BAB I

PENDAHULUAN

1.1. Latar Belakang

Pada tahun 1970-an muncul sebuah alat atau media komunikasi yang bernama *Instant Messaging* (IM) yang diawali dengan adanya teknologi *Internet*. Berawal dari munculnya teknologi *Internet* , *Instant Messaging* memanfaatkan teknologi *Internet* ini sebagai media komunikasi jalur pengiriman pesan. *Instant Messaging* atau yang lebih dikenal dengan *Chatting* ini menutupi beberapa kendala tersebut, *Instant Messaging* ini dapat dikatakan lebih murah biayanya dikarenakan hanya membayar layanan koneksi internet yang saat ini telah murah dan mudah didapatkan, *Instant Messaging* ini dapat dikatakan lebih cepat dan *powerfull* dibandingkan dengan alat komunikasi lainnya karena dia bersfiat *real-time* dengan syarat memiliki koneksi *Internet* yang cepat dan baik.

Saat ini banyak vendor yang menyediakan layanan *Instant Messaging* yang diberikan secara gratis kepada setiap orang. Berikut beberapa contoh layanan *Instant Messaging* : Yahoo! Messenger, Blackberry Messenger, AIM, Google Talk, Skype, ICQ, dan masih banyak contoh lainnya. Yang membedakan antar vendor satu yang lainnya adalah layanan yang diberikan serta ketersediaan layanan yang diberikan serta port yang digunakan. Menurut SANS Institute (SANS Institute, 2003) pengguna *Instant Messaging* berdasarkan *IM-Client* terbesar pada saat itu mencapai 264 juta pengguna, dengan rincian AOL Instant Messaging (AIM) 100 juta pengguna, AOL ICQ's 122 juta pengguna dan Yahoo Messenger dengan 42 juta pengguna. Dan menurut Alex Taitague (Taitague, 2013) sebagai analis, saat ini perkembangan jumlah pengguna *Instant Messaging* hingga tahun 2013 mencapai 3,4 milyar pengguna.

Dengan semakin banyaknya pengguna *Instant Messaging* ini tak banyak orang yang tidak berkepentingan memanfaatkan kondisi ini untuk melakukan hal – hal yang tak seharusnya dilakukan seperti mencuri data/pesan yang dikirimkan melalui *Instant Messaging* . Menurut Declan McCullagh (Declan, 2008) yang ditulis dalam website News.cnet.com beberapa *Instant Messaging* yang sering digunakan pada saat ini biasanya hanya mengamankan pada saat login dan data pada saat masuk ke dalam server saja (*at rest*), mereka tidak tahu apa yang terjadi proses perjalanan pesan/data tersebut dikirimkan dari satu ke perangkat lain (*in motion*) aman tidaknya. Dengan mengetahui kondisi tersebut, ini sangat rentan sekali dengan pencurian data/pesan, belum lagi ditambah dengan orang dalam yang memiliki akses pada server sehingga dapat melihat seluruh isi pesan klien atau dapat menjual informasi tersebut kepada orang tidak berkepentingan.

Menurut SANS Institute (SANS Institute, 2003), salah satu yang membahayakan dari *Instant Messaging* adalah pencurian percakapan yang tidak disadari oleh beberapa pengguna dan dapat dimanfaatkan oleh beberapa orang untuk kepentingan dan maksud tertentu. Kondisi pencurian data/pesan melalui *Instant Messaging* ini dapat merugikan beberapa kliennya yang mana data tersebut sangatlah penting untuk *privacy* nya. Untuk menghindari pencurian data/pesan seperti itu dibutuhkan lah suatu sistem enkripsi yang langsung di enkripsi ketika data/pesan tersebut dikirimkan. Pengamanan ini sering disebut dengan pengamanan secara *in motion* , pengamanan seperti sangat penting agar data/pesan tak dapat dibaca oleh sembarang orang. Beberapa studi kasus telah membuktikan bahwa beberapa *Instant Messaging*, salah satunya adalah Yahoo Messenger itu tidak aman. Ini dibuktikan dengan menggunakan cara atau metode *Man-In-The-Middle* yang kemudian di *Capture* dengan menggunakan aplikasi Wireshark. Hasil Capture tersebut terlihat bahwa pesan yang dikirimkan dapat mudah terbaca begitu saja tanpa terenkripsi. Maka dari itu dibutuhkan sistem enkripsi untuk mengamankan pesan tersebut.

