Aplikasi Tanda Tangan Digital (*Digital Signature*) Menggunakan Algoritma *Message Digest* 5 (MD5)

Dhea Pungky Precilia[1)], Ahmad Izzuddin[2)]

[1)] Mahasiswa Program Studi Teknik Elektro, Fakultas Teknik, Universitas Panca Marga
[2)] Dosen Program Studi Teknik Elektro, Fakultas Teknik, Universitas Panca Marga
Jl. Yos Sudarso 107 Pabean Dringu Probolinggo 67271
Email : oedienpowerful@yahoo.com

Terima Naskah : 23 Januari 2015
Terima Revisi : 18 Maret 2015

ABSTRAK

Kriptografi mempunyai kemampuan untuk mengamankan sebuah pesan. Kriptografi mempunyai aspek keamanan berupa keabsahan pengirim, keaslian pesan dan anti penyangkalan. Aspek keamanan ini dapat diselesaikan dengan teknik autentifikasi yang salah satu caranya dengan menggunakan tanda tangan digital. Tanda tangan digital dapat dilakukan dengan menggunakan fungsi *hash*. Algoritma *message digest* 5 adalah salah satu fungsi *hash* yang digunakan untuk sistem tanda tangan digital.

Dalam paper ini, aplikasi tanda tangan digital menggunakan algoritma *message digest* 5 dibangun dengan menggunakan bahasa pemrograman *Visual Basic* 6.0. Pesan yang dibubuhi tanda tangan digital antara lain surat pemberitahuan dan surat penagihan. Perancangan dilakukan dengan beberapa tahap diantaranya adalah membaca isi dokumen, menyimpan isi dokumen digital, mencari nilai *hash* dengan algoritma *message digest* 5, kemudian menyimpan *message digest* pada dokumen digital.

Berdasarkan pengujian yang telah dilakukan, diketahui bahwa sistem dapat membandingkan antara nilai *hash* yang telah dibuat pada dokumen digital dengan nilai *hash* dari dokumen digital tersebut. Dari proses perbandingan nilai *hash* yang merupakan tanda tangan digital untuk dokumen digital dapat diketahui apakah sebuah dokumen digital telah mengalami perubahan atau tidak.

Kata kunci: Tanda Tangan Digital, Algoritma *Message Digest* 5, Nilai *Hash*.

ABSTRACT

Cryptography had the capability to secure a message. Cryptography have security aspects of the validity of the sender, the authenticity of a message and Non repudiation. It can be resolved by the security aspect of authentication by using to one digital signature. Digital signature can be done by using the function of hash. The message Digest 5 Algorithms is one of the functions hash applied to a system digital signature.

In this paper, application of digital signature using a message digest 5 algorithms constructed by using visual basic 6.0 programming language. A message that he has put other digital signature between notification letter and mail billing. Stage design do with some of them are read the document contents, stores the contents digital document, looking for the value of hash with a message digest 5 algorithms, then keep a digest digital message on a document.

Based on testing that has been done known that the system can compare between grades hash made in digital documents with a value of hash of the digital document. From the process of comparison hash value that is a signature digitally for digital document can be known whether a digital document has changed or not.

***Key words**: Digital Signature, Message Digest 5 Algorithms, Value Of Hash*

PENDAHULUAN

Seiring dengan pesatnya perkembangan teknologi, pengiriman pesan dalam dunia bisnis yang dilampirkan pada pengiriman *e-mail* (*electronic mail*) melalui internet semakin sering digunakan. Pesan yang dilampirkan biasanya

berupa surat pemberitahuan atau surat penagihan dalam bentuk dokumen digital. Meskipun pengiriman dokumen digital melalui internet merupakan pilihan yang efektif dan efisien, namun dari segi keamanan pengiriman dokumen digital melaui internet tidaklah begitu aman.Tanpa adanya pengamanan dari dokumen digital, pengirim dan penerima tidak dapat mengetahui adanya perubahan atas dokumen digital yang telah dikirimkan. Metode yang sering digunakan untuk mengamankan data adalah kriptografi.

