Jurnal TIMES , Vol. V No 2 : 11-15 , 2016
ISSN : 2337 - 3601

KEAMANAN DATA DENGAN METODE KRIPTOGRAFI KUNCI PUBLIK

Chandra
Program Studi Magister S2 Teknik Informatika Universitas Sumatera Utara
Jl. Universitas No. 9A Medan, Sumatera Utara
e-mail : chandra.wiejaya@gmail.com

Abstrak

Perkembangan ilmu dan teknologi komputer telah mempengaruhi segala aspek kehidupan manusia seperti di bidang pendidikan. Informasi dan data dapat dengan mudah dan cepat untuk dikirim ke konsumen melalui jaringan komputer. Hal ini tentu saja menimbulkan risiko jika informasi dan data yang dikirim bisa diakses oleh pihak yang tidak berhak sehingga mengakibatkan kebocoran data. Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Apabila mengganggu performansi sistem, masalah keamanan sering tidak dipedulikan, bahkan ditiadakan. Dalam kriptografi terdapat dua konsep utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi yang dikirim diubah menjadi bentuk yang tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk yang tersamar menjadi informasi awal. Dewasa ini telah banyak beredar program proteksi/enkripsi data baik yang bersifat freeware, shareware, ataupun komersial. Pada umumnya, program tersebut menyediakan beragam metode kriptografi sehingga kita dapat dipilih metode yang paling aman menurut kita. Salah satu metode kriptografi adalah Kriptografi kunci publik yang dilakukan dengan cara menggabungkan secara kriptografi dua buah kunci yang saling berhubungan, yaitu pasangan kunci publik dan kunci privat. Kedua kunci tersebut dibuat pada waktu yang bersamaan dan saling terhubung secara matematis. Salah satu jenis kriptografi adalah kriptografi simetris dimana kunci yang digunakan untuk enkripsi dan dekripsi adalah sama. Jika dibandingkan dengan kriptografi kunci publik, kriptografi simetris sangat cepat sehingga sangat cocok digunakan untuk melakukan enkripsi data yang sangat besar. Banyak yang menggabungkan algoritma kunci publik dengan simetris untuk memperoleh keunggulan dari masing-masing metode kriptografi. Dalam makalah ini, penulis akan membahas lebih lanjut tentang sistem keamanan data dengan metode kunci publik.

Kata Kunci : Kriptografi, Kunci Publik, Asimetris

1. Pendahuluan

Perkembangan ilmu dan teknologi komputer telah mempengaruhi segala aspek kehidupan manusia seperti di bidang pendidikan. Informasi dan data dapat dengan mudah dan cepat untuk dikirim ke konsumen melalui jaringan komputer. Hal ini tentu saja menimbulkan risiko jika informasi dan data yang dikirim bisa diakses oleh pihak yang tidak berhak sehingga mengakibatkan kebocoran data. Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (plaintext) ke dalam bentuk data sandi (ciphertext) yang tidak dapat dikenali. Ciphertext inilah yang kemudian dikirimkan oleh pengirim (sender) kepada penerima (receiver). Setelah sampai di penerima, ciphertext tersebut ditranformasikan kembali ke dalam bentuk plaintext agar dapat dikenali.

Proses tranformasi dari plaintext menjadi ciphertext disebut proses Encipherment atau enkripsi (encryption), sedangkan proses mentransformasikan kembali ciphertext menjadi plaintext disebut proses dekripsi (decryption).

Untuk mengenkripsi dan mendekripsi data. Kriptografi menggunakan suatu algoritma (cipher) dan kunci (key). Cipher adalah fungsi matematika yang digunakan untuk mengenkripsi dan mendekripsi. Sedangkan kunci merupakan sederetan bit yang diperlukan untuk mengenkripsi dan mendekripsi data.

Suatu pesan yang tidak disandikan disebut sebagai plaintext ataupun dapat disebut juga sebagai cleartext. Proses yang dilakukan untuk mengubah plaintext ke dalam ciphertext disebut encryption atau encipherment. Sedangkan proses untuk mengubah ciphertext kembali ke plaintext disebut decryption atau decipherment.

