Keamanan Pertukaran Kunci Kriptografi dengan Algoritma Hybrid : Diffie-Hellman dan RSA

Ana Wahyuni
Fakultas Ilmu Komputer Universitas AKI

Abstract

On the cryptographic, the safety of key exchange is needed, because the code message can only be analyzed with the appropriate key deals with this message. A secret message may be delivered either by symmetric cryptographic algorithm of coded key or by key exchange algorithm. One of the standard key exchange algorithm is Deffie Hellman key exchange algorithm. The safety strength of this algorithm can be improved by combining / hybridizing asymmetric key algorithm, that is RSA. Cryptanalyst difficulty in disclosing these algorithms is not only on the RSA key generation but also on the calculation of discrete logarithms in RSA and Deffie-Hellman. The result of this hybrid algorithm is the key strength and the confidentiality that can be used in symmetric cryptographic algorithms.

***Key words** : cryptographic, key exchange, RSA algorithm, Deffie-Hellman algorithm, hybrid algorithm: RSA and Deffie-Hellman.*

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 public 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, sehingga kerahasiaannya sangat terjaga. Walaupun algoritma kriptografi kunci publik popular 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.

Metode Penelitian

Metode yang digunakan pada penelitian ini mencakup:

a. Bahan penelitian yang meliputi literatur-literatur berupa jurnal dan buku-buku mengenai kriptografi.
b. Alat penelitian meliputi seperangkat komputer dengan processor Pentium III, sistem operasi Windows XP, dan *softwar*e Matlab 7.
c. Proses penelitian meliputi pengkajian literatur mengenai algoritma RSA dan pertukaran kunci Deffie-Helman secara matematis dan diimplementasikan pada komputasinya menggunakan Matlab.

Hasil dan Pembahasan

Algoritma RSA

Algoritma RSA dibuat oleh 3 orang 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. Pemfaktoran dilakukan untuk memperoleh kunci pribadi. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin. Algoritma enkripsi/dekripsi RSA dilakukan sebagai berikut :

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

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

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 $e.d \equiv 1 (\text{mod } \phi(n))$ yang ekivalen dengan $e.d = 1 + k\phi(n)$,

sehingga secara sederhana d dapat dihitung dengan $d = \frac{1 + k\varphi(n)}{e}$

Sedangkan proses enkripsi dan deskripsi pesan (*massage*) sebagai berikut :

B mengenkripsi *message* M untuk A, Yang harus dilakukan B :

1. Ambil kunci publik A yg otentik (n, e)
2. Representasikan message sbg integer M dalam interval [0,n-1]
3. Hitung C = M ^ e (mod n)
4. Kirim C ke A

Untuk mendekripsi *message*, A melakukan :

Gunakan kunci pribadi d untuk menghasilkan M = C^(d) (mod n)

Keamanan dari sistem kriptografi RSA didasari oleh dua problem matematika, yaitu :

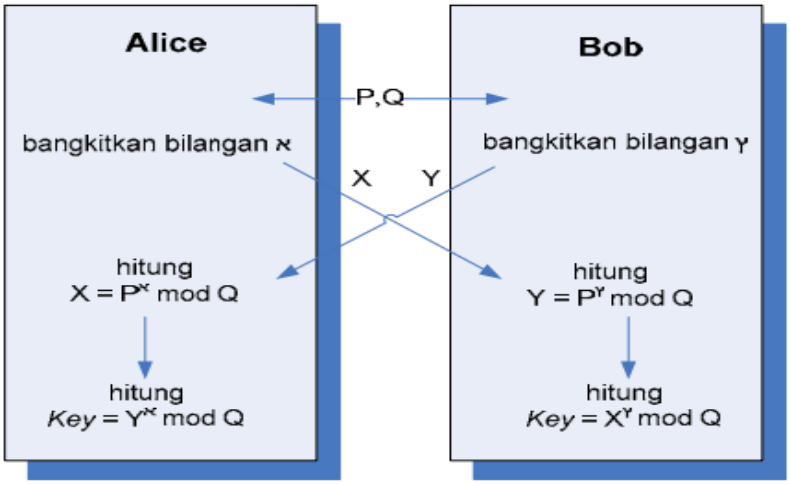
1. Problem dalam faktorisasi bilangan prima besar (jumlah bit besar)
2. Problem RSA, yaitu mencari modulo akar e^n dari sebuah bilangan komposit n yang faktor-faktornya tidak diketahui

Algoritma Deffie-Helman

Algoritma pertukaran kunci Diffie-Hellman (protokol Diffie-Hellman) beguna untuk mempertukarkan kunci rahasia pada komunikasi menggunakan kriptografi simetris. Kekuatan algoritma ini adalah pada sulitnya melakukan perhitungan logaritma diskrit. 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 1: Protokol Pertukaran Kunci Diffie-Hellman

Algoritma Hibrid : Diffie-Hellman dan RSA

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.

