Double-Protection Secret Messaging

Melindungi Pesan dengan Perlindungan Ganda (*Lock* dan *Encryption*)

Cilvia Sianora Putri 13512027
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
cilvia.sianora@gmail.com

***Abstract*—Dalam zaman dahulu, orang menggunakan surat dan dikirimkan melalui pos untuk mengirimkan suatu pesan. Namun kini, orang berpindah menggunakan pesan instan untuk mengirimkan pesan. Selain waktunya yang cepat sampai, pesan instan juga memiliki biaya yang lebih murah. Akan tetapi, pesan instan yang biasa digunakan tidak aman untuk mengirimkan pesan yang bersifat rahasia.**

Keywords—double-protection; encryption; lock; message; pesan instan;

I. PENDAHULUAN

Manusia diciptakan sebagai makhluk sosial yang tidak bisa hidup sendiri, pasti membutuhkan orang lain. Untuk itu, manusia berkomunikasi satu sama lain dengan bertatap muka dan berbicara. Namun, hambatan terjadi jika manusia ingin berkomunikasi dengan manusia lain yang tidak terjangkau oleh suaranya. Akan tetapi, hal ini dapat ditangani dengan surat. Surat adalah alat komunikasi dimana si pengirim menuliskan pesan yang ingin disampaikan pada sebuah kertas dan mengirimkannya ke penerima melalui perantara.

Dalam masa kini, pertukaran pesan dapat dilakukan dengan mudah menggunakan pesan instan, tidak seperti dulu lagi yang harus menggunakan surat, dikirimkan melalui pos, dan menunggu berhari-hari untuk sampai. Pesan instan adalah suatu sistem pengiriman pesan dengan cepat melalui perantara berupa jaringan internet. Meskipun telah ada surat elektronik, teknologi pengiriman pesan instan ini menutupi kelemahan surel yang terkadang kurang cepat dan tidak dalam waktu nyata (*real-time*). Daya tarik dari pesan instan adalah waktu cepatnya dalam menyampaikan pesan ke pihak penerima. Berbagai macam pesan instan pun bermunculan dengan daya tariknya masing-masing. Pesan instan ini biasa digunakan untuk melakukan percakapan sehari-hari antar orang yang lokasinya berjauhan, seperti menanyakan tugas, mengobrol masalah hobi, dan lain-lain. Akan tetapi, pesan instan yang ada tidak aman untuk melakukan pertukaran pesan yang bersifat rahasia. Pesan yang dikirimkan akan langsung dapat dilihat oleh pihak penerima dalam bentuk *plaintext*, sehingga siapapun yang memiliki akses terhadap akun si penerima dapat juga melihat pesan tersebut. Oleh karena itu, dalam makalah ini akan dibahas aplikasi pesan instan yang cocok untuk melakukan pertukaran pesan yang bersifat rahasia.

II. DASAR TEORI

A. Pesan Instan

Dahulu kala, orang yang lokasinya berjauhan satu sama lain berkomunikasi menggunakan surat dan dengan perantara pos. Dengan semakin majunya teknologi, muncullah surel (surat elektronik) yang mengubah cara orang berkomunikasi dari cara konvensional untuk mengirimkan surat. Surel dikirimkan menggunakan perantara jaringan internet, sehingga waktu yang diperlukan untuk menyapaikan pesan jauh lebih lebih cepat daripada melalui pos. Biasanya surat yang melalui pos membutuhkan waktu berhari-hari untuk sampai, tetapi surel hanya membutuhkan waktu beberapa detik untuk sampai. Namun, penggunaan surel ini dirasa masih kurang karena cara berkomunikasinya tidak terasa sama seperti berbicara langsung dengan lawan bicaranya. Hal ini menjadi kelemahan surel yang tergolong kurang cepat dalam menyampaikan pesan dan tidak dalam waktu nyata (*real-time*). Oleh karena itu, muncullah pesan instan yang diciptakan untuk menutupi kelemahan surel tersebut.

