ENKRIPSI DATA SISTEM KRIPTOGRAFI KUNCI PUBLIK MENGGUNAKAN ALGORITMA DIOPHANTINE

Oleh:

Heri Sutarno

Jurusan Pendidikan Matematika dan Ilmu Komputer FPMIPA
Universitas Pendidikan Indonesia

ABSTRAK

Sistem keamanan data dengan menggunakan "Enkripsi Data Sistem Kriptografi Kunci Publik Menggunakan Algoritma Diophantine" merupakan salah satu upaya dalam menghadapi ancaman terhadap pengrusakan hak kepemilikan data. Perkembangan teknologi informasi diikuti dengan kebutuhan akan keamanan yang tinggi terhadap data. Salah satu langkah pengamanan data adalah dengan menggunakan sistem kriptografi atau penyandian data. Dalam sebuah sistem kriptografi dikenal dua komponen utama yaitu algoritma kriptografi dan kunci. Algoritma kriptografi mencakup transformasi data ke bentuk sandi atau dikenal sebagai enkripsi dan transformasi data dari bentuk sandi kembali ke data awal atau disebut sebagai dekripsi. Jenis kriptografi yang sekarang banyak dikembangkan adalah kriptografi kunci publik. Kelebihannya terletak pada kunci yang digunakan tidak sama atau asimetri antara proses enkripsi dan proses dekripsi. Dalam tulisan ini persamaan Diophantine merupakan materi utama yang digunakan dalam pembuatan algoritma kriptografi. Secara umum tulisan ini menguraikan tentang sistem kriptografi kunci publik menggunakan algoritma Diophantine dimulai dengan penjelasan teori yang mendasari, algoritma yang dipakai, desain dan analisis algoritma Diophantine.

Kata kunci: *Keamanan Data , Sistem Kriptografi, Persamaan Diophantine*

LATAR BELAKANG MASALAH

Perkembangan teknologi komputer saat ini sangat pesat. Hal tersebut harus diikuti dengan peningkatan sistem keamanan yang melindungi sistem komputer. Perlu diingat bahwa perkembangan teknologi komputer ini diikuti dengan perkembangan teknologi untuk merusak sistem komputer baik itu pembajakan, penyusupan, perusakan sistem dan sebagainya. Ada aspek penting yang perlu dijaga dalam suatu sistem komputer, yaitu keamanan data dan keamanan jaringan. Keamanan data dipergunakan untuk melindungi data yang isi informasi dari data tersebut bersifat penting dan rahasia. Keamanan jaringan dipergunakan untuk transmisi data dalam suatu jaringan dimana isi informasi data tersebut sangat penting. Salah satu cara yang digunakan dalam menangani dua buah aspek diatas ialah dengan pengkodean atau penyandian data.

Ilmu yang mempelajari pengkodean atau penyandian data disebut sebagai kriptografi. Adapun inti dari teknik kriptografi adalah mentransformasikan data jelas *(plaintext)* menjadi bentuk sandi *(chipertext)* menggunakan suatu kunci, juga proses sebaliknya. Proses transformasi dari *plaintext* menjadi *chipertext* disebut sebagai enkripsi, sedangkan proses kebalikannya disebut dekripsi.

Teknik kriptografi terbagi menjadi dua jenis yaitu kriptografi tradisional dan kriftografi modern. Untuk saat ini tentunya yang dipergunakan yaitu kriptografi modern. Kriptografi modern pun terdiri dari berbagai macam bentuk, salah satunya adalah kriptografi kunci publik yang selanjutnya menjadi topik utama dalam pembahasan tulisan ini. Ciri khas dari kriptografi kunci publik adalah penggunaan kunci asimetris dalam proses enkripsi dan dekripsi, yang berarti teknik ini memiliki dua buah kunci yang berbeda. Enkripsi dan dekripsi diproses menggunakan kunci yang berbeda.

Teknik kriptografi kunci publik terdiri dari berbagai macam jenis hal ini tergantung dari penggunaan algoritma dalam proses enkripsi dan dekripsi. Semua kemungkinan terus digali demi menghasilkan algoritma yang baik untuk digunakan dalam teknik ini, hal ini akan berpengaruh terhadap tingkat keamanan yang dihasilkan. Semakin baik algoritma yang dipakai maka semakin tinggi tingkat keamanan yang diperoleh.

Salah satu algoritma yang cukup baik adalah algoritma yang dihasilkan dari persamaan Diophantine. Algoritma ini memberikan kemudahan bagi pengguna baik dalam proses enkripsi maupun proses dekripsi.

BATASAN MASALAH

Makalah ini hanya membahas tentang algoritma Diophantine beserta penjelasan teori yang mendasarinya, dalam hal ini tentang kriptografi, kriptografi kunci publik, dan persamaan Diophantine.

