International Science and Technology Journal
المجلة الدولية للعلوم والتقنية
Volume 30 العدد
July 2022 يوليو
المجلة الدولية للعلوم والتقنية
ISTJ

توظيف خوارزمية AES256 كإحدى تقنيات التشفير المتماثل لإثبات بيانات الوثائق والشهادات الرقمية

مصعب عبد الله الدالي[1]، إيمان علي فيدالله[2]، نهى صالح ميلاد[3]
[1، 2، 3] قسم هندسة الحاسوب ، كلية العلوم التقنية – درنة

Emails:
[1] musabaldalii.1984@gmail.com
[2] nuha.karaim@gmail.com
[3] Imanhasse@gmail.com

الملخص

يعدّ التوقيع الرقمي مرحلة متقدمة من مراحل تطور الحكومات الإلكترونية ومعياراً لنضجها، وهو من أهمّ العلوم التي تعتمد على علم التشفير، حيث يستخدم في توقيع المستندات والوثائق الإلكترونية من عقود ومعاملات واتفاقيات عن طريق تشفيرها لحماية البيانات المستخدمة في التحقق من موثوقية التوقيع. تقترح هذه الدراسة آلية لتوظيف معايير التشفير المتقدمة AES كإحدى تقنيات التشفير المتماثل في إنشاء توقيع رقمي على الشهادات الرسمية الصادرة عن كلية العلوم التقنية – درنة وهي خوارزمية AES256 والتي تعتمد استخدام مفتاح سري واحد لتشفير وفك تشفير أي محتوى نصي وهي طريقة سهلة وسريعة مقارنة بتقنيات التشفير الأخرى، وتتمثل فكرة هذه الآلية في تطوير نظام بشقين، يتم في الشق الأول التوقيع على الشهادات عن طريق إنشاء رقم سري للشهادة بخوارزمية حذف واستبدال وإضافة تُجْرى على بيانات الشهادة يستخدم لخزن بيانات الشهادة، من ثم يتم تحويله إلى سلسلة مشفرة لتوليد رمز استجابة سريعة (QR) تتم طباعته على الوثائق كتوقيع رقمي، وقد تم تصميم صفحة ويب تعمل تحت بيئة موقع الكلية كشق ثانٍ للنظام وذلك للتحقق من بيانات الشهادة بعد عملية فك التشفير وقد تم تزويد الصفحة بقارئ (QR) لاسترجاع بيانات المفتاح. وقد تم تطبيق آلية التشفير المذكورة وإجراء محاكاة سليمة للنظام المقترح ووجدنا أن النظام قادر على إصدار شهادات موقعة رقمية والتحقق منها بكفاءة وموثوقية عالية، الأمر الذي يجعل احتمال اعتراض بيانات الشهادات وانتحال شخصية أصحاب التوقيع أمراً شبه مستحيل.

الكلمات المفتاحية: شهادة رقمية – التوقيع الإلكتروني – التشفير المتماثل – فك التشفير – رموز الاستجابة السريعة QR – مصادقة – معايير التشفير المتقدم – AES256

Abstract

Digital signature is an advanced level of E-Government development stages which evaluate criterion for its maturity, in addition to being one of the most cryptography-based sciences, which is reliable in signing electronic documents such as contracts and agreements through encrypting the contents in order to verify reliability of signature. This study proposes a mechanism for employing advanced encryption standards AES as one of the symmetric encryption techniques in creating a digital signature on the official certificates issued by College of Technical Sciences - Derna, which is the algorithm of AES256 in producing a secret key for signing certificates digitally through a rapid and easy encryption mechanism. The main idea of this mechanism is to develop a two-pronged system, the documents are signed with encoded string generated through deletion, replacement and addition algorithms that are performed on data of certificate for generating one secret key used as a primary key in an intermediate.

An encryption algorithm turns the primary key into a cipher text which is used to print a QR code on documents to save key data at first part. A WEB-Based Application with QR reader is acting as a second part of the system which was designed for retrieving data of decoded secret key. As a result of applying the stated encryption mechanism and experimenting the proposed system, the researchers have concluded that the system is capable for issuing and verifying certificates with high efficiency and reliability, which makes the possibility of intercepting certificate data and impersonating the signature owners almost impossible.

Keywords: Digital Certificate - Electronic Signature - Symmetric Encryption – Decryption - QR Code - Authentication - AES - AES256.

1. مقدمة:

يتميز عصرنا الراهن بالتدفق العظيم والانتشار الواسع للبيانات والمعلومات، الأمر الذي جعل عملية التأكد من مصدر المعلومات وحمايتها من التزوير ضرورة ملحة، ويعتبر التوقيع الرقمي آلية أساسية لحماية المعلومات والتأكد من هوية مصدر هذه المعلومات، حيث أنه يعتبر من أهم الطرق المستخدمة لضمان صحة الوثائق وتوفير الضمانات الموجودة في التوقيع اليدوي بل تفوقها، بعكس التوقيع التقليدي والذي له مساوئ كثيرة أهمها قابليته للتقليد بدقة عالية والذي أصبح فيه تزوير الشهادات والوثائق الرسمية أمراً سهلاً ومشكلة حقيقية تعاني منها جميع المؤسسات خاصة التعليمية منها مثل الجامعات والمعاهد، ومن ناحية أخرى نجد في ضوء الواقع الحالي في مجتمعنا أن معظم المعاملات والوثائق والتشريعات القانونية تعتمد على المعاملات الورقية الروتينية التي تعتمد على التوقيع التقليدي، لذلك كان لابد من مواكبة التطورات التكنولوجية في التواقيع الرقمية والتي أثبتت درجة عالية من الأمان وإزالة الشك الحاصل فيها في مجتمعاتنا والذي تسبب انعدام العمل بها.

