PENGGUNAAN *DIGITAL SIGNATURE* DALAM SURAT ELEKTRONIK DENGAN MENYISIPKANNYA PADA *DIGITIZED SIGNATURE*

Ari Wardana – 135 06 065

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if16065@students.if.itb.ac.id

Extended Abstract

Penggunaan surat elektronik saat ini sudah menjadi hal yang biasa. Baik itu yang melalui e-mail atau hanya berupa surat yang didigitalisasi saja yang dikirimkan dari orang ke orang tanpa melalui protokol e-mail, hanya dengan memindahkan filenya saja dari suatu komputer ke komputer lain. Penggunaan surat elektronik ini sama halnya seperti penggunaan surat yang ditulis di kertas tidak lepas dari masalah pemalsuan. Pada surat yang ditulis di kertas, tanda tangan pengirimnya dijadikan suatu alat bukti keasliannya, walaupun hal itu tidak dapat dikatakan kuat. Pada surat-surat yang sudah didigitalisasikan (*digitized document* atau *digitized mail*) sering disisipkan gambar tanda tangan (*digitized signature*) pengirimnya, namun kekuatan tanda tangan ini untuk membuktikan keaslian suatu surat elektronik menjadi lemah karena dalam dokumen-dokumen elektronik, gambar tanda tangan (*digitized signature*) dengan mudah dapat diperbanyak dan digunakan dalam suatu surat elektronik yang lainnya. Hal ini memungkinkan pemalsuan dapat terjadinya semakin besar. Oleh karena itulah, digunakan *digital signature* (tanda tangan digital) dalam sebuah dokumen elektronik, dalam hal ini surat elektronik.

Penggunaan *digital signature* yang disisipkan pada surat elektronik seringkali menggangu tampilan surat itu dan sering "mengundang" hal-hal yang tidak diinginnkan. Oleh karena itu, penulis mengusulkan suatu cara untuk menyisipkan *digital signature* pada *digitized signature*. Dengan begitu, keberadaan *digital signature* menjadi tersembunyi dan surat elektronik terlihat seperti surat yang ditulis di kertas.

Pada makalah yang akan dibuat, pembangkitan *digital signature* dilakukan dengan menggunakan algoritma DSA. DSA ini menggunakan fungi *hash SHA*. DSA mempunyai dua fungsi utama:

1. Pembentukan tanda tangan digital (*signature generation*)
2. Pemeriksaan keabsahan tanda tangan digital (*signature verification*).

Kata Kunci : *digital signature, digitized signature*

1. Pendahuluan

Selain dengan merahasiakan isi pesan dengan suatu teknik kriptografi, kriptografi juga digunakan untuk menangani masalah keamanan yang mencakup dua hal berikut:

1. Keabsahan pengirim (*user authentication*).
   Hal ini berkaitan dengan kebenaran identitas pengirim. Dengan kata lain, masalah ini dapat diungkapkan sebagai pertanyaan: "Apakah pesan yang diterima benar-benar berasal dari pengirim yang sesungguhnya?"
2. Keaslian pesan (*message authentication*).
   Hal ini berkaitan dengan keutuhan pesan (*data integrity*).
   Dengan kata lain, masalah ini dapat diungkapkan sebagai pertanyaan: "Apakah pesan yang diterima tidak mengalami perubahan (modifikasi)?"
3. Anti-penyanggahan (*nonrepudiation*).
   Pengirim tidak dapat menyangkal (berbohong) tentang isi pesan atau ia yang mengirimkan pesan. Masalah ini masih berkaitan dengan dengan masalah pertama dan kedua. Jika keabsahan pengirim dan keaslian pesan dapat diverifikasi, maka pengirim tidak dapat melakukan sanggahan terhadap pesan yang dikirim.

Ketiga masalah ini dapat diselesaikan dengan teknik otentikasi (*authentication*). Teknik otentikasi (dalam komunikasi data) adalah prosedur yang digunakan untuk membuktikan keaslian pesan atau identitas pemakai.

