مجلة جامعة دمشق للعلوم الهندسية
المجلد 40- العدد 1 (2024) 75-86

Damascus University Journal for engineering sciences
Vol 40 No.1 (2024): 75-86

نماذج تشفير باستخدام خوارزميتي RSA وAES

علاء الدين الاحمد العلي[1]، د. رغد حيدري[2]

1طالب ماجستير- قسم الإحصاء ونظم المعلومات، كلية الاقتصاد، جامعة حلب.

2 مدرس في قسم الإحصاء ونظم المعلومات ـ كلية الاقتصاد ـ جامعة حلب.

الملخص

تعتبر عملية حماية البيانات بزمن تنفيذ قياسي هي الهدف الاساسي للباحثين في مجال حماية البيانات باستخدام آليات أو خوارزميات التشفير، انطلاقاً من هذا المفهوم تم اقتراح أربع نماذج لحماية البيانات النصية تعتمد هذه النماذج على خوارزميتي RSA وAES مع اضافة عمليات XOR إما مع كتلة نصية ثابته وهي الكتلة الأولى m_1 أو كتلة نصية ديناميكية متغيرة m_{i-1} وأعطت هذه النماذج درجة حماية أعلى من خوارزميتي RSA وAES من خلال حساب معدل الأنتروبي لكلٍ منها حيث بينت النتائج زيادة وتحسن قيمة الانتروبي للنماذج الأربعة عن قيمتها لخوارزميتي RSA وAES مما يثبت زيادة درجة حماية البيانات عند استخدام هذه النماذج وقد تم حساب متوسط زمن التنفيذ لإجراء التشفير وفك التشفير لهذه النماذج فتبين أن النماذج الأربعة ذات زمني تشفير وفك تشفير أقل من أزمنة خوارزمية RSA وتقارب أزمنة خوارزمية AES مما أثبت سرعة تنفيذ هذه النماذج المقترحة وقد بينت النتائج أن النموذج الأول هو الاسرع في حين أن النموذج الرابع هو الأعلى درجة حماية.

الكلمات المفتاحية: RSA، AES، التشفير، فك التشفير، أمن البيانات، نموذج تشفير.

تاريخ الإيداع: 2022/6/12
تاريخ القبول: 2022/8/23

Encryption models using RSA and AES algorithms

ALaeddin ALahmad ALali[1], Raghad Haidarey[2]

1Student, Master, Department of Statistics and Information Systems, Faculty of Economics, University of Aleppo.

2teacher in the Department of Statistics and Information Systems - Faculty of Economics - Aleppo University

Received: 12/6/2022
Accepted: 23/8/2022

Abstract

The process of data protection with a standard execution time is the main goal of researchers in the field of data protection using encryption mechanisms or algorithms. Based on this concept, four models for textual data protection have been proposed. These models depend on the RSA and AES algorithms with the addition of XOR operations either with a fixed text block, which is the block The first is m1 or mi-1 variable dynamic text block, and these models gave a higher degree of protection than RSA and AES algorithms by calculating the entropy rate for each of them, where the results show increasing entropy value for four models. Their entropy values are higher than entropy values for RSA and AES algorithms. So that improve their increasing in protection data degree when those models are used and the average execution time is calculated to perform Encryption and decryption of these models to implement the encryption and to implement the decryption, it is shown that times of encryption and decryption for four models are least than times of RSA algorithm and close to times of AES, which improve that proposed models have fast execution speed. The results show that the first model is the fastest, while the fourth model is the highest degree protection.

Keywords: RSA, AES, encryption, decryption, data security, encryption model.

1- المقدمة:

يعتبر تشفير البيانات الرقمية كأحد وسائل حماية البيانات من المجالات التي تلقى أهمية كبيرة لما لها من دور مهم في أمنها، وقد تم اقتراح العديد من خوارزميات التشفير منها المتناظرة (تستخدم نفس المفتاح للتشفير وفك التشفير) ومنها غير المتناظرة (تستخدم مفتاح للتشفير وآخر لفك التشفير)، إلا أنه عمدت العديد من الابحاث الحديثة إلى اقتراح نماذج تشفير تستخدم أكثر من خوارزمية تشفير بهدف زيادة سرية البيانات وتحقيق درجة حماية أعلى، حيث أن بعضها اقترح نظام هجين بالاعتماد على أربع خوارزميات تشفير [1] بهدف تأمين سرية عالية من خلال تشتيت المهاجمين بسبب وجود مفاتيح عديدة، إلا أن سلبية مثل هذه الأبحاث وجود زمن تنفيذ كبير لإجراء التشفير وفك التشفير. وانطلقت بعض الدراسات [2] من تحليل الهجمات على خوارزمية RSA ومعرفة محاسن هذه الخوارزمية ومساوئها، ليتم اقتراح استخدامها في نموذج هجين يعتمد على خوارزمية AES بالإضافة لها فيتم تشفير النص بخوارزمية AES وتشفير مفتاح AES باستخدام خوارزمية RSA ثم تخزين النص المشفر مع مفتاح التشفير المحمي باستخدام خوارزمية RSA في الحوسبة السحابية بغية اجراء العملية العكسية عند استرجاع البيانات من السحابة، وقد عمدت بعض الأبحاث إلى دمج أكثر من خوارزمية بعد تحسين احدى الخوارزميات المستخدمة في عملية الدمج حيث نجد أن الباحث ABROSHAN (2021،3) قام بدمج خوارزميتي MD5 (المستخدمة في التوقيع الرقمي) وخوارزمية Blowfish مع خوارزمية ECC (Elliptic Curve Algorithm) بعد أن قام بتحسين أداء خوارزمية Blowfish من خلال اضافة تابع تحسين يقوم بإجراء عمليات XOR ضمن ترتيب معين [3]. كما أن بعض الباحثين قاموا باستخدام نموذج تشفير هجين يعتمد على خوارزميتي AES و RSA من أجل ضمان عملية تخزين البيانات بشكل سري وذلك بالتمييز بين عملية تحميل البيانات وعملية تنزيل البيانات حيث تتم في المرحلة الأولى تشفير البيانات وفي الثانية يتم فك تشفيرها، مما يضمن تخزين شيفرة البيانات بدلاً من تخزين البيانات بشكل صريح، وتم استخدام ثلاث مفاتيح لإجراء عملية التخزين واسترجاع البيانات وهذه المفاتيح هي المفتاح العام والخاص لـ RSA والمفتاح السري لخوارزمية AES [4] كما أن دمج خوارزمية AES لم يقتصر على خوارزمية محددة بهدف ايجاد نموذج هجين، حيث قام بعضُ الباحثين بدمجها مع خوارزمية Blowfish من خلال تقسيم البيانات إلى قسمين يتم تشفير القسم الأول باستخدام خوارزمية AES أما القسم الآخر فيتم تشفيره باستخدام خوارزمية Blowfish مما يعطي سرية أعلى مقارنةً مع التشفير بخوارزمية واحدة [5]، وقام باحثون بدمج خوارزميتي AES وECC لإيجاد نموذج تشفير هجين يقوم بتشفير البيانات باستخدام خوارزمية AES بواسطة مفتاح ديناميكي، ومن ثم تشفير هذا المفتاح باستخدام خوارزمية ECC وفي النهاية يتم دمج البيانات المشفرة مع المفتاح الديناميكي المشفر لتشكيل البيانات التي يتم تخزينها أما عند استرجاع البيانات تتم العملية العكسية [6] كما قام بعض الباحثون باستخدام خوارزمية RSA لإيجاد نموذج تشفير هجين مع خوارزمية AES بهدف زيادة السرية مع الحفاظ على سرعة تشفير عالية مقارنة مع خوارزمية RSA [7] حيث قام الباحثان (Samir G, Mahmood Z, 2021)