Salah satu cara untuk mengamankan *Instant Messaging* tersebut adalah dengan menerapkan sistem enkripsi pada *Instant Messaging* tersebut dengan menggunakan algoritma RSA. Menurut Rinaldi Munir (Munir, 2006), algoritma RSA merupakan algoritma kriptografi kunci-publik yang paling popular yang dibuat oleh 3 peneliti dari *MIT (Massachussets Institute of Technology}* pada tahun 1976, yaitu Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor – faktor prima. Menurut Evgeny (Evgeny, 2009) dalam makalahnya yang berjudul *The RSA Algorithm* pun menjelaskan bahwa Algoritma RSA memiliki keamanan yang lebih tinggi dari algoritma simetris namun membutuhkan waktu yang lama dalam pengerjaan prosesnya. Menurut Linda (Linda, 2011) dalam penelitiannya algoritma RSA dianggap lebih efisien dalam masalah ambiguitas hasil dekripsi dalam artian tidak banyak biaya komputasi dibandingkan dengan algoritma Rabin, selain itu dibandingkan dengan algoritma Rabin dan ElGamal, Algoritma RSA ini algoritma yang tidak terlalu sederhana dan tidak terlalu rumit sehingga algoritma RSA ini merupakan algoritma yang pas jika hendak mengimplementasikan algoritma kriptografi kunci publik.

Mayoritas pengguna *Instant Messaging* ini adalah para pengguna *smartphone* yang salah satunya adalah platform Android. Menurut Lisa Eadicicco (Lisa, 2012) dalam website Digital Trends mengatakan bahwa platform android saat ini merupakan platform mobile terpopuler dengan presentase sebagai berikut Android telah mengklaim pasar hingga 68,3 %, Apple 18,8% dan sisanya ada pada Blackberry 4,% dan Windows phone 2,6%. Jadi dalam penelitian ini, sistem enkripsi ini diterapkan pada *instant messaging* dengan menggunakan algoritma RSA pada platform android. Hal tersebut dilakukan agar data/pesan yang dikirimkan melalui *instant messaging* ini dapat terenkripsi dengan aman sehingga tidak mudah terbaca orang lain khususnya untuk pengguna Android .

1.2. Rumusan Masalah

Berdasarkan latar belakang di atas, maka yang menjadi rumusan adalah "Bagaimana menggunakan algoritma kriptografi RSA sebagai pengaman data berupa pesan pada *Instant Messaging"*, dengan rincian :

1. Bagaimana cara kerja perangkat lunak sistem enkripsi dengan menggunakan algoritma RSA bekerja mengamankan pesan pada *Instant Messaging* Yahoo Messenger yang diterapkan pada platform Android.
2. Bagaimana efektifitas dan akurasi sistem enkripsi *Instant Messaging* dengan menggunakan algoritma RSA pada platform Android.
3. Bagaimana perbandingan keamanan sebelum dan setelah diterapkan sistem enkripsi dengan menggunakan Algoritma RSA.

1.3. Tujuan Penelitian

Sejalan dengan permasalahan yang telah dirumuskan, maka tujuan yang ingin dicapai pada penelitian ini adalah :

1. Memberikan gambaran cara kerja perangkat lunak sistem enkripsi dengan menggunakan algoritma RSA bekerja mengamankan pesan pada *Instant Messaging* Yahoo Messenger yang diterapkan pada platform Android.
2. Bagaimana efektifitas dan akurasi sistem enkripsi *Instant Messaging* dengan menggunakan algoritma RSA pada platform Android.
3. Memberikan perbandingan keamanan sebelum dan setelah diterapkan sistem enkripsi dengan menggunakan Algoritma RSA

1.4. Batasan Masalah

Batasan masalah yang akan dikaji pada penelitian ini adalah:

1. Perangkat lunak yang dibuat adalah *Instant Messaging* pada platform Android.
2. *Instant Messaging* yang digunakan adalah Yahoo Messenger sebagai *Client-side*.
3. Sistem Enkripsi menggunakan algoritma RSA.
4. Panjang *bitlength* yang digunakan 1024 bit.

