

SISTEM KRIPTOGRAFI KUNCI PUBLIK MULTIVARIAT

Muhamad Zaki Riyanto

Pendidikan Matematika, FKIP, Universitas Ahmad Dahlan, Yogyakarta
S2 Matematika (Aljabar), FMIPA, Universitas Gadjah Mada, Yogyakarta
E-mail: zaki@mail.ugm.ac.id

Abstrak

Sistem kriptografi kunci publik merupakan skema enkripsi yang menggunakan pasangan kunci publik dan kunci rahasia. Sistem ini digunakan apabila pengiriman pesan rahasia dilakukan melalui jalur yang tidak dapat dijamin keamanannya, sehingga rawan terjadi penyadapan. Tingkat keamanan dari sistem ini diletakkan pada suatu permasalahan matematika yang sulit untuk dipecahkan. Beberapa sistem kriptografi kunci publik yang telah dikenal luas saat ini adalah RSA, ElGamal dan ECC. Dalam makalah ini dibahas mengenai konstruksi dan desain sistem kriptografi kunci publik yang didasarkan atas ring polinomial multivariat $K[x_1, \dots, x_n]$ atas lapangan hingga K yang disebut dengan sistem kriptografi kunci publik multivariat. Tingkat keamanan dari sistem ini diletakkan pada sulitnya menyelesaikan sistem persamaan polinomial multivariat atas lapangan hingga.

Kata kunci: asimetris, kriptografi kunci publik, multivariat, ring polinomial

1. Pendahuluan

Kriptografi berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data (Menezes dkk, 1996). Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi.

Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan. Ketika suatu pesan dikirim dari suatu tempat ke tempat lain, isi pesan tersebut mungkin dapat disadap oleh pihak lain yang tidak berhak untuk mengetahui isi pesan

tersebut. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain.

Enkripsi adalah sebuah proses penyandian yang melakukan perubahan sebuah kode atau pesan dari yang bisa dimengerti, disebut dengan plainteks, menjadi sebuah kode yang tidak bisa dimengerti, disebut dengan cipherteks. Sedangkan proses kebalikannya untuk mengubah cipherteks menjadi plainteks disebut dekripsi. Proses enkripsi dan dekripsi memerlukan suatu mekanisme dan kunci tertentu.

Kriptanalisis adalah kebalikan dari kriptografi, yaitu suatu ilmu untuk memecahkan mekanisme kriptografi dengan cara mendapatkan kunci dari cipherteks yang digunakan untuk mendapatkan plainteks. Kriptologi adalah ilmu yang mencakup kriptografi dan kriptanalisis.

Ada empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi, yaitu:

- (1) *Kerahasiaan*, adalah aspek yang berhubungan dengan penjagaan isi informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka informasi yang telah dienkripsi.
- (2) *Integritas data*, adalah aspek yang berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubstitusian data lain kedalam data yang sebenarnya.
- (3) *Autentikasi*, adalah aspek yang berhubungan dengan identifikasi atau pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
- (4) *Non-repudiation* (menolak penyangkalan), adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman suatu informasi oleh yang mengirimkan, atau harus dapat membuktikan bahwa suatu pesan berasal dari seseorang, apabila ia menyangkal mengirim informasi tersebut.

(Menezes dkk, 1996).

2. Sistem Kriptografi

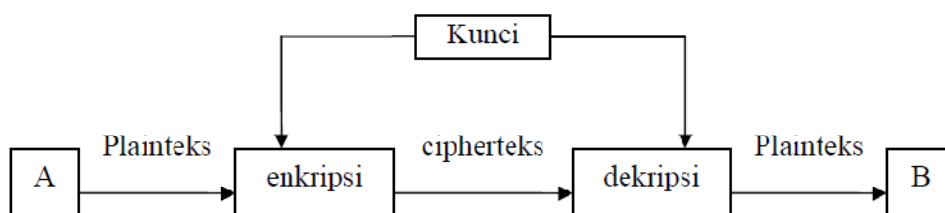
Sistem kriptografi atau sering disebut dengan cipher adalah suatu sistem atau kumpulan aturan-aturan yang digunakan untuk melakukan enkripsi dan dekripsi. Ada dua macam sistem kriptografi, yaitu sistem kriptografi kunci rahasia atau sering disebut dengan sistem kriptografi simetris dan sistem kriptografi kunci publik atau sering disebut dengan sistem kriptografi asimetris.