Kriptografi mempunyai aspek-aspek keamanan yaitu, kerahasian pesan, keabsahan pengirim, keaslian pesan dan nirpenyangkalan. Kerahasiaan pesan dapat diselesaikan dengan enkripsi dan dekripsi sedangkan aspek-aspek lainnya dapat diselesaikan dengan teknik autentifikasi. Tanda tangan digital merupakan salah satu cara dari kriptografi untuk autentifikasi dari sebuah pesan atau dokumen.

Tanda tangan digital yang dibubuhkan dalam suatu dokumen digital dapat memvalidasi darimana data tersebut berasal. Tanda tangan digital dapat dilakukan melalui enkripsi atau menggunakan fungsi *hash*. Algoritma yang biasanya dipakai untuk membuat sebuah tanda tangan digital yaitu Algoritma *Message Digest 5* (MD5).

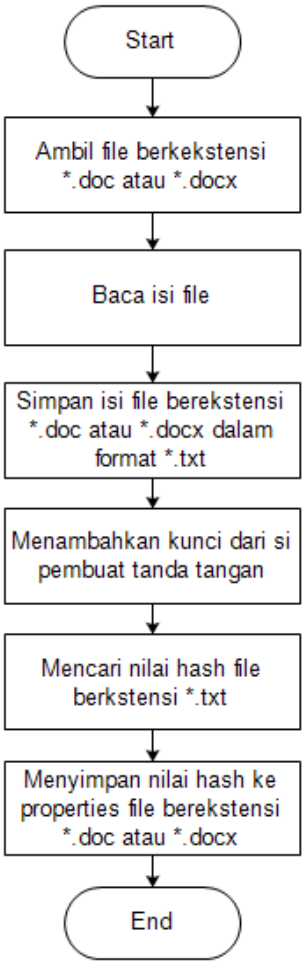
Algoritma *Message Digest 5* (MD5) menghasilkan *message digest* yang dihasilkannya bersifat '*one way hash*'. Sehingga berapapun masukan yang diberikan hasilnya tetap sepanjang 32 karakter. Tujuan dari penelitian ini adalah membangun aplikasi tanda tangan digital dengan menerapkan metode MD5.

METODE

Penelitian ini dilaksanakan dalam beberapa tahapan, tahapan pertama dilakukan dengan melakukan pengambilan data. Data diambil di Kantor Notaris Dewi Meutia Cipta Ningrum, S.H., M.H. di Probolinggo. Tahapan berikutnya adalah sesuai dengan metode pengembangan perangkat lunak yaitu metode *waterfall* yaitu : analisis, desain sistem, implementasi/pengkodean dan pengujian.

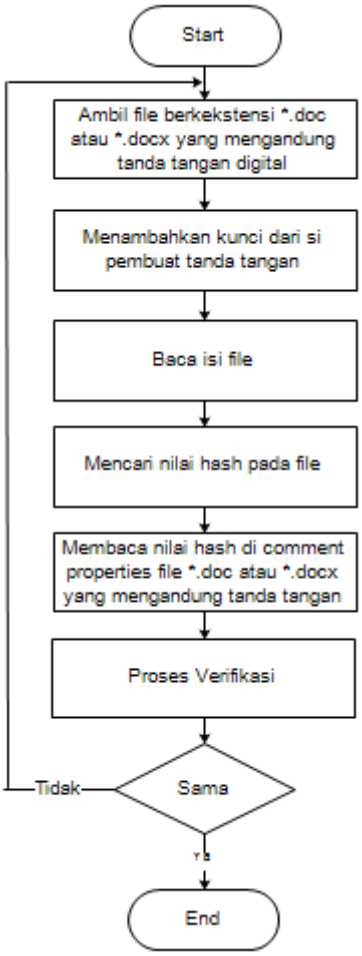
Tahapan analisis dilakukan dengan mengkaji kelemahan-kelemahan metode konvensional yang dilakukan oleh Kantor Notaris dalam melakukan pengiriman berkas-berkas digital yang berekstensi *.doc atau *.docx, sekaligus mencari solusi atas permasalahan yang ada dalam bentuk membangun aplikasi.

