SEKURITAS SISTEM DENGAN KRIPTOGRAFI

Oleh : Rosdiana, ST., M.Kom
STAIN Palopo
e-mail: yosh.diana01@gmail.com

Abstrak :
Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Istilah kriptografi lebih dikenal dengan *criptosystem,* dimana suatu criptosistem terdiri dari sebuah algoritma dari seluruh kemungkinan plaintext, chippertext, dan kunci-kunci. Dalam kriptosystem RSA ada beberapa persyaratan yang hendaknya dipenuhi, yaitu plaintext di enkripsi ke dalam blok-blok dengan tiap-tiap blok bernilai biner kurang dari *n* adalah integer positip. Dengan demkian panjang maksimal tiap-tiap blok adalah kurang dari atau sama dengan $\log_2(n)$.

Kata Kunci *: Kriptografi, Kriptosistem, plaintext, chippertext,Cryptography, Hellman Knapsack.*

A. Pendahuluan

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner dalam bukunya "Applied Cryptography", kriptografi adalah ilmu pengetahuan dan seni menjaga *message-message* agar tetap aman (secure). Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Prinsip-prinsip yang mendasari kriptografi yakni:

1) *Confidelity* (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.
2) *Data integrity* (keutuhan data) yaitu layanan yang mampu mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain).
3) *Authentication* (keotentikan) yaitu layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.

4) *Non-repudiation* (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

Teknologi yang sangat maju membuat manusia dapat berkomunikasi dan saling bertukar informasi/data secara jarak jauh. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat. Begitu banyak pengguna tidak meinginkan informasi yang disampaikannya diketahui oleh orang lain atau kompetitornya atau negara lain. Oleh karena itu dikembangkanlah cabang ilmu yang mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi.

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal.

Istilah kriptografi lebih dikenal dengan *criptosystem,* dimana suatu criptosistem terdiri dari sebuah algoritma dari seluruh kemungkinan plaintext, chippertext, dan kunci-kunci.

Secara umum criptosistem digolongkan menjadi 2 yaitu:

1) *Symetric Criptosistem*; Kunci yang digunakan untuk enkripsi dan dekripsi pada prinsipnya identik, tetapi salah satu kunci dapat diturunkan dari kunci lainnya. Kunci-kunci ini harus dirahasiakan, sehingga kunci ini disebut secret-key criptosistem.
2) *Assymetric criptosistem;* Metode ini juga menggunakan 2 buah kunci yang disebut public-key, yang dapat dipublikasikan, sedang kunci lainnya adalah private-key yang harus dirahasiakan. Proses system ini, diawali ketika A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci public B, dan bila B ingin membaca surat tersebut, ia perlu mendeskripkan surat itu dengan kunci privatnya. Dengan demikian , kedua pihak dapat menjamin asal surat serta keaslian surat tersebut. Contoh metode ini antara lain RSA Schema dan Merkle-Hellman Schema.

Suatu kriptosistem yang baik harus memiliki karakteristik sebagai berikut:

1) Keamanan system terletak pada kerahasiaan kunci dan bukan pada kerahasian algoritma yang digunakan.

2) *Cryptosystem*, yang baik memiliki ruang kunci (keyspace) yang besar.
3) *Cryptosystem* yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistic yang dilakukan terhadapnya.
4) *Cryptosystem* yang baik mampu menahan seluruh serangan yang telah dikenal sebelumnya.

Bila suatu c*ryptosystem* berhasil memenuhi seluruh karakteristik diatas, belum tentu ia merupakan system yang baik. Banyak *cryptosystem* lemah yang terlihat baik pada awalnya. Kadang kala untuk menunjukan bahwa suatu *cryptosystem* kuat atau baik dapat dilakukan dengan menggunakan pembuktian matematika.

Pada tahun 1970-an, terdapat terobosan matematika yang memungkinkan cara enkripsi yang menggunakan metode kunci publik, yaitu kunci tersebut perlu diketahui oleh umum sebelum proses komunikasi berlangsung.

