan nomor *port*. Alamat IP dapat menggunakan alamat dari *Local Area Network* (LAN) maupun alamat dari jaringan internet. Sedangkan nomor *port* dibutuhkan untuk identifikasi antar node yang hendak berhubungan. Suatu proses yang hendak berkomunikasi dengan proses lain lewat mekanisme *socket* harus mengikatkan dirinya dengan salah satu port pada computer [1]. *Socket programming* dapat diterapkan pada *file transfer*, tetapi *socket programming* pada dasarnya tidak dilengkapi dengan keamanan yang mempuni, sehingga rentan terjadi penyadapan, maupun pencurian data sangat rentan terhadap penyadapan, dan rentan terjadinya kebocoran informasi oleh pihak yang tidak berhak [2]. Maka dari itu dibutuhkan *secure file transfer*, dimana *secure file transfer* merupakan sebuah metode *data sharing* yang menggunakan protokol keamanan dan enkripsi untuk mengamankan data yang dikirim. Salah satu protokol keamanan tersebut adalah metode kriptografi [3].

Terdapat beberapa metode kriptografi diantaranya AES-256, DES, dan IDEA. Ketiga metode kriptografi tersebut merupakan algoritma simetris yang memiliki keunggunalan pada waktu komputasi yang lebih baik, dibandingkan dengan kriptografi asimetris [4], selain itu metode kriptografi AES-256 dan IDEA merupakan metode yang dikembangkan untuk menggantikan metode DES yang dianggap telah usai karena faktor keamanan [5]. Disamping itu ketiga algoritma memiliki kemampuan untuk melakukan enkripsi file, sehingga file yang dikirimkan akan menjadi lebih aman. Kriptografi merupakan sebuah ilmu yang mempelajari keamanan (kerahasiaan) dari suatu tulisan. Teknik Kriptografi diyakini mampu menangani masalah keamanan data atau informasi karena selain menggunakan bahasa pemrograman komputer, kriptografi juga

menggunakan rumus-rumus matematika mulai dari rumus yang sederhana hingga yang kompleks. Terdapat dua konsep pada kriptografi, yaitu enkripsi dan dekripsi. Enkripsi merupakan proses di mana data atau informasi diubah dengan metode tertentu ke dalam format yang tidak dikenali atau dikaburkan isi informasinya. Sementara itu, dekripsi mengubah bentuk yang tidak diketahui kembali ke data aslinya [6].

Penelitian oleh Meko pada tahun 2018 membuktikan adanya perbedaan waktu proses enkripsi dan dekripsi serta ukuran file dari ke-empat algoritma enkripsi yaitu DES, AES, IDEA, dan Blowfish. Dimana pada penelitian ini menunjukkan algoritma AES memiliki kecepatan paling tinggi dalam proses enkripsi maupun dekripsi data kemudian diikutin oleh Blowfish, DES, kemudian IDEA [7]. Sementara itu, penelitian Simpony pada tahun 2017 mengatakan bahwa port yang terbuka pada *socket programming* merupakan celah keamanan yang dapat dimanfaatkan oleh pihak yang memiliki niat buruk, sehingga perlu ditambahkan tindak pengamanan pada sistemnya [8].

Untuk mengatasi hal tersebut maka akan dilakukan percobaan penerapan algoritma pada *socket programming* serta akan dilakukan perbandingan performa dari masing-masing algoritma. Sehingga dapat diketahui algoritma mana yang memiliki performa paling baik diantara ketiganya. Berdasarkan permasalahan tersebut penulis mengambil topik *"**Comparasion Analysis of The Performance of Application of AES-256, DES, and IDEA Algorithms in Secure File Transfer using Socket Programming"***.

1.2 RUMUSAN MASALAH

Berdasarkan latar belakang yang diuraikan diatas, dapat disimpulkan rumusan masalah yaitu:

1. Bagaimana merancang *secure file transfer* menggunakan *socket programming* dengan algoritma AES-256, DES, dan IDEA ?
2. Bagaimana analisis kinerja algoritma AES-256, DES, dan IDEA berdasarkan kecepatan proses enkripsi dan dekripsi *file* ?

1.3 BATASAN MASALAH

Batasan masalah dari penelitian ini adalah:

1. Penelitian ini dilakukan pada jaringan *virtual* menggunakan satu *server*, satu *client*, dan satu router os.
2. Penelitian ini menggunakan 7 tipe file yaitu : *Microsoft Office Word Document* (.docx), PDF *Document* (.pdf), *Text Document* (.txt), WinRAR *archieve* (.rar), JPG *File* (.jpg), MP3 *File* (.mp3), dan MP4 *File* (.mp4).
3. Penelitian ini hanya mengukur waktu dan kecepatan yang diperlukan untuk melakukan enkripsi dan dekripsi serta membandingkan ukuran file hasil enkripsi dari masing-masing algoritma.
4. Penelitian ini menggunakan algoritma AES-256, DES, dan IDEA.

1.4 TUJUAN

Adapun tujuan yang hendak dicapai dalam penelitian ini adalah :

1. Mengetahui proses kerja dari *secure file transfer* menggunakan *socket programming* dengan algoritma AES-256, DES, dan IDEA bekerja.
2. Mengetahui waktu dan kecepatan yang diperlukan dari ketiga algoritma (AES-256, DES, IDEA) dalam melakukan enkripsi dan dekripsi.
3. Mengetahui salah satu algoritma yang memilki performa paling baik diantara ketiganya (AES-256, DES, IDEA)

1.5 MANFAAT

Dari penelitian yang dikerjakan, terdapat beberapa manfaat yaitu :

1. Memberikan gambaran mengenai *secure file transfer* dengan menggunakan algoritma AES-256, DES, dan IDEA pada *socket programming.*
2. Mengetahui performa dari masing-masing algoritma (AES 256, DES, dan IDEA) saat diterapkan pada *secure file transfer* menggunakan *socket programming.*
3. Memberikan pengetahuan mengenai pentingnya keamanan pada *secure file transfer.*

1.6 SISTEMATIKA PENULISAN

Sistematika penulisan penelitian ini dibagi menjadi 5 bab sebagai berikut:

BAB 1: PENDAHULUAN

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

BAB 2 : DASAR TEORI

Bab ini membahas tentang literatur yang berhubungan dengan materi yang berhubungan dengan pengerjaan skripsi.

BAB 3 : METODE PENELITIAN

Bab ini mencakup pembahasan mengenai metode penelitian yang diambil, alur penelitian, skenario pengujian, perancangan *system*.

BAB 4 : HASIL DAN PEMBAHASAN

Bab ini berisi hasil dari pengujian mengenai parameter yang digunakan untuk kebutuhan analisi perbandingan.

BAB 5 : PENUTUP

Bab ini berisi kesimpulan dari penelitian skripsi beserta saran untuk pengembangan penelitian selanjutnya.