Pesan instan adalah suatu sistem yang mendukung bentuk komunikasi secara langsung antara dua orang atau lebih menggunakan teks yang diketik dan dikirimkan melalui perantara jaringan internet. Kelebihan dari pesan instan ini adalah waktunya yang sangat cepat dalam menyampaikan pesan, sehingga terasa seperti dua orang berbicara langsung dengan bertatap muka, tetapi dalam bentuk teks. Pada mulanya, penggunaan pesan instan ini hanya dapat diakses melalui komputer, sehingga cukup merepotkan jika ingin menghubungi orang saat berada di luar rumah. Namun kini, pesan instan sudah dapat diakses melalui telepon genggam sehingga memungkinkan untuk diakses kapan saja dan dimana saja.

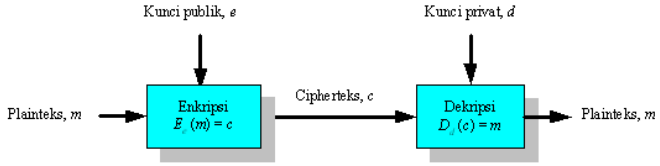
Pada saat ini, pengiriman pesan instan memiliki banyak fitur, yaitu pesan singkat (mengirimkan pesan pada seseorang dalam waktu nyata), obrolan (membuat ruang obrolan atau diskusi yang dapat diakses lebih dari dua orang), tautan web (berbagi pranala mengenai suatu situs web), bicara (berguna seperti layaknya telepon), berbagi video, gambar, dan berkas komputer, serta fasilitas dalam genggaman (mengirimkan pesan instan melalui telepon genggam). Dengan teknologi yang masih terus berkembang, pesan instan pun akan berkembang dan memiliki lebih banyak fitur. Namun, dalam

makalah ini hanya akan membahas pesan instan yang mengirimkan pesan berupa teks pada seseorang.

B. Kriptografi Kunci Publik

Kriptografi kunci-simetri hanya memerlukan satu kunci rahasia. Akan tetapi, mengiriman kunci rahasia tersebut ke penerima melalui saluran umum sangatlah tidak aman. Para penyadap dapat mendapatkan kunci rahasia tersebut dan mengetahui isi pesan yang dikirimkan. Untuk itu, kunci rahasia harus dikirimkan melalui saluran khusus yang sangat aman, tetapi saluran khusus tersebut biasanya membutuhkan waktu yang lama untuk sampai dan biaya yang mahal. Hal ini merupakan kelemahan dari kriptografi kunci-simetri. Oleh karena itu, muncul kriptografi kunci publik yang menangani masalah ini.

Dalam kriptografi kunci publik, setiap orang, pengirim maupun penerima, memiliki sepasang kunci, yaitu kunci publik untuk mengenkripsi pesan dan kunci privat untuk mendekripsi pesan.



Gambar 1 Kriptografi Kunci Publik
Sumber: http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2014-2015/Kriptografi%20Kunci-Publik%20(2015).ppt

Ketika pengirim ingin mengirimkan pesan, pengirim mengenkripsi pesan tersebut terlebih dahulu menggunakan kunci publik milik penerima. Kunci publik ini dapat dikirimkan melalui saluran umum yang tidak aman sekalipun. Meskipun penyadap dapat mendapatkan kunci tersebut, penyadap ini tidak dapat mengetahui isi pesan yang dikirimkan karena untuk mendekripsi pesan diperlukan kunci privat milik penerima. Kunci privat ini hanya diketahui oleh pemilik masing-masing.

