Peningkatan Keamanan Pertukaran Kunci Diffie-Hellman Dengan Pengimbuhan Algoritma RSA

Dadan Ramdan Mangunpraja [1)]

1) Jurusan Teknik Informatika, STEI ITB, Bandung, email: if14087@if.itb.ac.id

Abstract *– Algoritma pertukaran kunci Diffie-Hellman merupakan suatu teknik mempertukarkan kunci sesi (kunci rahasia untuk komunikasi dengan kriptografi simetri) antara 2 orang atau lebih. Teknik pertukaran ini bisa dipecahkan dengan perhitungan logaritma diskrit, walaupun hal tersebut sangat sulit dilakukan.*

Berbeda dengan Diffie-Hellman, teknik RSA digunakan untuk mengenkripsi pesan rahasia. Kekuatannya terdapat pada belum ditemukannya suatu algoritma yang mangkus untuk bisa memfaktorkan bilangan besar menjadi faktor-faktor primanya.

Makalah ini membahas bagaimana cara mengimbuhkan teknik RSA dalam teknik pertukaran kunci Diffie-Hellman. Kekuatan pertukaran kunci Diffie-Hellman setelah dikombinasikan dengan RSA bisa menjadi berlipat-lipat, karena selain sulitnya melakukan perhitungan logaritma diskrit, juga ditambah dengan lamanya memfaktorkan bilangan besar menjadi faktor-faktor primanya.

Kata Kunci*: Pertukaran Kunci, Diffie-Hellman-RSA*

1. PENDAHULUAN

Dalam dunia kriptografi, kunci untuk mengenkripsi dan mendekripsi suatu pesan rahasia adalah satu elemen terpenting. Kuncilah yang menentukan sebuah *chipertext* dapat dibaca atau tidak. Kerahasiaan kunci justru menjadi hal yang bisa lebih krusial dan penting daripada kerahasiaan *chipertext* itu sendiri, dalam artian pesan (*chipertext* boleh bocor tetapi kunci tidak boleh bocor).

Berbagai cara dilakukan untuk menjaga kerahasiaan kunci. Teknik atau algoritma kriptografi kunci publik merupakan satu cara yang dikembangkan untuk mengatasi hal tersebut. (kerahasiaan kunci). Kriptografi kunci publik mensyaratkan ada dua buah kunci, yaitu kunci publik yang diinformasikan secara bebas dan digunakan tanpa kerahasiaan, serta kunci privat yang hanya digunakan secara khusus oleh satu orang dan tidak pernah diinformasikan kepada siapapun, sehiangga kerahasiaannya sangat terjaga.

Walaupun algoritma kriptografi kunci publik populer karena hal tersebut, algoritma kriptografi kunci simetri pun masih banyak digunakan karena lebih mudah penggunaannya, namun perlu dipikirkan bagaimana cara menjaga kerahasiaan kuncinya. Algoritma yang ditemukan Diffie dan Hellman adalah teknik untuk menjaga kerahasiaan kunci simetri. Ide mengkombinasikan suatu algoritma kriptografi kunci publik ke dalam algoritma pertukaran kunci Diffie-Hellman yang digunakan untuk algoritma kunci simetri sangat menarik. Hal tersebut secara teori tentunya akan membuat cara pemecahannya menjadi lebih kompleks, sehingga penggunaan kriptografi kunci simetri bisa lebih leluasa dilakukan.

Dalam makalah ini, algoritma kriptografi kunci publik yang digunakan untuk memperkuat algoritma pertukaran kunci Diffie-Hellman adalah RSA. RSA digunakan dengan alasan tingkat keamanannya sangat tinggi.

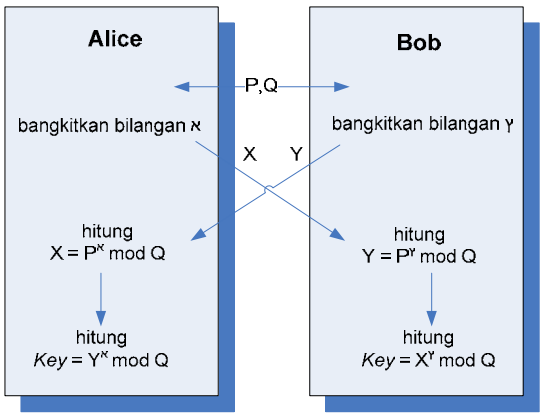
2. PENJELASAN ALGORITMA

2.1 Protokol Pertukaran Kunci Diffie-Hellman

Algoritma pertukaran kunci Diffie-Hellman (protokol Diffie-Hellman) beguna untuk mempertukarkan kunci rahasia untuk komunikasi menggunakan kriptografi simetris. Langkah-langkahnya adalah sebagai berikut,