1.5. Manfaat Penelitian

Dari pembuatan skripsi ini diharapkan adanya manfaat penelitian ini adalah agar *Instant Messaging* memiliki keamanan yang lebih baik.

1.6. Metodologi Penelitian

Metodologi yang digunakan dalam penulisan skripsi ini adalah sebagai berikut :

1.6.1 Metode Pengumpulan Data

Metode pengumpulan data yang digunakan adalah studi pustaka. Pengumpulan data dengan cara mengumpulkan beberapa literature , *browsing* internet dan buku yang berkaitan dengan *Instant Messaging*, keamanan data, dan algoritma RSA.

1.6.2 Metode Pembuatan Perangkat Lunak

Metode analisis data yang digunakan dalam pembuatan perangkat lunak adalah *waterfall*, dengan rincian sebagai berikut :

1. Analisis

   Analisis dalam penelitian ini dimulai dengan menentukan keperluan dan batasan untuk aplikasi *Instant Messaging*, pengumpulan materi dari algoritma RSA , pemrograman android, dan cara kerja *Instant Messaging*.

2. Desain

Tahap lanjutan dari hasil analisis yang dituangkan dalam bentuk tampilan antarmuka sehingga dapat dimengerti oleh pengguna.

3. Coding

Tahap melakukan penambahan kode pemrograman dalam hal ini android, sehingga dapat menjalan seluruh fungsi yang diharapkan dalam pembuatan perangkat lunak *Instant Messaging* sesuai dengan desain antarmuka yang telah dikerjakan dari tahap sebelumnya.

4. Testing

Tahap melakukan pengujian terhadap perangkat lunak yang telah dibuat agar dapat berjalan sesuai dengan yang diinginkan.

1.7. Sistematika Penulisan

Dalam penyusunan skripsi ini, sistematika penulisan dibagi menjadi beberapa bab sebagai berikut :

BAB I PENDAHULUAN

Bab ini menguraikan tentang latar belakang masalah, rumusan masalah, maksud dan tujuan, batasan masalah, metode penelitian dan sistematika penulisan. Dalam hal ini menguraikan tentang masalah yang muncul dari penggunaan *Instant Messaging* dan bagaimana cara mengamankan data yang ada pada *Instant Messaging*.

BAB II TINJAUAN PUSTAKA

Bab ini memaparkan beberapa teori yang mendukung dalam pembuatan perangkat lunak seperti teori *Instant Messaging*, Kriptografi, Kriptografi Kunci

Publik, Sistem Enkripsi, Platform Android, Algoritma RSA dan Gambaran Aplikasi Sistem Enkripsi *Instant Messaging*.

BAB III METODOLOGI PENELITIAN

Bab ini merupakan penjabaran dari implementasi Algoritma RSA untuk Sistem Enkripsi *Instant Messaging*. Mencakup analisis, dan desain model sistem.

BAB IV IMPLEMENTASI

Pada bab ini akan dibahas secara mendalam hal-hal yang akan menjawab apa yang sudah dirumuskan dalam rumusan masalah. Dalam hal ini mengenai implementasi pembuatan perangkat lunak *Instant Messaging* yang telah dilengkapi sistem enkripsi secara detil termasuk tampilan antar muka dan pengujian perangkat lunak yang telah dibuat.

BAB V. KESIMPULAN DAN SARAN

Pada bab ini berisi tentang kesimpulan dari BAB IV dan saran yang diajukan agar dapat menjadi bahan pertimbangan untuk rekomendasi penelitian selanjutnya.