بسم الله الرحمن الرحيم

جامعـــة أم درمان الاســـلامية

كلية العـــلوم والتقانة

علـــوم الحاسوب

الـــرابعة

تقرير في مقرر أمن المعومات والشبكات بعنوان :

التوقيع الإلكتروني

Digital Signature

إعداد الطلاب:

- طلال حسن أمين حسين
- الارقم قاسم الزين
- مأمون عادل مأمون
- محمد عبد المنعم
- أحمد علي محمد

إشرا

ف الاستاذ :

محمد عبد الرحمن

المحتويات

المقدمة :

يلعب الانترنت دوراً رئيسياً في حياة الافراد حيث نجد انه قلص الزمان والمكان من بما يقدمه من خدمات متعددة استفاد منها الافراد والمؤسسات استفادة قصوي وحتي تكتمل هذه الاستفادة فانه يجب ان تتضمن هذه الخدمات السرية والحماية خصوصاً في المعاملات التجارية وغيرها من المعاملات الخاصة التي يفترض ان لا تتعرف عليها الا الجهة المخول لها بذلك.

في هذا الموضوع سنتحدث عن التوقيع الإلكتروني كألية لحماية المعلومات وذلك بالتاكد من هوية مصدر المعلومات(الرسالة) حيث انها تعتبر من اهم الطرق المستخدمة لضمان الوثائق المرسلة بجعل مستقبل الرسالة او الوثيقة مطمئن من الطرف الذي أرسلها له. وكان أول اعتراف بالتوقيع الإلكتروني في عام 1989 في مجال البطاقات الإئتمانية حيث أقرت محكمة النقض الفرنسية صحة التوقيع الإلكتروني واعتبرت أنه يتألف من عنصرين هما إبراز البطاقة الإئتمانية وإدخال رقم حامل البطاقة السري وأكدت هذه المحكمة كذلك أن هذه الوسيلة توفر الضمانات الموجودة في التوقيع اليدوي بل تفوقها .

وصدر في 13 كانون أول 1999م إرشاد عن الاتحاد الأوروبي حول التوقيع الإلكتروني .الا أن اول توقيع الكتروني صدر في امريكا في الاول من اكتوبر عام 2000م .

مصطلحات التقرير:

Terms	Abbreviations
ANS	American National Standards
CA	Certificate Authority
DH	Diffie-Hellman Algorithm
DSA	Digital Signature Algorithm
DSS	Digital Signature Standards
MAC	Message Authentication Code
MD5	Message Digest

NIST	National Institute of Standards and .Technology
PKCS	Public Key Cryptography Standards
RSA	Algorithm developed by Rivest ,Shamir and Adelman
VME	Virtual Matrix Encryption

التوقيع الإلكتروني :

التوقِّيع عموماً هو علامة شخصية يمكن من خلالها تمييز هوية الموقِّع وتتكون هذه العلامة من أحد الخواص الاسمية للموقع وهي اسمه ولقبه فالاسم هو روح التوقيع ، ووظيفته الاساسية هي التعبير عن رضا الموقع بما صدر منه ويجب ان يصدر من شخص كامل الاهلية. ويجب ان يكون التوقيع بخط يد الموقع ، ولكن لاعتبارات معينه أجازت التشريعات التوقيع بالختم والبصمة

اما التوقيع الإلكتروني فهو عبارة عن عملية تشفير مكون من بعض الحروف والرموز والأرقام الإلكترونية، تصدر عن إحدى الجهات المتخصصة والمعترف بها حكوميا ودوليا. تعمل على توثيق الملفات بشتى أنواعها والتي تتم عبر الإنترنت. فيتم من خلالها ربط هوية الموقع بالوثيقة، وبحيث يمكن لمستلم الوثيقة التحقق من صحة التوقيع، وأيضا من السهل لكل شخص الحصول على هذا التوقيع من الجهات المختصة لإصدار الشهادات.

ويستخدم هذا التوقيع لإغراض عدة منها أغراض الشخصية او سياسيه أو تجاريه، وغيرها من المجالات الأخرى, ويجب أن يحقق وظائف التوقيع حيث يحدد هوية الموقع والتعبير عن إرادته بالموافقة على مضمون رسالة البيانات.

الفرق بين التوقيع العادي والتوقيع الإلكتروني هو أن التوقيع العادي عبارة عن رسم يقوم به الشخص بمعني انه فن وليس علم ومن هنا يسهل تزويره، أما التوقيع الإلكتروني فهو علم وليس فن ويعصب تزويره.

