إثبات أصالة الوثائق والشهادات باستخدام تقنيات التشفير والتوقيع الرقمي ورمز الاستجابة السريع

*د. رامز الخطيب

(الإيداع: 14 آب 2018 ، القبول: 7 كانون الثاني 2019)

الملخص:

لمجال أمن المعلومات دو هامٌ في حماية وتأمين المعلومات، ومن أهم مجالات أمن المعلومات علم التشفير الذي يحظى اليوم بمكانة مرموقة بين العلوم، إذ تنوعت تطبيقاته العملية لتشمل مجالاتٍ متعددةً وتوسع نطاق تطبيقات علم التشفير كثيراً في العصر الحديث بعد تطور الاتصالات والأنترنيت بما تتطلب من وثوقيه وحاجة إلى ضمان عدم التنصت ومنع التجسس والقرصنة الإلكترونيين وتأمين سبل التجارة الإلكترونية. وتعد تقنيات التصويت الإلكتروني والنقد الرقمي تطبيقات عملية معتمدة على علم التشفير. ومن أهم هذه التقنيات التوقيع الرقمي الذي يستخدم في توقيع معظم المستندات الإلكترونية من عقود واتفاقيات ومعاملات مع إمكانية تشفيرها. حيث يستخدم للتحقق من موثوقية صاحب المعلومة بالإضافة الى صحة المعلومة نفسها،

تتناول هذه الدارسة اقتراح طريقة لحل مشكلة تزوير الشهادات الجامعية وذلك باستخدام تقنية التوقيع الرقمي على الشهادة اعتمادا على خوارزمية التوقيع الرقمي DSA إحدى أهم خوارزميات التشفير الغير متماثِل. الفكرة الأساسية تقوم على إعطاء الموقع على الشهادة مفتاحين اثنين تربط بينهما علاقة، ويُدعى هذان المفتاحان بالمفتاح العام (public key)، والمفتاح الخاص (private key). يستخدم المفتاح الخاص لتوقيع الشهادة والمفتاح العام يستخدم من قبل اي شخص للتحقق من صحة التوقيع بالإضافة لذلك تم الاستفادة من تقنية رموز الاستجابة السريعة(QR) لحفظ المحتويات النصية المشفرة لبيانات الوثيقة مهما كان حجمها بطريقة مختصرة ومناسبة للطباعة والقراءة. هذه الطريقة المقترحة ستكون حلا عمليا في تأمين الوثائق الرسمية الورقية وحمايتها من التزوير وبذلك زيادة ثقة المؤسسات المحلية والعالمية بالوثائق الرسمية الموقعة رقميا.

*عضو هيئة تدريسية في قسم تقنيات الحاسوب، الكلية التطبيقية، جامعة حماة.

Degree Certificate Authentication using Cryptography, Digital Signature and QR Code Techniques

*Dr. Ramez ALKHATIB

(Received:14 August 2018, Accepted:7 January 2019)

Abstract:

The field of information security plays an important role in the protection and security of information. One of the most important areas of information security is cryptography, which occupies today a prominent place among the sciences. Its practical applications have varied to many fields. The scope of applications of cryptography has expanded greatly in modern times after the development of communications and the Internet. And the need to ensure that prevention of eavesdropping and Spyware, electronic piracy and securing e-commerce. Electronic voting techniques and digital criticism are practical cryptographic applications. The most important of these technologies is the digital signature, which is used to sign most electronic documents from contracts, agreements and transactions with the possibility of encryption. Where it is used to verify the reliability of the owner of the information in addition to the authenticity of the information itself.

This study propose a method to solve the problem of forging certificates using digital signature technology on the certificate based on the DSA algorithm one of the most important asymmetric encryption algorithms. The basic idea is to give the certificate site two related keys, called the public key, and the private key. Where the private key is used to sign the certificate and the public key is used by any person to verify the validity of the signature. In addition, the QR code was used to save the textual contents of the document, whatever its size, in a concise manner suitable for printing and reading. This proposed method will be a practical solution in securing official paper documents and protecting them from forgery, thereby increasing the confidence of local and international institutions in the official documents signed digitally.

*Dept. of Computer Techniques, Applied Faculty, University of Hama

1- مقدمة:

يتميز عصرنا الراهن بالسيل العظيم والانتشار الواسع للبيانات والمعلومات لذلك عملية التأكد من مصدر المعلومات وحمايتها من التزوير أضحى ضرورة ملحة ويعتبر التوقيع الرقمي ألية أساسية لحماية المعلومات وذلك بالتأكد من هوية مصدر المعلومات حيث انه يعتبر من أهم الطرق المستخدمة لضمان الوثائق وأصبح يوفر الضمانات الموجودة في التوقيع اليدوي بل تفوقها. كما أن التوقيع التقليدي عبارة عن علامة شخصية يقوم بها الشخص يمكن من خلالها تمييز هوية الموقِّع. وللتوقيع التقليدي مساوئ كثيرة أهمها قابليته للتقليد بدقة عالية نتيجة لذلك تزوير الشهادات والوثائق الرسمية هي مشكلة حقيقية تعاني منها جميع المؤسسات خاصة التعليمية منها مثل الجامعات والمعاهد.

من ناحية نجد أن التوقيع الرقمي المتعارف عليه يستخدم في المعاملات الالكترونية أما في ضوء الواقع الحالي في مجتمعنا فإن معظم المعاملات والوثائق المتعامل بها تعتمد على المعاملات الورقية وأيضا جميع التشريعات القانونية إلى الآن تدعم المعاملات الورقية الروتينية التي تعتمد على التوقيع الحي التقليدي لذلك كان لابد من مواكبة التطورات التكنولوجية في التواقيع الرقمية التي اثبتت درجة عالية من الأمان ولكن بقيت موقع شك كبير في مجتمعاتنا، مما تسبب عدم العمل بها ومن هذا المنطلق اقترحنا في هذه الورقة البحثية استخدام تقنية التوقيع الرقمي على الشهادات الورقية والتحقق من مصدرها الكترونيا وذلك للاستفادة ولاكتساب الموثوقية العالية والأمان الموجودة في تقنيات التشفير والتوقيع الرقمي التي توفر الضمان وتؤكد بأنه لم يتم أجراء أي تعديل على الوثائق الموقعة وذلك بسبب صعوبة تزويرها والعبث بها والاستفادة من ثقة المتعاملين بالمعاملات التقليدية التي تعتمد على التوقيع اليدوي وأيضا تم الاستفادة من تقنيات الرموز الضوئية لتصغير حجم وطول التوقيع المقترح.