Cara enkripsi ini mempunyai banyak kelebihan, salah satunya adalah setiap orang hanya perlu memiliki satu set kunci, tanpa peduli berapa banyak orang yang akan diajak berkomunikasi. Jadi jika ada n orang yang berkomunikasi dengan cara ini, hanya dibutuhkan n set kunci saja. Selain itu, cara enkripsi ini tidak membutuhkan saluran yang aman untuk pengiriman kunci, sebab kunci yang dikirim ini memang harus diketahui oleh public. Cara enkripsi ini sangat praktis sehingga dapat digunakan oleh awam.

Setiap orang yang menggunakan enkripsi ini harus mempunyai dua buah kunci, yaitu kunci rahasia yang hanya diketahui oleh dirinya sendiri dan yang lain disebut kunci public yang disebarkan kepada orang lain. Kedua kunci ini dibuat secara acak secara matematis.

Jika A akan mengirimkan pesan kepada si B, si A harus meng-enkrip pesan itu dengan kunci public milik si B. Pesan si A yang telah dienkrip dengan menggunakan kunci public si B, hanya bisa dibuka dengan menggunakan kunci rahasia B. Walaupun dienkrip dengan menggunakan kunci public si B, pesan ini tidak bisa dibuka dengan kunci public itu sendiri. Si B wajib untuk menjamin keamanan kunci rahasianya.

B. Pembahasan

1. Kriptosistem Hellman Knapsack

Algoritma ini dikembangkan oleh Whitfield Diffie dan Martin Hellman pada tahun 1976, dan sebelumnya ditemukan Malcolm Williamson pada tahun 1974.

Sistem ini digunakan untuk penyandian pertukaran pesan antara 2 pihak secara interaktif. Pada awalnya, masing-masing pihak mempunyai sebuah kunci rahasia yang tidak diketahui pihak lawan bicara. Dengan berdasar pada masing-masing kunci rahasia ini, kedua pihak dapat membuat sebuah kunci (session key) yang akan dipakai untuk pembicaraan selanjutnya.

Pembuatan kunci sesi dilakukan seperti halnya suatu tanya jawab matematis, hanya pihak yang aktif mengikuti komunikasi ini saja yang bisa mengetahui kunci sesinya. Penyadap yang tidak secara aktif mengikuti tanya jawab ini, tidak akan bisa mengetahui kunci sesi ini.

Metode Diffie Hellman ini, seperti RSA juga menggunakan aritmetik modulus, tetapi hanya difokuskan pada bilangan prima, yang disebut P.

Dalam kriptosystem RSA ada beberapa persyaratan yang hendaknya dipenuhi, yaitu plaintext di enkripsi ke dalam blok-blok dengan tiap-tiap blok bernilai biner kurang dari *n* adalah integer positip. Dengan demkian panjang maksimal tiap-tiap blok adalah kurang dari atau sama dengan $\log_2(n)$. Atau secara praktis, tiap-tiap blok memuat *k* bit, dengan $2^k \leq n \leq 2^{k+1}$. Proses enkripsi terhadap *plaintext* M dan dekripsi terhadap *chipertext* C dapat dijelaskan sebagai berikut :

$$C = M^e \pmod{n}$$

$$M = C^d \pmod{n} = (M^e)^d \pmod{n} = M^{ed} \pmod{n}$$

Baik pengirim maupun penerima pesan harus mengetahui nilai *n*. pengirim mengetahui nilai *e*, dan hanya penerima yang mengetahui nilai *d*. jadi kriptosystem RSA mempunyai kunci public KP = {e, n}, dan kunci pribadi yang berpasangan dengan kunci public tersebut adalah KR = {*d, n*}. bilangan-bilangan *e, d,* dan *n* semuanya adalah integer positip.

Dalam system Diffie Hellman, ada 2 kelompok yang masing-masing berpikir dari angka acak rahasia yaitu X dan Y. masing-masing mengirim ke kedua komponen itu sehingga satu kelompok tahu ada X dan A^Y dan kelompok yang lain tahu ada Y dan A^X. masing-masing kelompok dapat menghitung A^(X*Y) yang dijabarkan menjadi (X^Y)^X dan juga (A^X)^Y.