باستخدام خوارزمية AES لإجراء التشفير لكن بمفتاح ديناميكي بدلاً من مفتاح ثابت ويتم ارسال هذا المفتاح إلى الطرف المستقبل باستخدام خوارزمية RSA، إن الآلية السابقة التي تقوم على دمج خوارزميتي AES و RSA والاستفادة من خوارزمية RSA لحماية المفتاح الديناميكي لخوارزمية AES استخدمت في العديد من الأبحاث لما لها من فعالية في زيادة السرية مع الحفاظ على زمن التشفير قليل نسبياً [8] في حين نهج باحثون منهجية التشفير المتسلسل باستخدام خوارزميتي AES وRSA، حيث يتم تشفير البيانات باستخدام خوارزمية AES أولاً ثم باستخدام خوارزمية RSA مما يعطي سرية عالية للبيانات ولكن على حساب الزمن الكبير نسبياً [9] كما اتبع باحثون آخرون اسلوب دمج خوارزميتي AES وRSA عن طريق وجود طرف ثالث يقوم بتأكيد عملية التشفير وفك التشفير من خلال ادارة المفاتيح المتبادلة مما يعطي وثوقية أعلى وحماية البيانات ضد المهاجمين أو المستخدمين غير الموثوقين [10] وبعض الباحثين اقترح نموذج للتشفير بخوارزميتي AES وRSA لحماية البيانات الهامة في الحواسيب المحمولة التي باتت جزء أساسي في مجالات العمل الحاسوبية، حيث يقوم هذا النموذج بحماية البيانات الموجودة على الحواسيب المحمولة بحيث لا يمكن الاطلاع على هذه البيانات إلا من قِبل أصحابها [11] وهكذا تتعدد الدراسات التي حاولت التوصل إلى نموذج تشفير يستخدم أكثر من خوارزمية لزيادة مستوى حماية البيانات بزمن تنفيذ أقل ما يمكن، وتعتبر خوارزمية RSA هي الأبرز من بين خوارزميات التشفير غير المتناظرة في حين تعتبر خوارزمية AES من أبرز خوارزميات التشفير المتناظرة وتمتازان بإمكانية الدمج مع بعضهما أو مع خوارزميات أخرى لهذه الأسباب تم اعتماد هاتين الخوارزميتين لإيجاد نماذج تشفير مما يضمن تحقيق مزايا تشابه كل من مزايا الخوارزميتين السابقتين وهذا ما تؤكده الدراسات المرجعية في هذا المجال حيث لا تكاد ولا تخلو دراسة تتعلق بدمج خوارزميات التشفير أو تهجينها إلا وتحوي على الأقل على احدى هاتين الخوارزميتين هذا وبالإضافة إلى وجود دراسات مرجعية عديدة تناولت دمج هاتين الخوارزميتين.

2 – هدف وأهمية البحث:

إن معظم الدراسات السابقة قامت باقتراح نماذج تستخدم أكثر من خوارزمية تشفير بهدف زيادة الحماية إلا أن هذا الأمر كان على حساب أزمنة التنفيذ التي زادت نتيجة الحاجة إلى زمن تنفيذ خوارزمية AES وRSA في حين أن بعض الدراسات التي ركزت على حماية مفتاح خوارزمية AES باستخدام خوارزمية RSA راعت موضوع الزمن لكن لم تكن درجة حماية البيانات عالية بالشكل الكافي والمرضي حيث أنه بالنتيجة فإن حماية البيانات مرتبطة فقط بخوارزمية RSA التي تحمي مفتاح خوارزمية AES، في حين تقوم فكرة هذا البحث على مراعاة استخدام كل من خوارزميتي AES وRSA في حماية البيانات مباشرة لزيادة درجة الحماية بشكل فعال دون زيادة زمن التنفيذ اللازم لذلك بشكل كبير ولا سيما في النموذجين الثاني والرابع مما يساهم في تحقيق الأهداف الآتية: 1– زيادة مستوى السرية للبيانات المرسلة عبر الشبكة الحاسوبية 2– تقليل الزمن اللازم لإجراء عمليتي التشفير وفك التشفير مما هو عليه في خوارزمية RSA وبزيادة طفيفة عن خوارزمية AES رغم استخدام الخوارزميتين معاً في النموذج الثاني والرابع المقترحين. 3– زيادة ثقة المستخدمين المتعاملين الكترونياً من خلال توفير

معايير التوثيق والتحقق وعدم الانكار وذلك بفترة زمنية قليلة.

كما تبرز أهمية البحث في زيادة مستوى الخصوصية والحماية للبيانات المتداولة حيث ساهمت بعض النماذج المقترحة في تحقيق ذلك بمستوى عالي من السرية ومستوى عالي من السرعة المتمثل بزمن تنفيذ قليل نسبياً لعمليتي التشفير وفك التشفير مقارنة بخوارزمية RSA بالنسبة للنماذج الأربعة، ويقارب نسبياً زمن تنفيذ خوارزمية AES بالنسبة للنموذجين الأول والثاني مما يضمن خصوصية التشفير وعدم الانكار ومعياري التحقق والتوثيق.

