Aplikasi Kriptosistem dengan Algoritma Mc Elliece

Ana Wahyuni

Fakultas Ilmu Komputer Universitas AKI

Abstract

Cryptosystem is a cryptographic system, that is science and art to maintain the safety of messages by encrypting it into a form that cannot be understood what the meaning is. Message safety includes confidentiality / privacy, authenticity / integrity, authentication and non repudiation. One of the cryptographic algorithms is Mc Ellice algorithm. Mc Ellice algorithm is based on matrix computation, so it has safety on the keys that are not easily solved. The result of this cryptosystem is a message in the form of a password / encryption, i.e. chipper text which is ready to be transmitted, for example, by means of e-mail. After that, the message receiver will describe that chip text and get the actual message content / plaintext.

***Key words** : Cryptosystem, cryptography, chipper text, plaintext, public key, private key, encryption, description*

Pendahuluan

Dalam arti umum, istilah kriptosistem digunakan sebagai nama lain untuk "sistem kriptografi" yaitu sebuah sistem kriptografi pada sistem komputer yang melibatkan kriptografi . Yang termasuk sistem tersebut misalnya, suatu sistem keamanan surat elektronik yang mencakup metode untuk tanda tangan digital , fungsi hash kriptografi , teknik manajemen kunci, dan sebagainya. Sistem kriptografi dibangun dari primitif kriptografi , dan biasanya rumit/ komplex. Karena itu, memecahkan kriptosistem adalah tidak terbatas untuk memecahkan algoritma kriptografi dasarnya, biasanya jauh lebih mudah untuk mematahkan sistem secara keseluruhan, misalnya, melalui kesalahpahaman pengguna sehubungan dengan kriptosistem tersebut.

Dalam arti khusus, kriptografi mengacu pada suatu algoritma yang diperlukan untuk melaksanakan suatu bentuk khusus dari enkripsi dan dekripsi .

Biasanya, kriptosistem terdiri dari tiga algoritma: satu untuk kunci pembangkit, satu untuk enkripsi, dan satu untuk dekripsi. *Cipher* panjang (kadang-kadang *nol)* sering digunakan untuk merujuk kepada sepasang algoritma, satu untuk enkripsi dan satu untuk dekripsi. Oleh karena itu, "kriptografi" istilah yang paling sering digunakan ketika algoritma pembangkitan kunci dipakai. Untuk alasan ini, istilah "kriptosistem“ umumnya digunakan untuk merujuk kepada teknik kunci publik, namun keduanya "cipher" dan "kriptografi" digunakan juga untuk teknik kunci privat.

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

1. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
2. Integritas data, adalah 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 pensubsitusian data lain kedalam data yang sebenarnya.
3. Otentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
4. Non-repudiasi, atau nir-penyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara dua himpunan yaitu yang berisi elemen teks terang /plaintext dan yang berisi elemen teks sandi/ciphertext. Enkripsi dan dekripsi merupakan fungsi transformasi antara himpunan-himpunan tersebut. Apabila elemen-elemen teks terang dinotasikan dengan P, elemen-elemen teks sandi dinotasikan dengan C, sedang untuk proses enkripsi dinotasikan dengan E, dekripsi dengan notasi D.

Enkripsi : $E(P) = C$

Dekripsi : $D(C) = P$ atau $D(E(P)) = P$

Secara umum berdasarkan kesamaan kuncinya, algoritma sandi dibedakan menjadi :

1. kunci-simetris/*symetric-key*, sering disebut juga algoritma sandi konvensional karena

umumnya diterapkan pada algoritma sandi klasik

2. kunci-asimetris/*asymetric-key*
3. Berdasarkan arah implementasi dan pembabakan jamannya dibedakan menjadi :
4. algoritma sandi klasik/ *classic cryptography*
5. algoritma sandi modern/ *modern cryptography*
6. Berdasarkan kerahasiaan kuncinya dibedakan menjadi :
7. algoritma sandi kunci rahasia / *secret-key*
8. algoritma sandi kunci publik / *publik-key*

Pada skema kunci-simetris, digunakan sebuah kunci rahasia yang sama untuk melakukan proses enkripsi dan dekripsinya. Sedangkan pada sistem kunci-asimentris digunakan sepasang kunci yang berbeda, umumnya disebut kunci publik(*public key*) dan kunci pribadi (*private key*), digunakan untuk proses enkripsi dan proses dekripsinya. Bila elemen teks asli dienkripsi dengan menggunakan kunci pribadi maka elemen teks sandi yang dihasilkannya hanya bisa didekripsikan dengan menggunakan pasangan kunci pribadinya. Begitu juga sebaliknya, jika kunci pribadi digunakan untuk proses enkripsi maka proses dekripsi harus menggunakan kunci publik pasangannya.