Misalkan seseorang mendengarkan perhitungan ini secara diam-diam, dia tidak mengerti maksudnya.

Bahaya yang akan terjadi ketika Diffie Hellman digunakan seseorang adalah pada kasus untuk beberapa nilai dari modulus P, memilih nilai A. Seperti A^X, hanya mempunyai angka kecil dari nilai yang mungkin, tidak peduli berapa pun nilai X, yang akan secara mudah untuk menemukan nilai X.

Diffie Hellman membuat algoritma dalam perhitungan aritmatikanya, dengan mengambil dasar dari algoritma pemecahan masalah *superincreasing* dari problem subset sum sebagai berikut:

1. for I = n downto I do
2. if $T \geq s_i$ then
3. $T = T - s_i$
4. $x_i = 1$
5. else
6. $x_i = 0$
7. if $x_i\, s_i = T$ then
8. X = $(x_i, \ldots, x_n)$ adalah penyelesaian
9. else
10. tidak ada penyelesaian.

Berikut ini contoh kecil penggambaran operasi enkripsi dan dekripsi pada Kriptosistem Merkle-Hellman.

Andaikan

s = (2, 5, 9, 21, 45, 103, 215, 450, 946)

adalah daftar ukuran superincreasing rahasia. Anggap p = 1302 dan a = 1291. Kemudian daftar ukuran publik adalah

t = (575, 436, 1104, 796, 1921, 569, 721, 1183, 1570).

Sekarang, jika Alice ingin mengenkrip plainteks x = (1, 0, 1, 1, 0, 0, 1, 1, 1), dia menghitung

y = 575 + 1104 + 796 + 721 + 1183 + 1570 = 6665.

Ketika Bob menerima cipherteks y, mula-mula dia menghitung

z = a-1 y mod p
= 317 x 6665 mod 1302
= 1643

Kemudian Bob memecahkan contoh problem Subset Sum I = (s, z) dengan menggunakan algoritma yang ditunjukkan dalam Gambar 5.12. Plainteks (1, 0, 1, 1, 0, 0, 1, 1, 1) diperoleh.

2. Implementasi Sistem Hellman-Knapsack Pada Plaintext Nama

Manual (dengan Aplikasi Ms. Excel)

a) andaikan daftar ukuran superincreasing rahasia adalah :

s = (3, 6, 9, 15, 21, 136, 158, 358)
dengan menganggapa nilai p=2003 dan a=1289
maka diperoleh daftar ukuran publik (t) sbb :
rumus → $t_i = a\ s_i \bmod p$
t_1 = 1289 x 3 mod 2003 = 1864
t_2 = 1289 x 6 mod 2003 = 1725
t_3 = 1289 x 9 mod 2003 = 1586
t_4 = 1289 x 15 mod 2003 = 1308
t_5 = 1289 x 21 mod 2003 = 1030
t_6 = 1289 x 136 mod 2003 = 1043
t_7 = 1289 x 158 mod 2003 = 1359
t_8 = 1289 x 358 mod 2003 = 772
sehingga diperoleh t = (1864, 1725, 1586, 1308, 1030, 1043, 1359, 772)
Mengenkrip plaintext nama : ROSDIANA
Terlebih dahulu plaintext dibawah ke nilai decimal (kode ASCII) untuk selanjutnya diberikan nilai biner dari nilai decimal tersebut ;
R → 82 = 01010010
O → 79 = 01001111
S → 83 = 01010011
D → 68 = 01000100
I → 73 = 01001001
A → 65 = 01000001
N → 78 = 01001110
A → 65 = 01000001
Sehingga diperoleh chyperteks y (data yang dikirim) sebagai berikut :
y(R) → {(0x1864) + (1x1725) + (0x1586) + (1x1308) + (0x1030) + (0x1043) + (1x1359) + (0x772)} = 4392
y(O) → {(0x1864) + (1x1725) + (0x1586) + (0x1308) + (1x1030) + (1x1043) + (1x1359) + (1x772)} = 5929
y(S) → {(0x1864) + (1x1725) + (0x1586) + (1x1308) + (0x1030) + (0x1043) + (1x1359) + (1x772)} = 5164
y(D) → {(0x1864) + (1x1725) + (0x1586) + (0x1308) + (0x1030) + (1x1043) + (0x1359) + (0x772)} = 2768
y(I) → {(0x1864) + (1x1725) + (0x1586) + (0x1308) + (1x1030) + (0x1043) + (0x1359) + (1x772)} = 3527
y(A) → {(0x1864) + (1x1725) + (0x1586) + (0x1308) + (0x1030) + (0x1043) + (0x1359) + (1x772)} = 2497
y(N) → {(0x1864) + (1x1725) + (0x1586) + (0x1308) + (1x1030) + (1x1043) + (1x1359) + (0x772)} = 5157