KONSEP DASAR KRIPTOGRAFI

1. Aspek Keamanan Data

Sebelum kita mengenal apa itu kriptografi terlebih dahulu kita harus menelaah aspek keamanan dan kerahasiaan data agar mempermudah pembahasan. Dalam aspek keamanan kita harus melihat apa saja yang diperlukan dalam suatu sistem keamanan sebagai persyaratan yang utama:

a. *Secrecy*. Berhubungan dengan akses membaca data dan informasi. Data dan informasi di dalam suatu sistem komputer hanya dapat diakses dan dibaca oleh orang yang berhak.

b. *Integrity*. Berhubungan dengan akses merubah data dan informasi. Data dan informasi yang berada dalam suatu sistem komputer hanya dapat dirubah oleh orang yang berhak.

c. *Availability*. Berhubungan dengan ketersediaan data dan informasi. Data dan informasi yang berada dalam suatu sistem komputer dapat dimanfaatkan oleh orang yang berhak.

2. Pengertian Kriptografi

Kriptografi berasal dari gabungan dua kata yaitu *"Crypto"* yang berarti rahasia dan *"graphy"* yang berarti tulisan. Dalam bahasa komputasi kriptografi diartikan sebagai ilmu dan seni untuk menjaga keamanan data. Ahli kriptografi disebut kriptografer. Adapun komponen kriptografi yang paling utama adalah algoritma kriptografi yang biasanya berupa persamaan matematik yang digunakan landasan utama untuk sistem perahasiaan data, juga kunci yang merupakan alat untuk merahasiakan data.

Algoritma kriptografi merupakan salah satu komponen penting dalam kriptografi merupakan satu susunan peraturan atau langkah-langkah yang tetap dalam melakukan transformasi. Dari sebuah algoritma kriptografi terdapat suatu proses untuk merahasiakan data atau pesan yang disebut sebagai chiper. Proses chiper ialah proses mentransformasikan suatu data jelas *(plaintext)* menjadi bentuk sandi *(chipertext)* dan sebaliknya. Proses ini dikenal sebagai enkripsi dan proses sebaliknya disebut sebagai dekripsi. Baik proses enkripsi maupun dekripsi keduanya menggunakan suatu kunci yang dihasilkan dari algoritma kriptografi berupa variabel yang terdiri dari urutan bit untuk mentransformasikan data.

Data yang dirahasiakan atau *plaintext* tidak hanya berupa teks tetapi juga berbagai file yang dikenal oleh komputer seperti file gambar, file suara, file biner dan sebagainya. Contohnya gif, jpg, wmv, mp3, exe, com, sys dan sebagainya.

3. Jenis Algoritma Kriptografi

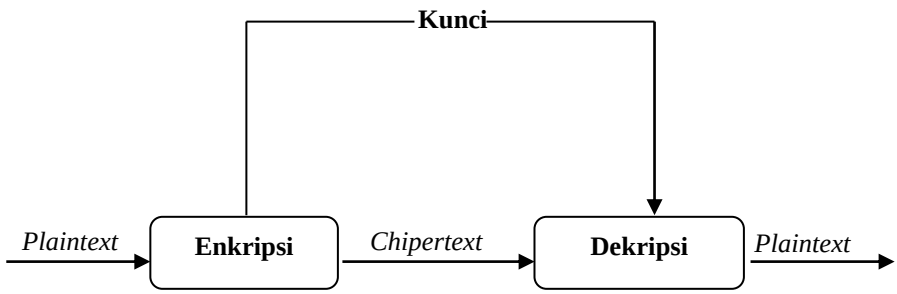
Salah satu yang membedakan jenis algoritma kriptografi adalah berdasarkan kunci yang dipakai baik dalam proses enkripsi maupun dalam proses dekripsi. Berdasarkan kunci terdapat dua jenis algoritma kriptografi yaitu:

a. Algoritma Simetri (Konvensional)

b. Algoritma Asimetri (Kunci Publik)