3 – خطوات البحث:

تم انجاز هذا البحث وفق الخطوات التالية:

1. دراسة خوارزميتي RSA وAES ومعرفة آلية عمل كل منهما.
2. اقتراح نموذج تشفير باستخدام خوارزمية AES.
3. اقتراح نموذج تشفير باستخدام خوارزميتي RSA وAES.
4. تطوير النموذجين السابقين والحصول على نموذجين جديدين مقترحين ديناميكيين.
5. برمجة النماذج المقترحة باستخدام بيئة ماتلاب وايجاد النتائج.

4 –خوارزميتي RSA وAES [12,13]:

أولاً: خوارزمية RSA: تعتبر خوارزمية RSA أبرز الخوارزميات غير المتناظرة وجاء اسمها من مخترعيها (Rivest, Shamir, and Adleman) وتُستخدم في إجراء التشفير غير المتناظر حيث تعتمد على مفتاحين هما المفتاح العام للتشفير والمفتاح الخاص لفك التشفير وفيما يلي آلية عمل خوارزمية RSA:

A – توليد المفاتيح [14,15]:

1. يتم اختيار رقمين عشوائيين أوليين p , q
2. نحسب جدائهما n= q×p
3. نحسب المعامل ø(n)=(q-1)*(p-1)
4. يتم اختيار عدد عشوائي e بشرط أن تكون قيمته أصغر أو تساوي ϕ(n) وأكبر من الواحد 1<e<ϕ(n)، وأن يكون القاسم المشترك الأكبر مع قيمة ϕ(n) يساوي الواحد ، أي أن يكون أولياً ل ϕ(n)، يمثل هذا الشرط بالعلاقة:

$$GCD(\emptyset(n),e) = 1 \qquad (1)$$

5. نقوم بإيجاد عدد صحيح (d) باقي قسمة جداءه مع e على ø(n) يساوي1 أي:

$$(d * e) \bmod \emptyset(n) = 1 \qquad (2)$$

ومنه يكون المفتاح العام Puk = {e , n} والمفتاح الخاص Prk = {d , n}

B – التشفير: تتم عملية التشفير وفق المعادلة الآتية:

$$C = M^e \bmod(n) \qquad (3)$$

حيث: M الرسالة المراد تشفيرها، C النص المشفر

C– فك التشفير: يتم فك تشفير النص المشفر (C) باستخدام المفتاح الخاص للمستقبل وفق العلاقة:

$$M = C^d \bmod(n) \qquad (4)$$

ثانياً: خوارزمية التشفير المعياري المتقدم (AES) Advanced Encryption Standard algorithm: فقد صدرت خوارزمية AES من قِبل المعهد الدولي للتقنيات والمعايير Implementation approaches for the Advanced Encryption Standard algorithm (NIST)[16] كخوارزمية تشفير متناظرة، وتعتمد هذه الخوارزمية على مفتاح متناظر واحد لكل

من عمليتي التشفير وفك التشفير، وتختلف أطوال المفاتيح تبعا لعدد الدورات:

1) 128 Bit (16 Byte) تتألف من 10 دورات وقد تم اعتمادها في هذا البحث.

2) 192 Bit (24 Byte) تتألف من 12 دورة

3) 256 Bit (32 Byte) تتألف من 14 دورة

وتعتمد آلية عمل خوارزمية AES – 128Bit [17] على المراحل التالية:

1) يتم تقسيم النص الصريح إلى مصفوفة كتل جزئية (Operational Blocks array) 4×4Byte

2) يتم التشفير عبر عشر دورات تحتوي كل دورة على أربع عمليات إلا الدورة العاشرة تحتوي على العمليات الثلاث الأولى فقط.

3) العمليات الأربعة هي:

- استبدال البايت Substitute Byte
- إزاحة الأسطر Shift Rows
- دمج الأعمدة Mix Columns
- إضافة مفتاح الدورة Add Round Key

وهذه العمليات الأربعة معروفة وموضحة في العديد من المراجع سواءاً في هذا البحث أو غيره وهي ليست موضوع تطوير هذا البحث.

5 – نماذج التشفير المقترحة:

تم اقتراح أربع نماذج كالآتي:

1 – النموذج الأول: يعتمد على خوارزمية AES المتناظرة مع اجراء معامل XOR مع الكتلة النصية الأولى m_1 من النص الصريح M.

2 – النموذج الثاني: يعتمد على خوارزميتي RSA وAES مع اجراء معامل XOR مع الكتلة النصية الأولى m_1 من النص الصريح M.