ومن هذا المنطلق اقترحنا استخدام تقنية التوقيع الرقمي على الشهادات الورقية والتحقق من مصدرها الكترونياً وذلك لاكتساب الموثوقية العالية والأمان في إنشاء التواقيع الرقمية وذلك باستخدام تقنيات بحيث يسمح فقط للأشخاص المخولين بالوصول إلى البيانات مع إمكانية التحقق من هويتهم وتأمين بيانات الشهادات من الاعتراض ومنع أي شخص غير مخول من إجراء التعديلات عليها.[1]

تتمثل مشكلة البحث في الحد من عمليات تزوير الشهادات الممنوحة من كلية العلوم التقنية درنة وانتحال شخصيات أصحابها، إضافة إلى معالجة قصور خوارزمية (AES) كإحدى خوارزميات التشفير المتماثل في إثبات صحة التوقيع الرقمي للشهادات الموقعة رقمياً كونه لا يمكن إثبات تبعية الشهادة لصاحب التوقيع والمكلف بإصدار هذه الشهادات.

وتهدف هذه الدراسة في إيجاد طريقة فعالة لبناء نظام أمن الشهادات الجامعية وتطبيق الطرق والأساليب العلمية الحديثة لزيادة موثوقية هذه الأنظمة، بحيث يتم مواكبة التطور التقني وتوظيف التكنولوجيا في إصدار شهادات رقمية ذات موثوقية واعتمادية عالية واستبدال الطرق التقليدية المستخدمة حالياً، بالإضافة إلى تسهيل عملية التأكد من صحة

الشهادات من قبل الجهات الحكومية باعتبارها فئة معنية بمثل هذه الإجراءات واكتشاف عملية التزوير فيها، الأمر الذي تزيد فيه ثقة هذه المؤسسات في بيانات الشهادات الموقعة رقمياً.

وقد أجريت هذه الدراسة في نطاق كلية العلوم التقنية – درنة حيث تم إنشاء نظام محاكاة لنظام إصدار الشهادات بالكلية يعمل كزرّ إصدار في نظام إصدار الشهادات الرسمية بعيداً عن قاعدة البيانات الخاصة بمكتب التسجيل والدراسة والامتحانات كونها مصدر بيانات الوثائق والشهادات وهي أكثر البيانات التي قد تكون عرضة للغش والتزوير، وقد تم تصميم نظام ذو شقين وتطويره باستخدام لغتي VB.NET ولغة ASP.NET العاملتان تحت بيئة Microsoft Visual Studio وهي بيئة تطوير متكاملة تستخدم لغات برمجة متطورة، وقد تم جمع البيانات الخاصة بالنظام من واقع المقابلات الشخصية بموظفي مكتب التسجيل والدراسة والامتحانات ومديرو الموقع الإلكتروني بالكلية لغرض إجراء محاكاة سليمة لنظام إصدار الشهادات دون أي تعارض قد يحدث بين خصائص النظام الموجود حالياً والنظام المقترح بهذا البحث، إضافة إلى مراجعة مجموعة من الكتب والمقالات والورقات العلمية ذات الصلة للتعرف على مفاهيم ومصطلحات البحث.

2. أعمال ذات صلة:

تناولت بعض المنشورات آلية لتشفير البيانات اعتماداً على خوارزمية (AES256) لتشفير الرسائل النصية وملفات الصوت والفيديو منها دراسة (M.Feldhofer, S.Dominikus, and J.Wolkerstorfer) حيث قدمت نصف حل باستخدام مصادقة متماثلة قوية مناسبة لمتطلبات اليوم فيما يتعلق باستهلاك طاقة منخفض بحجم القالب المنخفض كبروتوكول مصادقة يعمل كدليل مصادقة علامة تعريف تردد الراديو إلى جهاز قارئ لهذا التردد[3].

وعلى صعيد تشفير النصوص فقد اقترح [R. Al-Khatib] نظاماً لإثبات أصالة الشهادات الجامعية عن طريق التشفير الغير متناظر باستخدام تقنية التوقيع الرقمي على الشهادة اعتماداً على خوارزمية التوقيع الرقمي (DSA) إحدى أهم تقنيات التشفير الغير متماثل، وكانت الفكرة الأساسية في إعطاء الموقّع على الشهادة مفتاحين تربط بينهما علاقة (مفتاح

