RUANG LINGKUP KRIPTOGRAFI UNTUK MENGAMANKAN DATA

Oleh: Budi Hartono

1. PENDAHULUAN

Data menjadi sesuatu yang amat berharga di dalam abad teknologi informasi dewasa ini. Bentuk data yang dapat dilibatkan dalam hal ini adalah berbentuk digital atau elektronik. Perlakuan khusus terhadap data akan diperlukan apabila data ditujukan hanya untuk kalangan terbatas dan dikirimkan melalui jalur umum seperti Internet, sementara itu isi data tidak boleh berubah. Salah satu bidang ilmu yang dapat dipakai untuk membantu melakukan perlakuan khusus tersebut adalah menggunakan kriptografi. Tulisan ini akan menjelaskan secara singkat mengenai pemahaman, istilah-istilah didalamnya, dan ruang lingkup kriptografi untuk mengamankan data.

2. Pengertian kriptografi (*cryptography*)

Kriptografi adalah bidang ilmu pengetahuan yang mempelajari pemakaian persamaan matematika untuk melakukan proses penyandian data (Onno, 2000). Kriptografi bertujuan untuk mengamankan isi data atau menjaga kerahasiaan informasi dari orang yang tidak berhak untuk mengetahui isi data tersebut. Dengan teknik atau algoritma tertentu yang disebut proses enkripsi (*encrypt*), data diubah menjadi data sandi yang bentuknya berbeda dengan data aslinya. Orang yang berhak menerima data akan mengetahui algoritma dan memiliki kunci untuk mengembalikan data sandi menjadi bentuk data aslinya, proses ini disebut dekripsi (*decrypt*). Bentuk data sandi diperlukan pada saat proses penyimpanan atau proses pengiriman data.

Untuk dapat melakukan proses enkripsi dan dekripsi maka pihak pengirim dan penerima harus mengetahui algoritma kriptografi yang digunakan serta memiliki kunci yang sesuai. Tingkat keamanan dari data sandi terhadap upaya proses dekripsi secara paksa oleh orang yang tidak berhak ditentukan oleh kekuatan algoritma yang digunakan dan kerahasiaan kunci.

Kekuatan algoritma yang digunakan untuk proses enkripsi dan dekripsi berhubungan erat dengan penggunaan persamaan matematika. Semakin banyak dan rumit perhitungan dari persamaan matematika yang digunakan maka data sandi semakin aman (Alfred, 1997). Pemanfaatan kecepatan dan ketelitian dari kerja komputer sangat membantu untuk proses ini. Kerahasiaan kunci adalah bagaimana cara kunci tersebut disimpan dan didistribusikan kepada pihak yang berhak menerima data, karena kunci ini akan digunakan untuk melakukan dekripsi. Semakin rapi kunci disimpan dan didistribusikan maka data sandi semakin aman. Berikut ini adalah istilah-istilah yang berhubungan erat dengan kriptografi (Onno, 2000).

a. *Plaintext* / *cleartext* adalah data asli atau informasi bersifat terbuka yang

isinya dapat dibaca dan dipahami secara langsung. Menjadi sumber data untuk proses enkripsi.

b. *Ciphertext* adalah data sandi hasil proses dekripsi.

c. *Cipher* adalah algoritma untuk mengubah *plaintext* menjadi *ciphertext* menggunakan persamaan matematika. Hasil perubahan dapat berbentuk *substitution cipher*, *transposition cipher*, atau gabungan dari keduanya.

d. *Substitution cipher* adalah algoritma mengubah *plaintext* menjadi *ciphertext* dengan cara mengganti menggunakan persamaan matematika tertentu.

e. *Transposition cipher* adalah algoritma mengubah *plaintext* menjadi *ciphertext* dengan cara menggeser menggunakan persamaan matematika tertentu.

f. *Block Cipher* adalah algoritma mengubah *plaintext* menjadi *ciphertext* untuk setiap *block* data. Jumlah data atau besarnya *block* adalah tertentu.

g. Kunci (k*ey*) adalah data atau nilai yang sangat spesifik yang diketahui oleh pengirim dan penerima yang berhak. Digunakan bersama-sama dengan algoritma kriptografi untuk melakukan proses enkripsi dan dekripsi.

h. Enkripsi (*encryption*) adalah proses yang digunakan untuk menyamarkan/menyembunyikan *plaintext*. Hasil dari proses enkripsi adalah data sandi (*ciphertext*).