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 sehingga sulit dilacak.

Langkah-langkah algoritma hybrid : Deffie-Helman dan RSA 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 yaitu e_1, n_1 dan e_2 , n_2.
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:

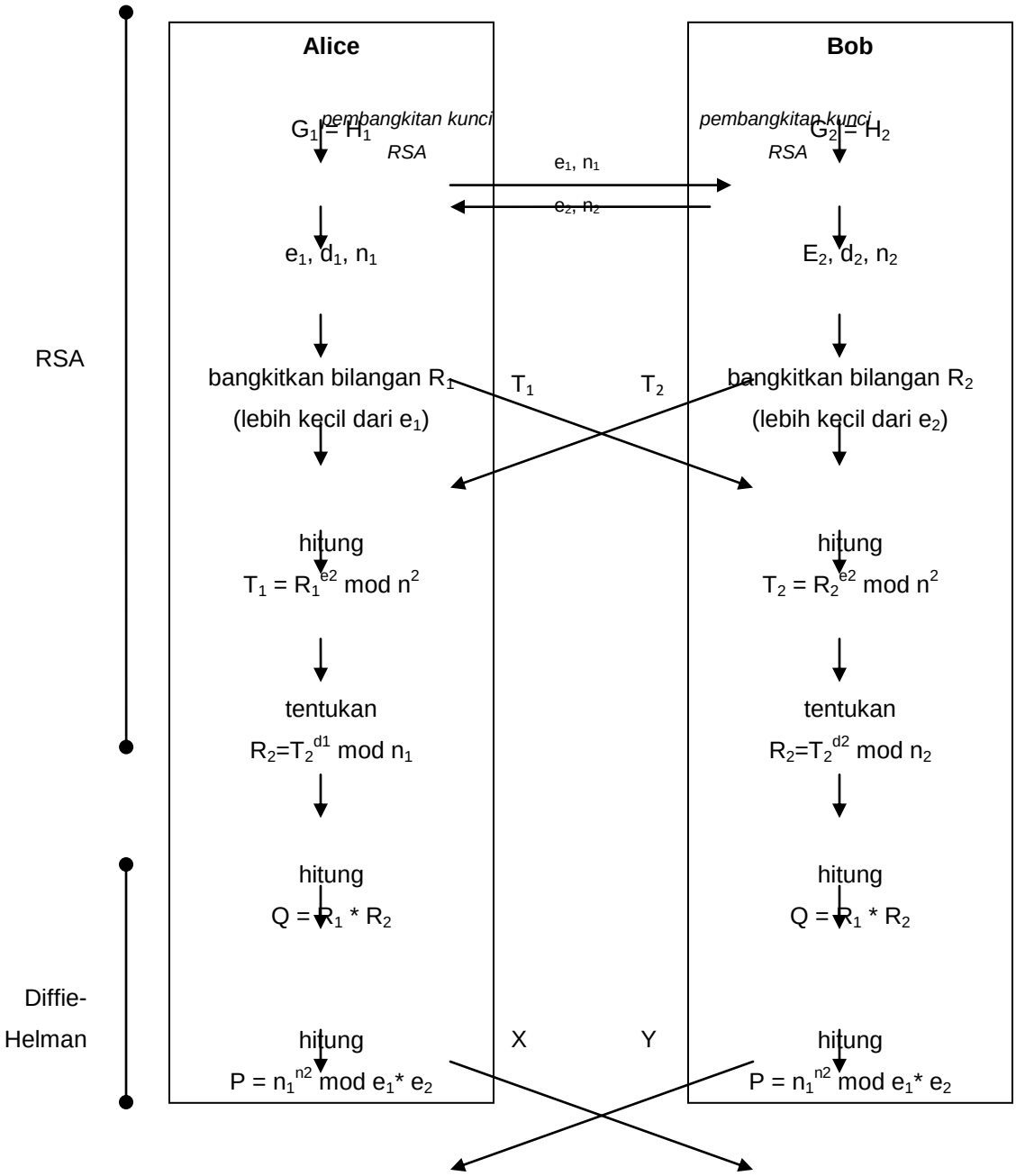
   $T2 = R_2^{e1} \bmod n_1$.

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 $R1 = T_1^{e2} \bmod n_2$.
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 $P = n1^{n2} \bmod (e_1 * e_2)$
7. Setelah masing-masing memperoleh nilai P dan Q, dilanjutkan pada langkah pertukaran kunci Diffie-Hellman (langkah selanjutnya).
8. Alice memilih bilangan sembarang x dan menghitung X dan memperoleh nilai K.
9. Bob memilih bilangan sembarang y dan menghitung Y dan memperoleh nilai K.
10. Setelah itu mereka saling memberikan informasi mengenai nilai X dan Y tersebut.
11. Nilai K (tidak dipublikasikan) digunakan untuk enkripsi dan deskripsi pesan rahasia dengan algoritma simetris.