عام، ومفتاح خاص) يستخدم المفتاح الخاص للتوقيع على الشهادة ويستخدم المفتاح العام من قبل أي شخص للتحقق من صحة التوقيع، بالإضافة إلى ذلك تم الاستفادة من تقنية رموز الاستجابة السريعة (QR) لحفظ البيانات المشفرة لبيانات الوثائق بطريقة مختصرة ومناسبة للطباعة والقراءة، وقد كان النظام المقترح حلاً عملياً في تأمين الوثائق والتحقق من صحتها وصحة صاحب التوقيع، ومن جهة أخرى فإن النظام المقترح هو نظام خاص بالمؤسسة ولا يمكن لأحد من خارج المؤسسة التحقق من بيانات الشهادة، وقد أفادت هذه الدراسة بقصور تقنية التشفير المتماثل من ضمنها معايير التشفير المتقدمة (AES) في التحقق من هوية صاحب الشهادة وهذا ما دفعنا إلى اقتراح هذا النظام.[1]

3. مصطلحات البحث:

1.3 التشفير:

يعرّف التشفير أو التعمية على أنه العلم الذي يستخدم الرياضيات للتشفير وفك تشفير البيانات ويُمكّنُك من تخزين المعلومات الحساسة أو نقلها عبر الشبكات غير الآمنة – مثل الإنترنت – وعليه لا يمكن قراءتها من قبل أي شخص ما عدا الشخص المرسل له، وحيث أن التشفير هو العلم المستخدم لحفظ أمن وسرية المعلومات، فإن تحليل وفك التشفير (Cryptanalysis) هو علم لكسر وخرق الاتصالات الآمنة، ويحظى هذا العلم اليوم بمكانة مرموقة بين العلوم، إذ تنوعت تطبيقاته العملية لتشمل مجالات متعددة نذكر منها: المجالات الدبلوماسية والعسكرية، والأمنية، والتجارية، والاقتصادية، والإعلامية، والمصرفية والمعلوماتية في شكلها المعاصر.

وقد تم بذل العديد من الجهود في جميع أنحاء العالم لإيجاد الطرق المثلى التي يمكن من خلالها تبادل البيانات مع عدم إمكانية كشف هذه البيانات، ومازال العمل والبحث في مجال علم التشفير مستمراً إلى وقتنا هذا وذلك بسبب التطور السريع للكمبيوتر والنمو الكبير للشبكات وبخاصة الشبكة العالمية (الإنترنت).[4]

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

- 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 حروف النص المقروء حسب قاعدة استبدال محددة تعرف بمفتاح التشفير.

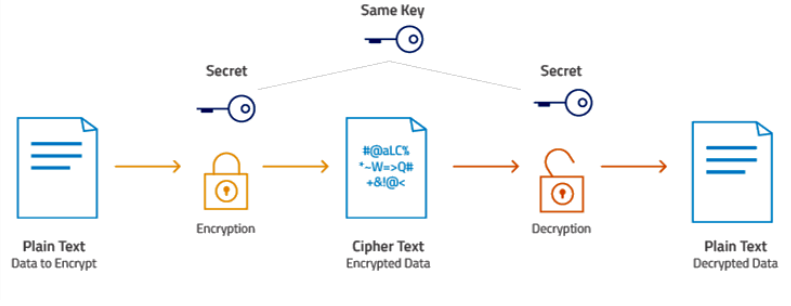
ويعتبر نظام يوليوس قيصر للتشفير الذي يستخدم خوارزمية ROT13 لتشفير الرسائل المكتوبة باللغة اللاتينية نظاماً مبنياً على مبدأ الاستبدال حيث يستبدل كل حرف بالحرف الذي يليه بثلاثة عشر موقعاً في ترتيب الأبجدية اللاتينية، ولكن نلاحظ أن هذا النظام يمكن كسره بسهولة بدون معرفة المفتاح وذلك عن طريق حساب تواتر الحروف في لغة النص، ثم حساب تواتر الحروف في النص المشفر، وبعد ذلك يمكن أن نخمن أكثر الحروف تواتراً في النص الأصلي يقابله أكثرها تواتراً في النص المشفر.

وكمثال على مبدأ الإبدال نذكر نظام التشفير أحادي الأبجدية حيث يتم فيه تغيير مواقع الحروف في النص الأصلي ويتم هذا التغيير حسب قاعدة معينة يعبر عنها المفتاح[6]، وتطورت أساليب خوارزميات التشفير وأصبحت تعتمد على أسلوبين هما:[1]

- التشفير المتناظر أو المتماثل (Symmetric Cryptography).
- التشفير الغير متناظر (asymmetric cryptography).

أ. ماهية التشفير المتناظر:

ويعرف أيضاً 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(1).



الشكل1. يوضح كيفية عمل تشفير المفتاح المتماثل[5]

ويعتمد هذا النوع بالأخص على سرية المفتاح المستخدم، 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 قد تم إرسالها من قبل المرسل المفترض وليس من قبل شخص آخر تنكر بشخصية المرسل وبهذا يمكن للمرسل أيضاً أن ينكر إرساله للرسالة، ومن أشهر خوارزميات هذا الأسلوب (RC2-RC6-DES-3DES-IDEA-AES).[1]

ب. معايير التشفير المتقدمة AES:

معايير التشفير المتقدمة Advanced Encryption Standards واختصاراً (AES) وهي معايير حددها المعهد الوطني للمعايير والتكنولوجيا (NIST) تستخدم على نطاق واسع في التشفير المتماثل وهي معايير التشفير الأولى والوحيدة المتاحة للجمهور والمعتمدة من قبل وكالة الأمن القومي الأمريكية (NSA) لحماية المعلومات السرية للغاية، وتم تسمية AES لأول مرة باسم Rijndael تيمناً بمطوريها، وهما البلجيكيان Vincent Rijmen و Joan Daemen.[7]

تستخدم خوارزمية (AES) لتشفير المفتاح المتماثل، والذي يتضمن استخدام مفتاح سري واحد فقط لتشفير وفك تشفير المعلومات، وقد اعتمدت هذه الدراسة خوارزمية التشفير (AES) بمفتاح 256 بت لتحقيق أهدافها.