أهمية التوقيع الإلكتروني:

تنبع أهمية التوقيع الإلكتروني في تصديق أن الرسالة لم يتم تغييرها، وتوفر الضمان والتأكد بأنه لم يتم أجراء أي تعديل عليها لأنه من

الصعب تزويره والعبث به، فهو أيضا يوفر 4 خواص وهي:

الخصوصية :

بحيث يمنع أي مستخدم غير شرعي من تعديل أي إجراء على البيانات.

التحقق:

يعني التحقق من هوية المرسل ومصادر البيات عن طريق جهة الشهادات التصديق الإلكترونية المرخص لها دوليا.

وحدة البيانات:

التأكد من تكاملية البيانات بإستخدام تقنية تشفير البيانات ومقارنة بصمة الرسالة المرسلة مع بصمة الرسالة المستقبلة.

خاصية عدم الإنكار :

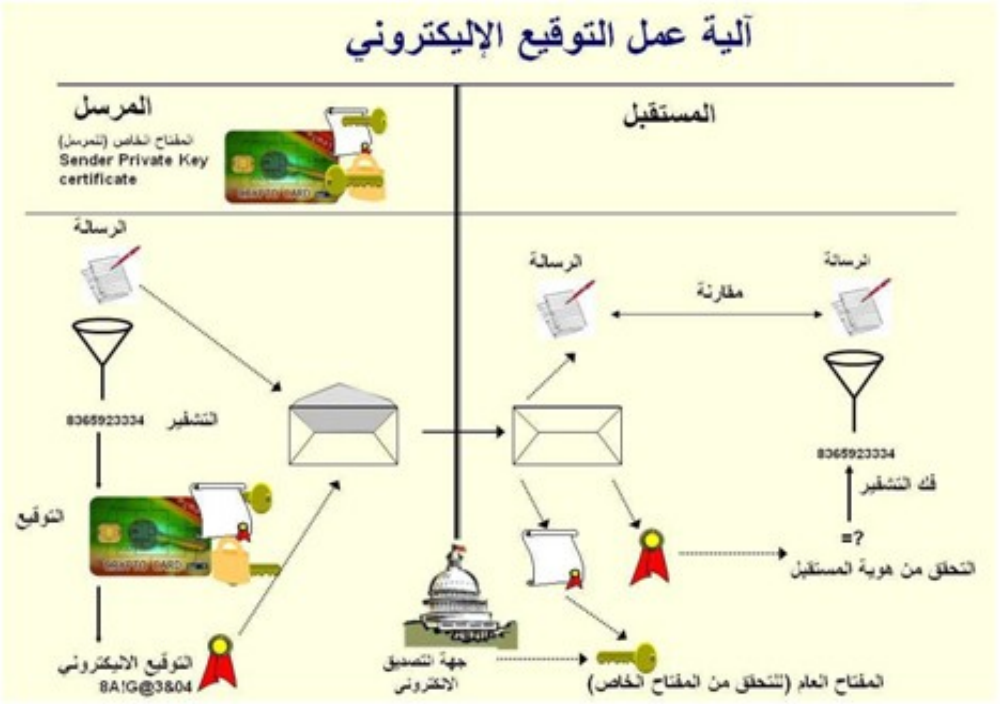
عدم قدرة المرسل من الإنكار لوجود الطرف الثالث "جهة تصديق معينه" وعدم قدرة المستقبل أيضا بالإنكار من استقبال الرسالة .كلما أراد المرسل أن يرسل رسالة لابد أن تمر على هذه الجهة المختصة، وكذالك كلما استقبل المستقبل الرسالة.

طريقة عمل التوقيع الإلكتروني :

لعمل التوقيع الإلكتروني لابد من التقدم إلى إحدى الجهات المختصة بإصدار الشهادات حتى يتم إصدار الشهادة للمستخدم، ويكون معها مفتاحين احدهما عام والأخر خاص. فعندما يرسل هذا المستخدم المالك لشهادة رسالة سوف يتم تشفيرها بالمفتاح الخاص به أو المفتاح العام التابع للمستقبل، بحيث تتحول هذه الرسالة إلى رموز لا يمكن فهمها ويتم إرفاق معها توقيع المرسل.