2.1. Sistem Kriptografi Kunci Rahasia

Sistem kriptografi kunci rahasia adalah sistem kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Sistem ini mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu sebelum mereka saling berkomunikasi. Keamanan sistem ini tergantung pada kunci, membocorkan kunci berarti bahwa orang lain dapat mengenkripsi dan mendekripsi pesan.

Agar komunikasi tetap aman, keberadaan kunci harus tetap dirahasiakan. Sifat kunci yang seperti ini membuat pengirim harus selalu memastikan bahwa jalur yang digunakan dalam pendistribusian kunci adalah jalur yang aman atau memastikan bahwa seseorang yang ditunjuk membawa kunci untuk dipertukarkan adalah orang yang dapat dipercaya.

Masalah akan menjadi rumit apabila komunikasi dilakukan secara bersama-sama oleh sebanyak n pihak dan setiap dua pihak yang melakukan pertukaran kunci, maka akan terdapat sebanyak $C_2^n = \frac{1}{2}n(n - 1)$ kunci rahasia yang harus dipertukarkan secara aman.



Gambar 1. Sistem Kriptografi Kunci Rahasia

Contoh dari sistem kriptografi kunci rahasia adalah DES (*Data Encryption Standard*), Blowfish dan AES (*Advanced Encryption Standard*).

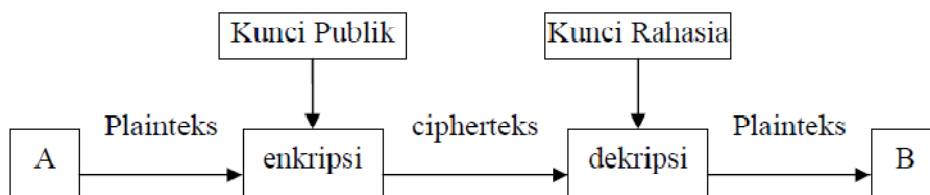
2.2. Sistem Kriptografi Kunci Publik

Sistem kriptografi kunci publik, atau sering disebut dengan sistem kriptografi asimetris, menggunakan dua jenis kunci, yaitu *kunci publik* (*public key*) dan *kunci rahasia* (*secret key*). Kunci publik merupakan kunci yang digunakan untuk mengenkripsi pesan. Sedangkan kunci rahasia digunakan untuk mendekripsi pesan. Kunci publik bersifat umum, artinya kunci ini tidak dirahasiakan sehingga dapat dilihat oleh siapapun, termasuk pihak penyerang. Sedangkan kunci rahasia adalah kunci yang dirahasiakan dan hanya orang-orang tertentu saja yang boleh mengetahuinya. Keuntungan utama dari sistem ini adalah memberikan jaminan keamanan kepada siapa saja yang melakukan pertukaran informasi meskipun di antara mereka tidak ada kesepakatan mengenai keamanan pesan terlebih dahulu maupun saling tidak mengenal satu sama lainnya. Ada beberapa syarat yang perlu diperhatikan pada algoritma asimetris, yaitu:

- (1) Penerima B membuat pasangan kunci, yaitu kunci publik K_{pB} dan kunci rahasia K_{rB} .
- (2) Pengirim A dengan kunci publik B dan pesan x , pesan dienkripsi dan diperoleh cipherteks $c = e_{K_{pB}}(x)$.
- (3) Penerima B untuk mendekripsi cipherteks menggunakan kunci privat B untuk mendapatkan kembali pesan aslinya

$$d_{K_{rB}}[e_{K_{pB}}(x)] = d_{K_{rB}}(c) = x.$$

- (4) Dengan mengetahui kunci publik K_{pB} , bagi penyerang akan kesulitan dalam melakukan untuk mendapatkan kunci rahasia.
- (5) Dengan mengetahui kunci publik K_{pB} dan cipherteks c , bagi penyerang akan mengalami kesulitan untuk mengetahui pesan x .



Gambar 2. Sistem Kriptografi Kunci Publik

Beberapa sistem kriptografi kunci publik yang telah dikenal luas saat ini adalah RSA, ElGamal dan ECC (*Elliptic Curve Cryptography*). Jintai Ding dkk (2006) telah memberikan deskripsi dan motivasi mendasar mengenai suatu sistem kriptografi kunci publik yang didasarkan atas ring polinomial multivariat $K[x_1, \dots, x_n]$ atas lapangan hingga K . Dalam makalah ini dibahas mengenai konstruksi dan desain sistem kriptografi kunci publik yang didasarkan atas $K[x_1, \dots, x_n]$ yang disebut dengan sistem kriptografi kunci publik multivariat.