يدعم AES-256 والذي يبلغ طول مفتاحه 256 بت أكبر حجم للبت وهو عمليًا غير قابل للكسر بالقوة الغاشمة استنادًا إلى قوة الحوسبة الحالية، مما يجعله أقوى معيار للتشفير كون مجموعات المفاتيح المحتملة تزيد أضعافًا مضاعفة مع حجم المفتاح.[8]

2.3 التوقيع الرقمي أو الإلكتروني:

التوقيع الإلكتروني هو آلية لحماية المعلومات وذلك بالتأكد من هوية مصدر المعلومات (الرسالة) حيث أنها تعتبر من أهم الطرق المستخدمة لضمان الوثائق المرسلة بجعل مستقبل الرسالة أو الوثيقة مطمئناً من الطرف الذي أرسلها له.

وقد كان أول اعتراف بالتوقيع الإلكتروني في عام 1989 في مجال البطاقات الائتمانية حيث أقرت محكمة النقض الفرنسية صحة التوقيع الإلكتروني واعتبرت أنه يتألف من

عنصرين هما إبراز البطاقة الائتمانية وإدخال رقم حامل البطاقة السري وأكدت هذه المحكمة كذلك أن هذه الوسيلة توفر الضمانات الموجودة في التوقيع اليدوي بل تفوقها، وفي عام 1999م صدر إرشاد عن الاتحاد الأوروبي حول التوقيع الإلكتروني، إلا أن أول توقيع الكتروني صدر في الولايات المتحدة الأمريكية عام 2000م. [9]

3.3 المصادقة:

المصادقة تعني أن يثبت الشيء هويته المزعومة لشريكه في الاتصال، يمكن لهذه التقنية حل جميع مشاكل الأمان ويمكن تجنب تتبع المستهلك، إذا كانت العلامات تنقل هويتها إلى القراء المصادق عليهم فقط فلا يمكن للقارئ غير المصرح له الحصول على أي معلومات حول العلامات الموجودة حاليًا في مجالها.

مصادقة القارئ على العلامات تحل أيضاً مشكلة الوصول غير المصرح به ويمكن للقراء المعتمدين فقط القراءة من ذاكرة العلامة أو الكتابة إليها، مصادقة العلامة تعني أن العلامة تثبت هويتها للقارئ ولا يمكن للعلامة المزورة إقناع القارئ بأصالتها، لذلك يمكن التحايل على تزوير العلامات، ويميز[Menezes, Oorschot, and Vanstone] بين ثلاث طرق للتوثيق التلقائي وهي [10]:

- أنظمة كلمة المرور (مصادقة ضعيفة).
- مصادقة استجابة التحدي (مصادقة قوية).
- مصادقة مخصصة وخالية من المعرفة.

توفر أنظمة كلمات المرور مستوى ضعيفاً من الأمان وغالبًا ما ترتبط تقنيات عدم المعرفة بالمشكلات الرياضية "القوية" والتي تكون مكلفة للغاية في الحساب والتنفيذ، لذلك تم اعتماد النوع الثاني وهي تقنية التحدي والاستجابة لطباعة بيانات التوقيع على الشهادات بشكل مختصر ومناسب للطباعة وهي تقنية يتم استخدامها على نطاق واسع.[3]

4. الآلية المستخدمة في التوقيع على الوثائق والتحقق منها:

تم تصميم النظام ليكون بمثابة زرّ إصدار في نموذج طباعة التقارير الخاص بمنظومة قسم التسجيل والدراسة والامتحانات بالكلية، حيث يقوم برقمنة الشهادات والوثائق الصادرة عن مكتب التسجيل والدراسة والامتحانات بالكلية وذلك بإجراء التوقيع الإلكتروني عليها

وحفظ بياناتها في قاعدة بيانات مصممة لهذا الغرض. ولتوضيح الآلية المستخدمة في التوثيق على الوثائق والتحقق منها تم تصميم الشق الأول للنظام ليقوم بتنفيذ المراحل الآتية:

1.4 توليد المفتاح السري:

يتم اختزال مفتاح سري وهو عبارة عن سلسلة مكونة من (19) حرفاً يتم اختزالها بخوارزمية حذف واستبدال تجرى على بيانات الشهادة وهي (الرقم الدراسي – نوع الشهادة – القسم – التخصص – الشعبة – تاريخ الإصدار بالسنة والشهر واليوم والساعة والدقيقة والثانية)، وقد تمت فهرسة البيانات وفقاً لما يأتي:

جدول 1. يوضح آلية استخراج المفتاح السري من بيانات الشهادة

Primary Key Structure

NO	TYP	DEP	SPC	MAJ	Y	M	D	H	MIN	SEC
001 – 99	5 - 0	5 - 0	*i* -0	*i* -0	- 00 99	01 – 12	- 01 31	- 01 12	- 00 59	00 - 59

حيث:

- (N) خانة رقم الطالب: تقع في النطاق 001 ≥ N ≥ 999 وتستخلص من الرقم الدراسي.
- (T) خانة نوع الشهادة: تقع ضمن النطاق0 ≥ T ≥ 5 وهي تخصيص فهرس لكل نوع من (6) أنواع من الوثائق الصادرة عن الكلية.
- (DEP) خانة القسم: تنتمي للنطاق 0 ≥ DEP ≥ 5 وهي تخصيص فهرس لكل قسم من (6) أقسام تابعة للكلية.
- (SPC) خانة التخصص: تنتمي للنطاق 0 ≥ SPC ≥ ***i*** وهي تخصيص فهرس لكل تخصص ويختلف عددها باختلاف الأقسام.
- (MAJ) خانة الشعبة: تنتمي للنطاق 0 ≥ MAJ ≥ ***i*** وهي تخصيص فهرس لكل شعبة ويختلف عددها باختلاف تخصصات كل قسم.
- (Y) خانة السنة: تنتمي للنطاق 00 ≥ Y≥ 99 وتستخلص من أول خانتين لقيمة سنة إصدار الشهادة.

- (M) خانة الشهر: تنتمي للنطاق 01≤ M ≤ 12 وهي شهر إصدار الشهادة بتنسيق (MM).
- (D) خانة اليوم: تنتمي للنطاق 01≤ D ≤ 31 وهي يوم إصدار الشهادة بتنسيق (DD).
- (H) خانة الساعة: تنتمي للنطاق 01≤ H ≤ 12 وهي ساعة إصدار الشهادة.
- (MIN) خانة الدقيقة: تنتمي للنطاق 00 ≤ MIN ≤ 59 وهي دقيقة إصدار الشهادة بتنسيق (mm).
- (SEC) خانة الثانية: تنتمي للنطاق 00 ≤ Y ≤ 59 وهي ثانية إصدار الشهادة بتنسيق (ss).

2.4 تشفير المفتاح السري:

في هذا البحث تم اقتراح نظام تشفير عالي الأداء يعتمد علىAES، وهي خوارزمية تشفير كتل وتدعم أطوال مفاتيح ونصوص متعددة، وقد تم تشفير المفتاح الأساسي المختزل من بيانات الشهادة باستخدام خوارزمية التشفير رايندال AES (RIJNDEAL) بمفتاح 256 بت مع إعادة عملية التشفير لعدد من الدورات طبقاً لطول مفتاح التشفير المستخدم وكتلة النص الأصلي.

مفتاح التشفير k هو مصفوفة ذات أبعاد $4\times N_k$ (أي أن طول المفتاح هو $4.N_k$ بايت)، وبما أن طول المفتاح المستخدم يساوي 256، وهكذا هو الحال بالنسبة للنص المشفر X فهو مصفوفة ذات أربع أبعاد $4\times N_b$ أي أن طول المفتاح $4.N_b$ بايت، لذلك فإن حجم كل كتلة يمكن تشفيرها سيكون مساوياً ل 8 بايت، ولهذا فقد تم تقسيم المفتاح الأساسي باعتباره النص الأصلي إلى ثلاثة سلاسلX1، X_2 ، X_3 بحجم 8 بايت لكل سلسلة وتشفير كل سلسة على حدة وفيما يلي تمثيل لأشكال مصفوفتي الكتلة الأولى للنص المشفر X1 ومفتاح التشفير K. [7][11]

$$X_1 = \begin{bmatrix} X1_{0,0} X1_{0,0} & \dots\dots\dots & X1_{0,N_{b-1}} \\ X1_{1,0} X1_{1,0} & \dots\dots\dots & X1_{1,N_{b-1}} \\ X1_{2,0} X1_{2,0} & \dots\dots\dots & X1_{2,N_{b-1}} \\ X1_{3,0} X1_{3,0} & \dots\dots\dots & X1_{3,N_{b-1}} \end{bmatrix}$$

$$K = \begin{bmatrix} K_{0,0}K_{0,0} & \dots\dots\dots & K_{0,N_{K-1}} \\ K_{1,0}K_{1,0} & \dots\dots\dots & K_{1,N_{K-1}} \\ K_{2,0}K_{2,0} & \dots\dots\dots & K_{2,N_{K-1}} \\ K_{3,0}K_{3,0} & \dots\dots\dots & K_{3,N_{K-1}} \end{bmatrix}$$

وهكذا لباقي مصفوفات النص المراد تشفيره X_1 ، X_2 حيث أن كل $K_{i,j}$ في هذه المصفوفة يمكن اعتباره 8 بت أو 1 بايت، وتكون قراءة كل من مصفوفة مفتاح التشفير K ومصفوفات الكتلة X على حد سواء حسب كل عمود من اليسار إلى اليمين لتصبح عناصر المصفوفتين كما هو موضح في التعبيرين (1) و(2) كالآتي:

$$\mathbf{K = (K_{0,0},\ K_{1,0}\ ,\ K_{2,0},\ K_{3,0},\ \dots\dots\dots,\ K_{0,N_{K-1}},\ K_{1,N_{K-1}},K_{2,N_{K-1}},\ K_{3,N_{K-1}})} \quad \mathbf{(1)}$$

$$\mathbf{X = (X_{0,0},\ X_{1,0},\ X_{2,0},\ X_{3,0},\ \dots\dots\dots\ ,\ X_{0,N_{b-1}},\ X_{1,N_{b-1}},\ X_{2,N_{b-1}},\ X_{3,N_{b-1}})} \quad \mathbf{(2)}$$