Agar data terlindungi, dapat digunakan program proteksi/enkripsi data yang telah banyak beredar baik yang bersifat freeware, shareware, ataupun komersial. Pada umumnya, program tersebut menyediakan beragam metode kriptografi sehingga kita dapat dipilih metode yang paling aman menurut kita. Salah satu metode kriptografi adalah Kriptografi kunci publik yang dilakukan dengan cara menggabungkan secara kriptografi dua buah kunci yang saling berhubungan, yaitu pasangan kunci publik dan kunci privat. Kedua kunci tersebut dibuat pada waktu yang bersamaan dan saling terhubung secara matematis. Salah satu jenis kriptografi adalah kriptografi simetris dimana kunci yang digunakan untuk enkripsi dan dekripsi adalah sama. Jika dibandingkan dengan kriptografi kunci publik, kriptografi simetris sangat cepat sehingga sangat cocok digunakan untuk melakukan enkripsi data yang sangat besar.

Dewasa ini, banyak yang menggabungkan algoritma kunci publik dengan simetris untuk memperoleh keunggulan dari masing-masing metode kriptografi. Dari pengamatan penulis, kekuatan dari berbagai metode kriptografi adalah pada kunci yang disepakati sehingga walaupun algoritma metode kriptografi telah diketahui secara umum dan tersebar

luas, pihak yang tidak berhak tidak akan bisa membongkar data tanpa kunci yang tepat. Walaupun untuk menemukan berbagai metode kriptografi diperlukan teori matematika yang rumit, tetapi intinya disini ialah bagaimana kita mengimplementasi metode-metode yang telah diakui secara umum sehingga kita dapat meningkatkan keamanan dari aplikasi yang kita buat.

Memang untuk membuat suatu metoda enkripsi yang sangat kuat (tidak dapat dibongkar) adalah cukup sulit. Ada satu peraturan tidak tertulis dalam dunia cryptography bahwa untuk dapat membuat metoda enkripsi yang baik orang harus menjadi cryptanalysis (menganalisa suatu metoda enkripsi atau mungkin membongkarnya) terlebih dahulu. Salah satu contohnya adalah Bruce Schneier pengarang buku Applied Crypthography yang telah menciptakan metoda Blowfish dan yang terbaru Twofish. Bruce Schneier (dan sejawatnya di Counterpane) telah banyak menganalisa metoda-metoda seperti 3-Way, Cast, Cmea, RC2, RC5, Tea, Orix, dll dan terbukti metoda yang ia buat yaitu Blowfish (yang operasi ciphernya cukup sederhana bila dibandingkan dengan DES misalnya) sampai saat ini dianggap salah satu yang terbaik dan tidak bisa dibongkar dan juga sangat cepat. Bahkan untuk menciptakan Twofish ia dan timnya di Counterpane menghabiskan waktu ribuan jam untuk menganalisanya dan sampai saat-saat terakhir batas waktu penyerahan untuk AES (15 Juni 1998) ia terus menganalisisnya dan menurutnya sampai saat inipun ia masih terus menganalisis Twofish untuk menemukan kelemahannya.

Seiring dengan perkembangan zaman, kriptografi mengalami perkembangan untuk menjaga pesan agar orang tidak dapat membaca pesan tersebut sehingga metode penyadian pesan semakin berkembang. Dalam kriptografi terdapat dua konsep utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi yang dikirim diubah menjadi bentuk yang tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk yang tersamar menjadi informasi awal.

Algoritma kriptografi berdasarkan jenis kunci yang digunakan dapat dibedakan menjadi dua jenis yaitu:

1. Kriptografi Simetri (Kriptografi Klasik), dimana kunci yang digunankan untuk proses enkripsi dan dekripsi adalah kunci yang sama.
2. Kriptografi Asimetri (Kriptografi Publik), dimana kunci yang digunakan untuk proses enkripsi dan dekripsi menggunakan kunci yang berbeda.

Terlihat bahwa kriptografi asimetri memiliki tingkat pengamanan yang lebih tinggi daripada simetri. Pengirim pesan menggunakan kunci publik untuk mengenkripsi pesan yang disampaikan, kunci publik bisa saja diketahui semua pihak ketiga, namun kunci publik tidak bisa digunakan untuk mendekripsi pesan. Dekripsi pesan hanya bisa dilakukan dengan menggunakan kunci privat yang hanya boleh diketahui oleh penerima pesan yang sebenarnya. Namun, kriptografi asimetri memiliki kelemahan yaitu kecepatan yang lebih rendah dibandingkan kriptografi simetri. Kriptografi asimetri tidak tepat digunakan untuk data dalam jumlah besar. Dalam prakteknya, misalnya transfer data di internet, lalu lintas email, atau online banking yang digunakan adalah metode hibrid. Metode Hibrida mengenkripsi data sebenarnya secara simetris, tetapi kuncinya secara asimetris. Metode semacam ini mengkombinasikan pertukaran kunci yang aman dan data encryption yang cepat.