3. Sistem Kriptografi Kunci Publik Multivariat

Diberikan lapangan hingga K . Dalam suatu sistem kriptografi kunci publik multivariat, pemetaan enkripsi diberikan dalam suatu pemetaan $\bar{F}: K^n \rightarrow K^m$, yaitu

$$\bar{F}(x_1, \dots, x_n) = (p_1, \dots, p_m)$$

dimana setiap p_i merupakan polinomial dalam $K[x_1, \dots, x_n]$. Konstruksi dari sistem ini dimulai dengan membentuk suatu pemetaan $F: K^n \rightarrow K^m$ sedemikian hingga memenuhi dua kondisi berikut:

- (1) $F(x_1, \dots, x_n) = (f_1, \dots, f_m)$, dimana $f_i \in K[x_1, \dots, x_n]$.
- (2) Setiap persamaan

$$F(x_1, \dots, x_n) = (y'_1, \dots, y'_m)$$

dapat diselesaikan dengan mudah. Hal ini ekuivalen dengan mengatakan bahwa dapat dihitung dengan mudah prapeta dari (y'_1, \dots, y'_m) , dimana prapeta ini harus tunggal karena digunakan untuk enkripsi, dinotasikan dengan

$$F^{-1}(y'_1, \dots, y'_m).$$

Notasi F^{-1} di sini digunakan untuk mencari prapeta dan bukan dalam arti bahwa pemetaan F invertibel.

Setelah pemetaan F tersebut diperoleh, selanjutnya pemetaan enkripsi \bar{F} dikonstruksi menggunakan komposisi dari tiga pemetaan, yaitu

$$\bar{F} = L_1 \circ F \circ L_2,$$

dimana $L_1 : K^m \rightarrow K^m$ merupakan transformasi affine invertibel yang dipilih secara acak, dan $L_2 : K^n \rightarrow K^n$ merupakan transformasi affine invertibel yang dipilih secara acak. Dalam hal ini, kunci publik terdiri dari sebanyak m polinomial dalam \bar{F} dan lapangan hingga K . Sedangkan kunci rahasia terdiri dari pemetaan L_1 dan L_2 . Kunci publik \bar{F} dapat dinyatakan sebagai

$$(p_1, \dots, p_m) = L_1 \left(F \left(L_2(x_1, \dots, x_n) \right) \right).$$

Apabila digambarkan dalam bentuk diagram, diperoleh

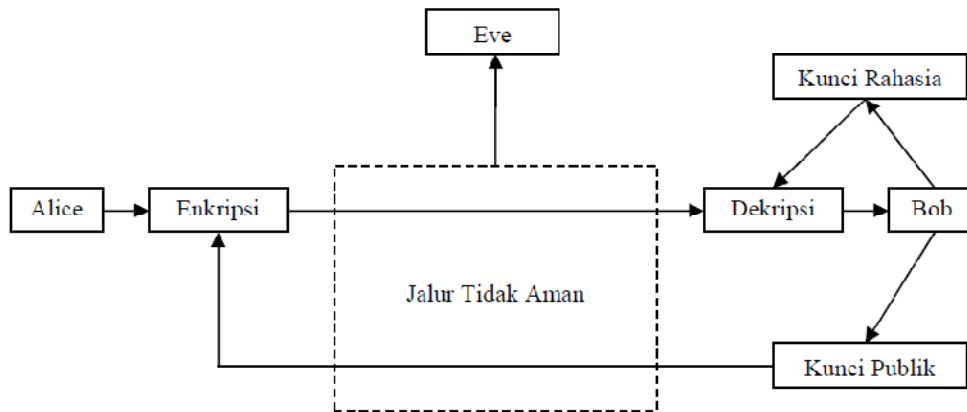
$$\begin{array}{ccccccc} K^n & \xrightarrow{L_2} & K^n & \xrightarrow{F} & K^m & \xrightarrow{L_1} & K^m \\ id \downarrow & & & & & & \uparrow id \\ K^n & \xrightarrow{\quad \bar{F} \quad} & & & K^m & & \end{array}$$

Gambar 3. Diagram Enkripsi

Untuk mengenkripsi pesan $X' = (x'_1, \dots, x'_n)$, dihitung $\bar{F}(X')$. Untuk mendekripsi suatu cipherteks $Y' = (y'_1, \dots, y'_m)$, ditentukan solusi sistem persamaan yang didefinisikan sebagai

$$\bar{F}(x_1, \dots, x_n) = Y'.$$

Untuk mencari solusi tersebut, langkah pertama adalah dihitung $Y_1 = L_1^{-1}(Y')$, selanjutnya dihitung $Y_2 = F^{-1}(Y_1)$, dan dilanjutkan dengan menghitung $X' = L_2^{-1}(Y_2)$. Sistem kriptografi multivariat seperti ini disebut dengan sistem bipolar.



