BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

RSA (Rivest-Shamir-Adleman) telah banyak dipilih dalam berbagai aplikasi internet dan browser semenjak dipublikasikan sebagai aplikasi paten. Algoritma yang dinamai berdasarkan tiga orang penemunya ini juga terpasang dalam perangkat lunak yang dijual secara komersial dan direncanakan akan digunakan pada banyak perangkat lunak lainnya. Selain itu dikabarkan lembaga-lembaga pemerintahan, perusahaan bidang bisnis dan ekonomi serta institusi pendidikan juga telah memanfaatkan secara internal seperti untuk keamanan komunikasi maupun perlindungan data. Dalam proses komunikasi data, walaupun data telah dienkripsi, terdapat kemungkinan data tersebut dapat diketahui oleh orang lain. Salah satu kemungkinannya 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 akan selalu melalui orang yang menyadap tersebut, sehingga sang penyadap dapat mengetahui semua informasi yang dikirimkan. Keadaan ini muncul karena kedua orang yang sedang berkomunikasi tidak dapat mem-verifikasi status dari orang yang berkomunikasi dengannya tersebut, dengan

mengambil asumsi bahwa proses penyadapan tersebut tidak menyebabkan gangguan dalam jaringan.

Problema *man-in-the-middle-attack* ini dapat diilustrasikan sebagai berikut, misalkan Alice dan Bob sedang berkomunikasi dan Mallory ingin menyadapnya. Ketika Alice mengirimkan kunci publiknya kepada Bob, Mallory dapat menangkap kunci ini dan mengirimkan kunci publiknya sendiri kepada Bob. Kemudian, ketika Bob mengirimkan kunci publiknya kepada Alice, Mallory juga dapat menangkap kunci tersebut dan mengirimkan kunci publiknya sendiri kepada Alice. Ketika Alice mengirimkan pesan kepada Bob yang dienkripsi dengan menggunakan kunci publik Bob, Mallory dapat menangkapnya. Karena pesan tersebut dienkripsi dengan menggunakan kunci publik Mallory, maka Mallory dapat mendekripsikan pesan tersebut dengan menggunakan kunci privatnya dan kemudian dienkripsi kembali dengan menggunakan kunci publik dari Bob dan mengirimkannya kepada Bob. Hal yang sama juga terjadi ketika Bob mengirimkan pesan kepada Alice. Mallory dapat mengetahui semua pesan yang dikirimkan oleh Bob dan Alice tersebut. Problema *man-in-the-middle-attack* ini dapat dicegah dengan menggunakan *interlock protocol*. Diciptakan oleh Ron Rivest dan Adi Shamir. Dua ilmuwan dari MIT (Massachusetts Institute of Technology) yang juga terlibat dalam pembuatan RSA. Algoritma inti dari *interlock protocol* 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. Dari uraian diatas maka akan dirancang interface yang mensimulasikan *man-in-the-middle-attack* pada komunikasi yang melibatkan 2 orang dan 1 orang lagi berlaku sebagai penyadap. Dan metode pencegahannya dengan *interlock protocol* yang akan menggambarkan penanggulangan yang nantinya dapat membuat seorang penyadap terdeteksi keberadaanya ketika memodifikasi pesan.

1.2 Rumusan Masalah

1. Bagaimana proses pembangkitan kunci pada algoritma RSA ?
2. Apakah *interlock protocol* mampu mencegah *man-in-the-middle-attack* pada komunikasi jaringan sekaligus mendeteksinya?
3. Bagaimana merancang software yang dapat mengimplementasikan simulasi tentang permasalahan yang tertulis di No.2?

1.3 Batasan Masalah

Berdasarkan latar belakang dan rumusan masalah diatas, maka perlu adanya batasan masalah agar diperoleh lingkup pembahasan tertentu sebagai berikut:

1. Aplikasi yang akan didesain memakai enkripsi dan dekripsi jenis kunci asimetris dengan algoritma kriptografi RSA dan nilai dari parameter-

parameter yang dibutuhkan dapat di-*input* secara manual atau dihasilkan secara acak oleh komputer

2. Fungsi *hash* satu arah yang digunakan adalah fungsi SHA-1.
3. Tidak mencakup penjelasan yang mendetail tentang teori bilangan dan aritmetika modulo serta faktor prima.
4. Proses kerja yang akan ditampilkan :
    a. Proses terjadinya *man-in-the-middle-attack*.
    b. Proses solusi mengatasi *man-in-the-middle-attack* dengan menggunakan *interlock protocol*.
5. *Interlock protocol* yang dibahas memiliki 2 alternatif berikut :
    a. Alternatif pertama, yaitu *message* terenkripsi dibagi menjadi 2 bagian yang sama besar.
    b. Alternatif kedua, yaitu pecahan pertama berupa nilai *hash* dari *one way hash function* dari *message* dan pecahan kedua berupa *message* terenkripsi.
6. Panjang pesan (*message*) dibatasi maksimal 50 karakter.