Sebenarnya, algoritma kriptografi simetri sudah memberikan solusi untuk masalah keamanan pertama dan kedua, karena kunci simetri hanya diketahui oleh pengirim dan penerima. Jadi, jika *B* menerima pesan dari *A*, maka ia percaya pesan itu dari *A* dan isinya tidak mengalami perubahan, karena tidak ada orang lain yang mengetahui kunci selali mereka berdua. Namun, algoritma kriptografi simetri tidak dapat menyediakan cara untuk mengatasi masalah keamanan yang ketiga, yaitu jika salah satu dari dua pihak, *A* dan *B*, membantah isi pesan atau telah mengirim pesan.

Sejak berabad-abad lamanya, tanda tangan (tanda tangan yang ditulis tangan) digunakan untuk membuktikan otentikasi dokumen kertas (misalnya surat, piagam, ijazah, buku, karya seni, dan sebagainya). Fungsi tanda tangan pada dokumen kertas juga diterapkan untuk otentikasi pada data dijital seperti pesan yang dikirim melalui saluran komunikasi dan dokumen elektronis yang disimpan di dalam memori komputer.

Dengan tanda tangan digital, maka integritas data dapat dijamin, disamping itu ia juga digunakan untuk membuktikan asal pesan (keabsahan pengirim dan anti-penyanggahan). Hanya sistem kriptografi kunci-publik yang cocok dan alami untuk pemberian tanda tangan digital. Hal ini disebabkan karena skema tanda tangan digitalberbasis sistem kunci-publik dapat menyelesaikan masalah *nonrepudiation* (baik penerima dan pengirim pesan mempunyai pasangan kunci masing-masing).

Namun, keberadaan tanda tanda yang ditulis tangan masih sering dijumpai dalam dokumen resmi. Akan tetapi karena tanda tangan ini tidak cukup kuat untuk membuktikan keabsahan suatu dokumen digital maka akhirnya ditambahkan juga tanda tangan digital. Keberadaa tanda tangan digital dalam suatu dokumen sering terlihat mengganggu karena biasanya tanda tangan digital berisi untaian karakter yang tidak bermakna. Contohnya
"4EFA7B223CF901BAA58B991DEE5B7A".
Untuk itu penulis, mengusulkan untuk menyembunyikan tanda tangan digital ini di dalam tanda tangan konvensional (ditulis dengan tangan) yang di-*scan*.

2. *Digitized Signature* dan *Digital Signature*

Digital signature merupakan tanda tangan digital yang dibuat berdasarkan *Digital Signature Algorithm* (DSA). Tanda tangan digital ini adalah suatu nilai kriptografis yang bergantung pada pesan dan pengirim pesan (Hal ini kontras dengan tanda tangan pada dokumen kertas yang bergantung hanya pada pengirim dan selalu sama untuk semua dokumen).
Sedangkan *digitized signature* adalah hasil scan dari tanda tangan konvensional kita.

Gambar 1 Contoh digitized signature

3. *Digital Signature Algorithm* (DSA)

Pada bulan Agustus 1991, NIST (*The National Institute of Standard and Technology*) mengumumkan algoritma tanda tangan digital yang disebut *Digital Signature Algorithm* (DSA). DSA dijadikan sebagai bakuan (*standard*) dari *Digital Signature Standard* (DSS). DSS adalah standard, sedangkan DSA adalah algoritma.

Standard tersebut menggunakan algoritma DSA, sedangkan algoritma ini adalah bagian dari standard (selain DSA, DSS menggunakan *Secure Hash Algorithm* atau SHA sebagai fungsi *hash*). DSA termasuk ke dalam sistem kriptografi kunci-publik. Meskipun demikian, DSA tidak dapat digunakan untuk enkripsi. DSA mempunyai dua fungsi utama:

1. Pembentukan tanda tangan digital (*signature generation*)
2. Pemeriksaan keabsahan tanda tangan digital (*signature verification*).

Sebagaimana halnya pada algoritma kriptografi kunci-publik, DSA menggunakan dua buah kunci, yaitu kunci publik dan kunci rahasia. Pembentukan tanda tangan digital menggunakan kunci rahasia pengirim, sedangkan verifikasi tanda tangan digital menggunakan kunci publik pengirim. DSA menggunakan fungsi *hash* SHA (*Secure Hash Algorithm*) untuk mengubah pesan menjadi *message digest* yang berukuran 160 bit.