Gambar 4. Jalur Komunikasi

Sebagai contoh yang sangat sederhana, misalkan ada dua pihak yang akan berkomunikasi, yaitu Alice dan Bob. Selain itu ada pihak ketiga sebagai penyerang, yaitu Eve sebagaimana yang tertera dalam Gambar 4. Alice dan Bob sepakat untuk menggunakan sistem kriptografi multivariat. Dalam hal ini Alice ingin mengirimkan suatu pesan kepada Bob. Oleh karena itu, Bob harus membuat pasangan kunci, yaitu kunci publik dan kunci rahasia sebagai berikut.

Keduanya sepakat untuk menggunakan lapangan hingga $K = GF(2)$ dan ring multivariat $K[x_1, x_2, x_3, x_4]$. Bob menentukan pemetaan $F : K^4 \rightarrow K^4$ dengan definisi

$$F(x_1, x_2, x_3, x_4) = (f_1, f_2, f_3, f_4),$$

dengan $f_1 = x_1x_2 + x_3x_4$, $f_2 = x_1^2 + 1$, $f_3 = x_1 + x_1x_2 + 1$ dan $f_4 = x_1x_4$ merupakan polinomial-polinomial dalam $K[x_1, x_2, x_3, x_4]$. Selanjutnya, Bob menentukan

transformasi affine invertibel $L_1 : K^4 \rightarrow K^4$ dan $L_2 : K^4 \rightarrow K^4$ dengan definisi

$$L_1(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, x_4) + (1, 0, 1, 0)$$

dan

$$L_2(x_1, x_2, x_3, x_4) = (x_1, x_2, x_3, x_4) + (0, 1, 1, 0).$$

Kemudian dihitung komposisi pemetaan $\bar{F} = L_1 \circ F \circ L_2$, yaitu:

$$\begin{aligned}
(p_1, p_2, p_3, p_4) &= L_1(F(L_2(x_1, x_2, x_3, x_4))) \\
&= L_1(F(x_1+1, x_2, x_3+1, x_4+1)) \\
&= L_1((x_1+1)x_2 + (x_3+1)(x_4+1), (x_1+1)^2, (x_1+1) + (x_1+1)x_2+1, (x_1+1)(x_4+1)) \\
&= L_1(x_1x_2 + x_2 + x_3 + x_3x_4 + x_4 + 1, x_1+1, x_1+1 + x_1x_2 + x_2, x_1x_4 + x_1 + x_4 + 1) \\
&= (x_1x_2 + x_2 + x_3 + x_3x_4 + x_4 + 1, x_1+1, x_1+1 + x_1x_2 + x_2, x_1x_4 + x_1 + x_4 + 1) + (1, 0, 1, 0) \\
&= ((x_1x_2 + x_2 + x_3 + x_3x_4 + x_4 + 1) + 1, x_1, (x_1+1 + x_1x_2 + x_2) + 1, x_1x_4 + x_1 + x_4 + 1) \\
&= (x_1x_2 + x_2 + x_3 + x_3x_4 + x_4 + 1, x_1, x_1 + x_1x_2 + x_2 + 1, x_1x_4 + x_1 + x_4 + 1)
\end{aligned}$$

Sehingga diperoleh kunci publik (p_1, p_2, p_3, p_4) , dengan

$$\begin{aligned}
p_1 &= x_1x_2 + x_2 + x_3 + x_3x_4 + x_4 \\
p_2 &= x_1 \\
p_3 &= x_1 + x_1x_2 + x_2 + 1 \\
p_4 &= x_1x_4 + x_1 + x_4 + 1
\end{aligned}$$

Dari sini, Bob telah mempunyai pasangan kunci publik dan kunci rahasia. Sebagai kunci publik adalah lapangan $K = GF(2)$ dan pemetaan \overline{F} yang direpresentasikan sebagai 4-tuple polinomial (p_1, p_2, p_3, p_4) . Sedangkan kunci rahasia adalah pemetaan L_1 dan L_2 . Kunci publik kemudian dikirimkan oleh Bob kepada Alice melalui jalur yang tidak aman, oleh karena itu pihak Eve juga mengetahui kunci publik tersebut.

