# Analisis Terhadap Kelemahan *Digital Signature*

Parel Wellman Hutahaean 13507138[1]
*Program Studi Teknik Informatika*
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia*
*[1]parel_hutahaean@students.itb.ac.id*

***Abstrak*— Tandatangan telah lama digunakan untuk otentikasi dokumen kertas. Berkembangnya teknologi informasi, memunculkan ide untuk mengadaptasi tandatangan untuk dokumen-dokumen digital, yaitu tandatangan digital (digital signature). Salah satu implementasinya yaitu dengan fungsi hash dan algoritma kunci publik, dimana hanya pengguna yang memiliki kunci privat yang dapat menandatangani dokumen. Berbeda dengan tandatangan pada dokumen kertas yang selalu sama untuk semua dokumen, tandatangan digital berbeda-beda antara satu dokumen dengan dokumen lainnya, bergantung pada isi dokumen yang akan ditandatangani. Ide tandatangan digital ini sebenarnya cukup baik, apalagi secara matematis kekuatan algoritma kriptografi yang digunakan tidak diragukan. Tetapi sayangnya ada satu hal yang terlupa, bahwa pada dunia komputasi manipulasi terhadap program dan sabotase terhadap komputer pengguna bukanlah hal yang sulit dilakukan. Seseorang bisa saja menyabotase komputer orang lain untuk menandatangani dokumen tanpa sepengetahuan orang yang bersangkutan. Dengan kata lain, tandatangan digital hanya memberikan otentikasi antara dokumen dengan komputer, tetapi tidak memberikan otentikasi keterkaitan antara komputer dengan pemilik kunci privat yang sah. Jika seseorang berada di pengadilan dan ditanya tentang tandatangan digital miliknya pada sebuah dokumen, dia dapat saja mengatakan bahwa ia tidak pernah menandatangani dokumen tersebut, dan ketika saksi ahli dihadirkan ia akan menjelaskan bahwa mungkin saja dokumen diberi tandatangan digital tanpa sepengetahuan si pemilik kunci privat.***

***Kata kunci*—About four key words or phrases in alphabetical order, separated by commas.**

## I. PENDAHULUAN

Tandatangan telah lama digunakan untuk membuktikan otentikasi dokumen kertas (misalnya surat piagam, ijazah, buku, karya seni, dan sebagainya). Seseorang yang tandatangannya tertera pada suatu dokumen kertas tidak akan dapat menyangkal bahwa bukan ia yang menandatangani dokumen tersebut. Jika demikian, maka dapat didatangkan 'ahli tandatangan' untuk memastikan keaslian tandatangan tersebut.

Dengan berkembangnya teknologi, bentuk dokumen tidak lagi selalu 'nyata' seperti halnya dokumen kertas, tetapi muncul juga dokumen dalam bentuk digital. Terinspirasi dengan kegunaan tandatangan, maka para ahli komputer memikirkan cara untuk menerapkan tandatangan pada dokumen digital. Tandatangan digital memiliki karakteristik yang sedikit berbeda dengan tandatangan pada dokumen kertas. Jika tandatangan pada dokumen kertas selalu sama untuk semua dokumen, maka tidak demikian halnya dengan tandatangan digital. Tandatangan digital akan berbeda-beda dari satu dokumen dengan dokumen lainnya, ini karena tandatangan digital adalah suatu nilai kriptografis yang nilainya bergantung pada dokumen yang akan ditandatangani.

## II. FUNGSI *HASH* SATU ARAH DAN ALGORITMA KUNCI PUBLIK

Fungsi *hash* adalah fungsi yang menerima masukan string dengan panjang sembarang dan mengkonversinya menjadi string keluaran dengan panjang tetap.