مشكلة البحث:

إن ظاهرة التزوير هي قديمة بل ومتعددة لا تنحصر في تزوير الشهادات العلمية فقط ولكن ازدادت في الآونة الأخيرة عمليات تزوير الشهادات الجامعية، حيث تعد هذه القضية من أخطر القضايا التي بات يعاني منها سلك التعليم والعلم، خاصة أن تزوير الشهادات امتد إلى المهن الطبية التي لا يصح ولا يجوز مزاولتها بشهادة مزورة لما في الأمر من خطورة على أرواح الناس. وساعد في ذلك وجود أشخاص محترفون في التزوير وهنالك عوامل ساعدت في انتشار التزوير مثل أجهزة الحواسيب والطابعات فائقة الدقة لذلك من الطبيعي أن تطلب الدول معايير جديدة للشهادة الجامعية كإجراء احترازي لحماية الشهادات الجامعة من التزوير [R. L. Renesse ,1997]. يتم ذلك من خلال بناء نظام أمن الشهادات الجامعية يسمح فقط للأشخاص المخولين بالوصول الى البيانات مع إمكانية التحقق من هويتهم وسلامة البيانات عن طريق استخدام مفهوم التوقيع الرقمي والبصمة الرقمية لضمان تأمين بيانات الشهادات بوثوقيه وسلامة عالية لمنع أي شخص غير شرعي من تعديل أي إجراء عليها.

2- الهدف من البحث

يهدف هذا البحث إلى:

- اقتراح طريقة فعالة لبناء نظام أمن الشهادات الجامعية وذلك باستخدام وتطبيق الطرق والاساليب العلمية الحديثة في علم التشفير وتطبيقاته.
- مواكبة التطور التقني بوساطة استخدام تقنيات رموز الاستجابة السريعة
- اعتمادية نظام الشهادات الالكترونية لتحسين إدارة نظام الشهادات التقليدية بشكل آمن
- إمكانية التأكد من صحة الشهادات بالإضافة الى اتخاذ إجراءات دقيقة لمتابعة ومراقبة واكتشاف عملية التزوير في الشهادات الجامعية.
- تسجيل بيانات الشهادات الجامعية بصورة رقمية وحمايتها من وصول غير مخول به

- زيادة ثقة مؤسسات العمل بشهادات الجامعة

3- مواد وطرق البحث:

أجريت هذه الدراسة بإتباع منهج علمي ووصفي تحليلي، تناول البحث العديد من المراجع والبحوث التي تضمنت مفاهيم تحليل وتصميم الانظمة المعلوماتية ومفاهيم أمن المعلومات والحماية والتشفير وتم استخدم عدة طرائق مرجعية منها الكتب والمراجع والاوراق العلمية وتحليل الوثائق والمقابلات الشخصية الملائمة للدراسة ومن الجانب التطبيقي تم استخدام لغات برمجية متطورة مثل الجافا وبيئات عمل متكاملة مثل بيئة Eclipse لتصميم وبرمجة وتنفيذ النظام الالكتروني.

a. علم التشفير:

يحظى هذا العلم اليوم بمكانة مرموقة بين العلوم ويعد علم التعمية أو علم التشفير أحد أهم الوسائل المستخدمة لتوفير بيئة آمنة لتبادل المعلومات وحمايتها وهو فرع من الرياضيات ولقد تنوعت تطبيقاته العملية لتشمل مجالات متعددة. التشفير هو ممارسة إخفاء البيانات أو هو عملية تغيير البيانات من شكلها الطبيعي المفهوم لأي شخص الى رموز وارقام يصعب فهمها على من لا يملك معرفة سرية محددة. استخدم الناس التشفير عبر التاريخ لتبادل رسائل ومعلومات لا يمكن قراءتها من قبل أي كان ما عدا الشخص المقصود لتلقي الرسالة وذلك لضمان الخصوصية وأن المعلومات يجب أن تصل إلى الشخص المقصود والمعني بالأمر. استعمل التشفير منذ القدم خاصة في المراسلات الحربية وكذلك في الدبلوماسية والتجسس. وقد ذكر أن أول من قام بعملية التشفير للتراسل بين قطاعات الجيش هم الفراعنة منذ عام 2000 قبل الميلاد، وكان القصد هو إخفاء الشكل الحقيقي للرسائل حتى لو سقطت في يد العدو. من أمثلة استخدام التشفير قديما هو استعمال يوليوس قيصر خوارزمية ROT13 لتشفير الرسائل المكتوبة باللاتينية التي يتبادلها مع قواده العسكريين، وهو أسلوب تشفير يُستبدل فيه كل حرف بالحرف الذي يليه بثلاثة عشر موقعا في ترتيب الأبجدية اللاتينية، مع افتراض أن آخر حرف في الأبجدية يسبق الأول في حلقة متصلة. ومن الأمثلة على استخدام التشفير في العصر الحديث استخدام الجيش الألماني في الحرب العالمية الثانية لآلة إنجما لتحقيق تفوق على العدو في مجال الاتصالات، وفي سبعينيات القرن العشرين قامت المؤسستين العسكريتين الأمريكية والبريطانية بأبحاث جرت بشكل منفصل في كل منهما لتفتح عصر جديدا في علم التشفير بإنتاج تقنيات التشفير القوية المعتمدة على الحوسبة، وارتبط التشفير بنظرية المعلومات ونظرية الأعداد ونظرية التعقيد وعلوم الجبر.

