BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam proses komunikasi data, walaupun data telah dienkripsi, terdapat kemungkinan data tersebut dapat diketahui oleh orang lain. Salah satu kemungkinan tersebut adalah orang tersebut menyadap media komunikasi yang digunakan oleh kedua orang yang sedang berkomunikasi tersebut. Hal inilah yang disebut dengan *man-in-the-middle attack*. Dalam keadaan ini, orang yang menyadap berada di antara kedua orang yang sedang berkomunikasi. Data-data yang dikirimkan oleh orang yang sedang berkomunikasi satu sama lain selalu melalui orang yang menyadap tersebut, sehingga orang yang menyadap tersebut dapat mengetahui semua informasi yang dikirimkan satu sama lain. Keadaan ini muncul karena kedua orang yang sedang berkomunikasi tersebut tidak dapat mem-verifikasi status dari orang yang berkomunikasi dengannya tersebut, dengan mengambil asumsi bahwa proses penyadapan tersebut tidak menyebabkan gangguan dalam jaringan.

Masalah *man-in-the-middle attack* ini dapat dicegah dengan menggunakan *interlock protocol*. *Interlock protocol* ini diciptakan oleh *Ron Rivest* dan *Adi Shamir*. Algoritma inti dari protokol ini

yaitu protokol ini mengirimkan 2 bagian pesan terenkripsi. Bagian pertama dapat berupa hasil dari fungsi *hash* satu arah (*one way hash function*) dari pesan tersebut dan bagian kedua berupa pesan terenkripsi itu sendiri. Hal ini menyebabkan orang yang menyadap tersebut tidak dapat mendekripsi pesan pertama dengan menggunakan kunci privatnya. Ia hanya dapat membuat sebuah pesan baru dan mengirimkannya kepada orang yang akan menerima pesan tersebut.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, maka dapat dirumuskan sebagai berikut :

1. Membuat implementasi *Man-In-The-Middle Attack* dengan menggunakan bantuan animasi gambar.
2. Menjelaskan proses kerja dari *interlock protocol* dengan menggunakan bantuan animasi gambar.
3. Membuat algoritma dari sistem kriptografi kunci publik metode RSA.
4. Merancang *interface* dari perangkat lunak simulasi.

1.3 Ruang Lingkup

Ruang lingkup penelitian ini :

1. Proses kerja dari perangkat lunak ditampilkan dalam bentuk biner.

2. Proses enkripsi dan dekripsi pesan menggunakan algoritma RSA.
3. Fungsi *hash* satu arah yang digunakan adalah fungsi SHA-1.
4. Nilai-nilai yang dibutuhkan dalam algoritma RSA dan fungsi SHA-1 akan dihasilkan secara acak oleh komputer.

1.4 Tujuan Penelitian

Tujuan dibuatnya karya tulis ini adalah :

1. Merancang suatu perangkat lunak simulasi yang mampu untuk menjelaskan proses kerja dari *man-in-the-middle attack* dan pencegahan dengan menggunakan *interlock protocol*.