Algoritma kunci publik adalah algoritma kriptografi asimetri dimana kunci yang digunakan untuk mengenkripsi pesan berbeda dengan kunci yang digunakan untuk mendekripsi pesan. Ada dua jenis kunci pada algoritma kunci publik, yaitu kunci privat dan kunci publik. Setiap orang yang ingin menggunakan algoritma kunci publik harus memiliki sepasang kunci tersebut. Kunci publik tidak bersifat rahasia sehingga semua orang boleh mengetahuinya, sementara kunci privat bersifat rahasia dan tidak boleh diketahui oleh orang lain.

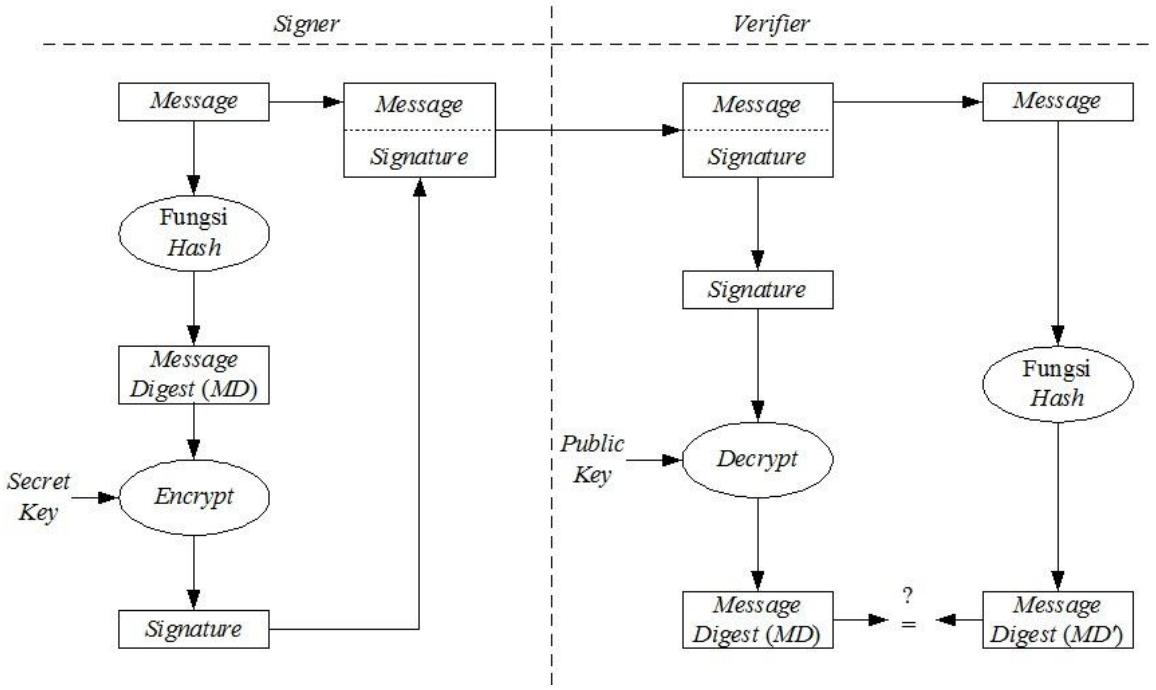
Umumnya kunci publik digunakan untuk mengenkripsi pesan, sementara kunci privat untuk mendekripsi pesan. Seseorang (katakanlah A) yang ingin mengirim pesan ke pihak lain (katakanlah B), akan mengenkripsi pesan yang ingin dikirimkannya dengan menggunakan kunci publik si B. Pesan terenkripsi ini mungkin saja 'disadap' oleh pihak lain yang tidak berhak, tetapi karena hanya si B yang mengetahui kunci privatnya, maka hanya si B yang dapat mengetahui isi pesannya.

Berbeda dengan mekanisme pada pengiriman pesan biasa, penggunaan algoritma kunci publik pada tandatangan digital justru menggunakan kunci privat untuk proses enkripsi dan kunci publik untuk proses dekripsi.