y(A) → {(0x1864) + (1x1725) + (0x1586) + (0x1308) + (0x1030) + (0x1043) + (0x1359) + (1x772)} = 2497

y = (4392, 5929, 5164, 2768, 3527, 2497,5157,2497)

b) Proses Dekripsi :

Data chipertext yang diterima mula-mula dihitung nilai z, dengan menggunakan rumus :

$$z_i = a^{-1} \times y_i \mod p$$

dimana $a^{-1} \rightarrow a \times a^{-1} = 1$

$$1289 \times a^{-1} = 1$$

$$1289 \times 317 = 408613 \bmod 2003 = 1$$

sehingga diproleh nilai $a^{-1} = 317$

jadi nilai dekripnya :

z(4392) = 317 x 4392 mod 2003 = 179
z(5929) = 317 x 5929 mod 2003 = 679
z(5164) = 317 x 5164 mod 2003 = 537
z(2768) = 317 x 2768 mod 2003 = 142
z(3527) = 317 x 3527 mod 2003 = 385
z(2497) = 317 x 2497 mod 2003 = 364
z(5157) = 317 x 5157 mod 2003 = 321
z(2497) = 317 x 2497 mod 2003 = 364

kemudian dengan menggunakan superincreasing rahasia (s), diperoleh nilai biner sebagai berikut :

s	**z1**		**z2**		**z3**		**z4**		**z5**		**z6**		**z7**		**z8**	
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	1	6	1	6	1	6	1	6	1	6	1	6	1	6	1	6
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	1	15	0	0	1	15	0	0	0	0	0	0	0	0	0	0
21	0	0	1	21	0	0	0	0	1	21	0	0	1	21	0	0
136	0	0	1	136	0	0	1	136	0	0	0	0	1	136	0	0
158	1	158	1	158	1	158	0	0	0	0	0	0	1	158	0	0
358	0	0	1	358	1	358	0	0	1	358	1	358	0	0	1	358
Jumlah		179		679		537		142		385		364		321		364

Untuk z1 (01010010) nilai decimal = 82 (R)
Untuk z2 (01001111) nilai decimal = 79 (O)
Untuk z3 (01010011) nilai decimal = 83 (S)
Untuk z4 (01000100) nilai decimal = 68 (D)
Untuk z5 (01001001) nilai decimal = 73 (I)
Untuk z6 (01000001) nilai decimal = 65 (A)
Untuk z7 (01001110) nilai decimal = 78 (N)
Untuk z8 (01000001) nilai decimal = 65 (A)

Jadi diperoleh plaintext yang telah dienkrip :

ROSDIANA

c) Programing (dengan Aplikasi Matlab)