عندئذٍ يقوم المستقبل بإرسال نسخه من التوقيع الإلكتروني إلى الجهة المختصة بإصدار الشهادة، لتأكد من صحة التوقيع ومن ثم تقوم أجهزة الكمبيوتر التابعة للجهة المختصة بالتحقق من صحة التوقيع وتعاد النتيجة للمستقبل مرة أخرى، ليتأكد من صحة وسلامة الرسالة، فيقوم المستقبل بقراءة الرسالة وذلك باستخدام مفتاحه الخاص إذا كان التشفير قد تم على أساس رقمه العام أو بواسطة الرقم العام للمرسل إذا تم التشفير بواسطة الرقم الخاص للمرسل، ومن ثم يجيب على المرسل باستخدام نفس الطريقة وهكذا تتكرر العملية، ويستخدم أيضا مع التوقيع الإلكتروني عملية الهاش التي توفر اقل تكلفه من تشفير الرسالة بحيث تقوم بإنشاء قيمة رقمية معينة تكون اصغر من الرسالة بحيث تضمن الرسالة من أي تغيير يتم عليها بحيث عندما يستقبل المستخدم الرسالة والهاش يقوم بعملية الهاش مرة أخرى على الرسالة ومن ثم

يقارن الهاش الذي استقبله بالهاش بالذي عمله إذا كانت متساوية فيدل على سلامة البيانات من التحريف والتزوير وإذا اختلفت دل على تزويرها . كما في الشكل التالي:



أنواع التوقيع الإلكتروني:

توجد أنواع كثيرة من التوقيع الإلكتروني منها :-

1. التوقيع الرقمي أو الكودي:

هو عدة أرقام يتم تركيبها لتكون في النهاية كود يتم التوقيع به، ويستخدم هذا في المعاملات البنكية والمراسلات الإلكترونية التي تتم بين التجار أو بين الشركات وبعضها، ومثال له بطاقة الإئتمان التي تحتوي علي رقم سري لا يعرفه سوي العميل.

2. التوقيع الشخصي:

يقوم علي أساس التحقق من شخصية المتعامل بالإعتماد علي الصفات الجسمانية للأفراد مثل البصمة الشخصية، مسح العين البشرية، التعرف علي الوجه البشري،
خواص اليد البشرية، التحقق من نبرة الصوت، والتوقيع الشخصي. ويتم التأكد من شخصية المتعامل عن طريق إدخال المعلومات للحاسب الألي أو الرسائل الحديثة مثل التقاط صورة دقيقة لعين المستخدم أو صوته أو يده ويتم تخزينها بطريقة مشفرة في ذاكرة الحاسب الألي ليقوم بعد ذلك بالمطابقة، ويعتري هذا النظام العديد من المشاكل منها أن صورة التوقيع يتم وضعها علي القرص الصلب للحاسب الألي ومن ثم يمكن مهاجمتها أو نسخها بواسطة الطرق المستخدمة في القرصنة الإلكترونية.

3. التوقيع بالقلم الإلكتروني:

هنا يقوم مرسل الرسالة بكتابة توقيعه الشخصي بإستخدام قلم إلكتروني خاص علي شاشة الحاسب الألي عن طريق برنامج معين ويقوم هذا البرنامج البرنامج بالتقاط التوقيع والتحقق من صحته، ويحتاج هذا النظام الي جهاز حاسب ألي بمواصفات خاصة ويستخدم هذا التوقيع للتحقق من الشخصية. وهذا النوع أفضل من التوقيع اليدوي والذي يتم علي شاشة جهاز الحاسوب أو لوحة خاصة معدة لذلك بإستعمال قلم خاص عند ظهور المحرر الإلكتروني علي الشااشة، وهذا النوع لا يتمتع بدرجة عالية من الأمان ولا يتضمن حجية قانونية في الإثبات. الصورة التالية توضح عملية التوقيع بإستخدام القلم الالكتروني:

خوارزميات التوقيع الإلكتروني :

هنالك العديدمن خوارزميات التوقيع الإلكتروني نذكر منها ما ياتي:

خوارزمية التشفير ذات المفتاح العام PKCS (اللامتماثِل) :

هي خوارزمية جاءت حلاً لمشكلة التوزيع غير الآمن للمفاتيح في التشفير المتماثل، فعوضاً عن استخدام مفتاح واحد، يستخدِم التشفير اللامتماثِل مفتاحين اثنين تربط بينهما علاقة, ويُدعى هذان المفتاحان بالمفتاح العام (public key)، والمفتاح الخاص (private key).يتم تشفيرها بمفتاح عام ويفك التشفير بمفتاح خاص كما نلاحظ في الشكل التالي:

خوارزميات المفتاح العام.