Cara yang umum digunakan untuk 'membangkitkan' tandatangan digital yaitu dengan kombinasi fungsi *hash* satu arah dan algoritma kunci publik. Fungsi *hash* akan menghasilkan pesan ringkas (*message digest*) dari dokumen, kemudian pesan ringkas ini akan dienkripsi dengan menggunakan kunci privat orang yang akan menandatangani dokumen tersebut. Hasil enkripsi pesan ringkas inilah yang disebut sebagai tandatangan digital.

Tandatangan digital akan disertakan (*embedded)* pada dokumen digital terkait.

Verifikasi terhadap dokumen digital dilakukan dengan menggunakan kunci publik orang yang menandatangani. Mula-mula dokumen dipisahkan menjadi dua bagian, yaitu bagian isi dan tandatangan digital. Tandatangan digital kemudian didekripsi dengan menggunakan kunci publik si 'pemilik' dokumen untuk mendapat nilai *hash*-nya. Nilai *hash* ini kemudian dibandingkan dengan nilai *hash* dokumen (bagian isinya). Jika sama, berarti benar dokumen tersebut telah ditandatangani secara digital oleh orang yang memiliki kunci privat terkait. Gambar 1 menunjukkan mekanisme otentikasi pada tanda tangan digital.




Gambar 1. Mekanisme otentikasi dengan tandatangan digital

## III. KEABSAHAN TANDATANGAN DIGITAL

Sejak ditemukan pada tahun 1970-an, tandatangan digital diharapkan dapat berperan sebagaimana tandatangan pada dokumen kertas. Perkembangan teknologi yang pesat menjadikan tandatangan digital sebagai komponen penting dalam bisnis di *cyberspace* saat ini. Bahkan di beberapa negara maju, tandatangan digital telah memiliki kekuatan hukum.

Di saat tandatangan digital mulai lazim digunakan dan bahkan berkekuatan hukum, sebagian ahli di bidang informatika justru mulai mempertanyakan keabsahan tandatangan digital. Bukan karena lemahnya kekuatan matematis dari algoritma yang digunakan, tapi lebih kepada banyaknya celah-celah kelemahan pada saat implementasi tandatangan digital.

Misalkan, Alice (nama ini akan digunakan seterusnya untuk menyederhanakan penjelasan) memiliki kunci privat dimana hanya ia yang mengetahuinya. Saat ia ingin 'menandatangani' dokumen, ia akan menghitung nilai *hash* dari dokumen tersebut. Kemudian ia akan melakukan kalkulasi matematis terhadap nilai *hash* tersebut dengan menggunakan kunci privatnya (mengenkripsi). Hasil kalkulasi inilah yang kemudian disebut sebagai tandatangan digital. Semua orang dapat melakukan verifikasi terhadap tandatangan digital tersebut dengan menggunakan kunci publik Alice (mekanisme verifikasi telah dijelaskan pada bagian sebelumnya). Jika verifikasi berhasil, berarti benar bahwa Alice yang telah menandatangani dokumen tersebut, karena hanya ia yang mengetahui kunci privatnya.

Secara matematis, mekanisme di atas bekerja dengan baik. Tetapi tidak secara semantik. Contoh diatas tidak menjelaskan apapun tentang 'menandatangani'. Kenyataannya, 'tandatangan digital' mungkin adalah kesalahan tata nama terburuk dalam sejarah kriptografi.

Dalam hukum, tandatangan digunakan untuk mengindikasikan persetujuan, atau setidaknya pengakuan terhadap dokumen yang ditandatangani. Ketika dipersidangan misalnya, hakim / juri melihat dokumen kertas yang ditandatangani Alice, maka ia mengetahui bahwa Alice pernah 'memegang' dokumen itu sebelumnya, dan memiliki alasan untuk percaya bahwa Alice membaca dan menyetujui kata-kata pada dokumen tersebut. Seseorang tentu tidak dapat begitu saja membuat dokumen dengan tandatangan palsu dan mengatakan bahwa dokumen tersebut telah ditandatangani oleh Alice. Jika demikian, hal tersebut justru dapat membahayakan dirinya sendiri karena bisa saja 'ahli tandatangan' dihadirkan sebagai saksi. Untuk menghindari hal ini, maka untuk dokumen-dokumen yang sifatnya penting, digunakan tandatangan notaris.