أما في عصرنا الحالي فقد باتت الحاجة ملحة لاستخدام هذه العلم " التشفير " وذلك لارتباط العالم مع بعضه عبر شبكات مفتوحة، حيث يتم استخدام هذه الشبكات في نقل المعلومات إلكترونياً سواءً بين الأشخاص العاديين أو بين المنظمات الخاصة والعامة عسكرية كانت أم مدنية، وعليه لا بد من طريقة تحفظ سرية هذه المعلومات ولا يزال العمل والبحث في مجال علم التشفير مستمراً وذلك بسبب التطور السريع للكومبيوتر والنمو الكبير للشبكات وبخاصة الشبكة العالمية الإنترنت.

تتم عملية التشفير باستخدام خوارزميات رياضية عديدة ومتنوعة، ولكن معظم هذه الخوارزميات بنيت على مبدأين رئيسين هما:

- مبدأ الاستبدال: استبدال حرف من أبجدية النص المقروء بحرف أو أكثر من أبجدية النص المشفر حسب قاعدة استبدال محددة تعرف بمفتاح التشفير.
- مبدأ الإبدال:

تغيير مواقع أو حروف النص المقروء حسب قاعدة استبدال محددة تعرف بمفتاح التشفير

يعتبر نظام قيصر للتشفير الذي ذكرناه سابقا مبني على مبدأ الاستبدال ولكن نلاحظ أن هذا النظام يمكن كسره بسهولة بدون معرفة المفتاح وذلك عن طريق حساب تواتر الحروف في لغة النص الواضح، ثم حساب تواتر الحروف في النص المشفر، وبعد ذلك يمكن أن نخمن أكثر الحروف تواترا في النص الأصلي يقابله أكثرها تواترا في النص المشفر. كمثال

على مبدأ الإبدال نذكر نظام التشفير أحادي الأبجدية حيث يتم فيه تغيير مواقع الحروف في النص الأص1لي ويتم هذا التغيير حسب قاعدة معينة يعبر عنها المفتاح [Christof Paar, 2010].

تطورت أساليب خوارزميات التشفير وأصبحت تعتمد على اسلوبين هما:

- **التشفير المتناظر symmetric cryptography**

هو أسلوب من أساليب التشفير ويعرف أيضا بتشفير المفتاح الخاص حيث يستخدم فيه مفتاح سري واحد لتشفير رسالة ما وفك تشفيرها، ويسمى بالتشفير بالمفتاح المتناظر لأن المفتاح الذي يستخدم لتشفير الرسالة هو نفسه المستخدم لفك تشفيرها وذلك باستخدام خوارزمية خاصة كما في الشكل. ويعتمد هذا النوع بالأخص على سرية المفتاح المستخدَم، حيث أن الشخص الذي يملك المفتاح بإمكانه فك التشفير وقراءة المحتوى الأصلي للنص. لهذا توجب على مرسل الرسالة إيجاد طريقة أمنة لإيصال المفتاح إلى المتلقي. ومن عيوب هذه الطريقة أنه لا يمكن التأكد بان الرسالة المستقبلة فعلا تم ارسالها من قبل المرسل المفترض وليس من قبل شخص آخر تنكر بشخصية المرسل بهذا يمكن للمرسل أيضا أن ينكر أرساله للرسالة. ومن العيوب الأخرى لا يمكن استخدامها بين مجموعة كبيرة وإنما فقط بين طرفين لصعوبة توزيع مفتاح التشفير. ودائما يجب تجديد المفتاح بشكل دوري. من أشهر الخوارزميات هذا الأسلوب (DES-3DES-IDEA-AES)

- **التشفير الغير المتناظر asymmetric cryptography**

يعرف أيضا بتشفير المفتاح العام Public Key Encryption يعتمد هذا النوع على وجود مفتاحين أحدهما لتشفير الرسالة والآخر لفك التشفير يعرف الأول بالمفتاح العام (Public key) سمي بذلك لأنه يكون معروف للمستخدمين في البيئة المعينة ويستخدم لتشفير الرسائل أما الثاني فيعرف بالمفتاح الخاص (Private key) سمي بذلك لأنه معروف لمستخدم واحد فقط هو مالكه ويستخدم لفك الرسائل المشفرة بالمفتاح العام المقابل له. يعاب على هذه الطريقة كثرة المفاتيح المستخدمة في التشفير وفك التشفير. ولكن من فوائدها عند إضاقة مستخدم جديد للنظام لا نحتاج الا الى توليد زوج من المفاتيح ويمكن حذف أي مستخدم ببساطة دون أن يؤثر على بقية النظام وأيضا لا نحتاج الى توليد مفتاح الا في حالة كشف المفتاح الخاص لاحد المستخدمين. وعلى عكس طريقة التشفير المتناظر يمكن التأكد بان الرسالة المستقبلة فعلا تم ارسالها من قبل المرسل المفترض وليس من قبل شخص آخر تنكر بشخصية المرسل بهذا يمكن للمرسل ألا يمكن أن ينكر أرساله للرسالة. وأخيرا عملية توزيع المفاتيح سهلة من أشهر الخوارزميات هذا الأسلوب (ElGamal-RSA- DSS)

b. دوال الاختزال Hash Functions

إحدى أولويات طرق التشفير الحديث هو استخدام دالة الاختزال التشفيرية التيً تسمى عادة الدالة الهاشية ذات الاتجاه الواحد (One-way Hash Function) [M. Singh and D. Garg, 2009] عند استخدم دالة الاختزال في التشفير يكون لها الخواص التالية

- الدخل يمكن أن يكون بأي طول
- الخرج يكون طوله ثابت
- H(x) تكون سهله الحساب نسبيا لأي قيمة لـ x.
- دالة الاختزال هي دالة ذات اتجاه واحد
- تكون خالية من التصادم (collision free)

القيمة الدالة تمثل اختصاراً للعبارات الطويلة او الوثائق [John Edward S., 2013] التي قد تم حسابها منها لذا أحيانا يطلق عليها مختصر العبارة (message digest)