ويكون المفتاح العام في التشفير اللامتماثل معروفاً لدى أكثر من جهة أو شخص ، لتستطيع هذه الجهة تشفير أي رسالة ولكنها لا تُفتح إلا من صاحب الصلاحية بالمفتاح الخاص والذي هو سري. وفيما يلي أشهر الخوارزميات لهذا النوع من التشفير :

خوارزمية ديفي و هيلمان (DH) :

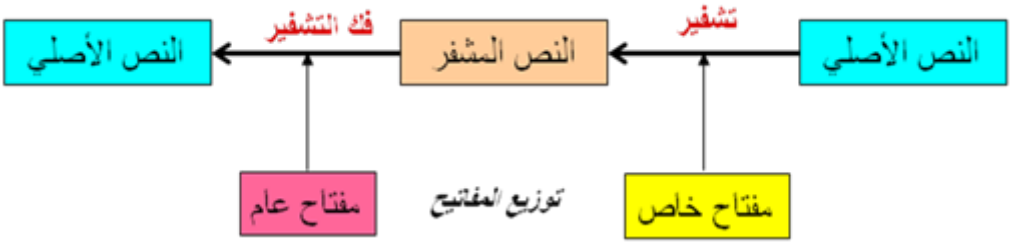
خوارزمية ديفي وهيلمان تعتبر أول خوارزمية ذات مفتاح عام وكانت 1976م وتعتمد على خاصية نظام اللوغاريتم الصحيح في تصميم نظام للتشفير. أن صعوبة كسر هذه الخوارزمية حسب ما هو معروف الآن تعادل صعوبة حل مسالة اللوغاريتم الصحيح إلا إنها خوارزمية بطيئة لأنها تعتمد على كثير من عمليات الرفع إلى قوة , لذلك ينصح باستعمالها لتشفير الرسائل القصيرة وخصوصا المفاتيح التي تستخدمها خوارزميات أخرى ويتم تبادلها بين الإطراف المتراسلة.

خوارزميات التوقيع الرقمي(DSA):

هو وسيلة التحقق من مصدر الرسالة المنقولة عبر وسائط إلكترونية كالبريد الإلكتروني . فهو عبارة عن ختم رقمي مشفر يملك مفتاحه صاحب الختم ويعني تطابق المفتاح مع التوقيع الرقمي على الرسالة الإلكترونية أن مرسل الرسالة هو من أرسلها فعلا وليس من قبل شخص آخر , ويضمن التوقيع الرقمي عدم تعرض الرسالة لأي نوع من أنواع التزوير أو التعديل بمحتواها.

لا تؤدي إضافة التوقيع الرقمي للرسالة إلى تشفير الرسالة ذاتها إذ يمكن توقيع رسالة بدون تشفيرها .

وفي التوقيع الرقمي يتم توقيع النص الأصلي بالمفتاح الخاص ويتحقق الطرف الآخر من هوية صاحب النص بمفتاحه العام كما في الشكل التالي:



طريقة عمل خوارزمية التوقيع الرقمي.

وهناك عدة خوارزمية للتوقيع الرقمي نذكر منها:-

خوارزمية التوقيع الرقمي (DSA):

خوارزمية التوقيع الرقمي صممها طاهر الجمل و **سكنور** للمعهد الوطني للمقاييس و التكنولوجيا (NIST) في الولايات المتحدة الأمريكية وقد أصدرت كمقياس للتوقيع الرقمي (DSS) وذلك عام 1994م.

وكان الإصدار الأول بمفتاح (512 بت) ونظرا لأهمية طول المفتاح في زيادة الأمان فقد اصدر منها إصدار ثاني بمفتاح (1024 بت), ونلاحظ بان احد عيوب هذا التوقيع إن أطول مفتاح له هو (1024 بت) و إذا كان المفتاح بهذا الطول فانه يجعل البعض قد يشك في إمكانية كسره.