Tahapan desain dilakukan untuk memberikan gambaran yang jelas menyangkut sistem yang akan dibangun agar memberikan kemudian dalam proses pengkodean. Desain sistem dalam penelitian ini dibuat menggunakan flowchart yang menggambarkan proses yang dilakukan dengan aplikasi. Terdapat dua tahapan proses yang dilakukan dalam aplikasi tanda tangan digital. Tahappertama adalah proses penandatanganan file berekstensi *.doc atau *.docx yang digambarkan dalam Gambar 1.



Gambar 1. Proses penandatanganan file berekstensi *.doc atau *.docx (sumber : diolah)

Tahap kedua adalah Proses Verifikasi file berekstensi *.doc atau *.docx yang telah diberi tanda tangan digital seperti tergambar dalam Gambar 2.

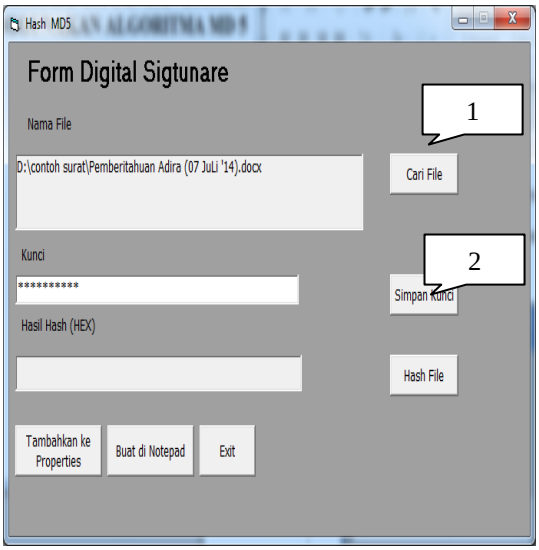


Gambar 2. Proses verifikasi file
(sumber : data diolah)

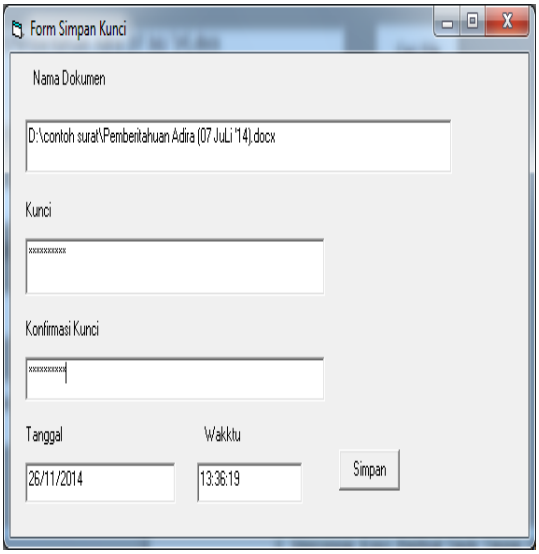
HASIL DAN PEMBAHASAN

Setelah desain sistem dibuat, langkah berikutnya adalah implementasi (men-*code*-kan menggunakan bahasa pemrograman). Bahasa pemrograman yang digunakan adalah bahasa pemrograman Visual Basic 6.0. Gambar 3 merupakan implementasi berupa form untuk membuat dan menyimpan kunci untuk keperluan enkripsi dan dekripsi. Kunci akan disimpan dalam format *.txt.

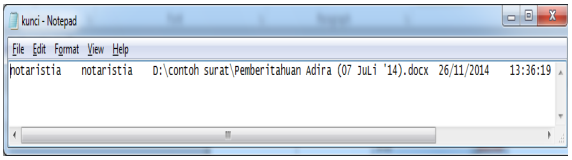
Langkah pertama yang dilakukan adalah mengambil file *.doc atau *.docx yang akan diberikan tanda tangan digital. Langkah kedua adalah memberikan kunci enkripsi, kunci disimpan dalam bentuk *.txt untuk diberikan kepada penerima dokumen digital untuk keperluan dekripsi dan autentifikasi.