a. Algoritma Simetri

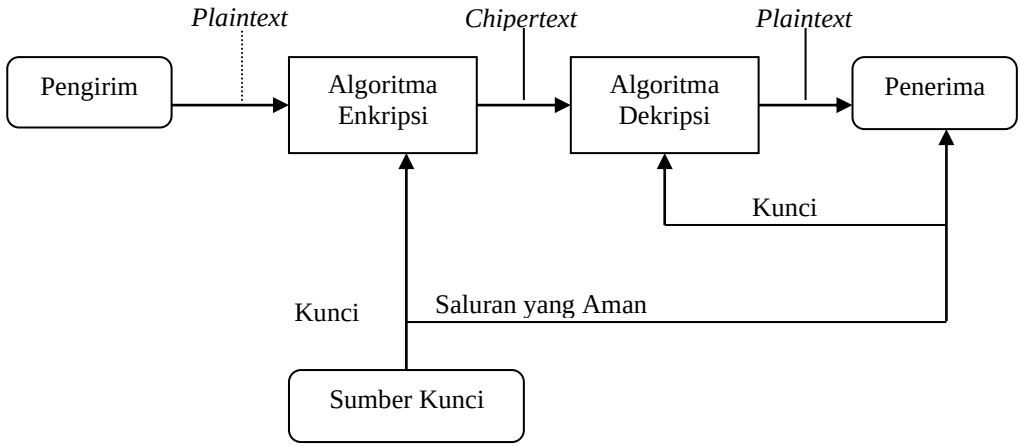
Algoritma simetri yang disebut juga sebagai algoritma konvensional adalah suatu algoritma kriptografi yang menggunakan kunci yang sama antara proses enkripsi dan proses dekripsi. Disebut konvensional karena algoritma jenis ini biasa digunakan orang sejak berabad-abad yang lalu. Algoritma simetrik sering juga disebut sebagai algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma kunci satu dan mengharuskan pengirim dan penerima kunci menyetujui suatu kunci tertentu sebelum mereka dapat berkomunikasi dengan aman. Keamanan algoritma simetri tergantung pada kunci, membocorkan kunci berarti bahwa orang lain dapat mengenkrip dan mendekrip pesan. Proses kriptografi simetri dapat dilihat pada gambar di bawah:



Gambar 1. Proses Kriptografi Simetri

Gambar diatas memperlihatkan *plaintext* dengan memakai suatu kunci melalui proses enkripsi ditransformasikan menjadi *chipertext* dan untuk mendapatkan kembali bentuk *plaintext* dilakukan proses dekripsi dengan memakai kunci yang sama pada proses enkripsi.

Dari algoritma ini dibentuk sistem dalam pengiriman data yang digambarkan pada gambar di bawah ini:



Gambar 2. Model Sistem Kriptografi Konvensional

Dari gambar diatas dapat dilihat bahwa pengirim data mengirimkan dua data. Pertama berupa data utama yang telah melalui proses enkripsi dengan menggunakan kunci yang berasal dari sumber kunci dan dikirimkan melalui saluran yang tidak aman *(unsecure channel)*. Yang kedua berupa kunci yang dipakai untuk mengenkripsi dikirimkan melalui saluran yang aman *(secure channel)*. Sedangkan penerima untuk mendapatkan data yang asli dari melakukan proses dekripsi pada *chipertext.* Notasi untuk proses enkripsi dan dekripsi pada algoritma jenis ini dituliskan dengan bentuk:

$$E_K(P) = C$$
$$D_K(C) = P$$

Artinya pada proses enkripsi dengan menggunakan kunci K terhadap *plaintext* P akan menghasilkan *chipertext* C, sedangkan pada proses dekripsi dengan menggunakan kunci K yang sama terhadap *chipertext* C akan menghasilkan *plaintext* P kembali.

b. Algoritma Asimetri

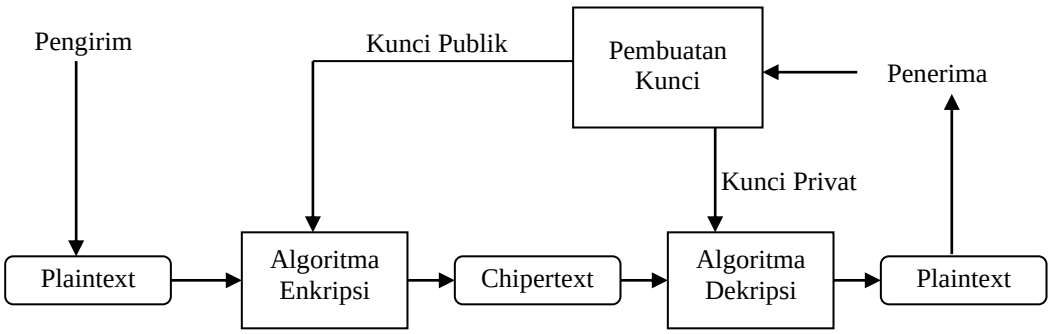
Algoritma ini disebut juga sebagai algoritma Kunci Publik didesain sedemikian sehingga kunci yang digunakan untuk proses enkripsi berbeda dengan kunci yang digunakan untuk proses dekripsi. Algoritma disebut kunci publik yang berarti semua orang boleh mengetahui salah satu kunci. Sembarang orang dapat menggunakan kunci enkripsi tersebut untuk mengenkrip data, namun hanya orang tertentu yang dapat mendekrip data tersebut yakni calon penerima data dan sekaligus pemegang kunci untuk proses dekripsi. Dalam sistem ini, kunci enkripsi disebut sebagai kunci publik, sementara kunci dekripsi disebut kunci privat.