DSA dikembangkan dari algoritma Elgamal. DSA menggunakan beberapa parameter sebagai berikut:

1. *p*, adalah bilangan prima dengan panjang *L* bit, yang dalam hal ini $512 \le L \le 1024$ dan *L* harus kelipatan 64.
   Parameter *p* bersifat publik dan dapat digunakan bersama-sama oleh orang di dalam kelompok.

2. *q*, bilangan prima 160 bit, merupakan faktor dari $p - 1$. Dengan kata lain, $(p - 1) \bmod q = 0$. Parameter *q* berisfat publik.

3. $g = h^{(p-1)/q} \bmod p$, yang dalam hal ini $h < p - 1$ sedemikian sehingga $h^{(p-1)/q} \bmod p > 1$. Parameter *g* bersifat publik.

4. *x*, adalah bilangan bulat kurang dari *q*. Parameter *x* adalah kunci rahasia.

5. $y = g^x \bmod p$, adalah kunci publik.

6. *m*, pesan yang akan diberi tanda tangan digital.

4. Steganografi

Steganografi adalah teknik penyembunyian data rahasia ke dalam sebuah wadah (media) sehingga data yang disembunyikan sulit dikenali oleh indera manusia. Steganografi membutuhkan dua properti: wadah penampung dan data rahasia yang akan disembunyikan. Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video. Penggunaan steganografi antara lain bertujuan untuk menyamarkan eksistensi (keberadaan) data rahasia sehingga sulit dideteksi, dan melindungi hak cipta suatu produk.

Penyembunyian data rahasia ke dalam citra digital akan mengubah kualitas citra tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data adalah:

1. Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.

2. Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra penampung. Bila pada citra dilakukan operasi pengolahan citra, maka data yang disembunyikan tidak rusak.

3. Data yang disembunyikan harus dapat diungkapkan kembali (*recovery*).

5. Implementasi

Saya membuat 3 buah program dalam mengimplementasikan masalah yang diberikan. Pertama, membuat membuat sebuah program yang bertugas untuk menghasilkan kunci privat dan kunci publik.

Gambar 2 Program untuk membuat kinci public dan private

Kedua, saya membuat sebuah program utama yang bertugas sebagai pembuat tanda tangan digital. Program ini ditempelkan sebagai Add-in pada Microsoft Office Word dengan bantuan VSTO SDK.

Gambar 3 Program pembangkit digital signature

Ketiga, saya mengunakan applikasi untuk melakukan *steganografi* untuk tanda tangan digital yang dihasilkan

Gambar 4 program steganografi

Pada program pertama saya membuat beberapa strategi dalam pengimplementasiannya. Untuk membangkitkan bilangan prima secara acak saya menggunakan sistem penampung sejumlah bilangan prima sampai bilangan prima tertentu, kemudian indeks dari penampung tersebut diacak dan kemudian diambil isi penampung bilangan prima pada indeks yang terpilih secara random.

```
Random random = new Random();
if (input != maxRandom)
{
     maxRandom = input;
     tempA.Clear();
     bool pass;
     for (int x = 2; x < maxRandom;
x++)
     {
         pass = true;
         for (int y = 2; y < x; y++)
         {
              if ((x % y) == 0)
              {
                  pass = false;
              }
         }
         if (pass)
         {
             tempA.Add(x);
         }
      }
}
int     output     =     random.Next(0,
tempA.Count);
if (output == -1)
{
     output = 0;
}
return tempA[output].ToString();
```

Intinya adalah pada program utama ini, saya menggunakan trik penampung untuk menghasilkan bilangan seperti bilangan prima dan bilangan yang relatif prima terhadap bilangan yang lain.

Pada program yang kedua, diimplementasikan dengan VSTO, saya mempunyai strategi menyimpan isi file yang sedang berada di memori program saat ini. Jadi, proses seperti tanda tangan, verifikasi, dan ekstraksi adalah melalui struktur data internal ini. Kemudian hasil tanda tangan digital yang sudah dibuat, dimasukkan ke dalam suatu file yang akan digunakan dalam program ketiga.