1. طرق تصميم تابع الاختزال

لتصميم تابع الاختزال مقاوم للتصادم يوجد طريقتين لتحقيق ذلك :

- الطريقة الأولى: تصميم تابع اختزال من الصفر مثل التابعين Message Digest (MD) و Secure Hash Algorithm (SHA)
- التابع :Message Digest (MD) جرى تصميم هذا التابع من قبل Ron Rivest ويرمز له وفقا لأحد المسميات التالية: MD2 MD4 MD5 :تتميز النسخة الأخيرة MD5 في كونها أقوى من سابقاتها، فهي تقوم بتقسيم الرسالة إلى كتل بحجم مساوي ل 512 بت وتنشئ بصمة بحجم 128 بت. يعتبر حجم البصمة هذا صغير جدا ليقاوم التصادم
- التابع(Secure Hash Algorithm (SHA :

وهو تابع معياري مصمم من قبل المعهد NIST يعتمد هذا المعيار على MD5 جرى تطويره عام 1995 تحت المسمى SHA-1 تمت مراجعته عدة مرات وأنتج ذلك النسخ التالية: $SHA-224; SHA-256; SHA-512: 384$ تتمتع كافة هذه النسخ بنفس البنية .

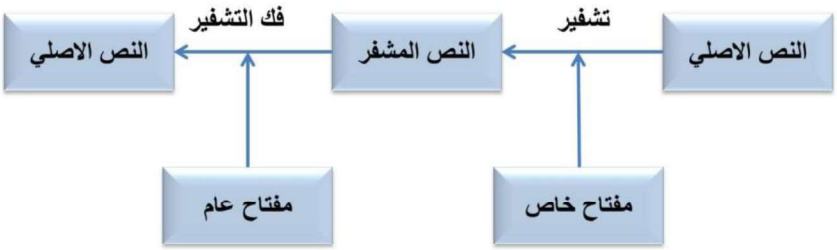
- الطريقة الثانية: استخدام طرائق تشفير كتلية

يمكن استخدام مشفر كتلي بمفتاح متناظر كتابع ضغط تم التفكير بذلك لأنه يتوفر لدينا العديد من خوارزميات التشفير الكتلي بمفتاح متناظر مثل (DES , AES) ولا داع للتفكير في بناء تابع ضغط جديد.

c. التوقيع الرقمي

التوقِيع عموماً هو علامة شخصية يمكن من خلالها تمييز هوية الموقّع 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 الرقمي فهو عبارة عن عملية تشفير مكون من بعض الحروف والرموز والأرقام الإلكترونية [POINTCHEVAL, D, 2000] ، 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 لعدة أغراض منها أغراض شخصية او سياسية 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 الرقمي هو أن التوقيع العادي عبارة عن رسم يقوم به الشخص بمعني انه فن وليس علم ومن هنا يسهل تزويره، أما التوقيع الرقمي فهو علم وليس فن ويصعب تزويره. نستخدم العديد من خوارزميات التوقيع الرقمي التي تعتبر وسيلة للتحقق من مصدر الرسالة المنقولة عبر وسائط إلكترونية كالبريد الإلكتروني فهو عبارة عن ختم رقمي مشفر يملك مفتاحه صاحب الختم [SCHNORR, C., 1995] 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 وفي التوقيع الرقمي يتم توقيع النص الأصلي بالمفتاح الخاص [ANSI X9, 1997] ويتحقق الطرف الآخر من هوية صاحب النص بمفتاحه العام كما في الشكل التالي:



الشكل رقم (1): الية عمل التوقيع الرقمي

1. قانونية التوقيع الرقمي:

كانت بداية الاعتراف بالتوقيع الرقمي في عام 1989 في مجال البطاقات الائتمانية في محكمة النقض الفرنسية وأكدت المحكمة أن هذه الوسيلة تفوق الضمانات الموجودة في التوقيع اليدوي. وبعد ذلك في عام 1999 صدرت ارشادات وشروط التوقيع الرقمي من قبل الاتحاد الأوربي وأهم هذه الشروط هي:

- ارتباط التوقيع الرقمي بالموقع فقط
- قدرة التوقيع الرقمي على تحديد شخصية الموقع
- أن ينشئ التوقيع الرقمي بوسائل تتم تحت سيطرة ورقابة الموقع
- يحتوي التوقيع الرقمي على معلومات يوثقها الموقع ولا يمكن للغير التعديل عليها أو التلاعب بها

ولتحقيق وضمان هذه الشروط كان لابد من وضع خصائص محددة يحققها التوقيع الرقمي والتي تتخلص بالآتي:

- **الخصوصية:** بحيث يمنع أي مستخدم غير مخوّل 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 باستخدام تقنية تشفير البيانات ومقارنة بصمة الرسالة المرسلة مع بصمة الرسالة المستقبلة.
- **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، وكذلك كلما استقبل المستقبل الرسالة.

d. الترميز الشريطي (Barcode)

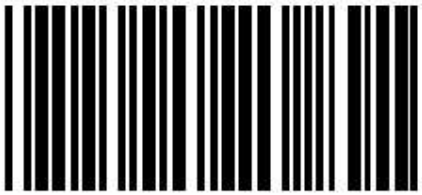
إن المعرف المؤتمت ومجمع البيانات (AIDC)، والمعروف أيضًا باسم معرف تلقائي أو إدخال البيانات بدون مفتاح ، هو المصطلح العام لعدد من التقنيات التي تساعد في القضاء على الأخطاء البشرية وتقليل الوقت والعمل عن طريق استبدال الأساليب اليدوية لإدخال البيانات وجمعها. يعد الترميز الشريطي (Barcode) واحدًا من العديد من تقنيات AIDC التي تتضمن أيضًا الشرائط المغناطيسية والبطاقات الذكية ومعرف ترددات الراديو (RFID) والشبكات المحلية اللاسلكية (WLAN). يعد الترميز الشريطي مدخل بيانات سريع وسهل ودقيق فبمجرد جمع البيانات المرمزة عن طريق ماسحة الرمز الشريطي ، يمكن تتبع النشاط بكفاءة ودقة وبسرعة تفوق استخدام أنظمة إدخال البيانات والقراءة اليدوية.