Fungsi Enkripsi dan Dekripsi Algoritma Sandi Kunci-Asimetris secara umum sebagai berikut :

Apabila Ahmad dan Bejo hendak bertukar berkomunikasi, maka:

1. Ahmad dan Bejo masing-masing membuat 2 buah kunci yaitu :
   a) Ahmad membuat dua buah kunci, kunci-publik $K_{publik[Ahmad]}$ dan kunci-privat $K_{privat[Ahmad]}$
   b) Bejo membuat dua buah kunci, kunci-publik $K_{publik[Bejo]}$ dan kunci-privat $K_{privat[Bejo]}$
2. Mereka berkomunikasi dengan cara:
   a) Ahmad dan Bejo saling bertukar kunci-publik. Bejo mendapatkan $K_{publik[Ahmad]}$ dari Ahmad, dan Ahmad mendapatkan $K_{publik[Bejo]}$ dari Bejo.
   b) Ahmad mengenkripsi teks-terang (*plaintext*) P ke Bejo dengan fungsi $C = E(P, K_{publik[Bejo]})$
   c) Ahmad mengirim teks-sandi (*chippertext*) C ke Bejo
   d) Bejo menerima C dari Ahmad dan membuka teks-terang dengan fungsi $P = D(C, K_{privat[Bejo]})$

Hal yang sama terjadi apabila Bejo hendak mengirimkan pesan ke Ahmad

1. Bejo mengenkripsi teks-terang P ke Ahmad dengan fungsi $C = E(P, K_{publik[Ahmad]})$
2. Ahmad menerima C dari Bejo dan membuka teks-terang dengan fungsi $P = D(C, K_{privat[Ahmad]})$

Salah satu contoh algoritma kunci asimetris adalah algoritma Mc Elliece. Pada paper ini akan dibahas aplikasi kriptosistem pada pesan teks menggunakan algoritma Mc Ellice yang bermanfaat dalam menjaga kerahasiaan pesan.

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 Mc Elliece secara matematis dan diimplementasikan pada komputasinya menggunakan Matlab.

Hasil dan Pembahasan

1. Algoritma Mc Elliece

Kriptosistem Mc.Eliece adalah algoritma kunci asimetris yang dibangun pada tahun 1978 oleh Robert Mc Eliece. Algoritma ini menggunakan kode Goppa dengan type kode koreksi kesalahan *(error-correcting code*). Algoritma menyamarkan kode Goppa dibuat dari plaintext sebagai kode linier umum. Kode Goppa mudah dikodekan, tapi membedakan mereka dari kode linier umum adalah sukar. Kunci privat & publik sebagai matriks yang tidak sama.

2. Aplikasi Kriptosistem dengan Algoritma Mc Ellice

Sebagai contoh aplikasi algoritma Mc. Ellice untuk menyandikan pesan (enkripsi)"MSI10". Pertama-tama proses pembentukan kunci dilakukan :

1. misalnya dipilih nilai k = 4 dan n = 7
2. pilih sembarang matriks A berdimensi k x (n-k) atau (4,3) misalnya

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

3. Tentukan matriks generator G = [Ik | A] , yang merupakan kunci pribadi yaitu :

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

4. pilihan matriks nonsingular S berdimensi k x k atau(4,4), yang merupakan kunci pribadi yaitu

$$S = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

5. pilih matriks permutasi P berdimensi n x n atau (7x7), yang merupakan kunci pribadi yaitu

$$P = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

6. hitung Ga = SGP, yang merupakan kunci publik

$$Ga = SGP = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

Perhitungan tersebut menghasilkan pasangan kunci, yaitu kunci publik matriks Ga dan kunci pribadi matriks-matriks P, G, dan S. Selanjutnya dilakukan enkripsi terhadap pesan 'MSI10', pertama-tama pesan tersebut diterjemahkan ke dalam kode ASCII menjadi :
0100110101010011010010010011000100110000. Karena k = 4, maka pesan tersebut harus di blok dengan panjang tiap blok adalah 4 bit, menjadi :
0100 1101 0101 0011 0100 1001 0011 0001 0011 0000