i. Dekripsi (*decryption*) kebalikan dari proses enkripsi yaitu mengembalikan *ciphertext* menjadi *plaintext*.

j. Kriptosistem (*cryptosystem*) adalah sistem kriptografi yang didalamnya terdiri dari: algoritma kriptografi, *plaintext*, *ciphertext*, *key*, dan unsur lain yang berpengaruh dalam sistem kriptografi.

k. *Cryptanalysis / code breaking* adalah kegiatan untuk mengubah *ciphertext* menjadi pesan aslinya tanpa mengetahui kunci yang sesuai, dengan coba-coba (*trial and error*) secara sistematis.

l. *Cryptology* adalah ilmu matematika yang mendasari *crypthography* dan *cryptanalysis*.

Untuk meningkatkan keamanan informasi (*information security*) setelah dilakukan proses pengiriman dan penerimaan informasi maka dapat dilakukan tindakan-tindakan berikut ini:

a. Membuktikan keaslian (a*uthentication*) yaitu proses yang memungkinkan penerima informasi untuk mengetahui asal atau pengirim informasi yang sebenarnya. Bertujuan mencegah pengacau yang mengirimkan informasi menggunakan identitas orang lain.

   Contoh:

   - Penyertaan foto, nama lengkap, dan tanda tangan pada sertifikat.
   - Mengirim pesan dengan diberi tanda tangan digital (*digital signature*).

b. Menjaga integritas data (*data integrity*) yaitu proses yang menjamin penerima informasi dapat memeriksa apakah informasi telah berubah sebelum diterimanya. Berubah karena secara sengaja dipalsukan oleh pihak lain atau secara tidak disengaja karena terjadi

kerusakan pada proses pengiriman informasi.

Contoh:

- Pemberian *Watermark* pada kartu identitas.
- Mengirim pesan diberi intisari pesan (*message digest*) hasil dari fungsi *hash*.

c. Membuktikan seseorang telah mengirimkan pesan (*non repudiation*) yaitu proses untuk menjamin pengirim informasi tidak dapat menyangkal bahwa dia telah mengirim informasi tersebut. Sebaliknya dapat juga digunakan untuk melindungi seseorang dari tuduhan yang menyatakan bahwa dia telah mengirimkan informasi padahal tidak.

Contoh:

- Tanda tangan notaris atau pejabat yang berwenang pada surat pernyataan.
- Mengirim pesan dengan diberi sertifikat digital (*digital certificates*).

d. Menjaga kerahasiaan (c*onfidentiality*) yaitu proses untuk menjamin informasi yang dikirimkan tidak dapat dipahami isinya oleh orang yang tidak berhak.

Contoh:

- Menulis pesan menggunakan tinta yang tidak kasat mata
- Mengirim pesan dalam bentuk data sandi.

3. Sejarah Kriptografi

Kriptografi telah dikenal kurang lebih pada tahun 2000 sebelum masehi oleh bangsa Mesir. Berbentuk tulisan *hieroglyphic* pada monumen. Bangsa Mesopotamia telah menggunakan kriptografi pada tahun 1500 sebelum masehi, selanjutnya dikenal juga oleh bangsa Yahudi dan bangsa Yunani (Stallings, 1999). Teknik kriptografi pada awalnya dilakukan dengan cara menggunakan simbol tertentu untuk mengganti simbol yang telah digunakan dan dikenal secara umum oleh masyarakat.

Teknik kriptografi sederhana yang dilakukan oleh Julius Caesar pada awal abad pertama masehi digunakan untuk keperluan militer, dengan cara menggeser tiga huruf alphabet. Teknik ini disebut dengan Caesar Cipher dan banyak varian yang dikembangkan untuk memperoleh *ciphertext* dengan cara menggeser bagian-bagian dari *plaintext*-nya menggunakan perhitungan matematika tertentu (Bruce, 1999). Berikut adalah contoh metode Caesar Cipher.