2. Kriptografi Kunci Publik

Algoritma kriptografi kunci publik adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Algoritma ini disebut juga algoritma asimetris karena kunci untuk enkripsi dibuat umum (public key) atau dapat diketahui oleh setiap orang, tapi kunci untuk dekripsi hanya diketahui oleh orang yang berwenang mengetahui data yang disandikan atau sering disebut kunci pribadi (private key). Contoh algoritma terkenal yang menggunakan kunci publik adalah RSA dan ECC.

Public key cryptography (lawan dari *symmetric key cryptography*) bekerja berdasarkan fungsi satu arah. Fungsi yang dapat dengan mudah dikalkulasi akan tetapi sangat sulit untuk dibalik/*invers* atau *reverse* tanpa informasi yang mendetail. Salah satu contoh adalah faktorisasi; biasanya akan sulit untuk memfaktorkan bilangan yang besar, akan tetapi mudah untuk melakukan faktorisasi. Contohnya, akan sangat sulit untuk memfaktorkan 4399 daripada memverifikasi bahwa 53 x 83 = 4399. *Public key cryptography* menggunakan sifat-sifat asimetrik ini untuk membuat fungsi satu arah, sebuah fungsi dimana semua orang dapat melakukan satu operasi (enkripsi atau verifikasi sign) akan tetapi sangat sulit untuk menginvers operasi (dekripsi atau membuat sign) tanpa informasi yang selengkap-lengkapnya.

Public key cryptography dilakukan dengan menggabungkan secara kriptografi dua buah kunci yang berhubungan yang kita sebut sebagai pasangan kunci publik dan kunci privat. Kedua kunci tersebut dibuat pada waktu yang bersamaan dan berhubungan secara matematis. Secara matematis, kunci privat dibutuhkan untuk melakukan operasi invers terhadap kunci public dan kunci publik dibutuhkan untuk melakukan operasi invers terhadap operasi yang dilakukan oleh kunci privat.

Jika kunci publik didistribusikan secara luas, dan kunci privat disimpan di tempat yang tersembunyi maka akan diperoleh fungsi dari banyak ke satu. Semua orang dapat menggunakan kunci publik untuk melakukan operasi kriptografi akan tetapi hanya orang yang memegang kunci privat yang dapat melakukan invers terhadap data yang telah terenkripsi tersebut. Selain itu dapat juga diperoleh fungsi dari satu ke banyak, yaitu pada saat orang yang memegang kunci privat melakukan operasi enkripsi maka semua

orang yang memiliki kunci publik dapat melakukan invers terhadap data hasil enkripsi tersebut.

Pada algoritma public key ini, semua orang dapat mengenkripsi data dengan memakai public key penerima yang telah diketahui secara umum. Akan tetapi data yang telah terenkripsi tersebut hanya dapat didekripsi dengan menggunakan private key yang hanya diketahui oleh penerima.

Sistem kriptografi kunci-publik juga cocok untuk kelompok pengguna di lingkungan jaringan komputer (LAN/WAN). Setiap pengguna jaringan mempunyai pasangan kunci publik dan kunci privat yang bersuaian. Kunci publik, karena tidak rahasia, biasanya disimpan di dalam basisdata kunci yang dapat diakses oleh pengguna lain. Jika ada pengguna yang hendak berkirim pesan ke pengguna lainnya, maka ia ia perlu mengetahui kunci publik penerima pesan melalui basisdata kunci ini lalu menggunakannya untuk mengenkripsi pesan. Hanya penerima pesan yang berhak yang dapat mendekripsi pesan karena ia mempunyai kunci privat. Dengan sistem kriptografi kunci-publik, tidak diperlukan

pengiriman kunci privat melalui saluran komunikasi khusus sebagaimana pada sistem kriptografi simetri. Meskipun kunci publik diumumkan ke setiap orang di dalam kelompok, namun kunci publik perlu dilindungi agar otentikasinya terjamin (misalnya tidak diubah oleh orang lain).