Kelebihan dari kriptografi kunci publik ini adalah tidak diperlukannya mengirimkan kunci rahasia untuk mendekripsi pesan. Selain itu, jumlah kunci yang digunakan lebih sedikit daripada kunci pada kriptografi kunci-simetri yang harus sering mengganti kuncinya secara periodik. Pasangan kunci publik dan kunci privat tersebut tidak perlu diubah, bahkan dalam periode waktu yang panjang. Jika seseorang mengetahui suatu kunci publik, secara komputasi hampir tidak mungkin untuk menurunkan kunci privat dari kunci publik tersebut. Kelebihan yang lainnya adalah hanya kunci privat yang perlu dijaga kerahasiaannya oleh setiap pemiliknya dan tidak ada keperluan untuk mengirimkan kunci privat tersebut seperti pada kriptografi kunci-simetri.

Akan tetapi, kriptografi kunci publik juga memiliki beberapa kelemahan. Enkripsi dan dekripsi datanya tergolong lebih lambat daripada kriptografi kunci-simetri karena kriptografi kunci publik menggunakan bilangan yang besar dan melibatkan operasi perpangkatan yang besar. Selain itu, ukuran cipherteksnya menjadi lebih besar daripada plainteksnya dan ukuran kunci yang digunakan tergolong lebih besar daripada yang digunakan pada kriptografi kunci-simetri.

Macam-macam algoritma enkripsi/dekripsi pesan dalam kriptografi kunci publik adalah RSA, Rabin, ElGamal, dan ECC. Selain itu, kriptografi kunci public juga digunakan untuk *digital signature* yang bertujuan untuk membuktikan otentikasi pesan atau pengirim dan terdiri dari algoritma RSA, ElGamal, DSA, dan ECC. Terdapat juga algoritma pertukaran kunci yang bertujuan untuk mempertukarkan kunci simetri, yaitu algoritma Diffie-Hellman.

C. Algoritma RSA

Algoritma RSA ini merupakan algoritma kunci-publik yang paling sering digunakan. Kelebihan algoritma RSA adalah pada sisi keamanannya, yaitu sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Langkah-langkah membangkitkan sepasang kunci (kunci publik dan kunci privat) adalah sebagai berikut.

1. Memilih dua bilangan prima (p dan q) dan sifatnya rahasia.
2. Menghitung n=pq.
3. Menghitung $\phi(n) = (p-1)(q-1)$.
4. Memilih bilangan bulat e sebagai kunci publik dan e relative prima terhadap $\phi(n)$.
5. Menghitung kunci dekripsi d menggunakan persamaan $ed \equiv 1 \pmod{\phi(n)}$ atau $d \equiv e^{-1} \bmod (\phi(n))$.

Langkah-langkah di atas menghasilkan kunci publik berupa pasangan (e,n) dan kunci privat berupa pasangan (d,n). Setelah didapatkan kunci publik dan kunci privat tersebut, dapat dilakukan enkripsi pesan dengan langkah-langkah sebagai berikut.

1. Pesan yang ingin dikirimkan dipecah menjadi blok-blok.
2. Menghitung setiap blok cipherteks c untuk blok plainteks m dengan persamaan $c = m^e \bmod n$ dan e adalah kunci publik.

Selain itu, dapat dilakukan dekripsi pesan dengan menggunakan persamaan $m = c^d \bmod n$ dan n adalah kunci privat.