Notasi untuk proses enkripsi dan dekripsi pada algoritma jenis ini dituliskan dengan bentuk:

$$E_{Ke}(P) = C$$
$$D_{Kd}(C) = P$$

Artinya pada proses enkripsi dengan menggunakan kunci publik Ke terhadap *plaintext* P akan menghasilkan *chipertext* C, sedangkan pada proses dekripsi dengan menggunakan kunci privat Kd terhadap *chipertext* C akan menghasilkan *plaintext* P kembali. Di sini Ke merupakan pasangan Kd. Artinya tidak ada Kd lain yang dapat digunakan untuk melakukan dekripsi terhadap C yang merupakan hasil enkripsi dengan menggunakan kunci Ke.

Dari algoritma jenis ini dibuat suatu model sistem kriptografi tanpa adanya prosedur pengiriman kunci rahasia sehingga tingkat keamanannya dirasakan lebih tinggi.



Gambar 3. Model Sistem Kriptografi Kunci Publik

Dari gambar di atas terlihat bahwa dalam sistem kriptografi kunci publik penerima data justru yang melakukan pembuatan kunci yakni kunci publik dan kunci privat. Kunci publik dikirimkan kepada pengirim yang telah disepakati oleh berdua, selain itu kunci publik tersebut bisa disebarkan kepada siapa saja orang yang hendak mengirimkan data rahasia. Selanjutnya pengirim melakukan prosedur enkripsi terhadap data yang akan dikirimkan. Kemudian data dikirimkan kepada penerima melalui saluran yang tidak aman. Pihak penerima yang menginginkan data dalam bentuk aslinya kemudian akan melakukan prosedur dekripsi terhadap data yang diterima dengan menggunakan kunci privat yang dimiliki. Dari sistem ini dapat dilihat kunci rahasia yakni kunci privat tidak mengalami pendistribusian, hal ini setidaknya lebih menjamin tingkat keamanan sistem kriptografi kunci publik.

Agar menjadi suatu sistem yang lebih stabil algoritma kriptografi kunci publik harus memenuhi beberapa kondisi, yaitu:

1) Untuk menghasilkan pasangan kunci publik dan kunci privat, metoda perhitungan harus mudah bagi si penerima.
2) Kunci privat akan sulit didapatkan, jika yang diketahui hanya kunci publik.
3) Prosedur memproses data jelas atau *plaintext* menjadi *chipertext* atau proses enkripsi harus mudah bagi pengirim.
4) Untuk mendapatkan *plaintext* sangatlah sulit bila menggunakan kunci publik dan *chipertext* saja.
5) Prosedur memproses kembali *chipertext* menjadi data jelas atau proses dekripsi harus mudah bagi si penerima.
6) Proses enkripsi merupakan kebalikan dari proses dekripsi.

Dari beberapa kondisi yang harus dipenuhi oleh sistem algoritma kriptografi kunci publik di atas dibuatlah sebuah prosedur untuk mempermudah proses pertukaran data, yaitu:

1) Pihak penerima data di dalam jaringan menghasilkan sepasang kunci, yaitu kunci publik dan kunci privat. Kunci privat dijaga kerahasiaannya oleh pihak penerima data sehingga tidak ada seorangpun yang mengetahuinya.
2) Pihak penerima data kemudian mempublikasikan kunci publik ke suatu media publik sehingga dapat diakses atau diterima oleh pihak pengirim data.
3) Pihak pengirim data kemudian melakukan prosedur enkripsi terhadap data yang akan ia kirimkan dengan menggunakan kunci publik dari pihak penerima data, dan mengirimkan hasilnya berupa *chipertext* kepada pihak penerima data.
4) Pihak penerima data kemudian akan melakukan prosedur dekripsi terhadap *chipertext* yang dia dapatkan dari pihak pengirim data, dengan menggunakan kunci privat yang dirahasiakan sehingga dia akan mendapatkan data asli.

Salah satu aspek penting yang wajib diperhatikan bagi pengguna sistem algoritma kriptografi jenis ini adalah manajemen kunci. Tujuan dari manajemen kunci adalah menyediakan suatu prosedur yang aman untuk menangani kunci kriptografi. Walaupun

sistem algoritmanya sangat sulit untuk dipecahkan, namun secara keseluruhan sistem tentunya akan mudah diketahui dengan cepat bila keamanan dan kerahasiaan kunci tidak cukup terlindungi.