Listing Program :

```
clc;
nama = 'ROSDIANA';
anama = abs(nama);
bnama = [];
for i=1:length(nama)
    am = dec2bin(anama(i));
    am = ['0' am];
    bnama = [bnama am];
end

permutasi = [3 6 1 2 5 4 8 7];
s = [2 5 9 21 45 103 215 450];
p = 2003; % bilangan prima yang lebih besar dari jumlahan s
a = 1289; % ini dipilih sendiri, yang gcd(a,p)=1

% cari nilai t
t = [];
for i=1:8
    t = [t mod(a*s(permutasi(i)),p)];
end

% cari y (integer pesan), kalikan t dengan nilai biner pesan,
% inilah pesan enkrip yang dikirim
ay = [];
pnama = length(bnama)/8;
k = 1;
for j=1:pnama
   y = 0;
   for i=1:8
       if bnama(k) == '1'
          y = y + t(i);
       end
       k = k + 1;
   end
   ay = [ay y];
end
```

```
    % cari nilai d, atau invers dari a
    ad = [];
    k = 1;
    for j=1:pnama
        d = 0;
        for i=1:8
            if bnama(k)=='1'
                d = d + s(permutasi(i));
            end
            k = k + 1;
        end
        ad = [ad d];
    end
% Dekrip pesan
pesan = [];
for j=1:pnama
  X = [];
  T = ad(j);
  for i=8:-1:1
      if T >= s(i)
          T = T - s(i);
          X = ['1' X];
      else
          X = ['0' X];
      end
  end

% kembalikan posisi biner sesuai permutasi
  XP = [];
  for i=1:8
      XP = [XP  X(permutasi(i))];
  end
  sXP = bin2dec(XP);
  pesan = [pesan sXP];
end
```

```
disp ('Plaintext: ');
disp (nama);
disp ('Publik key: ');
disp (t);
disp ('Private key: ');
disp ('P: ');
disp (p);
disp ('A: ');
disp (a);
disp ('S: ');
disp (s);
disp ('Data yang dikirim: ');
disp (ay);
disp ('D: ');
disp (ad);
disp ('Pesan konversi: ');
spesan = setstr(pesan);
disp (spesan);
```

Output program :

```
>> Plaintext:
ROSDIANA
Publik key:
  Columns 1 through 4

        1586         569         575         436

  Columns 5 through 8

        1921        1030        1183         721

Private key:
P:
        2003

A:
        1289

S:
     2     5     9    21    45   103   215   450

Data yang dikirim:
  Columns 1 through 4

        2188        5424        2909        1599

  Columns 5 through 8

        3211        1290        4703        1290

D:
   558   834   773   124   363   318   619   318

Pesan konversi:
ROSDIANA
>>
```

C. Penutup

Pada prinsipnya penggunaan metode kriptosistem baik dengan sistem manual ataupun dengan menggunakan bahasa pemrograman yang mendukung (Matlab) keduanya sama-sama mempuyai kelebihan, tinggal bagaimana pengguna sistem algoritma kriptografi mengaplikasikannya sesuai dengan kemampuan dan kebiasaannya.

Dari pembahasan di atas diperoleh bahwa dengan menggunakan bahasa pemrograman matlab, para pengguna /kriptoanalist tidak terlalu banyak menggunakan elemen-elemen yang digunakan sebagai kunci dalam pembahasannya jika dibandingkan dengan menggunakan Aplikasi Ms. Excel. Akhirnya mealui tulisan ini diharapkan kita mempunyai dasar pemahaman tentang pengenkrepsian suatu kunci tertentu dalam sistem sekuritas suatu informasi.

DAFTAR PUSTAKA

Bishop, David, Introduction to Cryptography with Java Applets, Jones and Bartlett Computer Science, 2003

Dony Ariyus, Pengantar Ilmu Kriptografi, 1st Published, 2008

Meyer, Carl H. & Matyas, Stephen M., Cryptography, A New Dimension in Computer Data Security, John Wiley & Sons, 1982.

Rinaldi Munir, Kriptografi, Informatika Bandung, 2006

Rinaldi Munir, Perancangan Algoritma Stream Cipehr dengan Chaos, Institut Teknologi Bandung, 2005.

Stalling, W., Cryptography and Network Security, Principle and Practice 2rdEdition, Pearson Education, Inc., 1998.