Berturut-turut sebagai m_1, m_2, m_3, m_4, m_5, m_6, m_7, m_8, m_9 dan m_{10}. Misalnya dengan mengambil vektor biner random e = (1 0 1 1 1 0 1), enkripsi untuk mendapatkan ciphertext c_1, c_2, c_3, c_4, c_5 , c_6, c_7, c_8, c_9 dan c_{10} dilakukan sebagai berikut :

$C_1=m_1G'\oplus e =$

$$(0100)\begin{pmatrix} 1011000 \\ 1010011 \\ 0011000 \\ 1101101 \end{pmatrix} \oplus (1011101) = (0001110)$$

$C_2=m_2G'\oplus e = (1111011)$

$C_3=m_3G'\oplus e = (1100011)$

$C_4=m_4G'\oplus e = (0101000)$

$C_5=m_5G'\oplus e = (0001110)$

$C_6=m_6G'\oplus e = (1101000)$

$C_7=m_7G'\oplus e = (0101000)$

$C_8=m_8G'\oplus e = (0110000)$

$C_9=m_9G'\oplus e = (0101000)$

$C_{10}=m_{10}G'\oplus e = (1011101)$

Proses Deskripsinya sebagai berikut :

Selanjutnya ciphertext c_1 c_2 c_3 c_4 c_5 …c_{10} ditransmisikan/ dikirim misal melalui e-mail. Ketika ciphertext c_1 c_2 c_3 c_4 c_5 …c_{10} diterima, proses dekripsi dilakukan dengan menggunakan kunci pribadi matriks-matriks P, G, dan S sebagai berikut :

Untuk mendapatkan m1 dari ciphertext c1 :

$x_1=c_1P^{-1}=$

$$(0001110)\begin{pmatrix}0010000\\0000010\\0000001\\0001000\\1000000\\0100000\\0000100\end{pmatrix}=(1101000)$$

$x_2=c_2P^{-1}=(0111111)$ dengan cara analog diperoleh :

x3=(0110110)

x4=(0001010)

x5=(1101000)

x6=(0011010)

x7=(0001010)

x8=(0000011)

x9=(0001010)

x10=(1011101)

Selanjutnya dihitung nilai y sebagai berikut :

$y_1 = x_1 + e_1 = (0110101)$ (catatan : $e_1 = e\ P^{-1}$) dengan cara analog diperoleh :

y2=(1100010)

y3=(1101011)

y4=(1010111)

y5=(0110101)

y6=(1000111)

y7=(1010111)

y8=(1011110)

y9=(1010111)

y10=(0000000)

dari m1 G = y_1 diperoleh m_1 = (0100)

dengan prosedur yang sama diperoleh :

m_2 = (1101)

m_3 = (0101)

m_4 = (0011)

m_5 = (0100)

m_6 = (1001)

m_7 = (0011)

m_8 = (0001)

m_9 = (0011)

m_{10} = (0000)

diperoleh plaintext m_1 m_2 m_3 m_4 m_5 ...m_{10}, akhirnya restrukturisasi kembali ke kode ASCII akan diperoleh pesan MSI10.

Catatan : perhitungan di atas dihitung dengan *software* matlab yang memudahkan operasi perhitungan dengan matriks.

Kesimpulan dan Saran

Algoritma Mc Eliece digunakan untuk menyandikan teks (huruf dan angka) dengan efektif. Kekuatan algoritma ini adalah pada kunci yang berbentuk matriks dan pada proses komputasinya. Penelitian ini dapat dikembangkan untuk pesan selain teks, misalnya *image* yang sudah dikonversi ke bit string. Dapat pula dikembangkan dengan membuat program sederhana misalnya dengan menggunakan GUI di matlab atau dengan bahasa pemrograman yang lain. Untuk melipatgandakan keamanan algoritma ini dapat dikombinasikan dengan algoritma pertukaran kunci, misalnya algoritma Deffie Helman.

Daftar Pustaka :

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