Comprehensive Journal of Science
Volume (10), Issue (37), (NOV. 2025)
SICST2025, www.sicst.ly
ISSN: 3014-6266

مجلة العلوم الشاملة
عدد خاص بالمؤتمر الدولي الثالث للعلوم والتقنية
المجلد (10)، العدد (37)، (نوفمبر2025)
ردمد: 3014-6266

دراسة مقارنة بين خوارزميات التشفير التقليدية وخوارزميات ما بعد التشفير الكمي في ظل التهديدات الكمية (إجراء مقارنة تحليلية بين خوارزمية التشفير المتماثل المتقدمة AES وخوارزمية ما بعد التشفير الكمي CRYSTALS-Kyber)

سالمين محمد بالقاسم الحاسي

المعهد العالي للعلوم والتقنية – اجدابيا

salmine.elhasy@gmail.com **ORCID ID 0009-0000-2409-7917**

Received: 30-09-2025; Revised: 10-10-2025; Accepted: 31-10-2025; Published: 25-11-2025

ملخص الدراسة

تهدف هذه الدراسة إلى تقديم مراجعة نظرية شاملة لمفاهيم التشفير الكلاسيكي والكمومي، مع تسليط الضوء على الفروقات الجوهرية بين الخوارزميات التقليدية وخوارزميات ما بعد الكمّ. وتُركّز الدراسة على إجراء مقارنة تحليلية بين خوارزمية التشفير المتماثل المتقدمة (AES) وخوارزمية ما بعد التشفير الكمي (CRYSTALS-Kyber)، من حيث مستوى الأمان، وكفاءة الأداء، كما تتناول الدراسة أبرز التحديات المرتبطة بالانتقال إلى بيئات تشفير مقاومة للهجمات الكمومية، مع تحليل للمزايا والعيوب التي تميز كل من الخوارزميات المدروسة، في ظل التقدم السريع في تقنيات الحوسبة الكمومية وتداعياته على أمن المعلومات في المستقبل. بالإضافة الي تقييم مدي جاهزية هذه الخوارزميات لمواجهة التحديات الأمنية المستقبلية عبر مقارنة دقيقة في مستوى الحماية بين الخوارزميتين .

الكلمات المفتاحية : معيار التشفير المتقدم AES ، انترنت الأشياء، التشفير الهجين ، خوارزمية CRYSTALS-Kyber ، الكيوبت.

Abstract

This study aims to provide a comprehensive theoretical review of classical and quantum cryptography concepts, highlighting the fundamental differences between traditional algorithms and post-quantum algorithms. An analytical comparison is conducted between the Advanced Encryption Standard (AES), a symmetric encryption algorithm, and the post-quantum encryption algorithm CRYSTALS-Kyber, focusing on security levels and performance efficiency. The study also addresses key challenges associated with transitioning to quantum-resistant cryptographic environments, offering an analysis of the strengths and weaknesses of each algorithm under review. This is particularly relevant in light of the rapid advancements in quantum computing technologies and their implications for

the future of information security. In addition to assessing the readiness of these algorithms to address future security challenges, the study provides a detailed comparison of the protection levels offered by each of the two algorithms.

1. المقدمة

يعد التشفير وحدة البناء الأساسية لأمن البيانات. وهو أبسط الطرق وأهمها لضمان عدم سرقة معلومات نظام الحاسوب أو قراءتها من جانب شخص يريد استخدامها لأغراض ضارة. يُستخدم تشفير البيانات لتأمينها على نطاق واسع من قبل المستخدمين الأفراد والشركات الكبيرة بغرض حماية معلومات المستخدم المرسلة بين المستعرض والخادم. قد تشمل تلك المعلومات أي شيء من بيانات الدفع إلى المعلومات الشخصية. ويتم استخدام برنامج تشفير البيانات، المعروف أيضًا باسم "خوارزمية التشفير" أو "التشفير" فحسب، لتطوير مخطط تشفير لا يمكن اختراقه نظريًا إلا بقوة حوسبية هائلة. وهنا يظهر تهديد الحوسبة الكمومية لأمن المعلومات الذي يمتاز بقدرته على كسر أساليب التشفير الحالية المبنية على المسائل الرياضية المعقدة، حيث للحواسيب الكمومية القدرة على حل هذه المسائل بسرعة أكبر بكثير من الحواسيب التقليدية. قد يُعرّض هذا البيانات الحساسة للخطر، ويُعرّض الاتصالات الآمنة للخطر. حيث يجب على المؤسسات الانتقال إلى التشفير المقاوم للحوسبة الكمومية للحد من هذه المخاطر، وتبني استراتيجيات استباقية لتأمين أنظمتها قبل أن تصبح الحواسيب الكمومية شائعة الاستخدام..

1.1. هدف الدراسة وأهميتها

تهدف هذه الدراسة إلى تقديم مراجعة نظرية شاملة لمفاهيم التشفير الكلاسيكي والكمومي، مع تسليط الضوء على الفروقات الجوهرية بين الخوارزميات التقليدية وخوارزميات ما بعد الكمّ. وتُركّز الدراسة على إجراء مقارنة تحليلية بين خوارزمية التشفير المتماثل المتقدمة (AES) وخوارزمية ما بعد التشفير الكمي (CRYSTALS-Kyber)، من حيث مستوى الأمان، وكفاءة الأداء، كما تتناول الدراسة أبرز التحديات المرتبطة بالانتقال إلى بيئات تشفير مقاومة للهجمات الكمومية، مع تحليل للمزايا والعيوب التي تميز كل من الخوارزميات المدروسة، في ظل التقدم السريع في تقنيات الحوسبة الكمومية وتداعياته على أمن المعلومات في المستقبل.

1.2. مشكلة الدراسة

تركزت غالبية الدراسات السابقة على تقييم كل فئة من خوارزميات التشفير بشكل منفصل، إما من خلال التحليل النظري أو عبر اختبارات محدودة النطاق، دون إجراء تقييم شامل يقارن أداء الخوارزميات التقليدية بتلك المصممة لما بعد التشفير الكمومي. وتُعد الدراسات التطبيقية التي تتناول المقارنة بين هذه الخوارزميات في سياقات واقعية، خاصة في ظل التهديدات الكمومية المتوقعة، محدودة نسبيًا. مما يُبرز

الحاجة الماسّة إلى أبحاث منهجية توضح أهمية وكفاءة خوارزميات ما بعد الكمّ ضمن بيئات حقيقية، مثل شبكات الاتصالات، وأنظمة إنترنت الأشياء، وحلول التخزين السحابي، مع الأخذ بعين الاعتبار متطلبات الأمان، والأداء، وقابلية التكامل.

وتتضمن هذه التقييمات ضرورة دراسة خصائص مثل استهلاك الموارد الحاسوبية (كالذاكرة)، وزمن التشفير وفك التشفير، في هذا الإطار، تمثل المقارنة المنهجية بين الخوارزميات التقليدية وخوارزميات ما بعد الكمّ خطوة أساسية نحو فهم تحديات التحول إلى أنظمة مقاومة للتقنيات الكمومية وضمان جاهزية البنية التحتية الرقمية لمواجهة التهديدات المستقبلية.

1.3. الإسهام العلمي

تقديم مقارنة بين خوارزمية التشفير المتماثل المتقدمة (AES) وخوارزمية ما بعد التشفير الكمي (CRYSTALS-Kyber) في اوجه مختلفة مثل استهلاك الذاكرة وزمن التنفيذ والامان، ومن خلال هذه الدراسة يمكن تقديم أسهاما علميا يتمثل في نتائج مقارنات قابلة للتعميم وتسهم في توجيه خيارات التصميم الأمني للباحثين ودعم قراراتهم بمدى جاهزية هذه الخوارزميات للاستخدام الفعلي في متطلبات امان مختلفة .

2. الدراسات السابقة

- مخططات الاتصالات الامنة للطائرات بدون طيار في تقنية الجيل الخامس Secured Schemes for UAVs in 5G (Communication) :

تُقدّم هذه الورقة بنية اتصالات آمنة للطائرات بدون طيار والمحطات الأرضية في شبكات الجيل الخامس، مُعالجةً التحديات الحرجة في أمن الشبكات. يدمج الحل المُقترح معيار التشفير المُتقدم (AES) وCRYSTALS-Kyber لتغليف المفاتيح، مُقدّمًا نموذج تشفيري هجين حيث يُخفّف الهجمات الكمومية،

تعتمد البنية على نموذج خادم-عميل، حيث تعمل الطائرات بدون طيار كعميل والمحطة الأرضية كخادم تُؤكّد النتائج التجريبية أن CRYSTALS-Kyber يُوفّر حماية قوية ضد التهديدات الكمومية مع الحد الأدنى من تكاليف الأداء، مما يجعله مُناسبًا للغاية للطائرات بدون طيار ذات الموارد المحدودة. وهذا بفضل دمجها مع معيار التشفير المتقدم AES

- تحليل الأداء لخوارزميات التشفير ما بعد الكم في الصناعة (Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms)

تستعرض الورقة دمج خوارزميات ما بعد الكم في صناعة الاتصالات مع التركيز على خوارزميتي ما بعد الكم CRYSTALS-Kyber وCRYSTALS-Dilithium حيث تستخدم

لتبادل المفاتيح والتوقيعات الرقمية ضمن انظمة المصادقة تقارن الدراسة اداء CRYSTALS– Kyber و CRYSTALS–Dilithium مع AES و ECDSA (خوارزميات تقليدية) من حيث سرعة توليد المفاتيح حيث يظهر ان Kyber و Dilithium يحققان اوقات تنفيذ فعالة ، مع الحاجة الماسة الي اجراء تعديلات في البنية التحتية للشبكة .