Plaintext:
"ABCDEFGHIJKLMNOPQRSTUVWXYZ",
digeser dengan urutan 3 huruf didepannya menjadi :

Ciphertext:
"DEFGHIJKLMNOPQRSTUVWXYZABC"

Ciphertext tersebut digunakan untuk mengubah Plaintext: "SEMARANG KOTA ATLAS", di peroleh hasil Ciphertext sebagai berikut : "VHPDUDQK NRWD DWODV"

Pada perkembangannya aplikasi kriptografi dimanfaatkan secara intensif untuk keperluan pengiriman data secara rahasia pada saat manusia berperang. Implementasi berupa alat atau mesin rotor yang dapat berfungsi sebagai penghasil *ciphertext* dan untuk mengembalikannya ke dalam bentuk *plaintext*. Contoh mesin jenis ini yang terkenal pada perang dunia II adalah Enigma, digunakan oleh pihak tentara Jerman untuk menyandikan informasi pada saat dikirimkan.

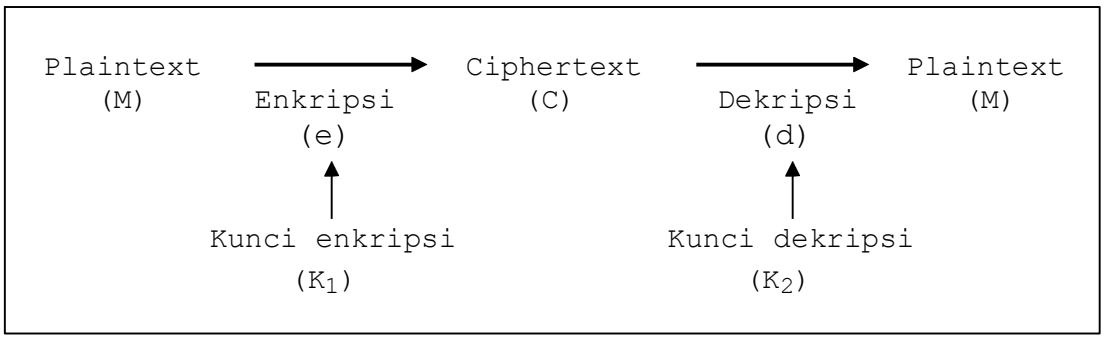
4. Teknik Kriptografi

Dari penjelasan sebelumnya pada bagian sejarah kriptografi nampak bahwa untuk menghasilkan *ciphertext* dan mengembalikan ke *plaintext* digunakan algoritma tertentu yang menyertakan perhitungan matematika. Pada cara ini tingkat keamanan tergantung pada bagaimana menjaga kerahasiaan algoritma kriptografi yang digunakan. Algoritma ini hanya boleh diketahui secara terbatas oleh pihak pengirim dan penerima saja (*restricted algorithm*). Kelemahannya adalah apabila ada orang lain yang tidak berkepentingan mengetahuinya maka algoritma ini harus diubah. Perubahan atau penggantian algoritma baru harus diketahui oleh pihak pengirim dan penerima, dimana cara mengkomunikasikan algoritma yang baru ini akan memunculkan masalah yang lain (Stallings, 1999). Ada dua jenis teknik kriptografi yang memiliki sifat *restricted algorithm*, yaitu:

a. *Substitution cipher*, beberapa contoh: Caesar cipher, Monoalphabetic cipher, General Monoalphabetic cipher, Vigenere cipher, Beauford cipher, Variant Beauford cipher.
b. *Transposition cipher*, beberapa contoh: Scytale cipher, Rail Fence cipher, Geometric Figure cipher, Row Transposition cipher, Nihilist cipher, Diagonal cipher.

Beberapa contoh *cipher* tersebut telah dikenal cukup lama sehingga disebut sebagai kriptografi klasik. Dikerjakan dengan menghitung secara manual, menggunakan peralatan bantu mekanik, atau peralatan komputer.

Untuk mengatasi kelemahan dari *restricted algorithm* maka dikembangkan algoritma kriptografi yang proses didalamnya melibatkan kunci. Kunci akan digunakan untuk proses enkripsi dan dekripsi, dengan nilai kunci bebas namun tetap memperhatikan aturan-aturan dari algoritma kriptografi yang digunakan. Disini algoritma kriptografi yang digunakan tidak perlu dirahasiakan lagi, sehingga boleh dipublikasikan dan dianalisa oleh orang yang berminat. Pada cara ini tingkat keamanan tergantung pada bagaimana merahasiakan kunci yang digunakan. Menjaga kerahasiaan dan mengkomunikasikan kunci relatif lebih mudah daripada algoritma kriptografinya karena ukuran kunci tersusun dari beberapa digit kombinasi nilai yang spesifik. Pada gambar 1. dapat dilihat alur proses enkripsi dan dekripsi yang menyertakan kunci.