ظهرت الرموز الشريطية ، مثل رمز شفرة المنتج العالمي المعروف (UPC) المستخدم على السلع المعبأة ، لأول مرة في المتاجر في أوائل السبعينيات. وبفضل التقنيات الجديدة مثل الطباعة المحمولة واللاسلكية، تطور الترميز الشريطي إلى أداة لتحسين الإنتاجية على نطاق واسع من قبل قطاع الأعمال والصناعة لجمع ومعالجة المعلومات. فعلى سبيل المثال ، تقدم شركة Zebra Technologies ترميزًا بارزًا لمجموعة متنوعة من الشركات في التصنيع والتوزيع والتنفيذ ، والضيافة ، والتعليم ، والسفر ، وتجارة التجزئة ، والأمن ، والرعاية الصحية.

تظهر أهمية استخدام الرموز الشريطية في سرعتها ودقتها مقارنة بالطرق التقليدية حيث تشير الدراسات إلى أن معدلات دخول وقراءة الخطأ عند استخدام تقنية الرمز الشريطي هي خطأ واحد تقريبًا لكل مليون حرف ، مقابل خطأ واحد لكل 300 حرف باستخدام إدخال مفتاح يدوي. بالإضافة إلى أن الرموز الشريطية تسمح للشركات بتتبع المعلومات والنشاط عند حدوثه ، مما يؤدي إلى اتخاذ قرارات مستندة على معلومات محددة وحديثة ودقيقة.

الرموز الشريطية ترمز البيانات (مثل رقم المنتج أو الرقم التسلسلي أو رقم المورّد أو الكمية أو رقم المناقلة الخ...) على شكل خطوط سوداء وبيضاء أو "أشرطة". وقد تم تطوير عدد من المعايير لهذه الرموز على مر السنين لتصبح لغات مقبولة تسمى

"symbologies". وهذه الرموز يمكن أن تكون رموز شريطية خطية أو ثنائية الأبعاد. يتكون الترميز الشريطي الخطي من صف واحد من الخطوط المظلمة والمساحات البيضاء ذات العرض والارتفاع المتفاوتين، كما هو موضح في المثال أدناه.



Linear bar code

أما الترميز الشريطي ثنائي الأبعاد عبارة عن مكدس معلومات يسمح بتخزين المزيد من المعلومات. ويتم تكوينه إما كرموز شريطية خطية مكدسة أو على شكل مصفوفة تستخدم خلايا سوداء أو بيضاء بشكل منتظم لترميز البيانات. فيمكن لترميز مصفوفي بقياس بوصة واحدة أن يخزن دستور الولايات المتحدة كاملا

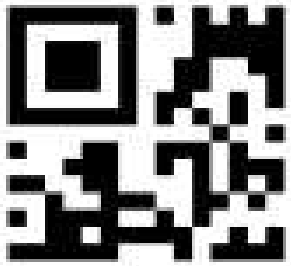
2-D symbology

1. رموز الاستجابة السريعة QR Code

هي نوع من أنواع الترميز المصفوفي له بعدين صمم في عام 1994 كتحسين للترميز مقارنة بسابقيه في البداية صمم لصناعة السيارات في اليابان ولاحقا أصبح شائع خارج عالم السيارات بسبب سهولة قراءته وقدرته التخزينية الكبيرة مقارنة بالرموز القياسية. أصغر رموز QR لها الحجم 21*21 والتي تدعى النسخة الأولى وأكبر نسخة تمتلك الحجم 177*177 وتدعى النسخة أربعون وترميز QR تتضمن بعض معلومات تصحيح الأخطاء وهذه المعلومات الإضافية تساعد قارئ الرموز في دقة القراءة وتمكننا من قراءة الترميز حتى إذا كان جزء منها غير قابل للقراءة. هناك أربع مستويات من تصحيح الأخطاء L,M,Q,H أخفضها مستوى هو L الذي يسمح بقراءة الكود بنسبة تصحيح أخطاء 7% المستوى الثاني M الذي يزود بنسبة تصحيح أخطاء 50% والمستوى الثالث Q المزود بنسبة تصحيح أخطاء 25% والمستوى الرابع H المزود بنسبة تصحيح أخطاء 30%.

a. أنواع رمز الاستجابة السريع QR

- **Micro QR code:** وهو أصغر نسخة من رموز QR حجمه محدود ويوجد أربع أحجام منه أصغرهم 11*11 وأكبرهم يحتوي على 35 رقم محرفي



الشكل رقم (2): micro qr code

- **IQR code:** نوع آخر من رموز QR طور بواسطة Denso wave ويمكن أن يكون بشكل مربع أو مستطيل حيث أنه يمكن أن يلائم نفس كمية المعلومات لكن بحجم أقل 30% هناك 61 نسخة من رموز QR على شكل مربع و15 نسخة من الترميز على شكل مستطيل بالنسبة للشكل المربع أصغره يكون بحجم 9*9 والمستطيل أصغره بحجم 9*15 ويحتوي على المستوى S من مصحح الأخطاء الذي يملك تصحيح أخطاء بنسبة 50%

الشكل رقم (2): IQR

- **SQRC:** هو نوع من أنواع رموز QR الذي يستخدم لتخزين المعلومات الخاصة وإدارة المعلومات الداخلية للشركة[K. M. Revathi, 2013]

الشكل رقم (3): SQRC

4- الطريقة المقترحة:

تم الاستفادة من تقنية التوقيع الرقمي من حيث الحماية والتشفير وطبقنا هذه التقنيات على التوقيع التقليدي لينتج معنا توقيع يتمتع بموثوقية وأمان عاليين وبنفس الوقت اكتساب ثقة المتعاملين بالمعاملات التقليدية التي تعتمد على التوقيع اليدوي وأيضا تم الاستفادة من تقنيات الرموز الضوئية لتصغير حجم وطول التوقيع المقترح.