Pada program ketiga, saya menggunakan program untuk menyisipkan suatu file ke suatu gambar. Program ini sudah disediakan di website Pak Rinaldi http://www.informatika.org/~rinaldi. File gambar *digitized signature* yang dihasilkan kemudian digunakan untuk mengganti gambar *digitized signature* yang sudah ada.

Kelebihan

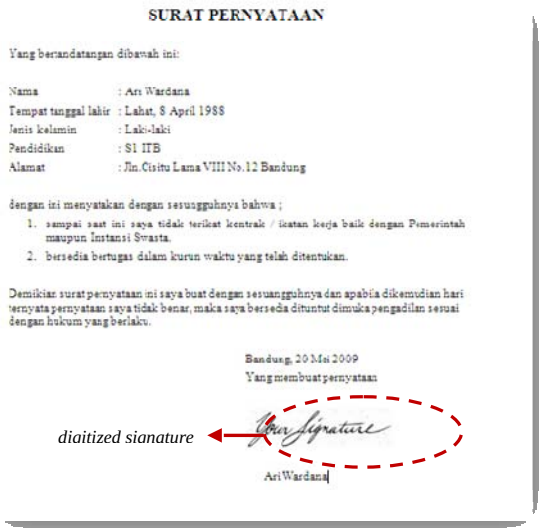
Pada model masalah ini, tanda tangan yang dihasilkan tidak ditampilkan tetapi disisipan ke *digitized signature* yang ada, sehingga memungkinkan file tetap terlihat seperti biasa, tidak ada tampilan tanda tangan digital. Hal ini juga memungkinkan tidak ada perubahan terhadap tanda tangan digital yang ada.

Kekurangan

Perlu proses tambahan untuk menambahakan tanda tangan ddigital dan menvalidasi file yang ditambahkan tanda tangan digital. Karena tanda tangan diletakkan didalam gambar *digitized signarute*.

6. Pengujian

Berikut ini sebuah surat pernyataan yang di dalamnya terdapat



SURAT PERNYATAAN

Yang berandatangan dibawah ini:

Nama : Ari Wardana
Tempat tanggal lahir : Lahat, 8 April 1988
Jenis kelamin : Laki-laki
Pendidikan : S1 ITB
Alamat : Jln.Cisitu Lama VIII No.12 Bandung

dengan ini menyatakan dengan sesungguhnya bahwa ;

1. sampai saat ini saya tidak terikat kontrak / ikatan kerja baik dengan Pemerintah maupun Instansi Swasta.
2. bersedia bertugas dalam kurun waktu yang telah ditentukan.

Demikian surat pernyataan ini saya buat dengan sesungguhnya dan apabila dikemudian hari ternyata pernyataan saya tidak benar, maka saya bersedia dituntut dimuka pengadilan sesuai dengan hukum yang berlaku.

Bandung, 20 Mei 2009
Yang membuat pernyataan

diaitized sianature

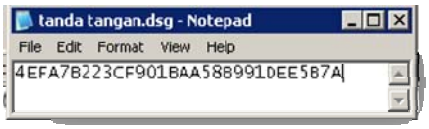
Ari Wardana

Gambar 5 Contoh surat

Pembuatan kunci public dan kunci private

Gambar 6 pembuatan kunci public dan private

Dengan menggunakan program kedua kita dapatkan file yang berisi tanda tangan digital



Gambar 7 tanda tangann digital yang dihasilkan

Proses memasukkan tanda tangan digital ke dalam gambar *digitized signature*

Gambar 8 proses *steganografi* untuk memasukkan file tanda tangan digital ke gambar *digitized signature*

Gambar 9 Hasil yang diperoleh

7. Kesimpulan

Penggunaan tanda tangan digital memungkinkan integritas data dapat dijamin, disamping itu ia juga digunakan untuk membuktikan asal pesan (keabsahan pengirim dan anti-penyanggahan).

Keberadaan tanda tangan digital dapat disisipkan ke dalam *digitized signature* dengan teknik *steganografi*.

8. Daftar Pustaka

[1] *Munir, Rinaldi.* Kriptografi, *Penerbit Informatika, 2006.*