BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi memberi pengaruh besar bagi segala aspek kehidupan. Begitu banyak manfaat yang dapat diimplementasikan dalam kehidupan. Teknologi saat ini telah memberikan kemudahan dalam penyampaian suatu informasi. Pada umumnya untuk menyampaikan suatu informasi melalui surat atau berkomunikasi melalui telepon, namun sekarang proses pengiriman informasi berupa *file*, dapat dilakukan melalui email.

Seiring dengan berkembangnya teknologi yang memberikan kemudahan, khususnya komputer, juga membawa dampak *negative* dalam penyebaran *file* itu sendiri. Hal ini dapat disebabkan karena adanya suatu serangan dari pihak yang tidak berhak untuk mendapatkan isi *file* tersebut dengan menggunakan berbagai cara, salah satunya adalah *sniffing*, sehingga dapat merugikan pemilik *file* tersebut.

Dalam upaya meningkatkan keamanan *file* tersebut, terdapat beberapa teknik, diantaranya adalah enkripsi *file*. Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara maupun organisasi-organisasi tertentu. Enkripsi *file* berfungsi untuk mengacak isi dari *file* atau *privacy* pada *file*, sehingga informasi yang ditransfer tidak mudah dikenali oleh pihak manapun, memberikan integritas sehingga memastikan informasi yang dienkripsi tidak mengalami perubahan.

1.2 Rumusan Masalah

Terdapat beberapa perumusan masalah yang akan dibahas dalam proyek akhir ini, yaitu sebagai berikut :

1. Bagaimana menerapkan algoritma RSA untuk mengenkripsi suatu *file*.
2. Bagaimana solusi untuk keamanan data melakukan transfer *file* secara aman.

1.3 Tujuan

Merancang perangkat lunak aplikasi yang dapat melakukan enkripsi pada suatu *file*, beserta dekripsi-nya, sehingga transfer *file* dapat dilakukan secara aman.

1.4 Batasan Masalah

Adapun batasan-batasan masalah dalam Proyek Akhir ini adalah sebagai berikut.

1. Dalam pengujian, data yang diuji dalam bentuk (*file*: *.doc dan .*.xls)
2. Proses *cryptography* menggunakan mekansime satu arah berbasis pada proses asimetrik.
3. Aplikasi yang dibangun bersifat *client-server* dan melibatkan *Server* FTP.
4. Tidak mengulas lebih jauh perihal DNS-*server* dan TCP/IP.
5. Dalam pengujian FTP bersifat searah, yakni proses *downloading* saja.
6. Skenario penyerangan berupa *interception.*
7. Yang dimaksud dengan aman ialah penyerang tidak dapat membaca *file* yang di-*transfer*.

1.5 Metodelogi Penelitian

a. Tahap Studi Literatur

Studi literatur, yaitu dengan mencari informasi dan referensi dari buku, jurnal, artikel maupun *internet* yang berkaitan dengan topik. Dalam mengerjakan proyek akhir ini terdapat teknik dalam pengumpulan data antara lain adalah:

1. Pencarian referensi dan sumber-sumber yang berhubungan dengan *enkripsi* dan pengimplementasiannya.
2. Pencarian referensi dan sumber-sumber yang berhubungan dengan kriptografi.

b. Tahap Perancangan Sistem dan Implementasi

1. Pengumpulan kebutuhan

   Mendefinisikan format seluruh perangkat lunak, meng*id*entifikasikan semua kebutuhan, dan garis besar sistem yang akan dibuat.
2. Pembuatan aplikasi enkripsi

   Membuat aplikasi menggunakan suatu perangkat lunak dan membuatnya dengan menggunakan algorima RSA.
3. Pembuatan jaringan *transfer file*

   Merancang dan membuat suatu jaringan dan media untuk transfer *file*.

c. Tahap Analisis dan Pengujian

Sistem akan dilakukan pengujian terhadap aplikasi enkripsi data yang telah dibuat, dengan tujuan untuk mengetahui integritas data, terjadi perubahan atau tidaknya pada pembuatan aplikasi Algoritma RSA untuk perlindungan data pada *Server* FTP.

d. Tahap Pembuatan Laporan

Pada tahap ini, akan dilakukan penyusunan laporan akhir dan pengumpulan dokumentasi dengan mengikuti ka*id*ah penulisan yang benar

dan sesuai dengan ketentuan-ketentuan atau sistematika yang telah ditetapkan oleh Politeknik Telkom Bandung.

e. Kesimpulan dan Saran

Pada bagian ini menjelaskan tentang kesimpulan dan saran berdasarkan hasil dari analisis, implementasi dan pengujian. Kesimpulan merujuk pada tujuan yang ingin dicapai dalam proyek akhir ini apakah sudah memenuhi atau belum memenuhi syarat. Pada bagian sar an berisi tinjauan terhadap penelitian untuk perbaikan maupun pengembangan lebih lanjut terhadap Algoritma RSA untuk perlindungan data pada *Server* FTP dalam penelitian proyek akhir yang telah dikerjakan.