Gambar 3. Pemberian kunci untuk enkripsi
(Sumber : data diolah)

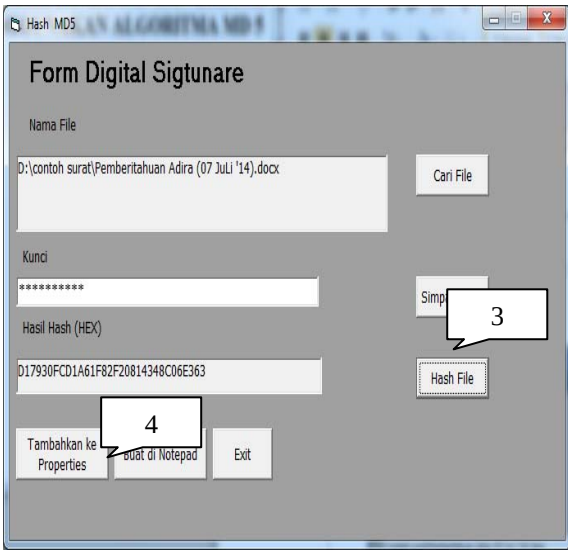


Gambar 4. Konfirmasi penyimpanan kunci
(Sumber : data diolah)



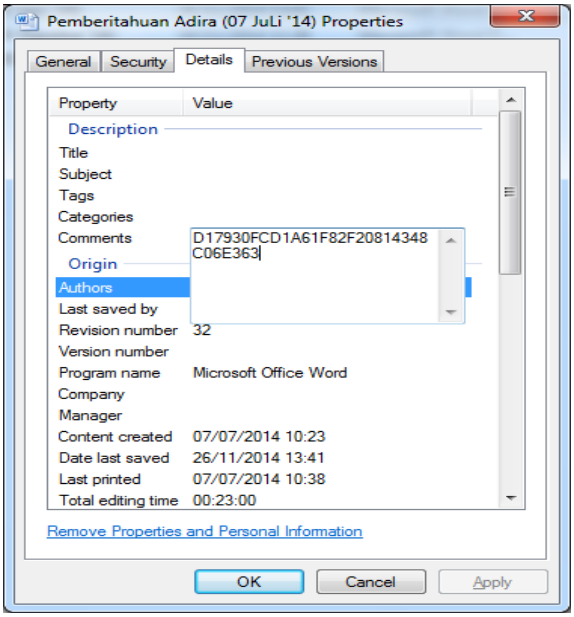
Gambar 5. Kunci yang tersimpan dalam file *.txt untuk dekripsi dan autentifikasi (Sumber : data diolah)

Langkah berikutnya adalah mencari nilai *hash* sebuah dokumen yaitu dilakukan dengan mencari nilai *hash* pada sebuah file *.doc atau *.docx seperti pada Gambar 6.

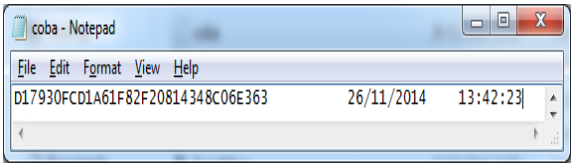


Gambar 6. Mencari nilai hash dari file *.doc atau *docx (*3) dan menyisipkannya ke properties comment (*4) (Sumber: data diolah)

Gambar 7. Menunjukkan nilah hash yang tersimpan sebagai properties comment dari sebuah file *.doc atau *.docx. Selain disisipkan sebagai properties dari file *.doc atau *.docx, nilai hash dapat juga disimpan dalam bentuk *.txt yang terpisah dari file yang akan dibubuhi tanda tangan digital seperti yang ditunjukkan dalam Gambar 8.