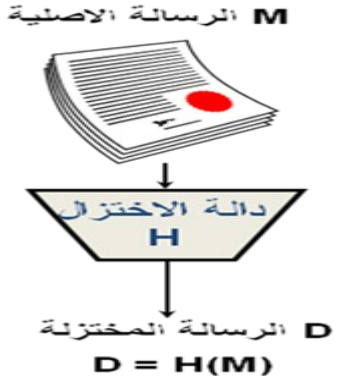
خوارزمية رشا للتوقيع الرقمي (RSA):

تعمل بعض خوارزميات المفتاح العام بشكل عكسي أي إن المفتاح العام وحده يستطيع فك مفتاح التشفير الخاص لذلك تستخدم خوارزمية رشا في التوقيع الرقمي والتي تم تحديدها من قبل ANS. وقد ورد شرح هذه الخوارزمية مسبق تحت عنوان خوارزميات التشفير بالمفتاح العام ولكن الفرق هنا إن خوارزمية رشا للتوقيع الرقمي يستخدم فيها مفتاح خاص لتوقيع النص الأصلي ويثبت الطرف الآخر التوقيع بمفتاحه العام.

دوال الإختزال:

في عملية التوقيع الرقمي كان هناك مشكلة وهي إن الرسالة الموقعة تكون بحجم الرسالة المشفرة وبذالك يصبح عندنا رسالتين رسالة مشفرة وأخرى موقعة وهذا يؤدي إلى زيادة حجم الإرسال للضعف إضافة إلى بطأ العملية.

لذلك ظهرت طريقة اختزال الرسالة إلى رسالة صغيرة كحل للمشكلة السابقة وهذه الرسالة الصغيرة المختزلة نقوم بتوقيع عليها وإرسالها مع الرسالة الأصلية المشفرة, ودوال الاختزال هي دوال اتجاه واحد تأخذ النص مهما كان طوله (آلاف بل ملايين البت) لتخرج نص بطول ثابت (مثلا 160بت أو 128بت) وإذا حصل أي تغيير في النص الداخل فان النص المختزل الخارج يتغير لذلك دوال الاختزال تستخدم أيضا لتأكيد من عدم التغيير في الرسالة المرسلة ويبين الشكل التالي عمل دوال الإختزال :



ملاحظة: الرسالة الناتجة من الإختزال تسمى الرسالة المختزلة أو بصمة الرسالة أو ما يعرف برمز توثيق الرسالة (MAC) وسنعرف فيما بعد انه من خلال الرسالة المختزلة يمكننا معرفة إذا كانت الرسالة قد تعرضت لأي تعديل أو تغيير.

خوارزمية الرسالة المختزلة (MD5):

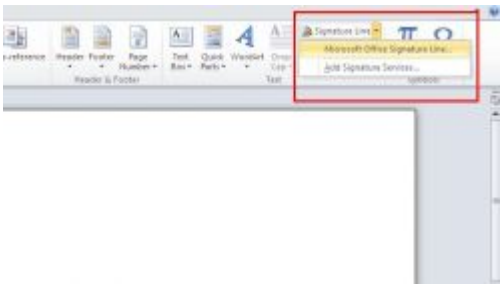
خوارزمية (MD5) والإصدارات التي سبقتها (MD2) و (MD4) طورها ريفيست لشركة (RSA Data Security) واغلب استخداماتها في التوقيع الرقمي كما إن جميع الإصدارات تنتج رسالة مختزلة بطول (128بت), أما أكثر هذه الخوارزميات أماناً فهي (MD5) وهي تستند أساساً إلى خوارزمية (MD4) مُضافاً إليها بعض خصائص الأمان الأكثر إحكاماً. ويمكن تطبيق خوارزمية (MD2) بوساطة أجهزة كمبيوتر ذات 8 بت ، بينما يلزم أجهزة كمبيوتر ذات 32 بت لتطبيق خوارزميتي (MD5) و(MD4).

تصميم التوقيع الإلكتروني:

سوف نتطرق هنا الى كيفية انشاء توقيع إلكتروني با ستخدام Microsoft Office كمثال تطبيق على انشاء توقيع إلكتروني فيما يلي الخطوت:

1) افتح ملف الكتابة Word File ثم أذهب بالمؤشر للمكان الذي تريد وضع التوقيع فيه .