a. إجراء التوقيع والتحقق منه

تتم خطوات توليد التوقيع المقترح وفق الخطوات الآتية:

- **الخطوة الأولى:** البيانات المدخلة هي بيانات الوثيقة (اسم المتعامل، عنوانه، مواليده، ....)
- **الخطوة الثانية:** ينم تشفير هذه البيانات بواسطة خوارزميات التشفير الغير متناظر باستخدام المفتاح الخاص حيث سيتم استخدام أحد أشهر هذا النوع من الخوارزميات وهي DSA
- **الخطوة الثالثة:** استخدام تقنية التقطيع (خوارزميات الاختزال) التي سينتج عنها شيفرة التوقيع الرقمي

- **الخطوة الرابعة:** نقوم بتحويل شيفرة التوقيع الى رمز QR وذلك للتقليل من حجمه وجعله بحجم ثابت قابل للطباعة على الوثيقة الورقية وقابل للقراءة بواسطة أداة قارئ الرموز أو الكاميرات الرقمية مما يتيح سهولة استخدامه وقراءته والتأكد منه لاحقا

1. خوارزمية التوقيع الرقمي المستخدمة

خوارزمية التوقيع الرقمي صممها طاهر الجمل للمعهد الوطني للمقاييس والتكنولوجيا (NIST) في الولايات المتحدة الأمريكية وقد صدرت كمقياس للتوقيع الرقمي (DSS) وذلك عام 1994 DSA [$FIPS, 2000$].تعرف كتقنية لتوليد والتحقق من التوقيع الإلكتروني وهذه التقنية طرحت لتزويدنا بتكاملية البيانات وعدم الإنكار بمحتويات ومنشأ الرسالة الالكترونية. وكان الإصدار الأول بمفتاح (512 بت) ونظرا لأهمية طول المفتاح في زيادة الأمان فقد أصدر منها إصدار ثاني بمفتاح (1024 بت)، ونلاحظ بان أحد عيوب هذا التوقيع إن أطول مفتاح له هو (1024 بت) وإذا كان المفتاح بهذا الطول فانه يجعل البعض قد يشك في إمكانية كسره. إنها نوع فعال من خوارزمية الجمل حيث أن خوارزمية الجمل كان لها عدة مساوئ والتي قامت خوارزمية DSA بحلها. الخطوات التي تم اتباعها لخوارزمية DSA

- الخطوة الأولى: توليد المفاتيح
- الخطوة الثانية: توليد التوقيع
- الخطوة الثالثة: التحقق من صحة التوقيع.

تستخدم هذه الخوارزمية العديد من التقنيات حيث تستخدم مفتاح عام ومفتاح خاص وتستخدم الأعداد الأولية وتستخدم أعداد عشوائية وسيتم شرح كل منها بالتفصيل

a. توليد المفتاح

المفتاح العام للتوقيع (p; q; g; A) ولتوليد هذا المفتاح نقوم بالخطوات الآتية:

- العدد الأولي q يتم اختياره ضمن المجال $2^{159} < q < 2^{160}$ وحيث أن طول بتات q عند التخزين هو 160
- العدد الأولي p يتم اختياره ضمن المجال $2^{511+64j} < p < 2^{512+64j}$ حيث إن: $j \in \{0,1,2,\dots,8\}$
  العدد الأولي q يقسم على p−1 وطول بتات p يكون بين 512 و1024 ومن مضاعفات 64
- يتم حساب g من القانون: $g = x^{(p-1)/q} \bmod p$ حيث $x \in \{1,2,\dots,p-1\}$
- يتم حساب A من القانون $A = g^a \bmod p$ وهو رقم عشوائي $A \in \{1,2,\dots,P-1\}$

b. توليد التوقيع

التوقيع عبارة عن الثنائية (r,s) على المستند x حيث الموقع سيوقع على المستند x ويستخدم تابع التقطيع SHA−1: $SHA-1: \{0,1\}^* \to \{0,1\}^{160}$ ومنه يتم حساب r حسب القانون $r = g^{k \bmod p} \bmod q$ وأيضا يحسب $s = k^{-1}(SHA-1(x) + ar) \bmod q$ حيث k−1 هي عكس k mod q

c. التحقق من التوقيع:

عند قيام الشخص بالتحقق من التوقيع فعليا هو سيتحقق من أن (r,s) هو للمستند x وسيتم التحقق بواسطة المفتاح العام (p; q; g; A) حيث سيتحقق من الشرط $1 \le s \le q-1$ وأيضا الشرط $1 \le r \le q-1$ وإذا لم يتحقق هذا الشرط فالتوقيع غير صحيح أما في حال تحقق يتابع بالتالي:

$$r = ((g^{(s^{-1}h(x)) \bmod q} A^{(rs^{-1}) \bmod q}) \bmod p) \bmod q.$$

وإذا تحقق فالتوقيع صحيح

d. اختيار العدد الأولي q:

يتم اختيار العدد الأولي q كالتالي:

1) نختار رقم بدائي Seed

$$\text{Seed} \in \{0,1\}^*,\ g = |\text{Seed}| \geq 160.$$

2) نحسب $U = \text{SHA-1}(Seed \oplus \text{SHA-1}(\text{Seed} + 1) \bmod 2^g$

3) q يؤخذ من المجموعة التي تحقق أقل ومعظم البتات الموجودة من u إلى 1 وبالتالي $2^{159} < q < 2^{160}$ سنحصل على مجموعة من الأرقام وسنأخذ الرقم المحقق لأقل ومعظم البتات الموجودة بين u إلى 1

4) ثم نستخدم العدد الاحتمالي الأولي بحيث احتمال الخطأ فيه على الأكثر 2^{-80} أي صغير جدا ويحسب حسب قانون Miller