- معيار CRYSTALS– Kyber وتقنية تبادل المفاتيح القائم على الشبكات والامن ضد هجمات النصوص المشفرة (CRYSTALS–Kyber : Secure model– lattice – based KEM) بحث أساسي يشرح بالتفصيل تصميم CRYSTALS –KYBER وطريقة التشفير وفق هذا المعيار بالإضافة الي تقييم امانه ضد الهجمات الكمومية المحتملة ، وتوضيح أهمية تطوير الحوسبة الكمومية خصوصا بعد اعلان NISTعن الحاجة الي معايير جديدة للتشفير الرقمي .
- تقرير شامل من (NIST) حول خوارزميات ما بعد الكم ومقارنتها بالمعايير التقليدية مثل معيار AES ومعيار RSA ( ) report on post quantum cryptography NIST (national institute of standards and Technology) : قدم تقرير حول تأثير الحوسبة الكمومية على طرق التشفير التقليدية وضرورة التركيز على تطوير خوارزميات مقاومة للكم .
- مفهوم التشفير الهجين (Hybrid Cryptography Conference) : تقرير يناقش مفهوم التشفير الهجين وطرق استخدامه كوسيلة انتقالية من الخوارزميات التقليدية الي خوارزميات ما بعد الكم .

2.1. **التشفير التقليدي:** طرق قديمة تستخدم لحماية البيانات عن طريق تحويلها إلى صيغة غير قابلة للقراءة وذلك بالاعتماد علي مفتاح (مفتاح التشفير وفك التشفير) حيث يتم إدخال البيانات المراد تشفيرها وتقوم الخوارزمية بتحويلها إلى نص مشفر باستخدام مفتاح معين ، حيث يكون هذا النص غير قابل للقراءة ، ثم تُستقبل هذه البيانات ويتم فك تشفير النص باستخدام نفس المفتاح (مفتاح التشفير وفك التشفير)

2.2. **خوارزمية التشفير المتماثل المتقدمة:(AES)** تعتبر من أهم خوارزميات التشفير التقليدي وهي خوارزمية واسعة الاستخدام مصممة لحماية البيانات الحساسة، تتميز بكفاءتها وأمانها وتعدد استخداماتها، مما يجعلها معيارًا عالميًا لتأمين المعلومات الرقمية. وخنا بعض التطبيقات الشائعة لمعيار التشفير (AES):

- الاتصالات الآمنة: من خلال تشفير البيانات المنقولة عبر الإنترنت أو الشبكات الخاصة. مثل: VoIP حيث يقوم بتأمين مكالمات الصوت والفيديو عن طريق تشفير بيانات الصوت والفيديو، HTTP يُستخدم في متصفحات الويب لتأمين البيانات المتبادلة بين مواقع الويب والمستخدمين
- تشفير الملفات والأقراص: يحمي الملفات وقواعد البيانات الحساسة المخزنة على الأجهزة الشخصية أو في السحابة.
- تشفير الأقراص ووسائط التخزين حيث يعتبر معيار AES الأساس لتقنيات تشفير القرص الكامل، حيث يعمل على حماية البيانات الموجودة على محركات الأقراص الصلبة وأجهزة التخزين.
- أمن الشبكات اللاسلكية: يتم استخدام AES في بروتوكولات الأمان اللاسلكية لحماية البيانات المنقولة عبر شبكات Wi-Fi. مثل WPA2: حيث يُشفّر AES حركة البيانات اللاسلكية لمنع التنصت أو التلاعب.
- التطبيقات الحكومية والعسكرية: تمت الموافقة على AES من قبل حكومات بعض الدول لتأمين المعلومات الحساسة والسرية.
- أنظمة الدفع والمعاملات المالية: توفر AES حماية للبيانات المالية الحساسة أثناء معالجة الدفع والمعاملات عبر الإنترنت. أمثلة لذلك: خدمات المصرفية الإلكترونية والمحافظ الرقمية.
- أمن التخزين ألسحابي: يقوم AES بتشفير البيانات المخزنة في بيئات السحابة لحمايتها من الوصول غير المصرح به. تستخدم خدمات مثل Google Drive وDropbox وبروتوكول AES لتأمين ملفات المستخدم.
- أدارة كلمة المرور: يقوم AES بتشفير كلمات المرور المخزنة في أدوات إدارة كلمات المرور، تستخدم برامج إدارة كلمات المرور مثل Pass Last نظام AES لتأمين بيانات الاعتماد المحفوظة.
- انترنت الأشياء: حيث يستخدم AES لتشفير البيانات المتبادلة بين الأجهزة الذكية المنزلية وخوادم التحكم.
- تطبيقات البرمجيات: يُستخدم معيار التشفير (AES) لتأمين بيانات التطبيقات. مثل تشفير البيانات في تطبيقات المراسلة مثل واتساب وتيليجرام.
- الرعاية الصحية والسجلات الطبية: تحمي AES السجلات الصحية الإلكترونية ومعلومات المرضى الحساسة لضمان الامتثال للوائح وكذلك تشفير ملفات المرضى في أنظمة المستشفيات.
- النسخ الاحتياطي للبيانات والأرشفة: يضمن AES أمان بيانات النسخ الاحتياطي لمنع الوصول غير المصرح به،

2.3. **الحوسبة الكمومية:** هي تقنية حديثة تعتمد على مبادئ ميكانيكا الكم لمعالجة البينات بدلا من استخدام البتات التقليدية (0-1) تستخدم الكيوبتات (Qubits) التي يمكن ان تكون (0و1) في نفس الوقت بسبب ظاهرة التراكب الكمومي حيث تسمح هذه الخاصية بإجراء عملية معقدة بسرعة عالية في مجالات متعددة مثل التشفير والذكاء الاصطناعي

2.4. **خوارزميتي AES وCRYSTALS والهجمات الكمومية:**

الخطر الأساسي لخوارزمية AES هي خوارزمية غروفر(خوارزمية كمومية) تقوم هذه الخوارزمية بالبحث غير المنظم والسريع عن مفتاح التشفير ، والتقليل من الوقت المطلوب لإيجاده ، ويعتبر مضاعفة طول المفتاح حل مؤقت وتوفير مسافة امان فقط، ولذلك لا ينصح باستخدام معيار التشفير المتماثل AES في البيانات الطويلة المدى .

هجوم (KayberSlash) : حدث هذا الهجوم للمرة الاولي على الخوارزميات الكمومية المعتمدة عام 2023 وأدى الي عمل تحديث عاجل من نسخة كريستال لدي المعهد الوطني للمعايير والتكنولوجيا (NIST) حيث يقوم الهجوم بأنشاء نصوص مشفرة خبيثة مكررة ويراقب المهاجم الوقت المستهدف لفك تشفير هذه النصوص وعن طريقه يتحصل علي معلومات جزئية عن المفتاح السري مع تكرار العملية عدة مرات يتحصل علي المفتاح السري بالكامل ، قام التحديث بوضع حد لهذه الثغرة من خلال توحيد ازمنة التنفيذ وهي تقنية تعرف ب (التنفيذ ذو الوقت الثابت).

2.5. مفاهيم مهمة في الحوسبة الكمومية:

- التراكب الكمومي (Quantum superposition):

هو قدرة الحواسيب الكمومية على معالجة كم هائل من البيانات بشكل متوازي مما يمنحها قوة حسابية هائلة، فالحوسبة التقليدية البت (Bit) يمكن أن يكون 0 أو 1 فقط، أما في الحوسبة الكمومية فان وحدة المعلومات الأساسية هي الكيوبت (Qubit) والتي يمكن أن تكون في الحالة 0 أو 1 أو مزيج من الحالتين في نفس الوقت

- الكيوبت(Qubit) :

هو الوحدة الأساسية للمعلومات في الحوسبة الكمومية، وهو يعادل البت في الحوسبة التقليدية، ولكن مع قدرات إضافية تسمح له بتمثيل وتخزين معلومات أكثر من البت التقليدي

- التشابك الكمومي (Quantum Entanglement):

يحدث التشابك الكمومي عندما يرتبط كيوبتان يبعضهما البعض، حيث ان معرفة حالة أحدهما تلقائيا تعنى معرفة حالة الأخر حيث تستخدم هذه الظاهرة في الحوسبة الكمومية لربط الكيوبتات داخل المعالج مما يسمح بتنفيذ عمليات متوازية كما تتيح انشاء قنوات اتصال آمنة بين الأجهزة.