Lalu bagaimana halnya dengan tandatangan digital? Bagaimana membuktikan kepada hakim / juri bahwa

benar Alice yang menandatangi dokumen tersebut? Atau bahkan membuktikan bahwa Alice pernah melihat dokumen tersebut. Apakah verifikasi digital dengan menggunakan kunci publik Alice cukup? Secara konsep seharusnya iya. Jika hasil verifikasi sesuai, berarti benar bahwa Alice yang telah menandatangani dokumen tersebut. Karena hanya dia yang 'dianggap' mengetahui kunci privat yang bersesuaian. Tetapi pada implementansinya, ternyata terdapat hal-hal yang menyebabkan keabsahan tandatangan digital menjadi cacat.

Masalahnya adalah tandatangan digital hanya memberikan otentikasi antara dokumen dengan komputer yang menandatangani dokumen tersebut, tetapi tidak memberikan otentikasi keterkaitan antara Alice dengan komputer. Perlu dicatat bahwa bukan Alice yang menghitung nilai tandatangan digital dari dokumen, melainkan komputer yang melakukannya untuk Alice. Hal ini berbeda dengan tandatangan pada dokumen kertas dimana Alice sendiri yang langsung menandatangani dokumen tersebut.

Sebagai contoh misalnya PGP (*Pretty Good Privacy*). Program ini memberikan tandatangan digital pada email. Antarmuka penggunanya sederhana, saat seseorang ingin memberikan tandatangan digital pada email, dia dapat memilih menu yang sesuai, memasukan *passphrase* pada kotak dialog, dan klik "OK". Program akan melakukan dekripsi dengan *passphrase* tadi untuk mendapatkan kunci privat. Dengan kunci privat ini kemudian dilakukan kalkulasi nilai kriptografi dari pesan tersebut, hasil kalkulasi (enkripsi) inilah yang kemudian disebut sebagai tandatangan digital dan kemudian disertakan (*embedded*) pada email. Suka atau tidak, pengguna hanya dapat percaya bahwa PGP melakukan kalkulasi tandatangan digital dengan valid, bahwa PGP menandatangani email sebagaimana yang diinginkannya, bahwa PGP tidak memberikan salinan (*copy*) kunci privatnya ke pihak lain, yang kemudian dapat menandatangani apa saja yang ia inginkan dengan menggunakan tandatangannya. Seseorang dapat dengan mudah menulis versi 'nakal' dari PGP yang kemudian menggunakan tandatangan digital pengguna untuk menandatangani pesan lainnya. Seseorang juga dapat menulis *back orifice plug-in* yang meng-*capture* kunci privat pengguna dan menandatangani dokumen lain tanpa ijin atau sepengetahuan pemiliknya. Kita bahkan telah mengenal virus komputer yang mencoba mencuri kunci privat PGP, yaitu varian dari *nastier*. Intinya, banyak cara yang dapat digunakan untuk menandatangani dokumen dengan tandatangan digital milik orang lain.

Ini menunjukan, betapa pun kuatnya nilai matematis kriptografi, tetap tidak dapat menjembatani jurang pemisah antara pengguna dengan komputer. Jadi tandatangan digital hanya memberikan otentikasi bahwa dokumen telah ditandatangani secara digital oleh komputer, tetapi tidak menjamin bahwa dokumen tersebut benar-benar ditandatangani oleh orang yang berhak. Hal ini dikarenakan pada dunia komputasi sebuah program mudah sekali dimanipulasi.