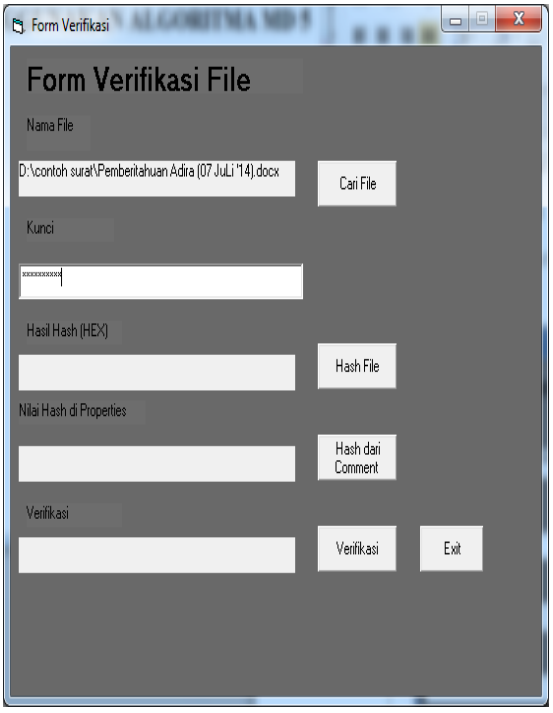
Gambar 7. Nilai hash yang tersimpan sebagai propertis comment file *.doc atau *.docx (Sumber: data diolah)



Gambar 8. Nilai hash yang disimpan dalam file *.txt (Sumber: data diolah)

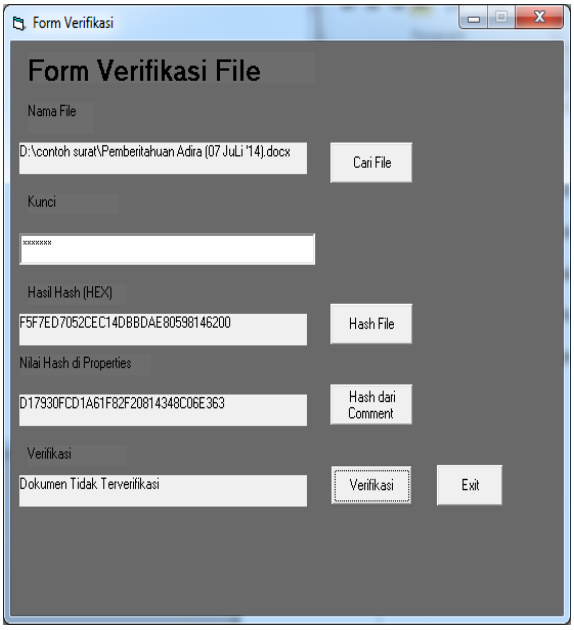
Setelah proses pemberian tanda tangan selesai dilakukan, langkah selanjutnya adalah proses verifikasi. Proses verifikasi dilakukan dengan cara membandingkan nilai hash yang didapat dari sebuah file *.doc atau *.docx dengan nilai hash yang tersimpan dalam properties comment.

Mendapatkan nilai hash dari sebuah file *.doc atau *.docx dilakukan dengan menggunakan form verifikasi file (Gambar 9). Kunci yang digunakan adalah kunci yang didapat dari pemberi tanda tangan digital. Jika nilai hash yang dihasilkan sama dengan nilai hash yang tersimpan dalam properties comment, maka *.doc atau *.docx terverifikasi sebagai dokumen asli. Mengambil nilai hash dari properties comment dilakukan dengan menggunakan tombol yang disediakan (Gambar 9).



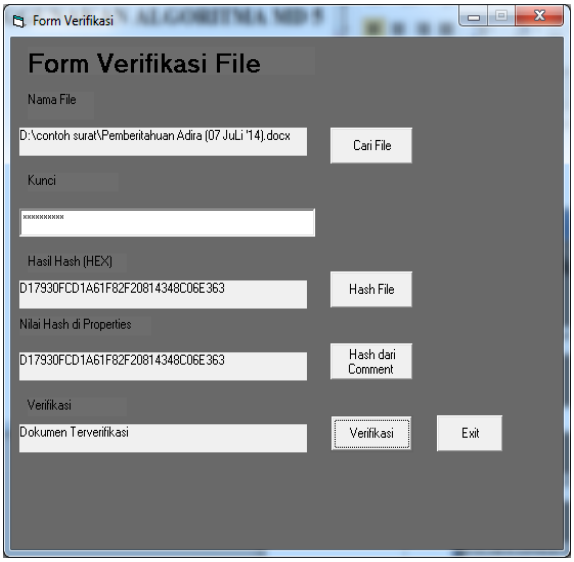
Gambar 9. Form verifikasi file
(Sumber : data diolah)