Sekarang ini orang lebih cenderung memilih sistem algoritma kriptografi jenis ini jika dibandingkan dengan sistem algoritma kriptografi simetri karena relatif lebih kuat dan aman. Adapun beberapa contoh sistem kriptografi yang menerapkan algoritma kriptografi jenis ini antara lain: *RSA, LUCAS Public Key Encryption, DSS* dan lain-lain.

Dapat kita simpulkan bahwa kriptografi asimetri cenderung lebih aman dan kuat dikarenakan memiliki dua buah kunci yang dipakai untuk proses enkripsi dan dekripsi secara berbeda. Untuk itu banyak kalangan sekarang mengembangkan jenis kriptografi ini dibandingkan menggunakan kriptografi simetri.

4. Hubungan Aspek Keamanan dengan Kriptografi

Metode kriptografi baik itu simetri maupun asimetri dalam hal kerahasiaan dan keamanan data memenuhi beberapa aspek keamanan, yaitu:

a. *Privacy*. Mencegah perolehan pesan atau data dari saluran komunikasi secara tidak sah oleh pihak yang tidak berhak atas data tersebut.

b. *Authenticity* dan *Integrity*. Mencegah modifikasi data ke dalam saluran komunikasi oleh pihak yang tidak berhak sehingga merugikan pihak yang berkepentingan dengan data tersebut.

Adapun jika kita memandang terhadap hubungan antara algoritma kriptografi secara langsung dengan kondisi keamanan yang dipenuhi oleh kriptografi itu sendiri adalah:

a. Untuk privasi dipenuhi karena dalam algoritma kriptografi kunci dekripsi sangatlah sulit untuk memecahkannya dari *chipertext* secara sistematis karena memerlukan perhitungan yang rumit. Juga sulit untuk mendapatkan data jelas atau *plaintext* secara sistematis dari *chipertext*.

b. Untuk keautentikan dan integritas dipenuhi karena sangat sulit memecahkan algoritma dan kunci enkripsi dari *chipertext* secara sistematis, juga sangat sulit untuk mendapatkan *chipertext* itu sendiri.

Dengan kata lain metode kriptografi memenuhi aspek keamanan dan kerahasiaan data sehingga dipandang cukup baik dalam melindungi data.

5. Kekuatan Algoritma Kriptografi

Ada tiga kondisi yang diperhatikan dalam menilai kekuatan sebuah algoritma kriptografi, yakni:

a. *Data Complexity*. Jumlah data yang diperlukan sebagai sarana yang digunakan kriptanalis untuk memecahkan algoritma. Semakin sedikit jumlah data yang diperlukan untuk memecahkan algoritma, berarti kualitas algoritma yang digunakan semakin tidak baik.

b. *Processing complexity*. Lama waktu yang tersedia untuk melakukan pemecahan algoritma. Ini disebut juga sebagai faktor kerja. Semakin cepat waktu yang dibutuhkan, berarti semakin buruk kualitas algoritma yang digunakan.

c. *Storage requirements*. Jumlah memori yang dibutuhkan untuk melakukan pemecahan kode.

Dari tiga kondisi diatas dapat kita telaah algoritma kriptografi dikatakan cukup aman atau kuat jika memenuhi hal seperti yang diuraikan di bawah ini:

a. Bila harga yang dipakai untuk memecahkan suatu algoritma kriptografi lebih besar dari nilai informasi yang dibuka, maka algoritma tersebut cukup aman. Misalnya, diperlukan komputer senilai 1 juta dolar untuk menjebol algoritma yang digunakan untuk melindungi informasi senilai 100 ribu dolar, maka algoritma yang digunakan termasuk kategori aman.

b. Bila waktu yang diperlukan untuk memecahkan algoritma kriptografi lebih lama dari lamanya waktu yang diperlukan oleh informasi tersebut harus tetap aman, maka algoritma tersebut aman. Misalnya waktu untuk memecahkan sebuah kartu kredit 1 tahun, sedangkan kartu tersebut sudah tidak berlaku dalam waktu kurang dari 1 tahun, maka algoritma tersebut aman.

c. Bila jumlah data yang dienkripsi dengan kunci dan algoritma yang sama lebih sedikit dari jumlah data yang diperlukan untuk menembus algoritma tersebut, maka algoritma yang digunakan termasuk aman. Misalkan diperlukan 100 chipertext untuk menebak kunci yang digunakan pada algoritma X. Sedangkan satu kunci hanya digunakan untuk satu pesan, maka algoritma tersebut aman.