1. Misalkan Alice dan Bob adalah pihak-pihak yang berkomunikasi. Mula-mula Alice dan Bob menyepakati 2 buah bilangan yang besar (sebaiknya prima) P dan Q, sedemikian sehingga P < Q. Nilai P dan Q tidak perlu rahasia, bahakan Alice dan Bob dapat membicarakannya melalui saluran yang tidak aman sekalipun.
2. Alice membangkitkan bilangan bulat acak x yang besar dan mengirim hasil perhitungan berikut kepada Bob :
   $X = P^x \bmod Q$.
3. Bob membangkitkan bilangan bulat acak y yang besar dan mengirim hasil perhitungan berikut kepada Alice:
   $Y = P^y \bmod Q$.
4. Alice menghitung
   $K = Y^x \bmod Q$.
5. Bob menghitung
   $K' = X^y \bmod Q$.

Jika perhitungan dilakukan dengan benar maka K = K'. Dengan demikian Alice dan Bob telah memiliki sebuah kunci yang sama tanpa diketahui pihak lain. Gambar di bawah ini mendeskripsikan diagram protokol pertukaran kunci Diffie-Hellman:



Gambar 1: Protokol Pertukaran Kunci Diffie-Hellman

2.2 RSA

Algoritma enkripsi/dekripsi RSA dilakukan sebagai berikut (dalam makalah ini tidak dijabarkan bagaimana pembuktian kebenaran formula ini).

$E_e(m) = c = m^e \bmod n$, dan

$D_d(c) = m = c^d \bmod n$,

dimana $E_e(m)$ merupakan fungsi enkripsi terhadap *plaintext* m, Dan $D_d(c)$ merupakan fungsi dekripsi terhadap *chipertext* c.

Nilai d, e, n itu sendiri merupakan pasangan kunci publik (e,n) dan kunci privatnya (d) yang diperoleh dengan menggunakan aturan pembangkitan kunci sebagai berikut:

1. Pilih dua buah bilangan prima sembarang, p dan q.
2. Hitung n = p.q (sebaiknya $p \neq q$, sebab jika p=q maka $n = p^2$ sehingga p dapat diperoleh dengan mudah dengan menarik akar pangkat dua dari n).
3. Hitung $\phi(n) = (p-1)(q-1)$.
4. Pilih kunci publik e, yang relatif prima terhadap $\phi(n)$.
5. Bangkitkan kunci privat dengan menggunakan persamaan $e.d \equiv 1 (\mod \phi(n))$ yang ekivalen dengan $e.d = 1 + k\phi(n)$, sehingga secara sederhana d dapat dihitung dengan