Misalkan Alice ingin mengirimkan pesan rahasia berupa plainteks $X' = (1, 1, 1, 1)$. Menggunakan kunci publik, Alice menghitung

$$\begin{aligned}
Y' &= (y'_1, y'_2, y'_3, y'_4) = F(1, 1, 1, 1) \\
&= (p_1(1, 1, 1, 1), p_2(1, 1, 1, 1), p_3(1, 1, 1, 1), p_4(1, 1, 1, 1)) \\
&= (1, 1, 0, 0)
\end{aligned}$$

Alice memperoleh cipherteks $Y' = (1, 1, 0, 0)$ dan mengirimkannya kepada Bob. Karena dikirimkan melalui jalur yang tidak aman, maka Eve juga berhasil mendapatkan cipherteks tersebut.

Selanjutnya, Bob menerima cipherteks $Y' = (1,1,0,0)$. Bob mengetahui kunci rahasia berupa transformasi affine invertibel L_1 dan L_2 , karena menggunakan lapangan dengan karakteristik 2, sehingga diperoleh $L_1^{-1} = L_1$ dan $L_2^{-1} = L_2$. Menggunakan kunci rahasia tersebut, Bob mendekripsi cipherteks dengan menghitung:

$$\begin{aligned} Y_1 &= L_1^{-1}(Y') \\ &= L_1^{-1}(1,1,0,0) \\ &= L_1(1,1,0,0) \\ &= (1,1,0,0) + (1,0,1,0) \\ &= (0,1,1,0) \end{aligned}$$

selanjutnya, ditentukan solusi dari sistem persamaan polinomial

$$Y_2 = F^{-1}(Y_1) = F^{-1}(0,1,1,0)$$

Misalkan $F(x_1, x_2, x_3, x_4) = (f_1, f_2, f_3, f_4) = (0,1,1,0)$, diperoleh sistem persamaan polinomial:

$$\begin{cases} x_1x_2 + x_3x_4 = 0 \\ x_1^2 = 1 \\ x_1 + x_1x_2 = 1 \\ x_1 + x_4 = 0 \end{cases}$$

Menggunakan perhitungan yang sederhana, dapat diperoleh bahwa $x_1 = 1$, $x_2 = 0$, $x_3 = 0$ dan $x_4 = 1$, diperoleh $Y_2 = (0,1,0,1)$. Selanjutnya, dihitung:

$$\begin{aligned} L_2^{-1}(Y_2) &= L_2^{-1}(0,1,0,1) \\ &= L_2(0,1,0,1) \\ &= (1,0,0,1) + (0,1,1,0) \\ &= (1,1,1,1) \end{aligned}$$

Sehingga Bob memperoleh plainteks yang dikirimkan oleh Alice yaitu $X' = (1,1,1,1)$.

Di pihak Eve, untuk mendapatkan plainteks, berdasarkan kunci publik dan cipherteks yang dipunyai, Eve harus menyelesaikan sistem persamaan polinomial:

$$\begin{cases} x_1x_2 + x_2 + x_3 + x_3x_4 + x_4 = 1 \\ x_1 = 1 \\ x_1 + x_1x_2 + x_2 + 1 = 0 \\ x_1x_4 + x_1 + x_4 + 1 = 0 \end{cases}$$

Akan tetapi, dalam penggunaan yang sebenarnya paling tidak dibutuhkan lapangan hingga $GF(2^8)$ dan $n = 32$. Hal ini dilakukan untuk mempersulit pihak penyerang untuk melakukan kriptanalisis (Jintai Ding dkk, 2006).

4. Penutup

Konstruksi sistem kriptografi kunci publik multivariat dimulai dari konstruksi tiga pemetaan dan pembentukan suatu komposisi pemetaan. Hal inilah yang dimanfaatkan sebagai proses untuk menyembunyikan informasi berharga berupa kunci rahasia. Oleh karena itu, tingkat keamanan dari sistem kriptografi kunci publik multivariat didasarkan pada kesulitan dalam menyelesaikan sistem persamaan polinomial yang dibentuk dari kunci publik dan cipherteks.

Perlu dilakukan penelitian mengenai penyelesaian sistem persamaan polinomial, hal ini perlu dilakukan untuk mendapatkan jaminan keamanan dari penggunaan sistem kriptografi kunci multivariat. Salah satu metode yang dapat digunakan adalah dengan teknik basis Groebner.

5. Daftar Pustaka

- Alfred J. Menezes, Paul C. van Oorschot dan Scott A. Vanstone, 1996, *Handbook of Applied Cryptography*, CRC Press, USA.
- Jintai Ding, Jason E. Gower, dan Dieter S. Schmidt, 2006, *Multivariate Public Key Cryptosystem*, Springer, USA.