KRIPTOGRAFI KUNCI PUBLIK MENGGUNAKAN DIOPHANTINE

1. Persamaan Diophantine

Persamaan Diophantine diambil dari nama seorang matematikawan Yunani, *Diophantus Alexandria*, yang lahir sekitar tahun 250 Masehi dan termasuk orang yang pertama kali mempelajari teori bilangan. Persamaan ini merupakan persamaan polinom dengan peubah banyak:

$$f(x_1, x_2, ..., x_n) = 0 \qquad (1)$$

dengan $x_i \geq 0$, i = 1, 2, 3,…, n, dan memiliki koefisien bilangan bulat, yang kemudian dicari solusi bilangan bulatnya.

Persamaan Diophantine yang dipakai dalam hal ini dibatasi hanya dalam bentuk persamaan Diophantine linear. Dalam persamaan linear peubah yang dipakai hanya berderajat satu. Bentuk umum persamaan Diophantine linear dengan n peubah adalah:

$$a_1x_1 + a_2x_2 + ... + a_nx_n = c \qquad (2)$$

dengan nilai a, x, dan c merupakan bilangan bulat yang tidak sama dengan nol. Persamaan (2) merupakan dasar utama dalam pembuatan sistem kriptografi kunci publik dimana nilai a sebagai nilai yang digunakan untuk menghasilkan kunci dan nilai x merupakan bagian *plaintext* yang akan dienkripsi, sedang c merupakan bagian yang berkoresponden dengan *chipertext*. Solusi dari persamaan ini yang diterapkan pada sistem kriptografi harus tidak negatif. Karena *plaintext* yang dienkripsikan berupa kode- kode ASCII yang tidak memiliki nilai negatif.

Teorema 1

Ada sejumlah bilangan bulat $x_1, x_2, ..., x_n$ sedemikian sehingga:

$$a_1x_1 + a_2x_2 + ... + a_nx_n = c, n > 1 \quad (3)$$

dimana a dan c merupakan bilangan bulat dengan nilai tidak sama dengan nol, jika dan hanya jika $FPB(a_1, a_2, ..., a_n)$ merupakan faktor dari c.

Teorema diatas memperlihatkan bahwa faktor persekutuan terbesar dari $(a_1, a_2, ..., a_n)$ atau $FPB(a_1, a_2, ..., a_n)$ harus merupakan faktor dari c. Hal ini dikarenakan untuk mendapatkan solusi berupa bilangan bulat. Misalkan:

$$d = FPB(a_1, a_2, ..., a_n) \quad (4)$$

Karena d merupakan faktor dari c maka dimisalkan ada suatu bilangan c_1 sehingga membentuk persamaan:

$$c = c_1d \quad (5)$$

Dengan kembali menentukan bilangan bulat $b_1, b_2, ..., b_n$, sehingga diperoleh persamaan:

$$d = a_1b_1 + a_2b_2 + ... + a_nb_n \quad (6)$$

Kemudian diperoleh

$$c = c_1d = a_1(c_1b_1) + a_2(c_2b_2) + ... + a_n(c_nb_n) \quad (7)$$

Sehingga persamaan diatas memiliki bilangan bulat dan dengan mempergunakan algoritma Euclidean kita dapat memperoleh nilai $b_1, b_2, ..., b_n$.

Agar mempermudah pemahaman tentang persamaan linear Diophantine maka kita akan melihat sebuah contoh permasalahan persamaan linear Diophantine. Misalkan suatu persamaan,

$$1027x + 712y = 1$$

kita akan menentukan solusi dari persamaan diatas.

Kita hitung :

$$\text{FPB}(1027,712) = 1$$

Karena nilai 1 merupakan faktor dari 1 maka persamaan diatas akan memiliki solusi bilangan bulat. Berdasarkan algoritma Euclid maka akan diperoleh:

$$\begin{array}{rcl|rcl}
1027 = 712 \cdot 1 + 315 & | & & 1 = -165 \cdot 1027 + 238 \cdot 712 & \uparrow \\
712 = 315 \cdot 2 + 82 & | & & 1 = 73 \cdot 712 - 165 \cdot 315 & | \\
315 = 82 \cdot 3 + 69 & | & & 1 = -19 \cdot 315 + 73 \cdot 82 & | \\
82 = 69 \cdot 1 + 13 & | & & 1 = 16 \cdot 82 - 19 \cdot 69 & | \\
69 = 13 \cdot 5 + 4 & | & & 1 = -3 \cdot 69 + 16 \cdot 13 & | \\
13 = 4 \cdot 3 + 1 & \downarrow & & 1 = 1 \cdot 13 - 3 \cdot 4 & | \\
 & & & 1 = 0 \cdot 4 + 1 \cdot 1 & |
\end{array}$$

Berdasarkan perhitungan diatas maka solusi yang didapatkan, $x = -165, y = 238$.

Dari contoh diatas secara umun solusi dari persamaan Diophantine linear dapat memiliki nilai negatif. Karena dalam sistem kriptografi kunci publik tidak mengenal nilai negatif maka solusi haruslah bernilai tidak negatif.

