BAB I

PENDAHULUAN

1.1 Latar Belakang

Internet telah memperkenalkan bentuk komunikasi baru yang telah mengubah paradigma semua orang. Seperti yang telah diketahui, melalui internet bisa mencari informasi yang dibutuhkan, melakukan transaksi, berkomunikasi dan lain-lain.

Penggunaan internet dari tahun ke tahun mengalami pertumbuhan yang sangat pesat. Di Indonesia, rata-rata penggunaan internet di kota urban masih 30 – 50 persen. Di tahun 2011 mengalami peningkatan dengan angka kisaran 40 – 50 persen. Jumlah pengguna internet di Indonesia pada tahun 2011 mencapai 55 juta orang, meningkat ditahun sebelumnya di angka 42 juta. Sebagai contoh, penggunaan *instant messenger* menjadi suatu bentuk komunikasi yang paling banyak digunakan.

Instant Messenger atau yang lebih dikenal dengan IM adalah suatu layanan komunikasi yang memungkinkan orang dapat melakukan percakapan (*chat)* privat dengan orang lain secara *real time* melalui internet. *Instant messenger* hadir dengan beberapa fitur yang telah umum disediakan diantaranya :

1. *Chat*

   Dapat melakukan percakapan dengan kontak baik berupa teks maupun berupa suara atau video.

2. *Buddy List & Online Information*

   Menyimpan daftar kontak yang telah didaftarkan sebagai daftar teman serta dapat mengetahui siapa saja dari kontak teman tersebut yang sedang *online* atau tersedia untuk melakukan percakapan.

3. *Conference*

   Selain dapat melakukan percakapan yang bersifat privat, juga dapat melakukan percakapan dengan orang banyak apabila masuk ke dalam *room chat* tertentu.

4. *File Transfer*

   Memungkinkan untuk dapat berkirim file dengan orang lain.

Karena beberapa fitur diatas, *instant messenger* merupakan aplikasi yang paling banyak digunakan saat ini. Tercatat penggunaan aplikasi *instant messenger* Windows Live Messenger mencapai 10 juta pengguna di Asia Tenggara dan 510.000 pengguna di Indonesia. Angka tersebut belum ditambah dengan aplikasi-aplikasi *instant messenger* lainnya telah banyak dipakai.

Dari data tersebut mencerminkan bahwa penggunaan teknologi informasi cukup pesat. Seiring dengan berkembangnya penggunaan *instant messenger* maka aspek keamanan menjadi salah satu hal yang sangat penting. Terutama pada pesan-pesan yang dikirimkan yang bersifat pribadi (*private*) yang memungkinkan orang lain tidak bisa membacanya.

Namun kebanyakan *instant messenger* dibangun bukan berdasarkan aspek keamanan yang menjadi pertimbangan utama melainkan mengedepankan aspek-aspek bisnis atau *profit* yang menguntungkan perusahaan tertentu.

Symantec Enterprise Security (2006:7) menyatakan bahwa, *instant messenger* rentan terhadap serangan :

1. *Eavesdroppingo*
   Mengingat bahwa kebanyakan sistem *instant messenger* tidak mengenkripsi lalu lintas jaringan maka pihak ketiga berpotensi besar untuk menguping pembicaraan yang sedang dilakukan dan umumnya menggunakan sebuah paket *sniffer* dan teknologi yang sejenis.
2. *Account Hijacking*
   Kebanyakan sistem *instant messenger* rentan terhadap pembajakan akun dan panyamaran. Sebagaimana yang dialami oleh Butet Kertaradjasa seorang pelawak dan pemain teater yang kehilangan uang Rp. 2,5 juta karena akun YM nya dibajak oleh orang yang tidak bertangguna jawab.
3. *Data Access and Modification*
   Seperti kebanyakan perangkat lunak yang terhubung ke internet, *instant messenger* bisa memiliki *bug* yang dapat menjadi celah penyerang untuk dapat mengakses data dan memodifikasinya.
4. *Worm and Blended Threats*
   Platform *instant messenger* juga memungkinkan untuk dapat menyebarnya cacing (*worm*) dan ancaman lainnya yang juga berbahaya.