5) إذا كان q ليس أولي نعود للخطوة الأولى وغير ذلك ينتج معنا q

e. اختيار العدد الأولي p:

يتم اختيار العدد الأولي p كالتالي:

1) نختار عدد j $j \in \{0,1,\dots,8\}$ و $2^{b-1} < q < 2^b$ و

$L = 512 + 64j$

2) نقسم L−1 مع الباقي على 160 $0 < b < 160$ و

$$L - 1 = 160n + b$$

3) نضع عداد = 0 والإزاحة Offset = 2

4) من أجل k =0,1,…,n $V_k = \text{SHA-1}\big((\text{Seed} + \text{offset} + k) \bmod 2^g\big)$

5) نضع $W = V_0 + V_1 * 2^{160} + \dots + V_{n-1} * 2^{160(n-1)} + (V_n \mod 2^b) * 2^{160n}$

و $X = W + 2^{L-1}$ عندئذ $0 < W < 2^{L-1}$ و $2^{L-1} < X < 2^L$

6) نضع $C = X \bmod 2q$ و $p \equiv 1 \bmod 2q$ ثم $C = X - (c-1)$ ونقسم 2q على p−1

7) إذا $p < 2^{l-1}$

8) نحسب الاحتمال الأولي للخطأ الذي سيختبر Pأولي أم لا حسب قانون Miller

9) عند نجاح الاختبار يتم زيادة العداد بمقدار 1 والإزاحة n+1

10) إذا كان العداد $\text{counter} > 2^{12} = 4096$ فولد رقم أولي جديد q وأعد الخطوات لتوليد P ثانية.

11) تخزن قيمة العدد البدائي وقيمة العداد من أجل التأكد من التوليد المسبق لكل من p,q

f. توليد الأرقام العشوائية a,k:

DSA تختار المفاتيح السرية بحيث تنتمي للمجال $\{1,2,\dots,q-1\}$ ولكل توقيع عدد اسي k ويتم اختيارهم وتوليدهم كالتالي: $G: \{0,1\}^{160} * \{0,1\}^* \to \{0,1\}^{160}$ حيث: $160 < b < 512$ وهذا التابع يتم انشاءه بواسطة تابع التقطيع SHA−1 أو خوارزمية DES ففي الحالة الأولى يتم اختيار P حيث $p \in \{160,\dots,512\}$ أما في الحالة الثانية يتم اختيار P من مجموعة تصل 160 نختار مفتاح سري a,j حيث $0 \leq j \leq m-1$ كالتالي:

1) نختار مفتاح $XKEY \in \{0,1\}^b$

2) ليكن لدينا عددT عبارة عن رقم هيكسا (سداسي عشر) 67452301 EFCDAB89 98BADCFE 10325476 C3D2EIFO.

3) حلقة لتكرار الخطوات السابقة $j = (0,1, \ldots., m-1)$

4) نضع $XVAL = (XKEY + XSEEDj) \; mod \; 2^b$

5) نضع $aj = G\,(t, XVAL) mod\; q$

6) نضع $\mathrm{XKEY} = (1 + XKEY + aj) \bmod 2^b$

ولتوليد العدد: K لكل m سنولد (k , k − 1 , r) كالتالي:

- يتم اختيار مفتاح سري KKEY ينتمي للمجال $b \in \{0,1\}$
- نختار عدد سداسي عشر T
- حلقة تكرار $j = (0,1, \ldots., m-1)$ تقوم بالخطوات التالية:

1) نضع $k = G\,(t, KKEY) mod\; q$

2) نضع $kj^{-1} = k^{-1} mod\; q$

3) نضع $rj = (g^k \; mod\; p) mod\; q$

4) نضع $KKEY = (1 + KKEY + K) mod\; 2^b$

وتحسب لكل مقطع ولكل رسالة حيث لكل رسالة m نحسب قيمة تابع التقطيع SHA−1 والذي فيه سنحسب لكل T قيمة r,k

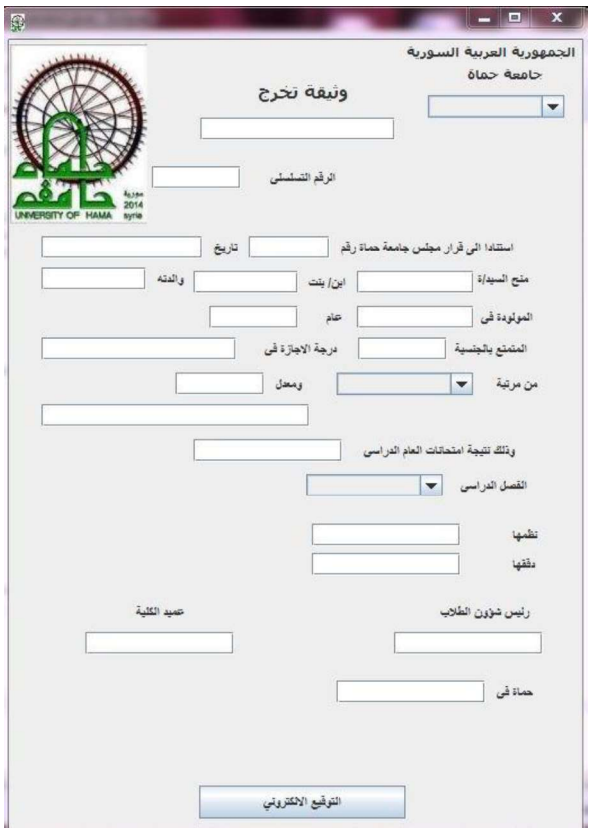
5- التطبيق العملي

تم استخدام حاسب محمول يعمل ضمن بيئة ويندوز7 وذاكرة رئيسية 4 جيجا بايت والحاسب مزود بكاميرا رقمية تستخدم لقراءة الترميز QR وموصول بطابعة لطباعة الوثيقة . وتم استخدام لغة برمجة جافا لبرمجة التطبيق و لقد قمنا باستخدام منصة العمل Eclipse واخترنا النسخة Neon منه لاحتوائها على الكثير من الميزات والأدوات التي تساعدنا في تسهيل برمجة التطبيق . يتألف الكود البرمجي للتطبيق من ثلاث حزم برمجية (package) أساسية هي كالآتي:

- الحزمة الأولى تسمى QR package وتحتوي على ثلاث صفوف أساسية وهي مولد رمز QR وقارئ رمز QR بالإضافة الى صف لقراءة QR عبر كاميرة الويب

- الحزمة الثانية حزمة DSA تتضمن ثلاث صفوف رئيسية الأولى مسؤولة عن توليد المفاتيح العامة والخاصة والصف الثاني يولد التوقيع وضمنه يتم تشفير البيانات المدخلة بواسطة خوارزمية DSA والصف الثالث مسؤول عن التحقق من التوقيع متضمنا خوارزمية فك التشفير
- الحزمة الثالثة حزمة الواجهات وهي تتضمن واجهة توليد المفاتيح وصف ثاني لواجهة توليد التوقيع والصف الثالث للتحقق من صحة التوقيع بالإضافة الى صف رابع مسؤول عن طباعة الوثيقة وتم استخدام العديد من المكتبات وذلك لتسهيل العمل والاستفادة من قوة ومتانة التطبيق وقد تم استخدام مكتبات أهمها مكتبة AWT ومكتبة SWING ومكتبات Java security ومكتبات zxing ومكتبات web cam ومكتبة sarxos وتم تطوير التطبيق بحيث يتلاءم مع العديد من الاختيارات فعلى سبيل المثال يمكن استخدام التطبيق بواسطة أوامر console لكتابة وتنفيذ الأوامر يدويا أو بواسطة واجهات سهلة الاستخدام لاستدعاء المفاتيح العامة والخاصة وصورة QR code بالإضافة إلى إمكانية

الشكل رقم (5) : توليد المفاتيح الخاصة والعامة



الشكل رقم (6): واجهة اصدار الشهادة مع التوقيع الالكتروني

الشكل رقم (7) : واجهة طباعة الشهادة متضمنة التوقيع بصيغة QR

الشكل رقم (4): واجهة التحقق من الشهادة

الشكل رقم(9) : واجهة قراءة QR عبر كميرا الويب

الشكل رقم (10): واجهة رسالة التحقق من صحة الشهادة

الشكل رقم (5) : واجهة الرسالة للشهادة المزورة

6- الخاتمة:

قدم هذا البحث دراسة شاملة لإمكانية استخدام التوقيع الرقمي على المستندات الورقية وذلك من أجل الحد من التزوير وتعديل المستندات والوثائق الرسمية وتم بناء نظام شهادات الكترونية لهذا الغرض معتمد على تقنيات التشفير والتوقيع الرقمي للحصول على موثوقية عالية حيث تم استبدال التوقيع التقليدي بتوقيع رقمي مطبوع على الشهادة ولكن بما أن التوقيع الرقمي يحتوي على بيانات مشفرة عن الموقع وخصوصيته بالآتي يمكن أن يكون حجمه كبير نسبيا وبالتالي عند استخدام عدة تواقيع على الوثيقة قد يصبح غير ملائم للاستخدام الورقي لذلك تم الاستفادة من تقنية الترميز الشريطي (Barcode) وبالتحديد تقنية رموز الاستجابة السريعة QR التي تمكننا من تخزين كثير من المعلومات بحيز صغير جداً.

الطريقة المقترحة تسهل عملية التحقق من أصالة الشهادات والوثائق بطريقة مبتكرة ورخيصة وفعالة من حيث التكلفة وسريعة جداً وبالآتي تساعد المؤسسات الحكومية والخاصة على إصدار شهادة ووثائق بدرجة عالية من الأمان وضمان عدم التلاعب أو التزوير وبدون أي تكاليف أو أعباء إضافية فيكفي لتحقيق ذلك نشر المفتاح العام للمؤسسات المعنية وكميرا رقمية لقراءة رموز الاستجابة السريعة.

1-المراجع العلمية:

1. K.M. Revathi, P. Annapandi, P.K.Ramya "Enhancing Security in Identity Documents Using QR Code" in International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 5, Oct-Nov, 2013.
2. R.L. Renesse, "Paper-based document security–A Review," in European Conf. on Security and Detection, 1997.
3. M. Singh and D. Garg, "Choosing best hashing strategies and hash functions," in International Advance Computing Conference, 2009, pp. 50 – 55.
4. QR Code Tutorial, http://www.thonky.com/qr-codetutorial
5. Digital http://technet.microsoft.com/enus/library/cc962021.aspx
6. Digital Signature, http://en.wikipedia.org/wiki/Digital_signature
7. QRCodes,http://www.qrcode.es
8. QRStuff,http://www.qrstuff.com
9. FIPS 186-2, Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186-2, U.S. Department of Commerce/N.I.S.T., National Technical Information Service, Springfield, Virginia, 2000.
10. POINTCHEVAL, D. , AND STERN, J. Security arguments for digital signatures and blind signatures. J. Cryptology 13 (2000), 361—396.
11. SCHNORR, C. Efficient signature generation by smart cards. In Advances in Cryptology –CRYPTO 89 (1991), Lecture Notes in Computer Science, Springer - Verlag, pp. 161—174
12. STANDARD, S. H. National Institute of Standars and Technology (NIST), FIPS Publication 180-1, April 1995.
13. ANSI X9.30:l-1997, Public Key Cryptography for the Financial Services Industry: Part1: The Digital Signature Algorithm (DSA). Available from the ANSI X9 Catalog, 1997.
14. Christof Paar & Jan Pelzl: Understanding Cryptography _ Heidelberg, Dordrecht, London, New York 2010.
15. John Edward S.:An Overview of Cryptographic Hash Functions and Their Uses_SANS Institute,p.1_4, 2003
16. leslie l.: Constructing Digital Signatures From A One Way Function,Microsoft.P., 1979