Solusi dari persamaan Diophantine linear dapat lebih dari satu atau memiliki kemungkinan banyak solusi, hal ini ditunjukan dalam teorema di bawah ini.

Teorema 2.

Persamaan linear $ax + by = c$ tidak mempunyai solusi jika FPB(a, b) tidak membagi c. Jika FPB(a, b) membagi c maka akan dihasilkan tak terbatas banyak solusi oleh:

$$x = x_0 + \frac{b}{\text{FPB}(a,b)}t, \quad y = y_0 - \frac{a}{\text{FPB}(a,b)}t,$$

dimana $x = x_0$, $y = y_0$ adalah sembarang solusi dengan sembarang bilangan bulat t.

2. Algoritma Diophantine Dalam Sistem Kriptografi Kunci Publik

Metode kriptografi kunci publik dengan memakai persamaan Diophantine linear sebagai algoritma kriptografinya disusun berdasar landasan matematis sebagai berikut:

z = ax + by

cz = acx + bcy

Jika ac = 1 mod d dan bc = e mod d, maka x = cz mod d mod e.

Dari landasan diatas maka dibentuk susunan algoritma sebagai berikut:

Menentukan pasangan bilangan $(d_1,t_1),(d_2,t_2),...,(d_n,t_n)$ yang harus memenuhi syarat sebagai berikut:

a. $\text{FPB}(d_i,d_j)=1$ untuk $i \neq j$, dengan t_i adalah suatu bilangan bulat positif.

b. $t_i > x_i$, x_i adalah bagian plaintext yang dienkripsi untuk $i=1,2,...,n$.

c. $d_i > t_i w(d_i \bmod t_i)$, dan $d_i \bmod t_i \neq 0$, untuk $i=1,2,3,...,n$. w adalah banyaknya pembagian plaintext untuk dienkripsi.

Kondisi diatas selanjutnya akan disebut sebagai kondisi DK, n buah pasangan bilangan (d_i,d_j) akan digunakan sebagai alat untuk membuat kunci publik. Setelah kondisi DK dipenuhi maka selanjutkan kita menghitung:

$$D_i = d_1 * d_2 * ... * d_{i-1} * d_{i+1} * ... * d_n = \prod_{\substack{j=1 \\ j\neq i}}^{n} d_i$$

$$R_i = \left\lceil \frac{d_i}{(t_i(d_i \bmod t_i))} \right\rceil$$

Kemudian kita tentukan nilai b_i berdasarkan algoritma Euclid sehingga memenuhi kondisi,

$$D_i b_i \bmod d_i = d_i \bmod t_i, \text{ untuk } i=1,2,3,...,n$$

Kemudian tentukan nilai

$$S_i = D_i b_i \text{ dan } a_i = R_i S_i \bmod D, \text{ untuk } i=1,2,3,...,n$$

Dengan

$$D = \prod_{i=1}^{n} d_i$$

Selanjutnya kita tentukan nilai $A=(a_1,a_2,...,a_n)$ yang merupakan nilai pembuat kunci publik serta pasangan bilangan $(d_1,t_1),(d_2,t_2),...,(d_n,t_n)$ sebagai nilai pembuat kunci privat.

3. Analisis Algoritma Diophantine

Setiap algoritma kriptografi dalam sebuah sistem kriptografi harus memiliki kekuatan yang cukup tinggi sehingga tingkat keamanan terhadap data yang dirahasiakan oleh sistem tersebut cukup sulit ditembus oleh para kriptanalis. Ada tiga serangan yang mungkin dilakukan oleh para kriptanalis, yaitu serangan terhadap *chipertext*, serangan dengan mencari kunci privat dan serangan dengan menggunakan FPB dari kunci publik.

a. Serangan Terhadap Chipertext

Dengan mengambil asumsi bahwa kriptanalis telah mendapatkan *chipertext* dan kunci publik. Kriptanalis akan berusaha mendekripsi *chipertext* tersebut dengan memakai acuan kunci publik sebagai data untuk memecahkan algoritma yang digunakan. Berdasarkan sumber terpercaya untuk memecahkan masalah ini diperlukan pengetahuan yang tinggi tentang teori bilangan *NP- complete* dan *Integer Knapsack Problems*. Dan untuk mendapatkan *plaintext* dengan teori tersebut memerlukan perhitungan yang rumit dan pengambilan contoh data yang banyak. Apalagi sistem komputer yang diperlukan harus memiliki tingkat paralelisme yang tinggi. Hal ini tidak memenuhi kondisi *Data Complexcity* dan *Storage Requirements* seperti yang telah dijelaskan dalam bab sebelumnya sehingga dengan serangan seperti ini sistem kriptografi cukup aman untuk digunakan.