Berdasarkan hasil analisis dari Symantec Enterprise Security, *eavesdroppingo* atau yang lebih dikenal dengan penyadapan menempati urutan pertama dalam kasus penyerangan terhadap *instant messenger*. Hal ini terjadi karena *instant messenger* yang banyak digunakan tidak mengekripsi pesan yang dikirimkan sehingga memudahkan pihak ketiga untuk membaca pesan tersebut.

Arie Karhendana (2006:14) melakukan pengujian keamanan paket data yang ditransmisikan selama proses komunikasi berlangsung terhadap program *instant messenger* yang populer saat ini yaitu Yahoo Messenger dan Windows Live Messenger. Hasil pengujian tersebut menunjukan bahwa layanan Yahoo Messenger dan Windows Live Messenger sama sekali tidak aman karena data yang ditransmisikan selama percakapan berlangsung berupa *plaintext* dan dapat dengan mudah disadap.

Oleh karena semakin banyaknya pengguna *instant messenger* ditambah dengan perlunya sistem keamanan yang menjaga privasi pesan dari setiap pengguna, maka kebutuhan akan enkripsi data menjadi suatu hal yang sangat penting.

Metode Kriptografi merupakan salah satu metode yang digunakan untuk meningkatkan keamanan data karena dapat melakukan proses enkripsi dan dekripsi. Kriptografi terbagi menjadi tiga bagian berdasarkan kunci yang digunakannya, yaitu :

1. Algoritma Simetris (menggunakan satu kunci untuk enkripsi dan dekripsinya)

2. Algoritma Asimetris (menggunakan kunci yang berbeda untuk enkripsi dan dekripsinya)
3. Hash Function

Ada beberapa algoritma enkripsi yang sudah terbuka untuk dipelajari seperti DES, AES, TwoFish, BlowFish, RC2, RC4, RC5, RSA (*Rivest, Shamir, Adleman*) dan lain-lain. Penelitian ini membahas implementasi algoritma enkripsi RSA untuk mengamankan pesan *instant messenger*.

RSA adalah metode enkripsi yang dikembangkan oleh Ron Rivest, Adi Shamir dan Leonard Adleman yang diperkenalkan pada tahun 1977 dan dipatenkan oleh MIT.

Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi bilangan faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci private. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang efisien, maka selama itu pula keamanan algoritma RSA tetap terjamin.

Oleh karena kelebihan algoritma RSA dalam mengenkripsi pesan maka penulis mencoba untuk mengimplementasikan algoritma tersebut dalam sebuah aplikasi *instant messenger* sehingga didapat sebuah aplikasi *instant messenger* yang dapat mengamankan pesan diantara sesama pengguna nya kelak.

1.2 Identifikasi dan Rumusan Masalah

Berdasarkan uraian latar belakang di atas, penulis mengidentifikasi dan merumuskan masalah mengenai beberapa hal yang berhubungan dengan masalah komunikasi data menggunakan media transmisi *instant messenger*.

1.2.1 Identifikasi Masalah

Permasalahan yang ditemukan terkait pembahasan di atas diantaranya :

1. Rentan nya keamanan pesan pada aplikasi *instant messenger*.
2. *Eavesdroppingo* atau penyadapan menempati posisi pertama dalam kasus penyerangan terhadap *instant messenger* sehingga memungkinkan pihak ketiga mengetahui suatu pesan.

1.2.2 Rumusan Masalah

Menanggapi tahap identifikasi permasalahan diatas maka perlu dibuatkan rumusan masalah untuk mencari solusi dari permasalahan tersebut. Adapun rumusan masalah nya yaitu :

“ Bagaimana algoritma RSA dapat mengamankan pesan pada aplikasi *instant messenger* ? “.