3 – النموذج الثالث: وهو تطوير للنموذج الأول بحيث يستخدم كتل ديناميكية ومتغيرة بدلاً من الكتلة الأولى الثابتة.

4 – النموذج الرابع: وهو تطوير النموذج الثاني بحيث يعتمد على كتلة ديناميكية متغيرة بدلاً من m_1.

5 – 1 – النموذج الأول المقترح:

تتم عملية التشفير في هذا النموذج كما هو مبين في الشكل(A-1) وفق الخطوات التالية:

1 – تقسيم نص الرسالة M إلى كتل جزئية m_i كما يلي:

$$M = \{m_1, m_2, \ldots\ldots\ldots\ldots m_i\} \quad \ldots\ldots\ldots (5)$$

2 – نقوم بإجراء XOR بين الكتلة الأولى m_1 وباقي الكتل النصية بدءاً من m_2 حتى آخر كتلة في الرسالة ثم يتم تشفير الناتج باستخدام خوارزمية AES وفق العلاقة:

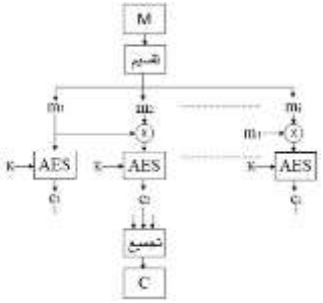
$$Ci = AES\ (m_i \text{ xor } m_1) \quad \ldots\ldots\ldots\ldots\ldots (6)$$

حيث c_i النص المشفر المقابل للكتلة m_i

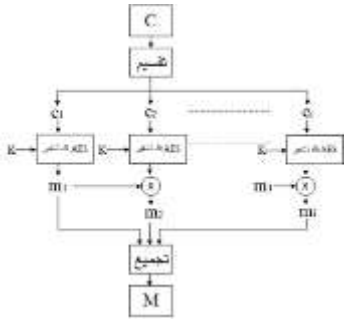
أما الكتلة الأولى فيتم تشفيرها باستخدام خوارزمية AES

3 – يتم تجميع الشيفرات الجزئية c_i للحصول على النص المشفر النهائي C.

أما عملية فك التشفير فتتم بشكل معاكس لعملية التشفير كما هو مبين في الشكل (B-1)



A– مخطط التشفير

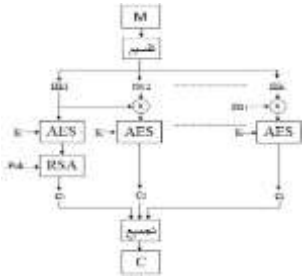


B- مخطط فك التشفير

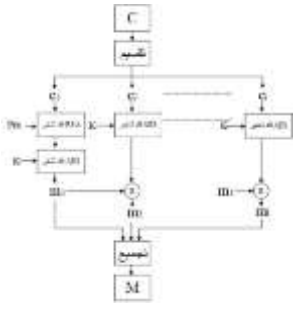
الشكل (1) النموذج الأول المقترح لحماية البيانات باستخدام خوارزمية AES، [المصدر اعداد الباحثين]

5 – 2 – النموذج الثاني المقترح:

في هذا النموذج تم استخدام خوارزميتين RSA وAES لتشفير الكتلة الأولى كما هو مبين بالشكل(2) بهدف زيادة مستوى حماية الكتلة الأولى التي تستخدم كطرف ثابت لإجراء عملية XOR مع باقي الكتل ثم تشفير الناتج باستخدام خوارزمية AES



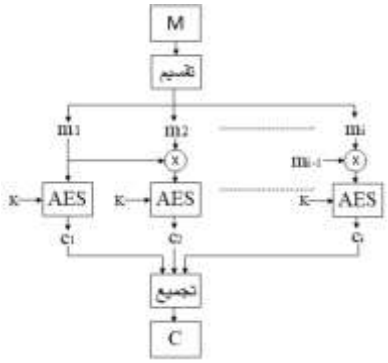
A- مخطط التشفير



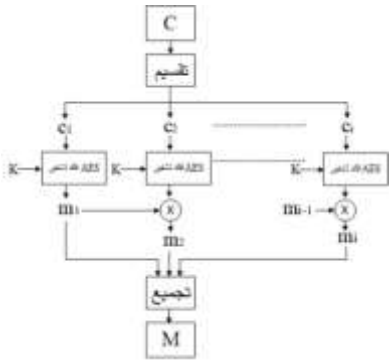
B- مخطط فك التشفير

الشكل (2) النموذج الثاني المقترح لحماية البيانات باستخدام خوارزميتي RSA وAES، [المصدر اعداد الباحثين]

5 – 3 – النموذج الثالث المقترح: تم في هذا النموذج الاعتماد على خوارزمية AES لإجراء التشفير وفك التشفير، لكن بعد اجراء معامل XOR لكل كتلة مع الكتلة التي قبلها بدءاً من الكتلة الثانية كما هو موضح بالشكل(3).