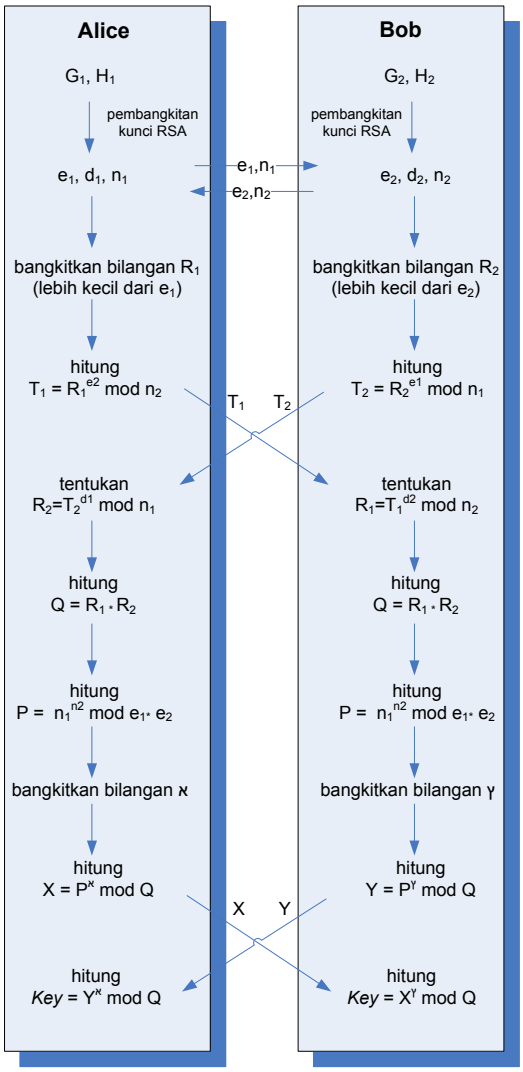
$$d = \frac{1 + k\phi(n)}{e}$$

2.3 Kombinasi Diffie-Hellman dengan RSA

Peran utama RSA dalam kombinasi ini adalah merahasiakan nilai P (pada diagram pertukaran kunci Diffie-Hellman) yang bisa disadap. Dengan algoritma baru ini, nilai P tersebut diperoleh sedemikian rupa dari penggunaan algoritma RSA. Langkah-langkahnya sebagai berikut:

1. Misalkan Alice dan Bob yang akan melakukan pertukaran kunci. Alice menentukan 2 bilangan prima G_1 dan H_1, begitu pula Bob menentukan 2 bilangan prima G_2 dan H_2. Nilai-nilai tersebut disimpan dan dirahasiakan.
2. Dengan pembangkitan kunci RSA, dari bilangan-bilangan tersebut Alice memperoleh kunci publik e_1, dan n_1 serta kunci privat d_1. Begitu pula Bob memperoleh kunci publik e_2, dan n_2 serta kunci privat d_2.
3. Alice dan Bob saling memberi informasi masing-masing kunci publiknya.
4. Alice membangkitkan bilangan bulat besar dan acak R_1 yang $< n_1$ lalu mengenkripsinya dengan algoritma RSA sehingga menghasilkan:
   $T_1 = R_1^{e2} \bmod n_2$.
   Begitu pula Bob membangkitkan bilangan bulat besar dan acak R_2 yang $< n_2$ lalu mengenkripsinya dengan algoritma RSA sehingga menghasilkan:
   $T_2 = R_2^{e1} \bmod n_1$.
   Setelah itu mereka saling memberikan informasi mengenai nilai T_1 dan T_2 tersebut.
5. Alice dan Bob masing-masing mendekripsi T_1 dan T_2 sehingga Alice mendapatkan nilai
   $R_2 = T_2^{d1} \bmod n_1$,
   dan Bob mendapatkan nilai
   $R_1 = T_1^{e2} \bmod n_2$.
6. Setelah Alice dan Bob memiliki nilai R_1 maupun R_2, tentukan P dan Q sedemikian rupa dari R_1 dan R_2 sehingga $P < Q$. Cara sederhananya adalah dengan menghitung
   $Q = R_1 * R_2$ dan
   $P = n_1^{n2} \bmod (e_1 * e_2)$
7. Setelah masing-masing memperoleh nilai P dan Q, langkah selanjutnya sama seperti langkah pada pertukaran kunci Diffie-Hellman biasa.

Gambar 2 di bawah ini memperlihatkan lebih jelas algoritma pertukaran kunci Diffie-Hellman setelah diimbuhkan RSA. Di akhir perhitungan, Alice dan Bob telah memiliki kunci rahasia yang sama, *Key*.



Gambar 2 : Diagram Pertukaran Diffie-Hellman setelah Ditambahkan RSA

3. HASIL DAN PEMBAHASAN

3.1 Contoh Pengujian

Untuk contoh pengujian, misalkan Alice dan Bob akan melakukan pertukaran kunci.