Gambar 1. Alur proses enkripsi dan dekripsi yang menyertakan kunci.

Secara persamaan matematika dapat dituliskan:

a. Proses enkripsi → $ek_1(M) = C$
b. Proses dekripsi → $dk_2(C) = M$
c. Proses pengujian (*checking*) dapat dilakukan dengan cara $dk_2(ek_1(M)) = M$

Dalam perkembangannya algoritma kriptografi yang menggunakan kunci dibedakan menjadi dua, berdasarkan nilai kunci yang digunakan, yaitu:

a. Algoritma simetris (*symmetric algorithm* atau *single key algorithm*)

   Kunci k_1 untuk proses enkripsi sama dengan kunci k_2 untuk proses dekripsi, sehingga $k_1=k_2=K$. Kunci K hanya boleh diketahui oleh pengirim dan penerima saja.

b. Algoritma kunci publik (*public key algorithm* atau *asymmetric algorithm*)

   Kunci k_1 untuk proses enkripsi tidak sama dengan kunci k_2 untuk proses dekripsi, sehingga $k_1 \neq k_2$. Kunci k_1 boleh diketahui oleh umum tetapi kunci k_2 hanya diketahui oleh pihak penerima saja yang akan melakukan proses dekripsi. Kunci k_1 dan k_2 memiliki sifat berpasangan.

c. Algoritma campuran (*hybrid algorithm*)

   Merupakan gabungan antara algoritma simetris dan algoritma kunci publik.

Hubungan antara kunci dan algoritma yang digunakan dengan tingkat keamanan *ciphertext* dari usaha *code breaking,* adalah sebagai berikut:

a. Semakin besar ukuran kunci yang digunakan maka *ciphertext* semakin aman, tetapi semakin lambat proses enkripsi dan dekripsi.
b. Semakin banyak perhitungan matematika yang dikerjakan oleh algoritma maka *ciphertext* semakin aman, tetapi semakin lambat proses enkripsi dan dekripsi.

4.1. Kriptografi algoritma simetris

Kriptografi kunci simetris memiliki kecepatan proses yang lebih

cepat dibandingkan dengan kriptografi kunci publik. Ini disebabkan karena algoritma untuk perhitungan matematika untuk proses enkripsi dan dekripsi adalah sama (Stallings, 1999). Contoh algoritma jenis ini adalah:

a. S-DES (*simplified-DES,* Data Encryption Standard), dikembangkan oleh profesor Edward Schaefer dari Santa Clara University. Dibuat untuk keperluan pendidikan. Menggunakan *block plaintext* 8 bit, kunci 10 bit, dan *block ciphertext* 8 bit, untuk proses enkripsi dan dekripsi. (Stallings, 1999).
b. DES (Data Encryption Standard), pengembangan dari S-DES, diadopsi oleh National Bureau of Standards, sekarang menjadi Institute of Standards and Technology. Selanjutnya DES digunakan secara meluas. Menggunakan *block plaintext* 64 bit, kunci 56 bit, dan *block ciphertext* 64 bit, untuk proses enkripsi dan dekripsi. (Stallings, 1999).
c. IDEA (International Data Encryption Algorithm), adalah *symmetric block cipher* dikembangkan oleh Xuejia Lai dan James Massey dari Swiss Federal Institute of Technology. Direkomendasikann penggunaannya untuk menggantikan DES dan banyak dipakai pada PGP. Menggunakan *block plaintext* 64 bit, kunci 128 bit, dan *block ciphertext* 64 bit, untuk proses enkripsi dan dekripsi. (Stallings, 1999).
d. BLOWFISH, adalah *symmetric block cipher* dikembangkan oleh Bruce Schneier. Menggunakan *block plaintext* 64 bit, kunci 32 bit sampai dengan 448 bit, dan *block ciphertext* 64 bit, untuk proses enkripsi dan dekripsi. (Bruce, 1996).

Masalah yang timbul adalah pada distribusi kunci (key distribution), yaitu bagaimana caranya agar kunci tersebut dapat dikirimkan secara aman ke penerima. Pengertian aman disini adalah kunci dapat disampaikan kepada penerima yang berhak tanpa ada orang lain yang mengetahuinya. Masalah yang lain adalah pada efisiensi jumlah kunci yang harus dibuat. Jika ada pengguna sebanyak n maka akan dibutuhkan sebanyak n(n-1)/2 buah kunci, sehingga untuk jumlah pengguna yang sangat banyak maka jumlah kunci yang diperlukan juga menjadi banyak.