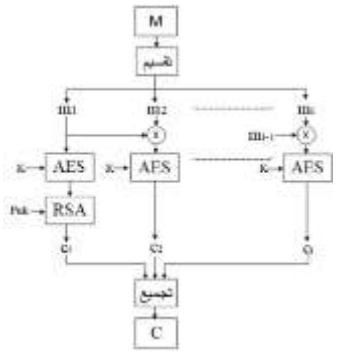
A- مخطط التشفير



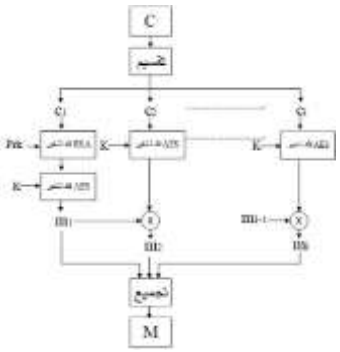
B- مخطط فك التشفير

الشكل (3) النموذج الثالث المقترح لحماية البيانات باستخدام خوارزمية AES، [المصدر اعداد الباحثين]

5 – 4 – النموذج الرابع المقترح: يتوافق هذا النموذج مع آلية عمل النموذج الثاني مع فارق استخدام الكتلة الديناميكية (المتغيرة) m_{i-1} بدلاً من الكتلة الأولى (الثابته) m_1 كما هو مبين بالشكل (4).



A- مخطط التشفير



B- مخطط فك التشفير

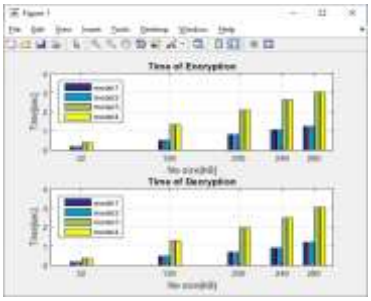
الشكل(4) النموذج الرابع المقترح لحماية البيانات باستخدام خوارزميتي RSA وAES، المصدر [اعداد الباحثين]

6 – النتائج والمناقشة:

تم برمجة النماذج الأربعة المقترحة باستخدام البيئة البرمجية ماتلاب كما هو مبين بالشكل (5)، حيث يتم ادخال الرسالة M إلى البرنامج في طرف المرسل ثم التشفير بأحد النماذج الأربعة بالضغط على الزر المناسب، أما في طرف المستقبل يتم اجراء عملية فك التشفير الموافقة لعملية التشفير المستخدمة في طرف المرسل.

الشكل (5) البرنامج المصمم لإجراء التشفير وفك التشفير وفق النماذج الأربعة المقترحة باستخدام بيئة ماتلاب. [المصدر إعداد الباحثين].

تم اختبار النماذج من ناحية زمن تنفيذ التشفير وفك التشفير بحساب هذه الأزمنة لخمس بيانات نصية بأحجام مختلفة KB {280 , 246 , 200 , 126 , 32} ومقارنة أزمنة التشفير وفك التشفير للنماذج الأربعة كما هو مبين في الشكل(6)



الشكل (6) أزمنة التشفير وفك التشفير للنماذج الأربعة المقترحة، [المصدر اعداد الباحثين]

كما تمت مقارنة هذه الأزمنة مع أزمنة خوارزميتي RSA وAES من خلال حساب متوسط زمن تشفير أحجام النصوص الخمسة السابقة كما هو مبين في الجدول (1)، كما تمت المقارنة مع أبرزت الدراسات المرجعية كما هو مبين في الجدول رقم (3)

الجدول (1) مقارنة متوسط أزمنة التشفير وفك التشفير

آلية التشفير	AES	RSA	Model 1	Model 2	Model 3	Model 4
متوسط زمن التشفير	0.622	2.686	0.6841	0.6846	1.8158	1.8162
متوسط زمن فك التشفير	0.68	2.796	0.7481	0.7484	1.8797	1.8799