- التشفير ما بعد الكم:(Post-Quantum Cryptography) هو مصطلح يشير إلى تطوير خوارزميات تشفير جديدة قادرة على مقاومة الهجمات التي قد تشنها الحواسيب الكمومية المستقبلية .يهدف هذا النوع من التشفير إلى حماية البيانات والمعلومات الحساسة من التهديدات المحتملة التي تشكلها أجهزة الكمبيوتر الكمومية، ظهرت الحاجة الي هذا النوع من التشفير لقدرة الحواسيب الكمومية على كسر المسائل الرياضية المعقدة التي تعتمد عليها الخوارزميات التقليدية،
- خوارزمية ما بعد التشفير الكمي (CRYSTALS-Kyber): واحدة من أهم خوارزميات تشفير بعد الكم، أي أنها آمنة ضد الحواسيب الكمومية وتم اختيارها من قبل المعهد الوطني للمعايير التقنية كخوارزمية مستقبلية قياسية لتأمين البيانات في عصر الحوسبة الكمومية.

2.6. المفاهيم الأساسية التي تقوم عليها خوارزميات التشفير ما بعد الكمي:

- التشفير القائم على التجزئة (**Hash-based cryptography**): هو نوع من التشفير يستخدم دوال التجزئة كأساس للأمان بدلا من العمليات الرياضية المعقدة ، حيث يتم تحويل مدخل أي رسالة الى قيمة ثابتة الطول لا يمكن عكسها هذه القيمة يتم استخدامها لأنشاء تواقيع رقيمة او مفاتيح مصادقة آمنة.
- التشفير القائم على أساس شبكي (**Lattice-based cryptography**): تعتمد هذه الخوارزميات على مشاكل رياضية صعبة ترتبط بالهياكل الشبكية في الرياضيات، والمقصود بالشبكة هنا هو نظام متعدد الأبعاد موزع بشكل منتظم تستخدم هذه الشبكات لحل مسائل مثل إيجاد أقرب نقطة معينه في الشبكة، استغلال الضوضاء في المعادلات لإخفاء البيانات.
- التشفير القائم على الكود (**Code-based cryptography**): التشفير القائم على الكود هو نوع من التشفير يعتمد على أكواد تصحيح الأخطاء لتأمين البيانات .يستخدم هذا النوع من التشفير أكوادًا خاصة، غالبًا لتصحيح الأخطاء، ولتحويل البيانات إلى شكل مشفر يصعب فك تشفيره دون المفتاح المناسب.

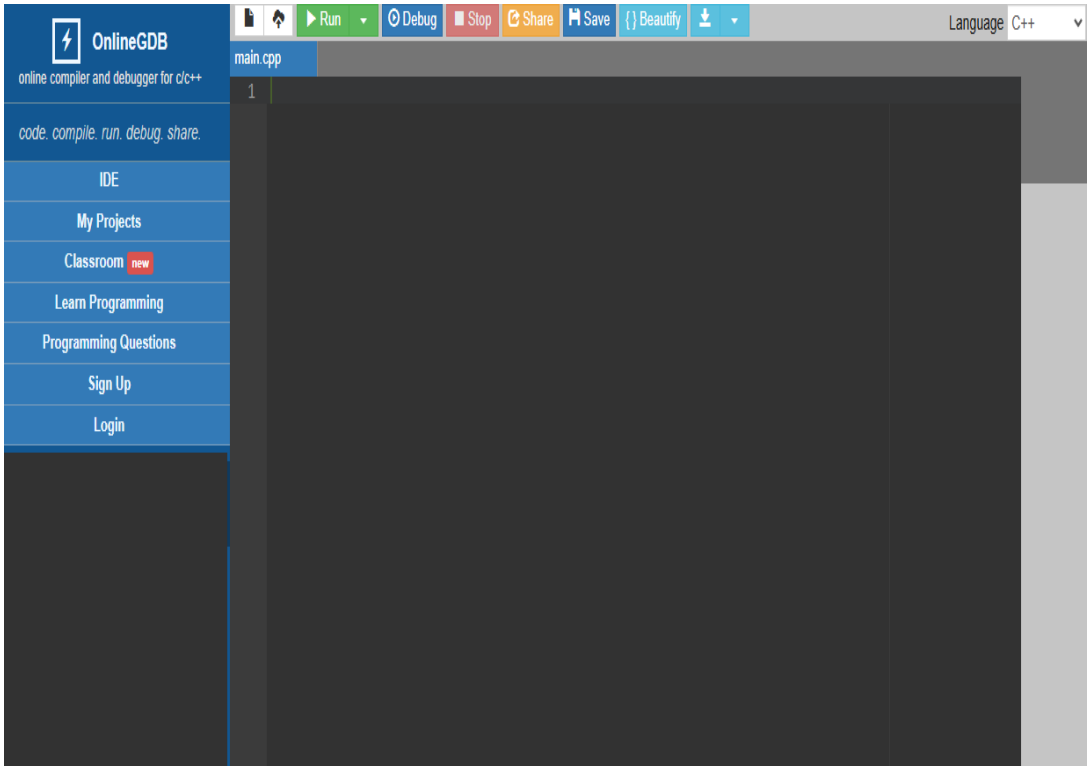
2.7. مراحل مشروع المعهد الوطني للمعايير والتكنولوجيا (national institute standard technology) لاعتماد تشفير ما بعد الكم:

- عام 2016: أطلق NIST مشروع مفتوح لتقييم وتوحيد خوارزميات ما بعد الكم ودعي كافة الباحثين لتقديم مقترحات جديدة.
- بين عامي 2017 _ 2022: تلقى المعهد أكثر من 80 خوارزمية مرشحة تم تقييمها على 3 جولات.
- عام 2022: الإعلان عن الخوارزميات التي تم قبولها وسيتم توحيدها وكان من ضمن الخوارزميات لتشفير المفاتيح خوارزمية CRYSTALS-Kyber

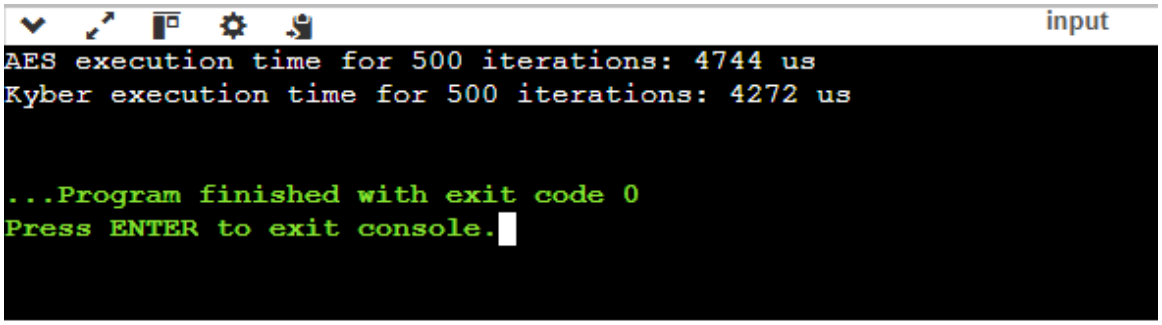
- من عام 2022 _ الآن: استقبال وتقييم خوارزميات إضافية لتوسيع الخيارات.