Dalam proses verifikasi terdapat dua hal yang mungkin terjadi, kemungkinan pertama adalah dokumen tidak terverifikasi, dan yang kedua adalah dokumen terverifikasi. Dokumen tidak terverifikasi disebabkan kesalahan kunci yang diberikan. Kunci yang salah dapat menghasilkan nilai hash yang berbeda. Penyebab lainnya adalah isi dokumen sudah berubah. Melakukan modifikasi terhadap isi dokumen menyebabkan nilai hash yang dihasilkan bebeda. Gambar 10 merupakan gambar yang menunjukkan dokumen tidak terverifikasi disebabkan kunci yang digunakan tidak sama dengan kunci yang diberikan oleh pemberi tanda tangan.



Gambar 10. Dokumen tidak terverifikasi karena menggunakan kunci yang salah atau berbeda
(Sumber: data diolah)

Jika kunci yang digunakan adalah kunci yang benar dan tidak dilakukan perubahan apapun terhadap isi file *.doc atau *.docx, maka dokumen akan terverifikasi asli seperti yang ditunjukkan Gambar 11.



Gambar 11. Dokumen terverifikasi
(Sumber: data diolah)

SIMPULAN

Dari hasil penelitian yang telah dilakukan, maka diperoleh kesimpulan sebagai berikut :

1. Penggunaan Algoritma *Message Digest* 5 untuk keperluan tanda tangan digital (*digital signature*) bisa memberikan jaminan keamanan data dalam hal ini meliputi integritas data, otentikasi dan nirpenyangkalan (*non-repudiation*) dari sebuah dokumen digital.
2. Implementasi pada tanda tangan digital (*digital signature)* tidak mempengaruhi isi dari dokumen digital, karena nilai *hash*diletakkan pada *comment* di *properties* sehingga tidak mengganggu keaslian dari sebuah dokumen digital.

DAFTAR PUSTAKA

[1] Bahari, Muhammad Ilmy. *Perbandingan Algoritma MD2, MD4, DAN MD5*. Program Studi Teknik Informatika, Institut Teknologi Bandung.2010.

[2] Coffey,Tom dan Puneet Saidha.*Non-Repudiation With Mandatory Proof Of Receipt*. University of Limerick. Ireland.

[3] Kromodimoeljo, Sentot. *Teori dan Aplikasi Kriptografi*. SPK IT Consulting.2009.

[4] Munir, Rinaldi. *Fungsi Hash Satu-Arah dan Algoritma MD5*.DepartemenTeknik Informatika Institut Teknologi Bandung. Bandung. 2004.

[5] Munir, Rinaldi. K*riptografi*. Informatika Bandung. Bandung. 2006.

[6] Munir, Rinaldi, dkk. *Analisis dan Perancangan Perangkat Lunak Digital Signature Signme Menggunakan Algoritma Rsa Dan Fungsi Hash Md5*. Seminar Nasional Sistem dan Informatika. Bali. 2007.

[7] Pasca, M. Nugraha. *Perbandingan Algoritma MD4 dan MD5 serta Implementasinya dalam Kehidupan Sehari-hari*.Program Studi Teknik Informatika, Institut Teknologi Bandung.2010.

[8] Rachmat, Antonius C. *Algoritma dan Pemrograman dengan Bahasa C.* Andi Yogyakarta. Yogyakarta.2010.

[9] Thabrani, Suryanto.*Mudah dan Cepat Menguasai Visual Basic*.Mediakita.Jakarta.2007.