[المصدر إعداد الباحثين]

حيث تبين أن النموذج الأول يعطي أقل زمن تشفير وفك تشفير من باقي النماذج لاعتماده على خوارزمية AES لإجراء التشفير وهي خوارزمية أسرع من خوارزمية RSA، كذلك النموذج الثاني الذي يقارب

زمنه من النموذج الأول لاستخدامه نفس الآلية مع فارق وجود تشفير الكتلة الأولى بخوارزمية RSA، أما النموذجين الثالث والرابع يحتاجان زمن أكثر من النموذجين الأول والثاني لوجود أزمنة تبديل الكتل النصية المطلوب تشفيرها والتي يتناسب عددها مع حجم النص الكلي وتزداد بازدياد عدد كتل النص أي بازدياد طول أو حجم النص المطلوب تشفيره، حيث أن اجراء المعامل XOR يكون مع الكتلة المتغيرة أو المتبدلة m_{i-1} بدلاً من الكتلة الثابتة m_1، لذلك فإن النموذج الرابع هو الأبطأ والأقل سرعة من باقي النماذج، وكذلك يتقارب زمن النموذج الثالث من زمنه لاعتماده نفس الآلية مع فارق تشفيره للكتلة الأولى بخوارزمية RSA والتي تستخدم لإجراء عملية XOR لباقي الكتل النصية.

قد تم حساب معدل الانتروبي وفق العلاقة (7) [18,19] للنماذج المقترحة ولخوارزميتي RSA وAES لمعرفة مدى درجة الحماية التي يبديها كل نموذج وخوارزميتي RSA وAES كما هو مبين في الجدول(2)

$$Entropy = \sum_{i=1}^{2N} P(Bi) \log\left[\frac{1}{P(Bi)}\right] \quad (7)$$

حيث: $P(B_i)$ احتمالية ورود البايت B_i في النص، N حجم النص بالبايت.

أعطى النموذج الرابع أعلى معدل انتروبي، ومنه فهو يعطي أعلى درجة حماية للبيانات، وكذلك نجد أن جميع النماذج المقترحة أعطت معدل انتروبي أعلى من خوارزميتي RSA وAES ومنه نستنتج أن هذه النماذج المقترحة كلها تعطي درجة حماية أعلى من خوارزميتي RSA وAES الاساسيتين.

الجدول(2) معدل الانتروبي للنماذج المقترحة ولخوارزميتي RSA وAES

النموذج	AES	RSA	Model 1	Model 2	Model 3	Model 4
معدل الانتروبي	3.74	2.9	4.01	5.09	5.98	6.67

[المصدر إعداد الباحثين]

يبين الجدول(3) اجراء عملية مقارنة بين النماذج المقترحة وأبرز الدراسات المرجعية من حيث زمني التشفير وفك التشفير للكتلة الواحدة التي تبلغ (16 Byte) أي (128 Bit) ومن حيث معدل الأنتروبي لمعرفة مدى سرعة النماذج المقترحة ودرجة الحماية التي تعطيها، وقد أعطى النموذجين الثالث والرابع أعلى درجة حماية من النماذج المرجعية المقارن معها وذلك لاعتماده كتلة ديناميكية لإجراء التشفير اضافة إلى خوارزمية AES وRSA كما تميزت النماذج المقترحة بسرعة تنفيذ عالية كما هو مبين في الجدول (3) حيث كان النموذجين الأول والثاني هما الاسرع من باقي النماذج وتجدر الاشارة إلى أنه تم حساب متوسط زمني التشفير وفك التشفير للكتلة الواحدة من أجل اجراء المقارنة على وحدة حجمية ثابته وموحدة لجميع الدراسات ولم يتم ادراج بعض الدراسات لعدم امكانية حساب هذين الزمنين

الجدول (3) مقارنة النماذج المقترحة مع بعض الدراسات المرجعية

الدراسة	متوسط زمن تشفير الكتلة الواحدة [ms]	متوسط زمن فك تشفير الكتلة الواحدة [ms]	الانتروبي
[1]	لم يذكر	لم يذكر	لم يذكر
[8]	4.425	6.521	لم يذكر
[9]	3.308	3.476	لم يذكر
[19]	16	40	5.95
[20]	52	56	3.59
Model 1	1.069	1.169	4.01
Model 2	1.096	1.198	5.09
Model 3	2.837	2.927	5.98
Model 4	2.878	2.976	6.67