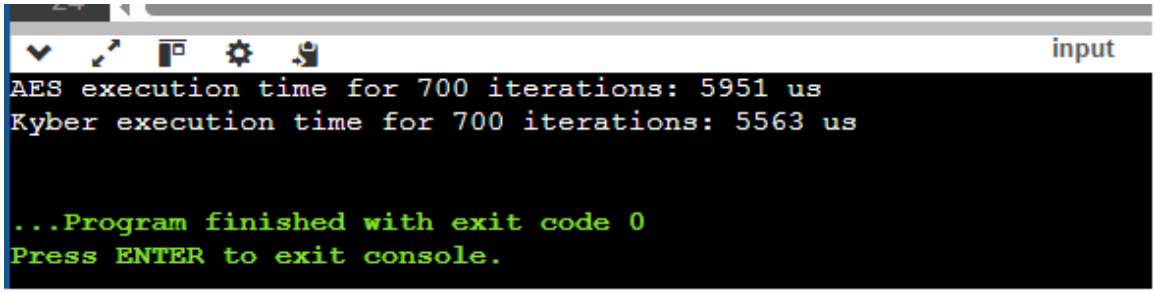
3. منهجية البحث

- منهجية البحث التي استخدمت في هذه الورقة تعتمد على المنهج التحليلي العملي المقارن والذي يجمع بين التحليل النظري والتطبيق العملي ،تمتاز هذه المنهجية بالموضوعية حيث النتائج فيها تعتمد على تنفيذ عملي وقياس مباشر ، وشملت هذه المقارنة :
  - الأداء الحسابي الذي يتمثل في (زمن التشفير وفك التشفير) وهو الوقت الذي تستغرقه الخوارزمية في معالجة البيانات
  - استخدام الذاكرة المتمثلة في سعة الذاكرة المطلوبة لتخزين المفاتيح والعمليات.
  - الأمان وذلك بتطبيق أطوال مختلفة لمفاتيح التشفير لخوارزمية AES .
  - قابلية الاستخدام في انترنت الأشياء وربطها باستخدام الذاكرة حيث تُعرف أجهزة انترنت الأشياء بذاكرتها المحدودة بالتالي صعوبة استخدامها مع خوارزميات تتطلب ذاكرة أكبر .
- بيئة الاختبار: تم اختبار خوارزميتي AES وCRYSTALS–Kyber على جهاز بنظام تشغيل Windows 10 ، والتطبيق البرمجي باستخدام بيئة تشغيل وتنقيح كود c++ عبر الانترنت (OnlineGDB) ، بالإضافة الى مكتبات AES تم استخدام مكتبة (OPENSSL) ، مكتبات CRYSTALS تم استخدام مكتبة (Chrono) .



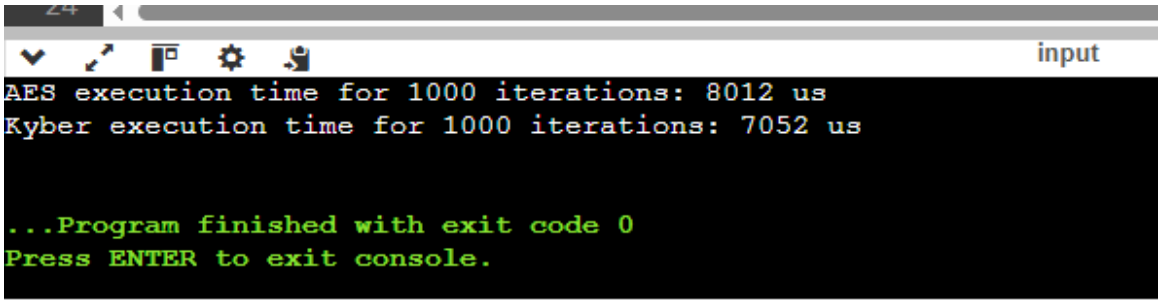
الشكل يوضح بيئة تشغيل الكود البرمجي عبر الانترنت



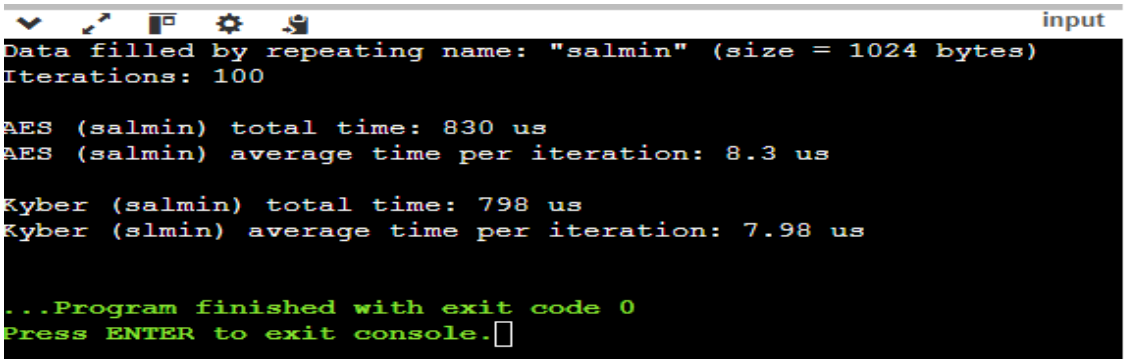


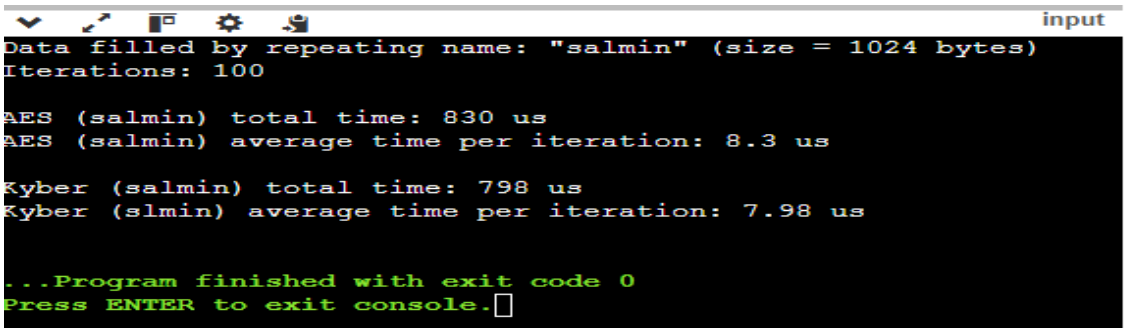
- **المعايير المستخدمة لتقييم الأداء :**

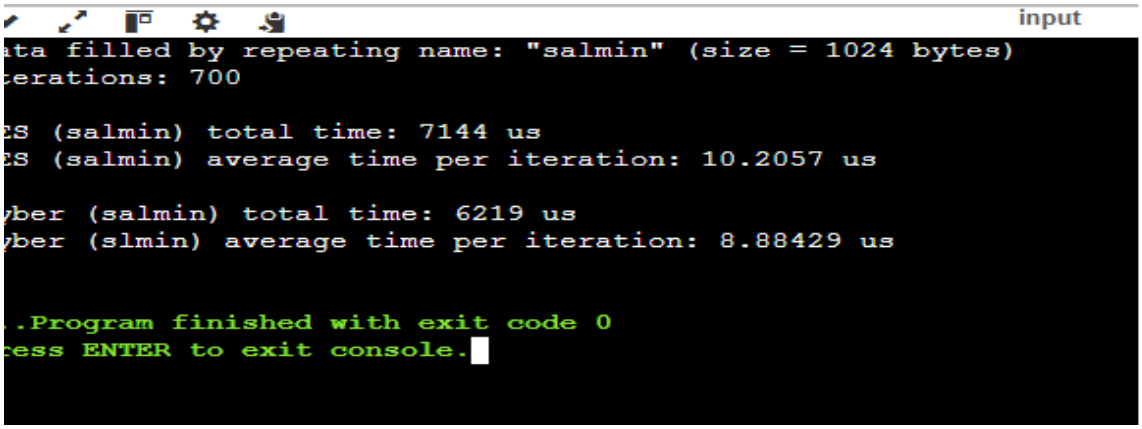
1. زمن التنفيذ : حيث تم قياس زمن التشفير وفك التشفير لكل خوارزمية على نفس حجم البيانات . في المرة الاولي تم استخدام vector لقيم مصفوفة من مجموعة اعداد ، وتم تغيير عدد التكرارات (500–700–1000) حيث تمثل التكرارات عدد مرات التشفير حيث يقوم البرنامج بتوليد مفتاح تشفير في كل تكرار .

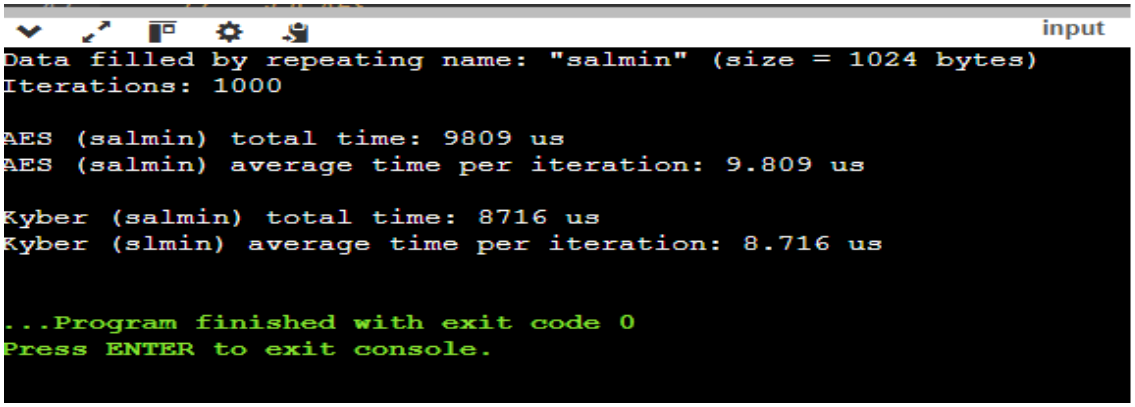


في المقارنة الثانية تم استخدام اسم ، وأعاده التكرارات وتسجيل الوقت .