b. Serangan Dengan Pencarian Kunci Privat

Dengan asumsi kriptanalis mengetahui beberapa kunci publik dan berusaha mendapatkan kunci privat dari kunci publik. Metode ini termasuk cukup sulit karena kriptanalis harus terlebih dahulu mengetahui algoritma kriptografi untuk proses pembuatan kunci dan dengan perhitungan rumit dimisalkan kriptanalis akan mendapatkan pasangan bilangan kunci privat. Metoda ini akan terbentur pada kondisi DK pasangan bilangan kunci privat yang telah dijelaskan dalam bab sebelumnya. Belum tentu pasangan bilangan kunci privat yang berhasil didapatkan oleh kriptanalis dapat memenuhi kondisi DK, sehingga perlu banyak perhitungan data untuk menemukan kunci privat tersebut. Tentu saja hal ini bertentangan dengan *Data Complexcity* sehingga algoritma kriptografi jenis ini aman terhadap serangan terhadap kunci privat.

c. Serangan Menggunakan FPB Kunci Publik

Dengan asumsi bahwa kriptanalis telah mengetahui kunci publik dan *chipertext* serta mengamati FPB dari kunci tersebut. Para kriptanalis berusaha membuat algoritma untuk mendapatkan *plaintext*. Adapun algoritma yang disusun para kriptanalis memerlukan perhitungan yang cukup memakan waktu, yaitu:

Tahap 1 : Menghitung nilai t_i, untuk $i = 1,2,3,...,n$:

$$t_i = \frac{FPB(a_1, a_2, ..., a_{i-1}, a_{i+1}, ..., a_n)}{FPB(a_1, a_2, ..., a_{i-1}, a_i, a_{i+1}, ..., a_n)}$$

Tahap 2 : Hitung $r_{ij} = ja_i \bmod a_i$, untuk $j = 1,2,3,...,n$ yang dalam hal ini $w = 2^b - 1$ dengan panjang sebuah sub pesan adalah b bits.

Tahap 3 : Hitung $h_i = C \bmod t_i$ untuk $j = 1,2,3,...,n$.

Tahap 4 : Tentukan k_i untuk $j = 1,2,3,...,n$ dari himpunan $\{r_{1i}, r_{2i}, ..., r_{wi}\}$, jika $h_i = r_{ki}$, maka $x_i = k$.

Dari tahap diatas x_i dapat disimpulkan dari c dan $A = (a_1, a_2, ..., a_n)$. Walaupun demikian jika suatu pesan dipecah menjadi sub-pesan dengan panjang setiap sub-pesan 100 bit, b = 100 dan $w = 2^b - 1$. Bilangan ini mempunyai nilai sebesar sekitar 10^{30}. Jika komputer yang digunakan untuk memecahkan *chipertext* dapat melakuakan perhitungan 10^6 setiap detik, hal ini akan membutuhkan waktu sekitar $2{,}7 \times 10^{16}$ tahun untuk menyelesaikan pencarian setiap h_i . Dari itu hal ini tidak dapat memenuhi *Processing Complexcity* sehingga algoritma kriptografi aman digunakan.

KESIMPULAN

Berdasarkan penjelasan dari bab – bab sebelumnya juga dari analisa program dapat ditarik kesimpulan. Dalam sistem jaringan komputer diperlukan pengamanan yang cukup guna melindungi hak pemilik data. Sistem kriptografi salah satu cara pengamanan jaringan komputer yang dipandang memiliki tingkat keamanan yang tinggi. Algoritma persamaan Diophantine cukup baik untuk digunakan sebagai algoritma kriptografi dalam suatu sistem kriptografi. Program enkripsi dengan mengacu pada sistem kriptografi kunci publik mempunyai tingkat keamanan yang lebih baik jika dibandingkan dengan program enkripsi yang berdasarkan pada sistem kriptografi asimetri atau kunci rahasia.

DAFTAR PUSTAKA

Brown,L. (1996). Number Theory and Public Key Cryptography.[online]. Tersedia: http://williamstallings.com/Extras/Security-Notes/lectures/publickey.html. [30 Januari 2006]

Chang, C.C.,Lin,C.H., Lee, R.C.T. *A New Public-Key Cipher System Based Upon the Diophantine Equation*. IEEE Trans. On Computer Vol 44. No. 1 January 1995

Kurniawan,Y. (2004). *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Penerbit Informatika :Bandung.

Wahana Komputer. (2003). *Memahami Model Enkripsi & Security Data*.

Andi Offset :Yogyakarta

Weisstein,E.W. (1999). Diophantine Equation.[online]. Tersedia : http://mathworld.wolfram.com/topics/DiophantineEquations.html. [27 April 2006]