Bayangkan situasi pengadilan dimana Alice ditanya perihal dokumen yang ditandatanganinya secara digital. Alice kemudian menjawab bahwa ia bahkan tidak pernah melihat dokumen tersebut. Dia mengakui bahwa secara matematis memang terbukti bahwa kunci privatnya yang menandatangani dokumen tersebut, tetapi dia bersikeras bukan dia yang menandatangani dokumen tersebut. Bahkan, Alice mengaku tidak pernah melihatnya. Saat seorang pakar dihadirkan pada sidang tersebut, ia akan menjelaskan bahwa mungkin saja Alice tidak pernah melihat dokumen tersebut, bahwa dapat ditulis sebuah program untuk menandatangani dokumen tanpa sepengetahuan Alice, dan bahwa apa yang disebut dengan 'tandatangan digital' sama sekali tidak membuktikan bahwa Alice yang menandatangani dokumen tersebut. Lalu dimana kekuatan 'tandatangan digital'. Jika demikian, apakah fungsi tandatangan digital untuk otentikasi pesan, otentikasi pengirim, dan anti-penyangkalan masih valid?

Konsep awal dari tandatangan digital ini memang sangat baik. Tapi ada satu hal yang terlupa, bahwa *gap* antara pengguna dan komputer cukup besar. Artinya, kita tidak benar-benar bisa memastikan apakah suatu komputer benar-benar digunakan oleh Alice untuk memberikan tandatangan digital, atau sebenarnya ada orang lain yang dengan kemampuannya mampu menyabotase komputer tersebut sehingga seolah-olah Alice yang memberi tandatangan digital. Berbeda dengan tandatangan pada dokumen kertas, sehebat-hebatnya seseorang menirukan tandatangan Alice, tetap tidak akan pernah persis sama karena setiap orang mempunyai pola 'goresan tulisan' yang unik. Hal ini dapat dibuktikan dengan menghadirkan 'ahli tandatangan'.

Tandatangan digital membuktikan secara matematis bahwa nilai rahasia yang dikenal sebagai kunci privat memang dimasukkan ke komputer. Tetapi sama sekali tidak membuktikan bahwa kunci privat tersebut dimasukan oleh orang yang berhak.

## IV. KESIMPULAN

Keabsahan tandatangan digital tidak dapat disamakan dengan keabsahan tandatangan pada dokumen kertas. Tandatangan pada dokumen kertas menunjukkan otentikasi dokumen dan tidak dapat disangkal. Tidak ada satu orang pun yang dapat menirukan secara persis tandatangan orang lain. Tandatangan pada dokumen kertas mengindikasikan bahwa pemilik tandatangan menyetujui atau mengetahui kata-kata yang tertera pada dokumen tersebut.

Tandatangan digital keabsahannya dapat dipertanyakan bukan karena lemahnya kekuatan matematis algoritma kriptografi yang digunakan, tetapi karena celah-celah keamanan saat seseorang menggunakan komputer. Banyak cara yang dapat dilakukan untuk memberi tandatangan digital tanpa sepengetahuan orang yang berhak (yang memiliki kunci privat). Ini disebabkan pada dunia maya sabotase terhadap komputer orang lain

bukanlah hal yang sulit dilakukan. Tandatangan digital hanya memberikan otentikasi antara dokumen dengan komputer, tetapi tidak memberikan otentikasi keterkaitan antara pemilik kunci privat yang sah dengan komputer.

## REFERENSI


[1] Ir. Rinaldi Munir, M.T., Digital Signature Standard (DSS), Informatika ITB, 2004.

[2] Bruce Schneier, Why Digital Signatures Are Not Signatures, http://www.schneier.com/crypto- gram-0011.html, diakses tanggal 16 Mei 2013

[3] Bruce Schneier, Security Pitfalls in Cryptography, http://www.schneier.com /essay-028.html, diakses tanggal 17 Mei 2013


## PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 20 Mei 2013

Parel Wellman Hutahaean
13507138