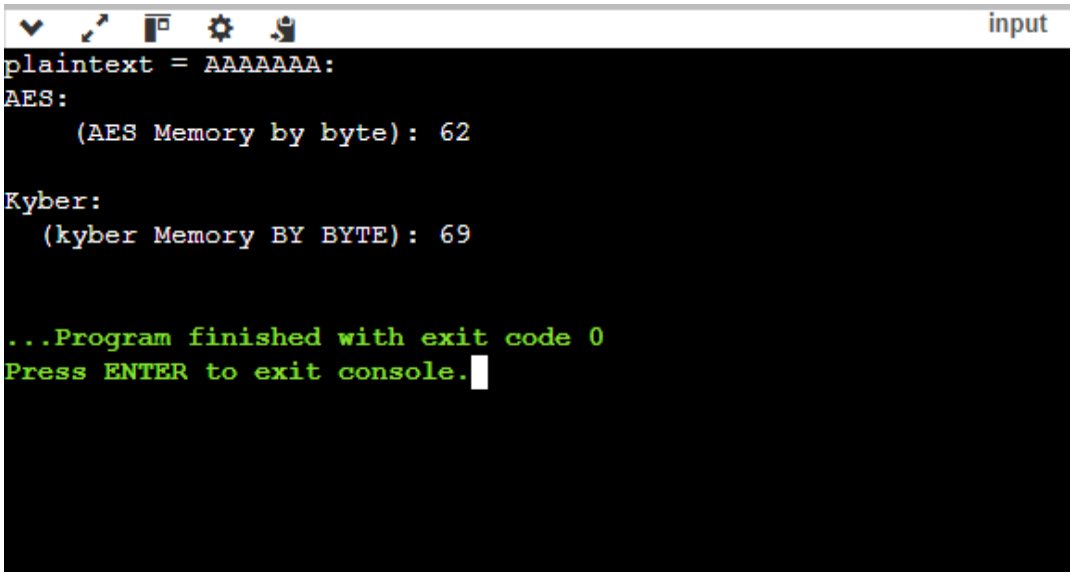


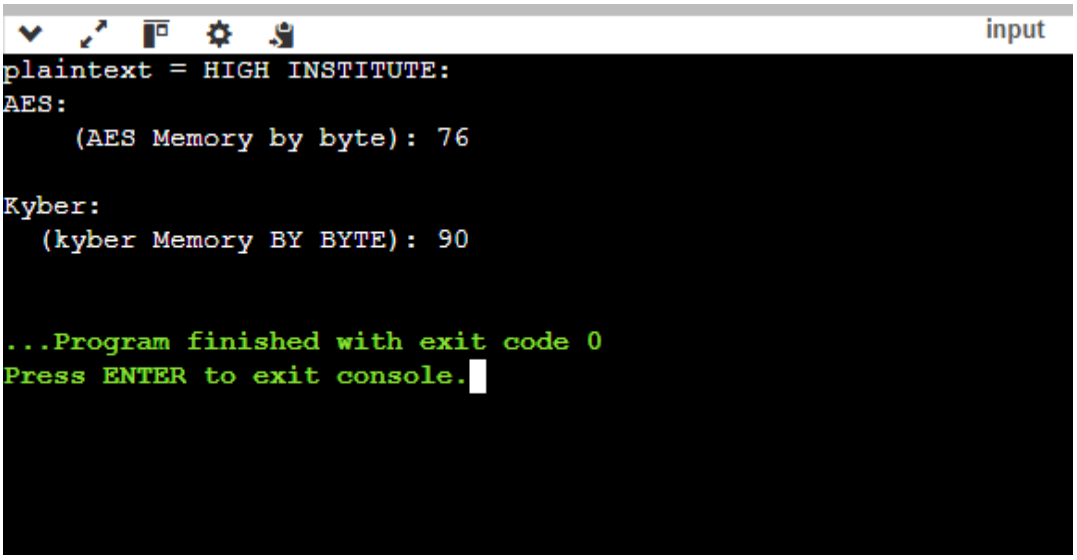


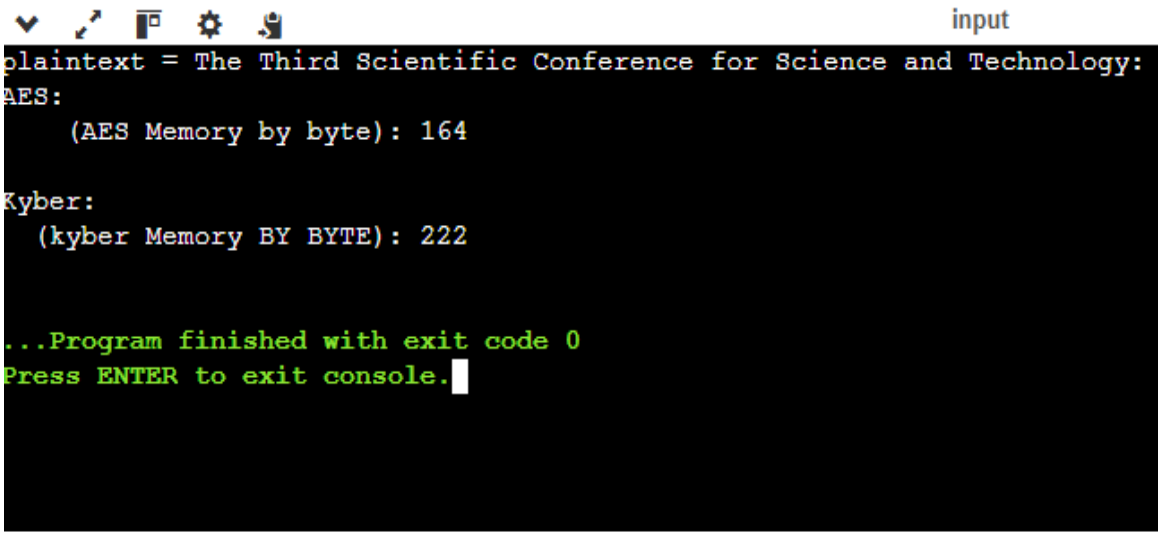


حيث يمثل الزمن الأول لكل خوارزمية الوقت الكامل للتنفيذ ، والوقت الثاني يمثل وقت التنفيذ لكل تكرار .الزمن يشمل (تسجيل وقت البدء – تنفيذ التشفير – تسجيل الوقت بعد الانتهاء – حساب الفرق بين الزمنين) تكرار العملية عدة مرات ،، مثلا (100– 500) ، ثم تكرار نفس الخطوات لفك التشفير .

2. استهلاك الذاكرة : وهي حجم الذاكرة التي تستخدمها الخوارزمية اثناء التنفيذ ، حيث تم ادراج نصوص مختلفة وقياس حجم الذاكرة المستهلكة اثناء التشفير وفك التشفير .







3. تقييم الأمان لخوارزمية (AES) : استخدام اطوال مفاتيح (32 – 56 – 64 ..... 512) حيث يتم تحديد المفاتيح المحتملة والوقت المحتمل لكسر الخوارزمية .