1.4 Tujuan Penelitian

Dalam penelitian ini ada beberapa tujuan yang ingin dicapai, yaitu:

1. Sebagai syarat memperoleh gelar sarjana pada Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.

2. Menerapkan ilmu dari mata kuliah kriptografi dan pemrograman yang menjadi salah satu matakuliah wajib.
3. Perangkat lunak dapat digunakan sebagai fasilitas pendukung dalam proses belajar mengajar, terutama untuk mata kuliah Kriptografi.

1.5 Manfaat Penelitian

Dengan penelitian ini nantinya diharapkan dapat memberikan manfaat sebagai berikut:

1. Membantu pemahaman proses terjadinya *man-in-the-middle attack* dan proses pencegahannya dengan menggunakan *interlock protocol*.
2. Memperlihatkan simulasi yang mampu untuk menjelaskan proses kerja dari *man-in-the-middle-attack* ini, dan proses solusi dengan menggunakan *interlock protocol*.

1.6 Metode Penelitian

1. Metode Tinjauan Pustaka (Studi Literatur)

   Melakukan pencarian dan pengumpulan data-data referensi mengenai teori dan konsep yang mendukung dan berguna untuk penulisan antara lain artikel dan jurnal tentang kriptografi, enkripsi-dekripsi RSA, *man-in-the-middle-attack*, *interlock protocol* dan pemrograman.
2. Analisis dan Perancangan Sistem

Tahap selanjutnya analisis terhadap kebutuhan sistem yang yang akan dibuat, lalu algoritma-algoritma enkripsi dan dekripsi dan teori-teori pendukung lainnya yang akan diperlukan dalam perancangan program serta mempelajari proses kerja dari problema *man-in-the-middle-attack* ini dan proses pencegahannya dengan menggunakan *interlock protocol*.

3. Implementasi dan Uji Coba Sistem

Membangun perangkat lunak dari hasil analisa ditahap sebelumnya dan untuk memastikan kelayakan sistem maka dilakukan pengujjian sebagai evaluasi program tersebut pada kesesuaianya terhadap tujuan.

1.7 Sistematika Penulisan

BAB I PENDAHULUAN

Pembahasan dalam BAB I meliputi latar belakang masalah, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian dan sistematika penulisan.

BAB II LANDASAN TEORI

Mencakup teori-teori yang relevan dan berkaitan dengan judul Perancangan Simulasi Man In The Middle Attack Pada Algoritma Kriptografi RSA Dan Pencegahannya Dengan Interlock Protocol; yaitu : hal-hal spesifik tentang algoritma RSA, serangan pada kriptografi dan protokolnya juga sedikit tentang beberapa teori-teori matematika.

BAB III ANALISIS DAN PERANCANGAN

Bab ini membahas langkah-langkah analisis program aplikasi dan perancangan tampilan serta desain protitipe dan sebagai dasar untuk bab selanjutnya.

BAB IV IMPLEMENTASI DAN PEMBAHASAN

Pada bab ini membahas rencana implementasi pengujian aplikasi, analisis mengenai hasil pengujian setelah aplikasi dijalankan.

BAB V PENUTUP

Bab V yang merupakan bab terakhir, didalamnya berisi kesimpulan dari keseluruhan pembahasan skripsi, beserta saran untuk pengembangan.

1.8 Jadwal Penelitian

Tabel 1.2 Tabel Rencana Kegiatan

NO	Kegiatan	Target Output	Juli 2012	
			1	2
1.	Studi Literatur.	Menentukan permasalan (latar belakang, rumusan, batasan dan tujuan masalah.		
		Mengumpulkan landasan teori permasalahan.		

2.	Perancangan Sistem.	Menganalisa masalah perancangan.		
		Membuat perancangan sistem.		
3.	Uji Coba Rancangan.	Simulasi uji coba rancangan.		
		Analisa untuk optimalisasi rancangan.		
4.	Implementasi	Mempelajari masalah implementasi sistem.		
		Implementasi rancangan ke dalam sistem.		
5.	Uji Coba Sistem.	Simulasi uji coba sistem.		
		Analisa sistem.		
6.	Penyusunan Laporan	Dokumentasi penelitian secara lengkap.		
		Penulisan laporan skripsi.		