3. Metode Penelitian

Pada sistem kriptografi kunci-publik, kunci kriptografi dibuat sepasang, satu kunci untuk enkripsi dan satu kunci untuk dekripsi. Kunci untuk enkripsi diumumkan kepada publik oleh karena itu tidak rahasia – sehingga dinamakan kunci publik (public key) disimbolkan dengan *e*. Karena ada kunci enkripsi kunci dekripsi, maka sistem kriptografi kunci-publik kadang-kadang disebut juga sistem kriptografi asimetri. Kunci untuk dekripsi bersifat rahasia – sehingga dinamakan kunci privat (private key), disimbolkan dengan *d*. Sistem kriptografi kunci-publik didasarkan pada fakta:

1. Komputasi untuk enkripsi/dekripsi pesan mudah dilakukan.
2. Secara komputasi hampir tidak mungkin (infeasible) menurunkan kunci privat, d, bila diketahui kunci publik, e, pasangannya.

Kedua fakta di atas analog dengan :

1. Perkalian vs Pemfaktoran
   Mengalikan dua buah bilangan prima, axb=n adalah mudah, tetapi memfaktorkan n dengan faktor –faktor primanya sulit.

Contoh : 31 x 47 = 1457 (perkalian)
1457 = … x … (pemfaktoran)

2. Perpangkatan vs logaritmik
   Melakukan perpangkatan y=ax adalah mudah, tetapi menghitung x=a log y sulit jika a tidak diketahui.
   Contoh : 12^5=248832
   x = ^{a}log 248832 = … (logaritmik)

Dari sekian banyak algoritma kunci publik yang pernah dibuat, algoritma yang paling populer adalah 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.

Besaran-besaran yang digunakan pada algoritma RSA:

1. p dan q bilangan prima (rahasia)
2. r = p . q (tidak rahasia)
3. ϕ (r) = (p – 1)(q – 1) (rahasia)
4. PK (kunci enkripsi) (tidak rahasia)
5. SK (kunci dekripsi) (rahasia)
6. X (plainteks) (rahasia)
7. Y (cipherteks) (tidak rahasia)

Algoritma RSA didasarkan pada teorema Euler yang menyatakan bahwa

$$a^{\phi(r)} \equiv 1 \pmod{r} \qquad (1)$$

Yang dalam hal ini,

1. a harus relatif prima terhadap r
2. $\phi(r) = r(1 - 1/p_1)(1 - 1/p_2) \ldots (1 - 1/p_n)$, yang dalam hal ini $p_1, p_2, \ldots, p_n$ adalah faktor prima dari r.

- $\phi(r)$ adalah fungsi yang menentukan berapa banyak dari bilangan-bilangan 1, 2, 3, …, r yang relatif prima terhadap r.
- Berdasarkan sifat $a^m \equiv b^m \pmod{r}$ untuk m bilangan bulat ≥ 1, maka persamaan (1) dapat ditulis menjadi

$$a^{m\phi(r)} \equiv 1^m \pmod{r}$$

atau

$$a^{m\phi(r)} \equiv 1 \pmod{r} \qquad (2)$$

- Bila a diganti dengan X, maka persamaan (2) menjadi

$$X^{m\phi(r)} \equiv 1 \pmod{r} \qquad (3)$$

- Berdasarkan sifat $ac \equiv bc \pmod{r}$, maka bila persamaan (3) dikali dengan X menjadi:

$$X^{m\phi(r)+1} \equiv X \pmod{r} \qquad (4)$$

yang dalam hal ini X relatif prima terhadap r.

- Misalkan SK dan PK dipilih sedemikian sehingga

$$SK \cdot PK \equiv 1 \pmod{\phi(r)} \quad (5)$$

atau

$$SK \cdot PK = m\phi(r) + 1 \quad (6)$$

- Sulihkan (6) ke dalam persamaan (4) menjadi:

$$X^{SK \cdot PK} \equiv X \pmod{r} \quad (7)$$

- Persamaan (7) dapat ditulis kembali menjadi

$$(X^{PK})^{SK} \equiv X \pmod{r} \quad (8)$$

yang artinya, perpangkatan *X* dengan *PK* diikuti dengan perpangkatan dengan *SK* menghasilkan kembali *X* semula.