Compiled Successfully. memory: 4096 time: 0 exit code: 0

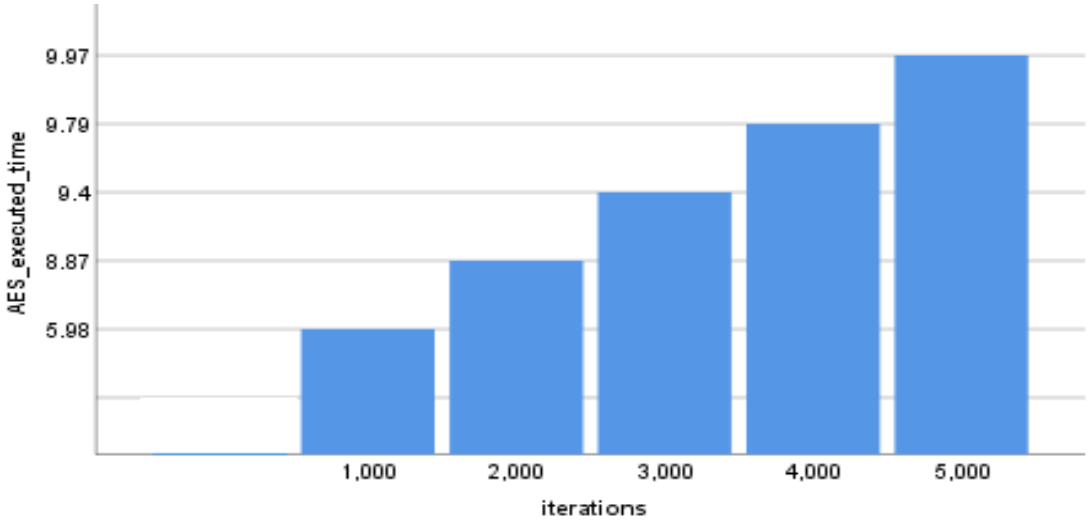
Key Size	Possible Keys (2^n)	Crack Time (Years)
32	4.295e+09	1.361e-07
56	7.206e+16	2.283e+00
64	1.845e+19	5.845e+02
80	1.209e+24	3.831e+07
96	7.923e+28	2.511e+12
112	5.192e+33	1.645e+17
128	3.403e+38	1.078e+22
160	1.462e+48	4.631e+31
192	6.277e+57	1.989e+41
224	2.696e+67	8.543e+50
256	1.158e+77	3.669e+60
512	1.341e+154	4.249e+137

4. النتائج والتحليل

في الشكل 1 ، تم اختبار زمن التنفيذ لخوارزمية (AES)، وذلك بتكرار تنفيذ الخوارزمية عدة مرات أي تكرار توليد مفتاح التشفير عدة مرات والحصول على ازمنة مختلفة. وذلك لضمان حساب متوسط زمن التنفيذ بدقة، ولمقارنة عادلة بين الخوارزميتين.

- لماذا لا يمكن احتساب الزمن بدون تكرارات؟

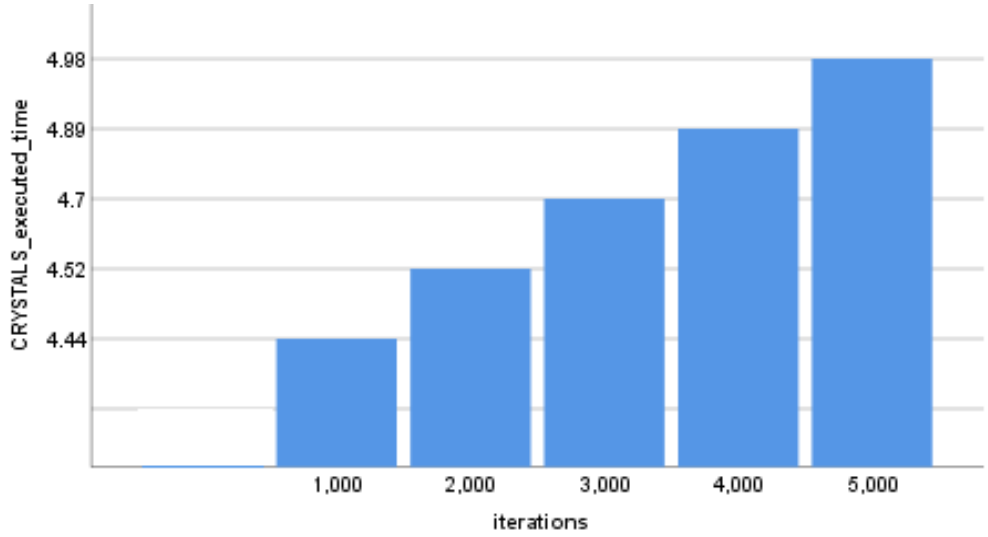
لان عملية تشفير واحدة فقط قد تستغرق ميكروثانية، وهذا الزمن غير دقيق لأنه يجب حساب زمن تأخير المعالج والذاكرة، كما لا يمكن تحديد المتوسط لزمن التنفيذ، إذا لابد من تكرارات متعددة لنتائج أدق.



شكل 1

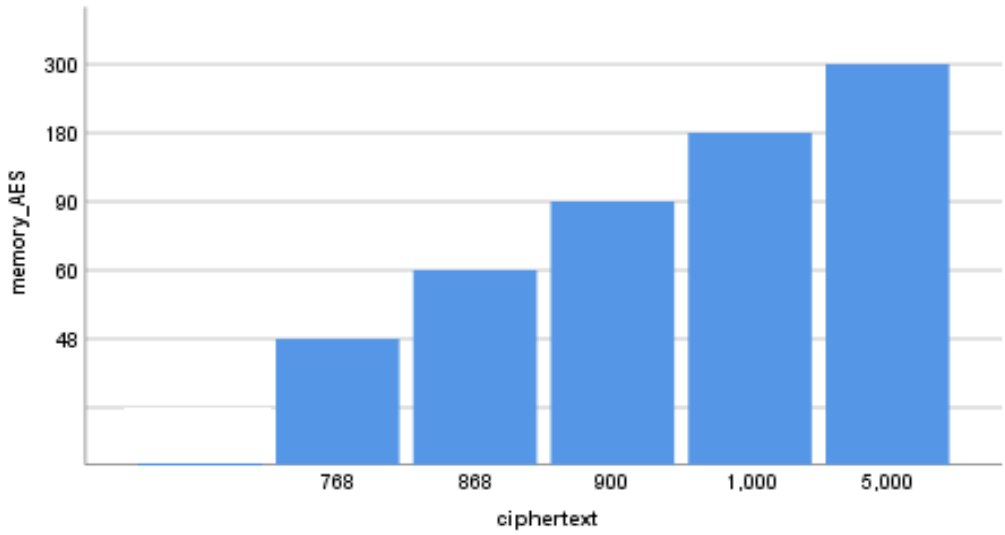
في الشكل 2 تم اختبار زمن التنفيذ لخوارزمية (KyberCRYSTALS–) وبأتباع نفس الخطوات ونلاحظ ان زمن التنفيذ يختلف مع الحفاظ علي نفس التكرارات .

نلاحظ من خلال المقارنتين ان خوارزمية (KyberCRYSTALS–) تحتاج وقت اقل في التنفيذ ، بينما وقت تنفيذ اكبر لخوارومية (AES) الكلاسيكية .



شكل 2

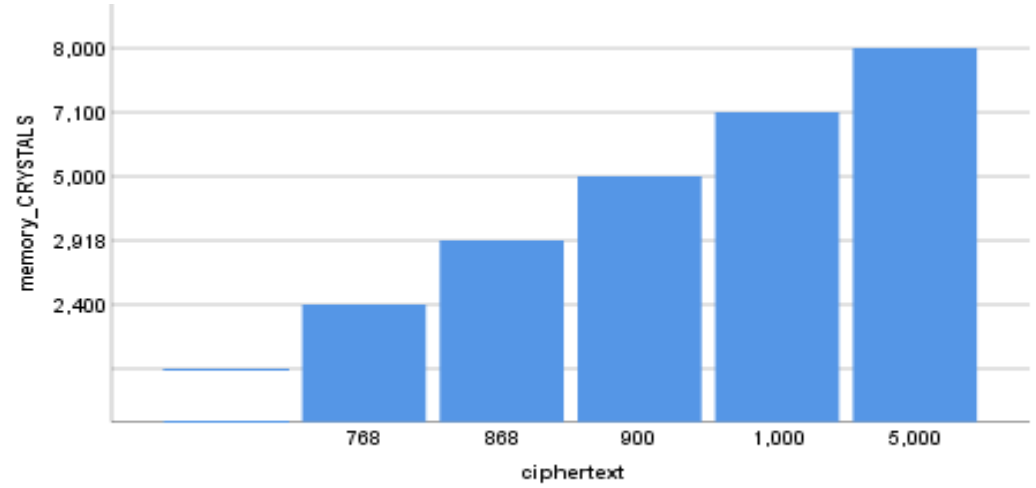
في الشكل 3 ، خوارزمية (AES) يوضح طول النص المشفر وعلاقته باستهلاك الذاكرة، حيث تم اختبار عدة أطوال مختلفة للنص المشفر والناتج من الذاكرة المستهلكة بالبايت (Byte)،