وضعياتRIJNDAEL عبارة عن مصفوفة متحولة ولتكن w حيث أن كل $W_{i,j}$ هو عدد صحيح، وتجرى على هذه الوضعيات مجموعة تحويلات Transformations تسمى الدورات iterations وعدد الدورات (N_r) يتعلق بطول المفتاح (N_k) وحجم أو طول الكتلة (N_b)، وفي هذه الحالة فإن طول المفتاح وطول الكتلة مساويان ل 8 بايت، ما يعني أن عدد الدورات هو 14 دورة[11]، أي أن:

$$RIJNDAEL(X) = Y = (T_{14} o \dots\dots o\ T_1 o\ T_0)$$

مجموعة التحويلات (الدورات) على وضعيات رايندل

فمثلاً الدورة الأولى T_0 هي عملية XOR بين سلسلة النص ومفتاح التشفير ويمكن يمكن تمثيلها كتعبير رياضي كما هو موضح في المعادلة (3).

$$T_0(X) = \begin{bmatrix} X1_{0,0}X1_{0,0} & \dots\dots\dots & X1_{0,N_{b-1}} \\ X1_{1,0}X1_{1,0} & \dots\dots\dots & X1_{1,N_{b-1}} \\ X1_{2,0}X1_{2,0} & \dots\dots\dots & X1_{2,N_{b-1}} \\ X1_{3,0}X1_{3,0} & \dots\dots\dots & X1_{3,N_{b-1}} \end{bmatrix} \oplus \begin{bmatrix} K_{0,0}K_{0,0} & \dots\dots\dots & K_{0,N_{K-1}} \\ K_{1,0}K_{1,0} & \dots\dots\dots & K_{1,N_{K-1}} \\ K_{2,0}K_{2,0} & \dots\dots\dots & K_{2,N_{K-1}} \\ K_{3,0}K_{3,0} & \dots\dots\dots & K_{3,N_{K-1}} \end{bmatrix} \quad (3)$$

كل w ⇢ w : T_i أي أن المجال والمدى هو وضعية RIJNDAEL عند كل دورة، وبالتالي فإن كل الدورات التي تأتي بعد هذا سوف تعنى بتحويل الوضعية الحالية، وعند تشفير كل سلسلة من سلاسل النص الأصلي تقوم وحدة التشفير بتحويل نص السلسلة إلى سلاسل نصية مشفرة بطول (44) رمزاً يتم تجميعها عند اكتمال عملية التشفير كوحدة واحدة لتشكل النص المشفر في صورته النهائية (Cipher).[10]

3.4 إجراء التوقيع:

يتم دمج النص المشفر المراد طباعته كتوقيع رقمي على الوثائق مضاف إلى عنوان صفحة التحقق (authentication.aspx) وهو عنوان أداة التحقق التابعة للكلية (الشق الثاني للنظام)، حيث تقوم الأداة بعدها بتوليد رمز QR من بيانات هذه السلاسل المدمجة ليسهل على الجهات الوصول لهذه الصفحة والتحقق من بيانات الشهادات.

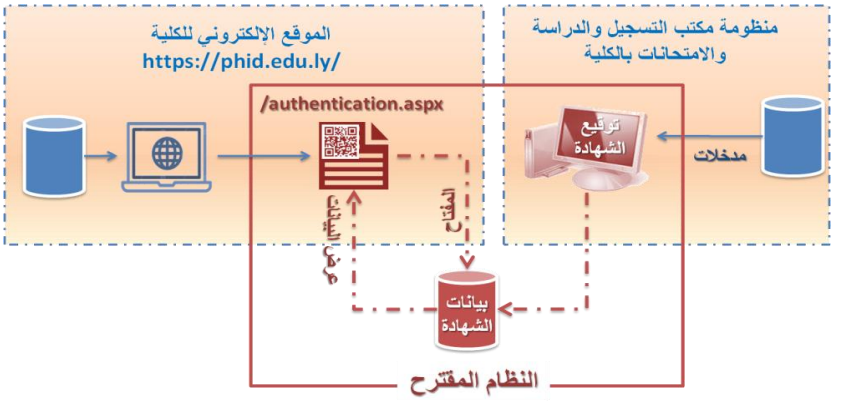
4.4 فك تشفير المفتاح:

كما تمت عملية التشفير بعدة دورات أو وضعيات على كل سلسلة من سلاسل النص المشفر، فإنه وبعد استخلاص النص المشفر من السلسلة الحرفية المقروءة بواسطة قارئ رمز الاستجابة السريع QR في صفحة التحقق وتجزئتها إلى 3 سلاسل مشفرة، فإن وحدة فك التشفير تقوم بعكس التحويلات التي تم إجراؤها عند التشفير على أن يتم البدء بآخر دورة (T_{14}) وانتهاء بالدورة الأولى (T_0) وذلك لكي تظهر النص المشفر واسترجاع بيانات المفتاح، بمعنى آخر يمكن تمثيل مجموعة التحويلات العكسية بالتعبير المبين في معادلة (4) كالآتي:

$$RIJNDAEL^{-1}(Y) = X = (T_0^{-1} o\ T_1^{-1} o\ \ldots\ldots\ o\ T_{N_{r-1}}^{-1} o\ T_{N_r}^{-1}) \qquad \textbf{(4)}$$