III. RANCANGAN APLIKASI DAN PEMBAHASAN

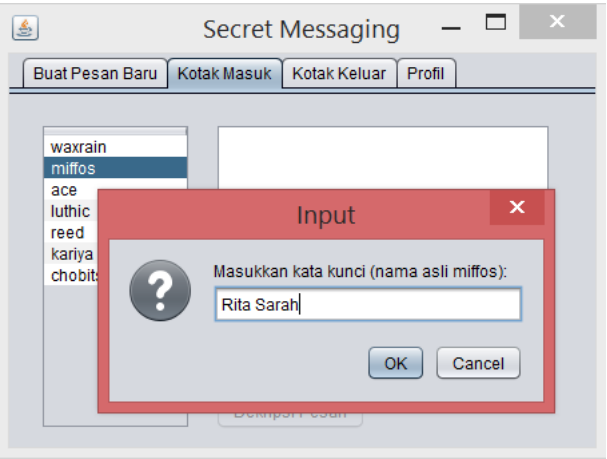
Aplikasi pesan instan yang dirancang memiliki dua kali perlindungan dalam melakukan pertukaran pesannya, yaitu dengan melakukan enkripsi pada pesan dan mengunci pesan tersebut. Setiap pengguna memiliki kunci privat dan kunci publik. Kunci privat hanya diketahui oleh pemiliknya, sedangkan kunci publik dapat diketahui oleh seluruh pengguna. Kunci privat dan kunci publik ini digunakan untuk mengenkripsi pesan. Algoritma enkripsi pesannya dapat menggunakan seluruh algoritma kriptografi kunci publik, tetapi dalam pembuatan makalah ini digunakan algoritma RSA. Setelah dienkripsi, pesan akan dikunci dan hanya bisa dibuka menggunakan suatu kata kunci. Kata kunci dimaksud adalah nama asli pihak pengirim yang tidak akan tertera pada laman

aplikasi. Orang yang melakukan pertukaran pesan pasti mengenal satu sama lain, sehingga pasti mengetahui nama asli satu sama lain.

Dalam aplikasi pesan instan ini, setiap pengguna memiliki *username* yang akan selalu tertera pada laman aplikasi dan *password*. *Username* di sini bersifat unik, sehingga tidak ada dua atau lebih pengguna yang memiliki *username* yang sama dan tidak boleh mengandung nama asli pengguna. Setiap pengguna juga harus mendaftarkan nama aslinya dalam aplikasi ini, tetapi tidak akan tampil pada laman aplikasi. Untuk memasuki aplikasi, pengguna cukup memasukkan *username* dan *password*.

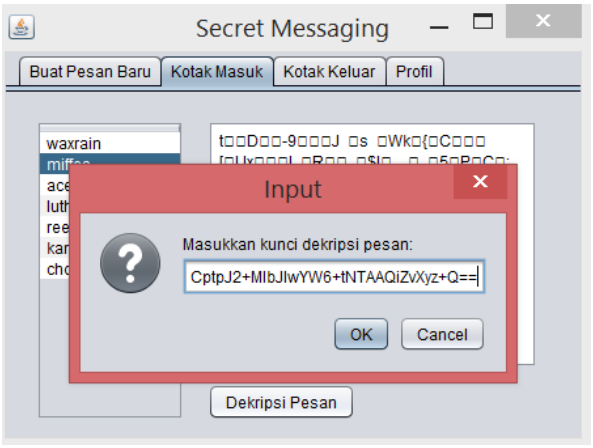
Untuk memulai pengiriman pesan, pengguna dapat menuliskan pesannya pada laman pesan baru dan menuliskan *username* milik penerima. Sebelum mengirimkan pesan, pengirim perlu memasukkan kunci publik dari pihak penerima yang akan digunakna untuk mengenkripsi pesan. Pesan akan dienkripsi dan otomatis terkunci, lalu dikirimkan ke pihak penerima.

Pihak penerima dapat melihat seluruh pesan yang didapatkan pada laman kotak masuk. Pada laman kotak masuk ini, pesan-pesan yang ada hanya menampilkan *username* dari pihak pengirim. Penerima tidak dapat langsung membaca pesan yang didapat. Pertama-tama penerima harus memasukkan kata kunci untuk membuka pesan yang terkunci ini. Kata kunci ini adalah nama lengkap dari pihak pengirim. Meskipun tidak tertera pada laman aplikasi, penerima pasti mengetahui nama asli pihak pengirim karena mereka mengenal satu sama lain. Sebelum memasukkan kata kunci dengan benar, penerima tidak dapat melihat isi pesannya maupun yang masih terenkripsi.