1. Untuk pembangkitan kunci publik dan kunci privatnya, Alice memilih $G_1 = 47$ dan $H_1 = 71$ (dalam praktek kedua bilangan ini haruslah bilangan yang sangat besar), sedangkan Bob memilih $G_2 = 53$ dan $H_2 = 97$.
2. Setelah kunci dibangkitkan, Alice memiliki $e_1 = 79$, $n_1 = 71$, dan $d_1 = 1019$. Sedangkan Bob memiliki $e_2 = 84$ $n_2 = 4992$ dan $d_2 = 2114$.
3. Alice membangkitkan bilangan
   R_1 yang < 1019, misalnya 107,
   dan Bob membangkitkan bilangan
   R_2 yang < 2114, misalnya 1015.
4. Alice dan Bob mengenkripsi masing-masing bilangan tersebut dan saling mengirimkan hasilnya
   $T_1 = 107^{84} \bmod 2214$
   $= 1452$, dan
   $T_2 = 1015^{79} \bmod 3337$
   $= 692$.
5. Alice mendekripsi T_2 menghasilkan R_2 dan Bob mendekripsi T_1 menghasilkan R_1
   $R_2 = 692^{1019} \bmod 3337$
   $= 1015$, dan
   $R_1 = 1452^{2114} \bmod 4992$
   $= 107$.
6. masing-masing menghitung nilai
   $Q = 1015 * 107$
   $= 108605$, dan
   $P = 71^{84} \bmod (3337 \times 4992)$
   $= 16658304$.
7. Alice kemudian membangkitkan lagi bilangan acak x, misalnya
   $x = 137$
   dan Bob membangkitkan bilangan acak y, misalnya
   $y = 461$.
8. Alice menghitung nilai
   $X = 108605^{137} \bmod 16658304$
   $= 7644321$,
   Bob menghitung nilai
   $Y = 108605^{461} \bmod 16658304$
   $= 11243217$.
   Kemudian mereka saling memberi informasi mengenai nilai tersebut.
9. Alice mengitung nilai kunci simetri
   $Key = 11243217^{137} \bmod 16658304$
   $= 8659087$,
   dan Bob juga menghitung nilai kunci simetri
   $Key' = 7644321^{461} \bmod 16658304$
   $= 8659087$.
   Dengan demikian Alice dan Bob telah memiliki kunci simetri yang sama tanpa diketahui oleh orang lain.

3.2 Kelebihan dan Kelemahan Algoritma

3.2.1 Kelebihan

Seperti telah dibahas sebelumnya, kekuatan masing-masing algoritma akan lebih meningkatkan tingkat keamanan bagi algoritma baru ini. Penyadap hanya bisa menyadap nilai e_1, n_1, e_2, n_2, T_1, T_2, X, dan Y. Agar dapat mengetahui nilai P, penyadap harus memecahkan T_1 dan T_2 menjadi R_1 dan R_2 yang mana sulit dilakukan karena tidak mengetahui kunci privatnya masing-masing dan akan

membutuhkan waktu lama untuk memecahkannya tanpa mengetahui secara pasti kunci privatnya. Setelah itu penyadap harus mencari nilai x dan y yang dibangkitkan Alice dan Bob berdasarkan nilai X dan Y yang disadap, di mana hal tersebut sangat sulit dilakukan karena harus menggunakan logaritma diskrit.

3.2.2 Kekurangan

Karena terlalu banyak bilangan yang dipertukarkan, serangan kriptografi yang paling berbahaya adalah pengacauan data. Jika satu saja data yang diinformasikan tidak benar, hal itu akan menggiring enkriptor dan dekriptor pada kesalahan dalam melakukan tugasnya. Pesan rahasia mungkin hanya akan menjadi pesan tanpa arti yang tidak akan pernah bisa dipecahkan sama sekali.

4. KESIMPULAN

Pada dasarnya penggabungan 2 algoritma atau lebih menjadi sebuah algoritma baru sudah banyak dan mudah dilakukan. Penggabungan tersebut biasanya menghasilkan suatu algoritma yang tingkat keamanannya menjadi lebih besar, setara dengan penjumlahan tingkat keamanan algoritma satu dengan lainnya.

Dari sekian banyak kemungkinan kombinasi algoritma, kombinasi algoritma RSA untuk memperkuat algoritma pertukaran kunci Diffie-Hellman bisa menjadi contoh bagaimana peningkatan keamanan itu terjadi. Pada kombinasi RSA dengan pertukaran kunci Diffie-Hellman, teori tersebut berlaku pula. Pertukaran kunci menjadi lebih kompleks dan lebih sulit untuk dipecahkan oleh para penyadap.

DAFTAR REFERENSI

[1] Munir, Rinaldi, "*Diktat Kuliah IF15054, Kriptografi"*, 2006, Bandung