شكل 3

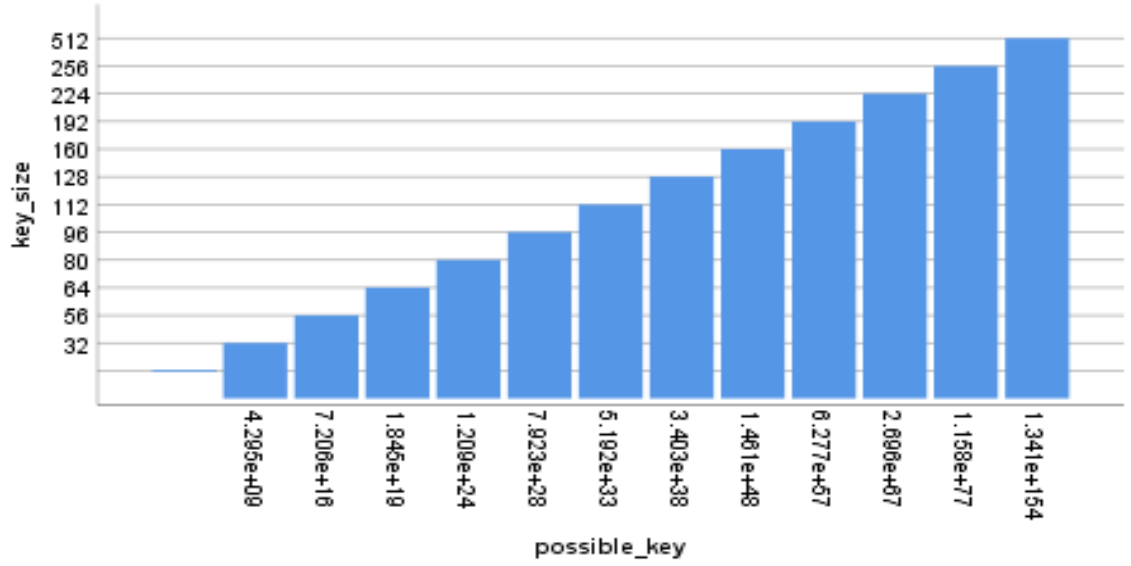
وهنا في الشكل 4، نفس الاختبار لخوارزمية (CRYSTALS–Kyber) مع توضيح استهلاك الذاكرة المستخدمة مع كل طول للنص المشفر.

نلاحظ من المقارنتين ان خوارزمية (CRYSTALS) تستهلك ذاكرة اكبر وذلك لان تركيبتها الرياضية والمفاتيح المستخدمة اكبر وتشفيرها قائم علي أساس شبكي فهي تستخدم مصفوفات ذات حجم كبير بالتالي تحتاج حيز اكبر في الذاكرة ، بينما خوارزمية (AES) تستخدم مفتاح تشفير متماثل فقط وعمليات حسابية بسيطة فاستهلاكها اقل .



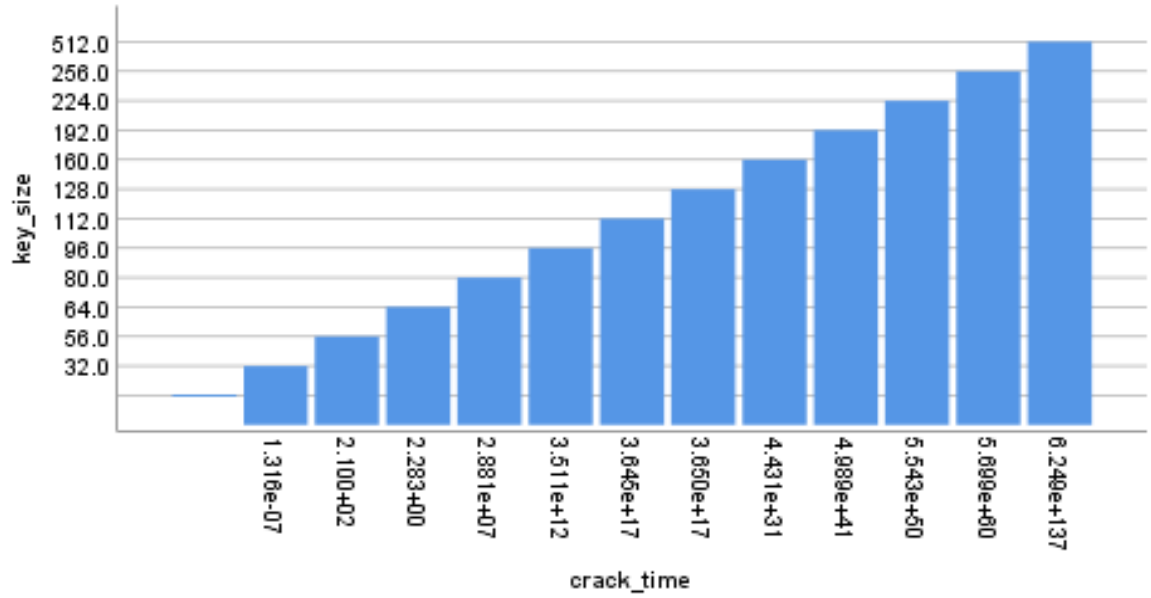
شكل 4

في الشكل 5 ، تم اختبار الأمان لخوارزمية (AES) حيث يقوم المهاجم بتجربة كل المفاتيح الممكنة ((KEY SIZE ، فكلما زاد طول المفتاح زاد عدد الاحتمالات (possible key) وبالتالي يصبح كسر المفتاح أصعب



شكل 5

وهنا في الشكل 6 ، نجد تناسب طردي بين الزمن اللازم لكسر مفتاح التشفير مع طول المفتاح. فكلما زاد طول المفتاح زاد الزمن المتوقع لكسر تشفير المفتاح.



شكل 6

- اختبار الأمان لخوارزمية (CRYSTALS-Kyber) :

لان تحديد مستوي الأمان في الخوارزميات ما بعد الكم لا يتم بكسر مفتاح التشفير، ذلك لأنها مصممة اعتمادا على مشاكل رياضية معقدة، بالتالي لا يمكن كسر هذه المفاتيح لا نظريا ولا عمليا، بالإضافة الي ان امان خوارزمية (CRYSTALS-Kyber) تم تقييمه نظريا بواسطة المعهد الوطني للمعاير

والتكنولوجيا (NIST) حيث وضع الخوارزمية تحت الاختبار لأكثر من 5 سنوات ولم تسجل حالة كسر للتشفير الي وقتنا الحالي.

- خوارزميتي (AES) (CRYSTALS-Kyber) وقابلية الاستخدام في انترنت الأشياء (IOT):

من خلال تجربة استهلاك الذاكرة يسهل تقييم مدى قابلية الخوارزميتين للاستخدام في أجهزة انترنت الأشياء التي تصنف اغلبها بقدرات محدودة للمعالج وانخفاض الذاكرة ووصول محدود للشبكة بالإضافة الي تقييد في الطاقة (ذلك لان اغلبها تعمل بالبطارية)، وهذا يجعل قابلية تطبيق خوارزميات التشفير ما بعد الكم صعب نسبيا، حيث تحتاج اغلبها لمساحة تخزينية كبيرة ومعالج لتنفيذ العليات الرياضية المعقدة، وتطبيقات مدعومة بالطاقة بشكل متصل وهنا يأتي دور خوارزميات الكلاسيكية التي تتلاءم مع أجهزة انترنت الأشياء، حيث تعتبر مثالية في اغلب التطبيقات. وهنا مقارنة بسيطة بين الخوارزميتين في استخدامهما في انترنت الأشياء:

المقارنة	خوارزمية AES	خوارزمية CRYSTALS-Kyber
نوع الخوارزمية	تماثلية	غير تماثلية
زمن التشفير وفك التشفير	سريع	بطيء
الامان	ممتاز ضد الهجمات الكلاسيكية فقط	عالي ضد الهجمات الكمومية
استهلاك الطاقة	اقل	أكبر
استهلاك الذاكرة	اقل	أكبر
الحاجة للطاقة	منخفضة	مرتفعة نسبيا
الملائمة IOT	ممتاز ولكن بأمان ضعيف	يحتاج الي تحسين موارد وبأمان أكبر

- من خلال النتائج السابقة يمكن تحليل نقاط الضعف والقوة لكل خوارزمية من حيث الأمان، واستهلاك الموارد، والزمن اللازم للتنفيذ.

- الأمان:

تعتبر خوارزمية (AES) موثوقة ومجربة منذ عقود لكنها غير مقاومة للهجمات الكمومية، فهي مناسبة أكثر للبيئة الكلاسيكية (بيئة غير معرضة للهجوم الكمي).

بينما تعتبر خوارزمية (CRYSTALS–Kyber) ذات اعتماد أقوى فهي مقاومة للهجمات الكمومية بالتالي مناسبة لبيئة الأجهزة الكمومية.

- استهلاك الذاكرة والموارد:

تحتاج خوارزمية (AES) ذاكرة اقل فهي ملائمة للأجهزة ذات القدرات المحدودة مثل الحساسات الصغيرة وأجهزة انترنت الأشياء.

بينما تحتاج (CRYSTALS–Kyber) ذاكرة أكبر فهي مناسبة في بيئة الأجهزة الكمومية.

- زمن التنفيذ:

خوارزمية (AES) سريعة التنفيذ عند استخدام مفاتيح متوسطة الطول، وتكون ابطأ في حالة استخدام مفاتيح أطول مثل (256 BIT) .