- Berdasarkan persamaan (8), maka enkripsi dan dekripsi dirumuskan sebagai berikut:

$$E_{PK}(X) = Y \equiv X^{PK} \bmod r \quad (8)$$

$$D_{SK}(Y) = X \equiv Y^{SK} \bmod r \quad (9)$$

- Karena $SK \cdot PK = PK \cdot SK$, maka enkripsi diikuti dengan dekripsi ekivalen dengan dekripsi diikuti enkripsi:

$$E_{SK}(D_{SK}(X)) = D_{SK}(E_{PK}(X)) \equiv X^{PK} \bmod r \quad (10)$$

- Oleh karena $X^{PK} \bmod r \equiv (X + mr)^{PK} \bmod r$ untuk sembarang bilangan bulat *m*, maka tiap plainteks *X*, *X* + *r*, *X* + 2*r*, …, menghasilkan cipherteks yang sama. Dengan kata lain, transformasinya dari banyak ke satu. Agar transformasinya satu-ke-satu, maka *X* harus dibatasi dalam himpunan {0, 1, 2, …, *r* – 1} sehingga enkripsi dan dekripsi tetap benar seperti pada persamaan (8) dan (9).

Prosedur Membuat Pasangan Kunci

1. Pilih dua buah bilangan prima sembarang, *p* dan *q*.
2. Hitung $r = p \cdot q$. Sebaiknya $p \neq q$, sebab jika $p = q$ maka $r = p^2$ sehingga *p* dapat diperoleh dengan menarik akar pangkat dua dari *r*.
3. Hitung $\phi(r) = (p - 1)(q - 1)$.
4. Pilih kunci publik, *PK*, yang relatif prima terhadap $\phi(r)$.
5. Bangkitkan kunci rahasia dengan menggunakan persamaan (5), yaitu $SK \cdot PK \equiv 1 \pmod{\phi(r)}$.

Perhatikan bahwa $SK \cdot PK \equiv 1 \pmod{\phi(r)}$ ekivalen dengan $SK \cdot PK = 1 + m\phi(r)$, sehingga *SK* dapat dihitung dengan

$$SK = \frac{1 + m\phi(r)}{PK} \quad (11)$$

Akan terdapat bilangan bulat *m* yang menyebabkan memberikan bilangan bulat *SK*.

Catatan: *PK* dan *SK* dapat dipertukarkan urutan pembangkitannya. Jika langkah 4 diganti dengan "Pilih kunci rahasia, SK, yang …", maka pada langkah 5 kita menghitung kunci publik dengan rumus yang sama.

Contoh 1. Misalkan $p = 47$ dan $q = 71$ (keduanya prima). Selanjutnya, hitung nilai

$$r = p \cdot q = 3337$$

dan

$$\phi(r) = (p - 1)(q - 1) = 3220.$$

Pilih kunci publik *SK* = 79, karena 79 relatif prima dengan 3220. *PK* dan *r* dapat dipublikasikan ke umum.

Selanjutnya akan dihitung kunci dekripsi *SK* seperti yang dituliskan pada langkah instruksi 5 dengan menggunakan persamaan (11),

$$SK = \frac{1 + (m \times 3220)}{79}$$

Dengan mencoba nilai-nilai $m = 1, 2, 3, \ldots$, diperoleh nilai *SK* yang bulat adalah 1019. Ini adalah kunci dekripsi yang harus dirahasiakan.

Enkripsi

- Plainteks disusun menjadi blok-blok $x_1, x_2, \ldots$, sedemikian sehingga setiap blok merepresentasikan nilai di dalam rentang 0 sampai $r - 1$.
- Setiap blok x_i dienkripsi menjadi blok y_i dengan rumus

$$y_i = x_i^{PK} \bmod r$$

Dekripsi

- Setiap blok cipherteks y_i didekripsi kembali menjadi blok x_i dengan rumus

$$x_i = y_i^{SK} \bmod r$$

Contoh 2. Misalkan plainteks yang akan dienkripsikan adalah

X = HARI INI

atau dalam sistem desimal (pengkodean ASCII) adalah

7265827332737873

Pecah X menjadi blok yang lebih kecil, misalnya X dipecah menjadi enam blok yang berukuran 3 digit:

$x_1 = 726$ $x_4 = 273$
$x_2 = 582$ $x_5 = 787$
$x_3 = 733$ $x_6 = 003$

Nilai-nilai x_i ini masih terletak di dalam rentang 0 sampai 3337 – 1 (agar transformasi menjadi satu-ke-satu).