2) أذهب الى Insert Tab ثم اختار Signature Lineثم اضغط السهم المشير للاسفل واختر Microsoft Office Signature line كما في الشكل:

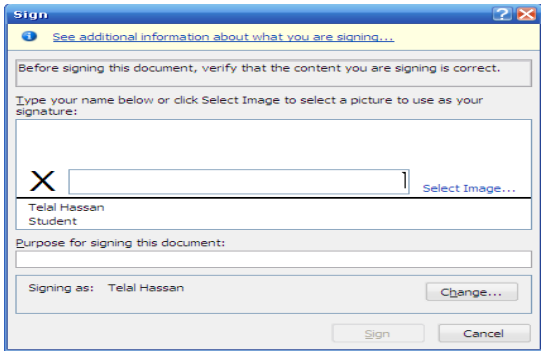


3) سوف يظهر صندوق قم بملئ بياناتك الشخصية (الإسم,العنوان,الإيميل) كما في الشكل:

4) الان قم بالضغط على Right Click في علامة التوقيع على شكل X ثم قم اختر الامر Sign...

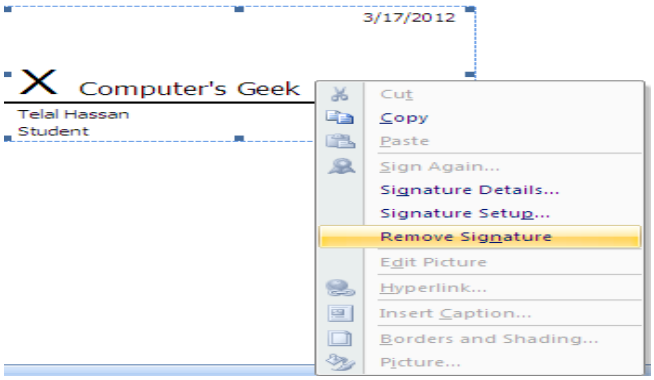
5) بعده سوف تجد خيارين كما في الشكل اختر الثاني ثم إملاء المتطلبات

6) سوف يطلب منك ان تدخل الاسم او صورة للتوقيع



7) الان تمت عملية التوقيع الإلكتروني على الملف Word File.

8) اذا اردنا إزالة التوقيع الإلكتروني نضع المؤشر التوقيع ثم نضغط Right click ثم نختار **Remove Signature ثم نحذفه**



وبذلك نكون قد ضمنا تكاملية وسلامة البيانات Data Integrity , وثوقية البيانات , اثبات البيانات بجعلها قير قابلة للإنكار Non-Repudiation .

قانونية التوقيع الإلكتروني:

اول قانون للتوقيع الإلكتروني ظهر في امريكا في العام 2000م اما في السودان فقد صدر قانون المعاملات الالكترونية لسنة

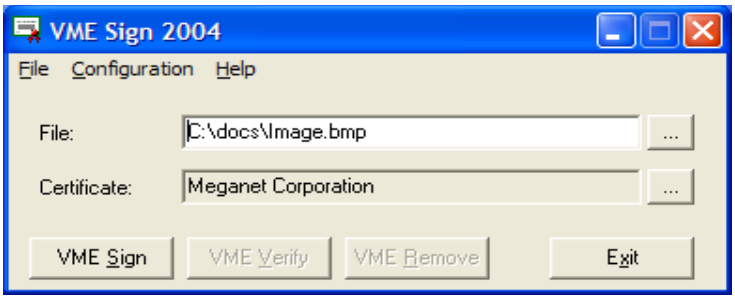
2007م من قبل اللجنة القومية للمصادقة الالكترونية والتي لها ادور الاساسي في اضفاء المصداقية على التوقيع الالكتروني في السودان وذلك بإصدار الشهادات المصادقة عنه.

ونجد ان هنالك متطلبات يجب ان يستوفيها التوقيع الإلكتروني حتي تكتمل قانونيته وتتمثل في الاتي:

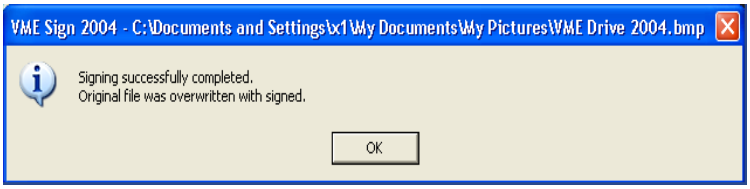
- ✓ المفتاح الخاص يجب ان يكون سراً لانه اذا تم اكتشافه سيكون من السهولة تقليد التوقيع.
- ✓ قوة الخوارزمية: حيث يجب ان تكون الخوارزمية المتبعة في التوقيع الالكتروني قوية بحيث يصبح من الصعوبة إختراقها لان هنالك بعض الخوارزميات ثبت ضعفها.