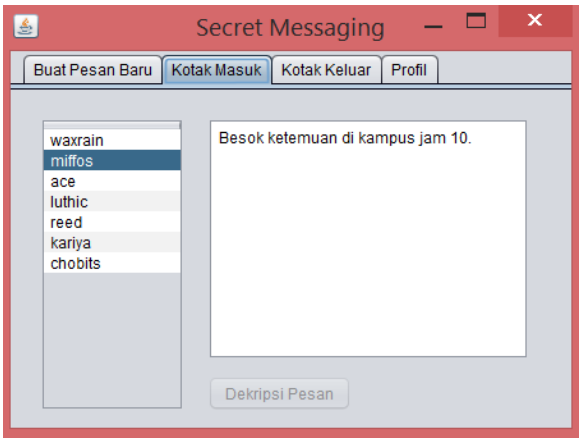


Gambar 2 Membuka pesan yang terkunci

Jika kata kunci yang dimasukkan benar, penerima akan dapat melihat isi dari pesan yang masih terenkripsi. Untuk melihat *plaintext* dari pesan tersebut, penerima harus memasukkan kunci privat miliknya. Pesan akan terdekripsi dan dapat dibaca oleh penerima.



Gambar 3 Mendekripsi pesan



Gambar 4 Pesan terdekripsi

Kelebihan dari aplikasi ini adalah perlindungan pesan yang ganda menggunakan kunci pesan dan enkripsi pesan. Perlindungan yang pertama adalah untuk membuka pesan, penerima harus mengetahui nama asli pengirim yang membuktikan bahwa mereka saling mengenal dan berhak untuk mengetahui isi pesan tersebut. Sebelum memasukkan kata kunci dengan benar, penerima tidak dapat melihat isi pesannya meski yang masih terenkripsi sekalipun, sehingga penerima tidak dapat melakukan kriptanalisis terhadap pesan tersebut. Setelah memasukkan kata kunci berupa nama asli pengirim tersebut, baru aplikasi akan menampilkan pesan yang masih terenkripsi kepada penerima. Berikut adalah perlindungan kedua yang aplikasi berikan pada pesan. Untuk mengetahui isi pesan tersebut, penerima harus memasukkan kunci privatnya yang bersifat rahasia dan tidak ada orang lain yang mengetahui kunci privatnya. Setelah melewati kedua perlindungan tersebut, penerima baru dapat melihat isi pesan sebenarnya yang dikirimkan oleh pengirim.

IV. Simpulan dan Saran

Pengiriman pesan menggunakan perlindungan ganda ini cocok untuk pengiriman pesan yang bersifat rahasia. Untuk mengetahui isi pesan dari pengirim, penerima harus mengetahui dua hal, yaitu kunci privatnya sendiri dan nama

asli pengirim. Meskipun orang lain memiliki akses ke akun si penerima, dia tidak tahu kunci privatnya dan nama asli pengirim. Jika dia tidak tahu nama asli pengirim, dia tidak dapat melakukan kriptanalisis karena tidak dapat melihat pesan yang masih terenkripsi.

Akan tetapi penguncian pesan menggunakan nama asli ini masih belum sempurna karena nama asli seseorang tergolong cukup publik diketahui di luar aplikasi ini. Aplikasi ini dapat dikembangkan ke depannya dengan kunci yang lebih baik.

REFERENSI

[1] Munir, Rinaldi, Diktat Kuliah IF5054 Kriptografi, Program Studi Teknik Informatika Institut Teknologi Bandung, 2006.

[2] Munir, Rinaldi, http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2014-2015/Kriptografi%20Kunci-Publik%20(2015).ppt diakses pada 10 Mei 2015 pukul 13.05

[3] Munir, Rinaldi, http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2014-2015/Algoritma%20RSA%20(2015).ppt diakses pada 10 Mei 2015 pukul 13.42

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 11 Mei 2015

Cilvia Sianora Putri 13512027