4.2. Kriptografi algoritma kunci publik

Masalah distribusi kunci dapat diatasi dengan metode kriptografi kunci publik (*public key cryptography*). Konsep ini dikenalkan pertama kali oleh Whitfield Diffie dan Martin Hellman pada tahun 1975. Kriptografi jenis ini bersifat asimetris, yaitu kunci yang digunakan untuk enkripsi dan dekripsi adalah berbeda. Kunci yang digunakan untuk proses enkripsi dan dekripsi bersifat berpasangan. (Stallings, 1999).

Untuk proses enkripsi digunakan kunci publik (*public key*) oleh pengirim, sedangkan untuk proses dekripsi digunakan kunci privat (*private key*) oleh penerima. Kunci publik dapat dimiliki oleh siapapun yang ingin mengirimkan data. Kunci privat tetap dirahasiakan oleh

pembuatnya yang tidak lain adalah pihak penerima. Siapapun yang memiliki kunci publik dapat mengenkripsi informasi, dimana informasi ini hanya bisa dimengerti isinya oleh orang yang memiliki kunci privat pasangannya.

Keuntungan adanya konsep kunci publik ini adalah memberikan jaminan keamanan kepada siapa saja yang melakukan pertukaran informasi meskipun diantara mereka tidak ada persetujuan mengenai keamanan data terlebih dahulu dan diantara mereka tidak saling mengenal sebelumnya. Beberapa contoh algoritma jenis ini adalah:

a. ElGamal dikembangkan oleh Taher ElGamal (Bruce, 1996).
b. RSA, dikembangkan pada tahun 1978 oleh Ron Rivest, Adi Shamir dan Leonard Adleman (Stallings, 1999).
c. Elliptic Curve Cryptosystems (ECC), diekembangkan pada tahun 1985 oleh Neil Koblitz dan Victor Miller (Onno, 2000).

4.3. Kriptografi algoritma campuran

Tujuannya adalah mengurangi kelemahan dan menggabungkan keunggulan dari sifat algoritma simetris dan kunci publik. Keunggulan algoritma simetris adalah memiliki kecepatan proses yang lebih tinggi sedangkan algoritma kunci publik memiliki tingkat kemanan yang lebih baik. Contoh algoritma ini adalah PGP yang dikembangkan oleh Phil Zimmermann, yang memiliki banyak kegunaan dan diaplikasikan untuk electronic mail serta penyimpanan file (Stallings, 1999). Terdapat beberapa pilihan algoritma yang dapat digunakan, untuk algoritma kunci publik adalah RSA, DSS, Diffie-Hellman, sedangkan algoritma kunci simetris adalah IDEA, 3DES, CAST-128.

5. PENUTUP

Tingkat kerumitan persamaan matematika yang digunakan untuk proses enkripsi dan banyaknya proses penghitungan sangat mempengaruhi terhadap tingkat keamanan *ciphertext*. Disamping itu untuk menambah tingkat keamanan dapat dilakukan dengan cara menjaga kerahasiaan kunci dan algoritma enkripsi yang digunakan. Tingkat keamanan dapat diukur dengan menghitung banyaknya seluruh kombinasi yang mungkin untuk dicoba secara sistematis (*brute force attack*) dan lamanya waktu yang dibutuhkan untuk melakukan hal tersebut . Apabila jumlah kombinasi yang harus dicoba sangat besar dan membutuhkan waktu yang sangat lama maka *ciphertext* dapat dinyatakan relatif aman.

DAFTAR PUSTAKA

1. Alfred J.M., Paul C.O., and Scott A.V, 1997, *Handbook of Applied Cryptography*. CRC Press LLC, Florida, USA.

2. Bruce S., 1996, *Applied Cryptography, Protocols, Algorithms, and Source Code in C*. John Wiley & sons, Inc.

3. Onno W.P., Aang Arif Wahyudi, 2000, *Mengenal eCommerce*. Elex Media Komputindo, Jakarta.

4. Stallings W., 1999, *Cryptography and Network Security Principles and Practice second edition*. Prentice Hall, New Jersey, USA.