5. تصميم النظام المقترح:

تم تصميم النظام ليعمل بصورة مستقلة عن قواعد بيانات الكلية (بيانات مكتب التسجيل – بيانات موقع الكلية) وذلك لحمايتها من هجمات المخترقين التخريبية، كونها تحوي بيانات حساسة والتي يؤدي تلفها أو تزويرها إلى مشاكل كبيرة قد لا يمكن معالجتها، ويبين الشكل (2) مخطط سير عمليات النظام المقترح والبيئة التي يعمل ضمنها.



الشكل 2. يوضح بيئة عمل النظام المقترح

عندما تتم قراءة رمز الاستجابة السريع من قارئ خارجي فإنه يقوم باسترجاع رابط صفحة التحقق إضافة إلى البيانات المشفرة للمفتاح، وعند النقر على الرابط يتم توجيه السلسة النصية إلى صفحة (authentication.aspx) حيث يتم فك تشفير بيانات المفتاح والتحقق من وجود سجل مطابق لهذا المفتاح.

1.5 تصميم أداة إصدار التوقيع (الشق الأول للنظام):

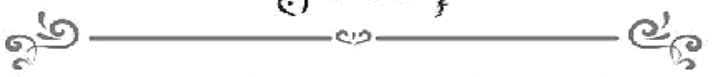
يمنح الطالب الدارس بالكلية (6) أنواع من الشهادات وهي: (شهادة تخرج – إفادة تخرج – كشف درجات – تعريف طالب – إثبات مستوى دراسي – حسن سيرة وسلوك)، يتم توليد مفتاح خاص لكل شهادة حسب نوعها وتاريخ ووقت إصدارها بالساعة والدقائق والثواني وبالتالي سيتم توليد مفتاح مختلف لشهادة بنفس البيانات ممنوحة لنفس الطالب باختلاف زمن إصدار الشهادة.

وكما تم التوضيح سالفاً بأن هذه الأداة تعمل بمثابة زر إصدار في نظام إصدار الشهادات بالكلية وهي الشق الأول للنظام المقترح، حيث يتم فيه توليد المفتاح بخوارزمية الحذف والاستبدال المذكورة ليتم تشفيره، ومن ثم يتم دمج المفتاح المشفر مع رابط صفحة التحقق (authentication.aspx) لتوليد رمز استجابة سريعة (QR) لطباعة التوقيع على الشهادة بطريقة مختصرة ومناسبة ويوضح الشكل (3) الشاشة الرئيسية لأداة الإصدار.

الشكل 3. شاشة الإصدار - الشق الأوّل للنظام المقترح

بعد استجلاب بيانات الشهادة من منظومة التسجيل والدراسة والامتحانات بالكلية واختيار نوع الشهادة، تتم عملية إصدار الشهادة بالنقر على زر الإصدار كما هو موضح بالشكل (3) حيث تقوم الأداة بحفظ بيانات الشهادة في قاعدة البيانات، وعند طباعة تقرير الشهادة يتم صرف رمز استجابة سريع (QR) كاختصار للتوقيع الإلكتروني المشفر على الشهادة بزمن إصدارها، ليتم التحقق منها لاحقاً من خلال قراءة الرمز المطبوع كما هو موضح بالشكل (4).

وزارة التعليم التقني والمهني
إدارة الكليات التقنية
كلية العلوم التقنية - درنة



إفَادة تخرّج

تشهد إدارة كلية العلوم التقنية درنة بأن الطالب:

مصعب عبدالله حسن الدالي

الرقم الدراسي: 165212045

قد استكمل متطلبات الحصول على درجة البكالوريوس التقني في مجال:

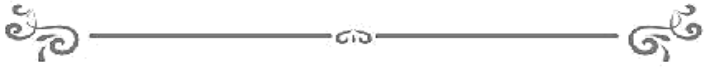
هندسة الحاسوب

التخصص: **تقنية المعلومات** الشعبة: **بلا**

بتقدير عام: **جيد** وبمعدل تراكمي **72.65**

عوض رمضان ساسي
رئيس قسم التسجيل والدراسة والامتحانات

د. منصف محمد المنصوري
عميد الكلية



الشكل 4.نموذج لإفادة تخرج موقعة رقمياً

2.5 تصميم صفحة التحقق (الشق الثاني للنظام):

وهي الشق الثاني للنظام المقترح هي عبارة عن صفحة ويب تعمل تحت بيئة الموقع الإلكتروني للكلية (https://phid.edu.ly) تم تصميمها أساساً لعرض بيانات الشهادة عند إتمام عملية التحقق (مطابقة المفتاح)، وتتيح هذه الصفحة لزوارها إمكانية قراءة رموز متعددة حيث تم تجهيزها بقارئ (QR) لقراءة رموز استجابة لشهادات أخرى

صادرة عن الكلية، ويوضح الشكل (5) صفحة التحقق (authentication.aspx/…) والتي يتم فيها عرض بيانات الشهادة بعد عملية فك التشفير واسترجاع البيانات.

