BAB I
PENDAHULUAN

1.1 Latar belakang

Perkembangan teknologi belakangan ini tumbuh dengan sangat pesat. Perkembangan teknologi ini banyak melahirkan keuntungan yang mempermudah kelangsungan hidup manusia. Tapi seiring dengan berkembangnya teknologi, muncul pula masalah-masalah baru, mulai dari privasi, keamanan, hingga hak cipta. Hal inilah yang sering dimanfaatkan oknum-oknum yang tidak bertanggung jawab untuk melakukan hal-hal negatif bahkan tindak kejahatan. Mudahnya penyebaran informasi palsu, pembobolan akun bank, dan maraknya pembajakan merupakan contoh sisi gelap dari perkembangan teknologi. Hal ini membuat para pengembang TI memutar otak untuk menangani masalah-masalah tersebut. Yang tidak pernah habis menjadi pembicaraan adalah pengembangan sistem keamanan.

Banyak cara yang dilakukan oleh pengembang TI dalam urusan keamanan, salah satunya menggunakan metode kriptografi. Kriptografi adalah sebuah ilmu yang mempelajari tentang penyembunyian huruf atau tulisan sehingga membuat tulisan tersebut tidak dapat dimengerti atau dibaca, proses ini disebut dengan enkripsi. Untuk membacanya kembali, dilakukan proses dekripsi atau pengembalian ke tulisan aslinya. Hal ini banyak dimanfaatkan untuk menyamarkan dokumen-dokumen penting sehingga hanya orang-orang tertentu yang dapat membuka dan membacanya. Selain itu membuat dokumen tersebut aman apabila jatuh ke pihak lain. Seiring dengan perkembangannya, kriptografi mulai dimanfaatkan untuk menyamarkan *file-file* non dokumen, seperti, gambar, video maupun suara.

Tapi bagaimana jika *file* hasil enkripsi dalam kriptografi ini dikirim melalui sebuah jaringan? Bagaimana jika *file* yang di kirim jatuh ke tangan kriptanalisis? Dalam tugas akhir ini penulis mencoba membuat sebuah perangkat lunak untuk melakukan pengiriman *file* hasil enkripsi dengan aman. Selain itu penulis juga akan membuat sebuah jaringan FTP *public* sebagai media transfer *file*. Algoritma yang dicoba untuk diimplementasikan oleh penulis adalah kriptografi RSA. Berdasarkan

hasil penelitian sebelumnya, kriptografi RSA telah dimanfaatkan dalam pengiriman pesan, seperti layanan *Chat*[7] dan SMS. Disini Penulis mencoba mengimplementasikan kriptografi RSA pada sebuah *file*. Dari tugas Akhir ini diharapkan dapat menjadi solusi untuk keamanan pada pengiriman *file.*

1.2 Tujuan dan Manfaat

Tujuan dan manfaat dari tugas akhir tentang pengaplikasian algoritma kriptografi RSA pada transfer data ini adalah sebagai berikut :

1. Membuat perangkat lunak berbasis FTP *Client*.
2. Implementasi algoritma RSA pada proses enkripsi dan dekripsi *file.*
3. Menjaga keutuhan data pada *file* hasil ekripsi.
4. Menerapkan algoritma RSA untuk meningkatkan keamanan komunikasi FTP standar.

1.3 Rumusan Masalah

Adapun rumusan masalah pada tugas akhir ini antara lain :

1. Bagaimana membuat perangkat lunak berbasis FTP *Client*?
2. Bagaimana proses enkripsi dan dekripsi *file* menggunakan kriptografi RSA?
3. Bagaimana keutuhan data pada *file* setelah dienkripsi?
4. Bagaimana analisis penerapan algoritma RSA dalam meningkatkan keamanan komunikasi FTP standar*?*

1.4 Batasan Masalah

Agar pembahasan tidak menyimpang dan meluas, maka masalah akan dibatasi sebagai berikut :

1. Kriptografi yang digunakan adalah algoritma RSA.
2. Proses enkripsi dan dekripsi dijalankan pada CPU.
3. Aplikasi Transfer *file* berbasis *Client-Server.*
4. Jaringan FTP *public* menggunakan *Filezilla Server*.
5. Jaringan yang digunakan adalah LAN (*Local Area Network*).

6. Tidak ada *folder* dalam *Database Server*.
7. Tidak dilakukan proses *brute-force* pada *file* hasil enkripsi.
8. JVM maksimal pada setiap percobaan adalah 2048 *megabytes*.

1.5 Metodologi

Metode pendekatan yang digunakan pada tugas akhir ini adalah

1. Study literature

   Mencari buku pedoman atau e-*book* yang berkaitan dengan yang akan dirancang pada tugas akhir ini, juga sebagai dasar teori BAB II.
2. Perancangan Algoritma

   Melakukan percobaan penerapan algoritma pada *file* yang akan dienkripsi dan membuat *file* kembali seperti semula pada saat dekripsi.
3. Analisis

   Melakukan analisa performansi dari segi keamanan, waktu dan *resource* memori yang dipakai.

1.6 Sistematika Penulisan

Sistematika penulisan laporan tugas akhir ini disusun sesuai dengan rencana berikut.

BAB I Pendahuluan

Bab ini menjelaskan latar belakang, tujuan dan manfaat, rumusan masalah, batasan masalah, metodologi penelitian, dan sistematika penulisan tugas akhir.

BAB II Dasar Teori

Bab ini menjelaskan teori dasar yang mendukung dalam perancangan program FTP *Client* dengan algoritma RSA.

BAB III Rancangan Sistem

Bab ini menjelaskan bagaimana membangun sistem berdasarkan kebutuhan general, beserta UML diagramnya.

BAB IV Analisis Hasil Implementasi

Bab ini menjelaskan performansi algoritma RSA dan skenario program yang dilakukan.

BAB V Kesimpulan dan Saran

Bab ini berisi kesimpulan yang dapat ditarik dari perancangan sistem dan skenario yang telah dilakukan serta saran bagi para pembaca untuk pengembangan tugas akhir ini.