Blok-blok plainteks dienkripsikan sebagai berikut:

$726^{79} \bmod 3337 = 215 = y_1$
$582^{79} \bmod 3337 = 776 = y_2$
$733^{79} \bmod 3337 = 1743 = y_3$
$273^{79} \bmod 3337 = 933 = y_4$
$787^{79} \bmod 3337 = 1731 = y_5$
$003^{79} \bmod 3337 = 158 = y_6$

Jadi, cipherteks yang dihasilkan adalah

Y = 215 776 1743 933 1731 158.

Dekripsi dilakukan dengan menggunakan kunci rahasia

SK = 1019

Blok-blok cipherteks didekripsikan sebagai berikut:

$215^{1019} \bmod 3337 = 726 = x_1$
$776^{1019} \bmod 3337 = 582 = x_2$
$1743^{1019} \bmod 3337 = 733 = x_3$
…

Blok plainteks yang lain dikembalikan dengan cara yang serupa. Akhirnya kita memperoleh kembali plainteks semula

P = 7265827332737873

yang dalam karakter ASCII adalah

P = HARI INI.

Kekuatan dan Keamanan RSA

1. Keamanan algoritma *RSA* terletak pada tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi faktor primanya, yang dalam hal ini $r = p \times q$.
2. Sekali r berhasil difaktorkan menjadi p dan q, maka $\phi(r) = (p - 1)(q - 1)$ dapat dihitung. Selanjutnya, karena kunci enkrispi PK diumumkan (tidak rahasia), maka kunci dekripsi SK dapat dihitung dari persamaan $PK \cdot SK \equiv 1 \pmod{\phi(r)}$.
3. Penemu algoritma *RSA* menyarankan nilai p dan q panjangnya lebih dari 100 digit. Dengan demikian hasil kali $r = p \times q$ akan berukuran lebih dari 200 digit. Menurut Rivest dan kawan-kawan, usaha untuk mencari faktor bilangan 200 digit membutuhkan waktu komputasi selama 4 milyar tahun! (dengan asumsi bahwa algoritma pemfaktoran yang digunakan adalah algoritma yang tercepat saat ini dan komputer yang dipakai mempunyai kecepatan 1 milidetik).

Untunglah algoritma yang paling mangkus untuk memfaktorkan bilangan yang besar belum ditemukan. Inilah yang membuat algoritma *RSA* tetap dipakai hingga saat ini. Selagi belum ditemukan algoritma yang mangkus untuk memfaktorkan bilangan bulat menjadi faktor primanya, maka algoritma *RSA* tetap direkomendasikan untuk menyandikan pesan.

4. Kesimpulan

1. Kriptografi kunci publik dilakukan dengan menggabungkan secara kriptografi dua buah kunci yang berhubungan yang disebut sebagai pasangan kunci public dan kunci privat.
2. Protokol kriptografi modern pada saat ini banyak yang menggabungkan algoritma kunci publik dengan algoritma simetrik untuk memperoleh keunggulan-keunggulan pada masing-masing algoritma.
3. Pendekatan multidimensi dalam desain dan implementasi sekuriti mencakup keseluruhan sumber daya, policy, dan mekanisme sekuriti yang komprehensif.

5. Daftar Pustaka

[1] Bruce Schneier,"*Applied Criptography: Protocols, Algoritms, and Source Code in C*," second edition, John Wiley & Sons, Inc., 1996.
[2] Budi Raharjo, "*Keamanan system informasi Berbasis Internet*" PT Insan Infonesia – Bandung & PT INDOCISC – Jakarta, 2002.
[3] http://www.tedi-h.com/papers/p kripto.html, Tedi Hariyanto, "*Pengenalan Kriptografi*", edisi Juni 1999.
[4] http://www.ilmukomputer.com/populer/afs/afs-security.pdf.
[5] Phil Zimmerman, "Sekilas Tentang Enkripsi", NeoTek, April 2002.