بينما خوارزمية (CRYSTALS–Kyber) تتفوق في التنفيذ في بيئة أنظمة ما بعد الكم.

5.المناقشة

تظهر نتائج المقارنة ان خوارزمية AES تتميز بالسرعة في المفاتيح المتوسطة الطول واستهلاك منخفض في الموارد مما يجعلها مثالية لتشفير البيانات اليومية مثل استخدامها في أجهزة انترنت الأشياء وتطبيقات الدفع الإلكتروني،

حيث ان في حالة أجهزة انترنت الأشياء نجد انها خفيفة على الموارد ذات استهلاك ذاكرة اقل ، وفي حالة تطبيقات الدفع الالكتروني نجد انها سريعة التنفيذ مثالية للمعاملات الفورية .

اما خوارزمية CRYSTALS–Kyber توفر أمانا مقاوما للهجمات الكمية (وهذا ما أكده NIST الذي أكد جاهزية الخوارزمية لتوحيدها كمعيار مقاوم للأجهزة الكمية) مما يجعلها الخيار الأفضل لتبادل المفاتيح من خلال انشاء مفتاح سرى مشترك بين طرقي قناة الاتصال ، بالإضافة الي حماية البيانات الحساسة مثل بيانات الهوية والمعلومات الطبية والبيانات البنكية ،

- تحديات مرتبطة ب CRYSTALS–Kyber: استهلاك الذاكرة الأعلى وزمن التشفير الأطول قد يكون مقبول علي الأجهزة القوية لكن يمثل تحديا للأجهزة منخفضة الطاقة ومن هنا نجد ضرورة

تحديث البنية التحتية للأنظمة الحالية لدعم التشفير ما بعد الكم . وللتعامل مع هذه التحديات يجب ان :

1- في أجهزة منخفضة الطاقة نستخدم CRYSTALS لتبادل المفاتيح الامنة واستخدام AES لتشفير البينات الفعلية لضمان سرعة الأداء وكفاءة الطاقة .

2- في حالة البيانات الحساسة كالتطبيقات المالية والبيانات الطبية استخدام CRYSTALS لتبادل مفتاح الجلسة بين الخادم والعميل واستخدام AES لتشفير باقي المعاملات اليومية .

3- البيانات طويلة الأمد او عالية الحساسة مثل السجلات الطبية التي يجب حفظها مدى الحياة للمريض والبيانات الحكومية والعسكرية وبيانات البنية التحتية الحيوية كأنظمة الطاقة والاتصالات يجب اعتماد CRYSTALS لتشفير البيانات والتوقيعات الرقمية لضمان بقاء الحماية صالحة على المدى البعيد .

ختاما نجد من خلال النتائج اهمية التوجه نحو التحول التدريجي للتشفير ما بعد الكم وذلك لسهولة كسر الخوارزميات التقليدية والتي قد تكون مستخدمة في بيانات حساسة ، بالإضافة الي الاعتماد الكامل اليوم علي البيانات الرقمية في كافة المجالات يجعل التهديد اكبر في حال ظهور وانتشار الأجهزة الكمية بشكل رسمي ، والتحول نحو التشفير ما بعد الكم يحتاج الي بنية تحتية رقمية قوية وجديدة وهذا التحول سيكون صعب بشكل مباشر وهنا تبرز أهمية التشفير الهجين (Hybrid Encryption) كحل انتقالي بدمج خوارزميتي AES و CRYSTALS-Kyber والذي يحقق التوازن بين السرعة والأمان .

6 .التوصيات:

- تأهيل وتدريب المجموعات المستهدفة المتمثلة في المطورين والفرق الأمنية على استخدام وفهم خوارزميات ما بعد الكم ومتابعة أي تحسينات او إصدارات، بالإضافة الي التدريب على نماذج المحاكاة للخوارزميات قيد الاختبار من قبل المعهد الوطني للمعايير والتكنولوجيا.
- مواكبة التطور في مجال الأجهزة الكمية والذي من شأنه قد يحدد نقطة النهاية للتشفير الكلاسيكي في أي وقت.
- تطوير أجهزة ملائمة للتشفير ما بعد الكم وذلك من خلال التركيز على نقاط الضعف لخوارزميات التشفير الكمية، كتطوير أجهزة انترنت الأشياء لتكون ملائمة من الناحية التشغيلية والتخزينية.
- تطبيق التشفير الهجين حيث يمكن اعتباره مرحلة انتقالية وبداية التحول نحو التشفير ما بعد الكم، مما يعطي تقبلا واستعدادا للتغيير الكلي نحو التشفير ما بعد الكم.

7 .الخاتمة

من خلال هذه الدراسة تم تقديم نموذج بحثي لمقارنة منهجية وعملية بين جيلين مختلفين من خوارزميات التشفير وهما خوارزمية التشفير المتماثل (AES) وخوارزمية ما بعد التشفير الكمي (CRYSTALS–Kyber) ، حيث يسعي العمل البحثي على المستوي النظري والتطبيقي على قياس كفاءة كل خوارزمية من حيث الوقت واستهلاك الموارد ، فأظهرت (AES) انها لا تزال خيارا مناسبا من حيث الوقت واستهلاك الموارد ، بينما تعتبر (CRYSTALS–Kyber) الأفضل من حيث الأمان وهذا يجعلها تتفوق حيث لا أهمية للوقت والموارد في مواجهة الهجمات الغاشمة.

قائمة المراجع

1. National Institute of Standards and Technology (NIST). (2022). Post Quantum Cryptography Standardization. Retrieved from https://csrc.nist.gov/projects/post-quantum-cryptography

2. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. Nature, 549(7671), 188–194. https://doi.org/10.1038/nature23461

3. Bos, J. W., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., & Stehlé, D. (2018). CRYSTALS – Kyber: A CCA-secure Module-Lattice-Based KEM. In 2018 IEEE European Symposium on Security and Privacy (Euro S&P) (pp. 353–367). IEEE. https://eprint.iacr.org/2017/634.pdf

4. Daemen, J., & Rijmen, V. (2002). The Design of Rijndael: AES – The Advanced Encryption Standard. Springer.

5. Borgaonkar, R., & Niemi, V. (2018). Security for Internet of Things: Analysis of Existing Protocols and Open Challenges. In Proceedings of the 2nd International Conference on Cryptography, Security and Privacy (pp. 99–104). ACM. https://doi.org/10.1145/3199478.3199503

6. Al-Janabi, S., & Kadhim, H. (2020). A Comparative Study of Lightweight Cryptography Algorithms for IoT Applications. International Journal of Electrical and Computer Engineering, 10(1), 676–684.

7. Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). Report on Post-Quantum Cryptography (NISTIR 8105). National Institute of Standards and Technology.

https://doi.org/10.6028/NIST.IR.8105

8. Bindel, N., Buchmann, J., Krausz, L., & Struck, L. (2017). Hybrid Post-Quantum TLS. In Post-Quantum Cryptography (pp. 206–221). Springer, Cham.

https://doi.org/10.1007/978-3-319-59879-6_12

9. Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). The Next Generation of Security for the Internet of Things: Cryptography and Machine Learning. IEEE Access, 7, 464–488.

10. Bertoni, G., Daemen, J., Peeters, M., & Assche, G. V. (2005).

The Road from AES to Keccak: The Case for a New Standard.

NIST Workshop on Hash Functions

https://www.researchgate.net/publication/263336812_The_making_of_KECCAK

11.Zhao,Z.,Zhang,H., & LI,X.(2024) " An elementary review on basic principle and development of quantum entanglement
https://pmc.ncbi.nlm.nih.gov/articles/PMC10948723/

12. M. Barbosa, F. Dupressoir, A. Hülsing, M. Meijers, and P.-Y. Strub, “A Tight Security Proof for SPHINCS+, Formally Verified,” IACR ePrint Archive, Report 2024/910, 2024. [Online].
Available: https://eprint.iacr.org/2024/910

13. A. Sharma, R. Patel, and N. Kumar, “Comparative analysis of lattice-based cryptographic schemes for secure IoT communications,” Journal of Network and Systems Security, vol. 12, no. 3, pp. 145–158, 2024. [Online]. Available: https://link.springer.com/article/10.1007/s43926-024-00069-2

14. T. Sharma, S. A. Soleymani, M. Shojafar, and R. Tafazolli, "Secured Communication Schemes for UAVs in 5G: CRYSTALS-Kyber and IDS," *arXiv preprint arXiv:2501.19191*, 2025. [Online]. Available: https://arxiv.org/abs/2501.19191

15. D. D. Demir, B. Bilgin, and M. C. Onbasli, “Performance Analysis and Industry Deployment of Post-Quantum Cryptography Algorithms,” arXiv preprint arXiv:2503.12952, 2025. [Online]. Available: https://arxiv.org/abs/2503.12952