الشكل 5. صفحة التحقق (authentication.aspx) - الشق الثاني للنظام

6. النتائج والتوصيات:

بعد تنفيذ النظام وإجراء محاكاة للآلية المقترحة، استنتج الباحثون أن هذه الأداة قادرة على إجراء توقيع رقمي موثوق لا يمكن اعتراضه من أطراف خارجية قد تتلاعب ببيانات الشهادات وتزويرها، ، إضافة إلى أن وجود صفحة تحقق خاصة بالكلية مزودة بآلية فك تشفير خاصة بها دون غيرها مما يزيد من ثقة المؤسسات المستقبلة لهذه الشهادات في صحة التوقيع وأصحابه، ويمكننا كذلك أن نستخلص أن هذه الدراسة قد عالجت القصور الحاصل في الخوارزمية المستخدمة، بحيث يمكن للجهات ومن خلال الموقع الرسمي للكلية بيان صحة التوقيع من عدمه إضافة إلى صحة بيانات الشهادة نفسها كون التزوير

قد يكون حاصلاً في التوقيع أو في بيانات الشهادة وإن كانت تحمل توقيعاً موثوقاً على حد سواء.

كما يمكن توظيف هذه الأداة مستقبلاً في إثبات الوثائق والمستندات الإدارية الصادرة عن الكلية بحيث يتم توليد توقيع رقمي من رقم إشاري لرسالة ما بحيث يسهل التحقق من أصليتها وأرشفتها إلكترونياً، كما يمكن استخدام هذه التقنية في إصدار بطاقات تعريف لكادر الكلية من أعضاء هيئة تدريس وموظفين واستخدامها في أغراض متعددة.

7. الخلاصة:

لقد اقترحت هذه الدراسة توظيف خوارزمية AES256 كإحدى تقنيات التشفير المتناظر في التحقق من التواقيع الرقمية على الوثائق الصادرة عن كلية العلوم التقنية درنة، وهي تقنية تشفير سهلة وسريعة مقارنة بتقنيات التشفير الأخرى، والتي سوف تسهم بشكل كبير في الحدّ من عمليات التزوير وانتحال شخصيات أصحاب هذه الشهادات، إضافة إلى بيان الشهادات التي تم إصدارها حديثاً أو قديماً كون بعض الشهادات مثل: تعريف الطالب يجب أن تكون حديثة الإصدار، وقد كان من أوجه القصور في هذه الخوارزمية أنه لا يمكن إثبات هوية جهة التحقق من التوقيع، وقد تم معالجة هذا الأمر بتصميم أداة التحقق بحيث تعمل تحت بيئة الموقع الرسمي للكلية، مما لا يدع مجالاً للشك في موثوقية عملية التحقق كون هذه الجهة هي صاحبة التوقيع والجهة الوحيدة المخولة لتأكيد صحته، ولقلة المراجع العربية في مجال تطبيقات علم التشفير، فقد تم إعداد هذه الدراسة باللغة العربية لتكون مرجعاً للباحثين في هذا المجال ولتطوير تطبيقات أخرى اعتماداً على هذه التقنية.

8. المراجع:

[1] R. Al-Khatib: Degree Certificate Authentication using Cryptography, Digital Signature and QR Code Techniques, Journal of Hama University vol.2 No.6-2019, pp 1-18.
[2] R.L. Renesse: "Paper-based document security-A Review," in European Conf. on Securityand Detection, 1997.
[3] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer: Strong Authentication for RFID Systems Using the AES Algorithm,

Institute for Applied Information Processing and Communications, Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria.

[4] Fouad, Hamza, Abd and Al-Sharifi: Science of Cryptography, publication of the College of Science at the University of Babylon, Babylon Open University Library, 12/10/2016 04:11:37.

[5] Mohit Arora: How Secure is AES 128 and 256 Encryption Against Brute Force Attacks?, EE Times, 05.07.2012. Available online at:

a. https://www.eetimes.com/document.asp?doc_id=1279619#. Last seen: Wednesday, May 18, 2022.

[6] Paar, Christof, and Jan Pelzl: Understanding cryptography: a textbook for students and practitioners. Springer Science & Business Media, 2009.

[7] National Institute of Standards and Technology (NIST). FIPS-197: Advanced Encryption Standard, November 2001. Available online at:

a. http://www.itl.nist.gov/fipspubs/.

[8] Y. Yuan, Y. Yang, L. Wu and X. Zhang, "A High Performance Encryption System Based on AES Algorithm with Novel Hardware Implementation," 2018 IEEE International Conference on Electron Devices and Solid State Circuits (EDSSC), 2018, pp. 1-2, doi: 10.1109/EDSSC.2018.8487056.

[9] B. Najmeddine: The Electronic Signature Mechanism and Its Application to Public Facility Management, Publications of the Faculty of Law and Political Sciences at the University of Sousse, Tunisia, 2019.

[10] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone: Handbook of Applied Cryptography. CRC Press, 1997.

[11] Daor, Joa&Daemen, Joan &Rijmen, Vincent. AES proposal: rijndael. 1999.