1.3 Maksud dan Tujuan Penelitian

1.3.1 Maksud Penelitian

Untuk mengatasi permasalahan yang sudah dijabarkan diatas, maka penulis bermaksud membuat solusi dengan mengimplementasikan algoritma RSA pada aplikasi *instant messenger*.

1.3.2 Tujuan Penelitian

Adapun tujuan yang ingin dicapai dalam penelitian ini yaitu : Membuat sebuah aplikasi *instant messenger* dengan mengimplemtasikan algoritma RSA didalamnya sehingga diharapkan dapat menjaga privasi setiap pengguna nya.

1.4 Manfaat Penelitian

Pada prinsip nya, setiap penelitian pasti selalu mempunyai manfaat yang ingin dicapai. Begitu juga penelitian ini mudah-mudahan dapat memberikan manfaat yaitu:

1. Bagi Pengembangan Ilmu

   Untuk pengembangan ilmu pengetahuan khususnya tentang kriptografi yang dapat berjalan diaplikasi *instant messenger*. Sehingga dengan adanya penelitian ini diharapkan dapat menguntungkan berbagai pihak nantinya.

2. Bagi Peneliti Lain

   Hasil dari penelitian diharapkan dapat menjadi referensi kepada peneliti yang mengambil kajian yang sama atau kajian yang sejenis tentang implementasi algoritma RSA pada perangkat *instant messenger*.

3. Bagi Penulis

   Diharapkan penelitian ini dapat menambah wawasan, kualitas keilmuan baik teori maupun praktek dalam mengatasi permasalahan , khususnya pada kasus penyadapan pesan di *instant messenger*.

1.5 Batasan masalah

Supaya penelitian ini tidak menyimpang dari tujuan yang telah ditentukan, maka diperlukan batasan-batasan sehingga penelitian ini tetap fokus terahadap masalah-masalah yang akan dikaji. Adapun batasan-batasan tersebut diantanya :

1. Input berupa teks yang dapat dirubah ke dalam bentuk ASCII.
2. Tidak memuat simbol dan karakter khusus.
3. Tidak mendukung input berupa *audio.*

4. Tidak mendukung fasilitas *add friend, delete friend* dan *block friend*.
5. Tidak mendukung operasi *file transfer*.

1.6 Jadwal Kegiatan

Berikut adalah tabel pelaksanaan rencana kegiatan :

Tabel 1.1

Tabel Jadwal Kegiatan Penelitian

No	Kegiatan	Tahun 2012															
		Maret				April				Mei				Juni			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Pustaka																
2	Analisis Kebutuhan Sistem																
3	Perancangan Sistem																
	a. Pembuatan Rancangan *instant messenger*																
	b. Pembuatan Rancangan Antar Muka																

No		Kegiatan	Tahun 2012															
			Maret				April				Mei				Juni			
			1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	c.	Pembuatan Model																
	d.	Pengembangan Algoritma RSA																
4	Pembuatan Perangkat Lunak																	
	a.	Struktur Program																
	b.	Struktur Menu																
5	Pengujian Sistem																	
6	Evaluasi Sistem																	

Referensi

1. http://www.tdwclub.com/f33/survey-penerapan-teknologi-informasi-di-indonesia-901/ diakses tanggal 21 maret 2012
2. http://inet.detik.com/read/2009/11/17/114632/1243153/398/pengguna-windows-live-messenger-cuma-501000 diakses tanggal 21 maret 2012
3. Symantec Enterprise Security. (2002). *Securing Instant Messaging*
4. http://news.detik.com/read/2010/05/27/151629/1365210/10/percakapan-butet-dengan-pembajak-akun-ym-jajang-c-noer diakses tanggal 21 maret 2012]
5. Karhendana, Ari . *Keamanan pada Layanan Instant Messaging: Studi Kasus Yahoo Messenger, Windows Live Messenger, dan Google Talk*.
6. Henry, Dane . RSA: *Asymmetric Cryptography and Algorithm Analysis for a Secure Computing Environment* . Department of Computer Sciences, Mathematics, and Engineering Shepherd University