الشهادات الرقمية :

لا يمكن تطبيق التوقيع الإلكتروني نهائياً الا في حالة وجود الشهادات الرقمية CA التي تصدر عن جهات التوثيق المرخص لها من قبل الجهات المسؤلة في الدولة لتشهد بأن التوقيع الإلكتروني صحيح وينسب الا من اصدره ويستوفي الشروط وتعرف الشهادات بال (Third-Party) اي الطرف الثالث بين المرسل والمستقبل ومن امثلة هذه الجهات عالمياً هنالك شركة Magenta Corporation في الولايات المتحدة والتي تعمل في مجال حماية المعلومات حيث اصدرة اداة التوقيع الإلكتروني VME Sign والشكل التاي يوضح طريقها:



بعد عملية التوفيع تظهر الرسالة :



ومتطلبات عمل هذه الاداء هي: Windows™ 98/ME/NT/2000/XP

فوائد التوقيع الإلكتروني:

- المصداقية : بالرغم من أن الرسائل تتضمن معلومات عن كيان أو محتوى الرسالة فإن في معظم الوقت لا تكون هذه المعلومات دقيقة، وبالتالي فإنه بالتوقيع الرقمي يمكن المصادقة على مصدر هذه الرسالة. "بمعنى أن التوقيع الرقمي يثبت صحة المرسل وليس صحة البيانات الموجودة بالرسالة" أهمية هذه المصادقة تظهر جلياً في المستندات المالية، على سبيل المثال إذا قام فرع لبنك ببعث رسالة إلى الفرع الرئيسي يطلب فيها تغيير حساب معين، فإذا لم يتأكد الفرع الرئيسي أن مصدر مرسل الرسالة مصرح له بإصدار هذه المعلومات فتغيير هذا الحساب يعتبر خطأً فادحاً.
- عامل الثقة والنزاهة : يمكن لباعث أو متلقي الرسالة أن يكون بحاجة للتأكد أو الثقة بأنه لم يتم المساس بالمعلومات خلال عملية الإرسال. وبما أن عملية التشفير تخفي مضمون الرسالة فإنه لا يمكن التغيير فيها، إذا كانت الرسالة موقعة رقمياً فإن إي تغيير فيها سيشكك بمصداقية التوقيع.
- ارتباط التوقيع الرقمي بختم التاريخ والتوقيت الصحيح : إن بروتوكولات التوقيع الرقمي تعطي تأكيداً واضحاً عن التاريخ والوقت الذي تم فيهما توقيع الملف.

التوصيات :

- الاسراع في تفعيل التوقيع الإلكتروني وجعله متاح للجميع من قبل الدولة لما سيسفر عنه من تكاملية, سرية, سرعة وموثوقية .
- نشر الثقافة الإلكترونية التي يتطلبها عصر التكنولوجيا بأهمية التوقيع الالكتروني وضرورته في الحد من الجريمة الإلكترونية.
- حصول كل مواطن على توقيع إلكتروني مسجل خاص به.
- ان يكون لاي موسسة توقيعها الخاص بها .
- سن القوانين الرادعة لمرتكبي الجرائم الإلكترونية والوقاية منها باستخدام التوقيع الالكتروني .
- تغيير التوقيع الإلكتروني بعد فترة زمنية مناسبة لزيادة الأمن والحماية.

المراجع :

د.أحمد عبد القادر صالح، المصادقة الالكترونية، اللجنة القومية للمصادقة الالكترونية، الخرطوم، 2009.

بحث بعنوان التوقيع الالكتروني ، تاريخ الاسترجاع 3/16/2012 على الرابط

.http:// www.shrta.com/article39.html

بحث بعنوان التوقيع الرقمي، تاريخ الاسترجاع 3/16/2012 على الرابط

.علم التوقيع الرقمي/http://ar.wikipedia.org/wiki

خوارزميات التشفير ذات المفتاح العام وخوارزميات التوقيع الرقمي ودوال الاختزال , تم الاسترجاع في 3/16/2012 على الرابط
. http://knol.google.com/k

Federal Information Processing Standards Digital_Signature_ .Standards U.S. Department of Commerce June, 2009

http://andromida.hubpages.com/hub/how-to-create-digital-electronic-signature-certificate-file-in-pdf-microsoft-word-excel-ppt.

.VME Sign, Meganet Corporation, Los Angeles 2004

X

Alargum G
CS Student