Misal ada penyadap katakan si Tono di perjalanan transmisi pesan tersebut. Tono hanya bisa mendapat informasi nilai e, n, X dan Y yang bukan merupakan kunci untuk memecahkan pesan tersebut. Ada kesulitan pada perhitungan logaritma diskrit untuk mendapat nilai K tanpa mengetahui nilai P dan Q yang tidak dipublikasikan. Dengan demikian Alice dan Bob dapat mengirim kunci yang disandikan (bukan kunci sebenarnya) dengan tingkat keamanan berlipat.

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



Gambar 2. Skema algoritma hibrid : Diffie-Helman dan RSA

Contoh implementasi algoritma Hibrid : RSA dan Deffie-Helman (*Problem Solving* dengan komputasi pada matlab):

A memilih P_1=47 Q_1=71 n_1=3337 $\phi(n_1)=(p-1)(q-1)$ $\phi(n_1)=46 \times 70 = 3220$ e_1=79 SK $d_1=1019 = \frac{1+k\phi(n)}{e}$	B memilih P2=53 Q2=97 n_2=5141 $\phi(n_2)=(p-1)(q-1)$ $\phi(n_2)=52 \times 96 = 4992$ e_2=53 SK $d_2=1019 = \frac{1+k\phi(n)}{e}$
A memilih $R_1 < e_1$ Jika R_1=70	B memilih $R_2 < e_2$ Jika R_2=50
A dan B mengenkrip masing-masing bilangan dan mengirimkan hasilnya	
$T_1=R_1^{e2} \bmod n_2$ $T_2=70^{53} \bmod 5141$ =2243	$T_2=R_2^{e1} \bmod n_1$ $T_2=50^{79} \bmod 3337$ =1662
A Mendekrip T_2 menghasilkan R_2 $R_2=T_2^{d1} \bmod n_1$ $=1662^{1019} \bmod 3337$ =50	B Mendekrip T_1 menjadi R_1 $R_1=T_1^{d2} \bmod n_2$ $=2243^{3485} \bmod 5141$ =70
Masing-masing menghitung harga P dan Q $Q=R_1 \times R_2$ =50 x 70 = 3500 $P= n_1^{n2} \bmod (e_1 \times e_2)$ $=3337^{5141} \bmod (79 \times 53) = 3828$	
Deffie- Helman	
A memilih x=137 A menghitung $X = P^x \bmod Q$ $=3828^{137} \bmod 3500$ =888	B memilih y=46 B menghitung $Y = P^y \bmod Q$ $=3828^{46} \bmod 3500$ =904
Hitung Key $k = Y^x \bmod Q$ $=904^{137} \bmod 3500$ 2584	Hitung Key $k= X^y \bmod Q$ $=888^{46} \bmod 3500$ =2584

↓

k = k Kunci ini siap digunakan untuk algoritma kriptografi simetris

Dengan demikian Alice dan Bob telah memiliki kunci simetri yang sama tanpa diketahui oleh orang lain dan dapat melakukan pertukaran pesan dalam bentuk chiper-teks yang sulit dipecahkan oleh penyadap.

Kekuatan dan Kelemahan Algoritma Hybrid : Deffie-Helman dan RSA

Kekuatan masing-masing algoritma akan lebih meningkatkan tingkat keamanan pada algoritma hybrid ini. Penyadap hanya bisa menyadap nilai e1, n1, e2, n2, T1, T2, X, dan Y. Agar dapat mengetahui nilai P, penyadap harus memecahkan T1 dan T2 menjadi R1 dan R2 yang 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 tidak mengetahui kunci privatnya masing-masing dan kesulitan dalam perhitungan logaritma diskrit. Kekurangan dari algoritma hybrid ini yaitu, 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.

Kesimpulan

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 penyadap. Algoritma hibrid : RSA dan Deffie-Helman bermanfaat dalam menjaga keamanan kunci yang digunakan pada penyandian pesan kriptografi simetris. Hasil dari algoritma ini adalah keamanan berlipat pada kunci pesan. Skema algoritma ini dapat dilanjutkan dengan algoritma kriptografi yang lain. Dapat pula dikembangkan dengan membuat interface pada GUI Matlab atau bahasa pemrograman yang lainnya.

Daftar Pustaka :

Kurniawan, A. 2008. Konsep dan Implementasi Cryptography dengan . NET, Dian Rakyat.

Kurniawan, Y. 2004. Kriptografi Keamanan Internet dan jaringan Komunikasi, Informatika, Bandung

Munir, R. 2006. Kriptografi, Informatika, Bandung

Stallings, W. 2004. Cryptography and Network Security, Pearson Education, India

Sujalwo. 2004. Skema Pertukaran Kunci Menggunakan Teori Matriks, Jurnal Penelitian Sains & Teknologi, Vol. 5, No. 1, UMS Surakarta.

http://id.wikipedia.org/wiki/Kriptografi