الأزمنة بـ ms [المصدر إعداد الباحثين]

7 – الخاتمة:

تم في هذا البحث اقتراح أربع نماذج اثنان منها يعتمدان على خوارزمية AES واثنان آخران يعتمدان على خوارزميتي RSA وAES، وتم برمجة هذه النماذج في بيئة ماتلاب، وحساب أزمنة تنفيذ التشفير وفك التشفير لخمس نصوص بأحجام مختلفة، وايجاد متوسط هذه الأزمنة بهدف معرفة النموذج الأسرع، حيث كان النموذج الأول هو الأسرع، بالإضافة لذلك تم حساب معدل الانتروبي للنماذج الأربعة لمعرفة درجة حماية كل نموذج، فكان النموذج الرابع هو الأعلى درجة حماية لإعطائه أعلى معدل انتروبي، وتجدر الاشارة أن جميع النماذج أعطت معدل انتروبي أعلى من خوارزميتي RSA وAES الاساسيتين ومن وبعض النماذج المقترحة في دراسات مرجعية أخرى مما تم الإشارة إليه في الجدول(3)، ويعزى سبب ذلك لأنها تعطي نصاً مشفراً هو خليط من خوارزميتي RSA وAES ومعامل XOR الأمر الذي يضيف عقبات أكثر أمام المخترق للحصول على النص الأصلي، وبالتالي فإنها تعطي درجة حماية أعلى منهما بالرغم من اختلاف درجة حماية كل نموذج عن الآخر.

التمويل: هذا البحث ممول من جامعة دمشق وفق رقم التمويل (501100020595).

المراجع References:

1. Levinia B. Rivera, Jazzmine A. Bay, Edwin R. Arboleda, Marlon R. Pereña and Rhowel M. Dellosa. (2019). **Hybrid Cryptosystem Using RSA, DSA, Elgamal, And AES**. International Journal Of Scientific & Technology Research, VOL.8, ISSUE 10, Page:1777 – 1781. ISSN 2277-8616.
2. Manoj Tyagi, Manish Manoria and Bharat Mishra. (2019). **Analysis and Implementation of AES and RSA for cloud, DSA, Elgamal, And AES**. International Journal of Applied Engineering Research, Vol 14, Number 20, Page:3918 – 3923. ISSN 0973-4562.
3. Abroshan, Hossein. (2021).**A Hybrid Encryption Solution to Improve Cloud Computing Security using Symmetric and Asymmetric Cryptography**

Algorithms, International Journal of Advanced Computer Science and Applications, Vol. 12, No. 6. Page : 31-37. Ghent University Ghent, Belgium.

4. Keshao D. Kalaskar1, Shipra Yadav2 and Pankaj Dhumane3. (2021). **Recovery Techniques Of Data Security In Cloud Using Encryption And Decryption By Implementing Hybrid (Rsa & Aes) Algorithm**, International Journal of Advance and Innovative Research,Vol 8, Issue 1 (IV). Page: 262-268. ISSN 2394 – 7780.
5. Dhanush U, Prasannasai S Hulikatti, Raghavendra H Malager, Sandur Shreesha and Prakash Biswagar. (2021**). A Secure File Transfer over Virtual Machine Instances using Hybrid Encryption Technique,** Journal of University of Shanghai for Science and Technology, Vol 23, Issue 6. Page: 77-84. ISSN: 1007-6735.
6. Saba Rehman, Nida Talat Bajwa, Munam Ali Shah, Ahmad O. Aseeri and Adeel Anjum. (2021). **Hybrid AES-ECC Model for the Security of Data over Cloud Storage**.Electronics, 10, 2673.
7. Samir G.Chaloop and Mahmood Z. Abdullah. (2021). **ENHANCING HYBRID SECURITY APPROACH USING AES AND RSA ALGORITHMS,** Journal of Engineering and Sustainable Development, Vol. 25, No. 04. Page: 58-66. ISSN 2520-0917.
8. Abhishek Guru and Asha Ambhaikar. (2021). **AES AND RSA-BASED HYBRID ALGORITHMS FOR MESSAGE ENCRYPTION & DECRYPTION,** IT in Industry Kalinga University, Vol. 9, No.1. Page: 273-279 . ISSN (Online): 2203-1731.
9. K Jaspin, Shirley Selvan, S Sahana and G Thanmai. (2021). **Efficient and Secure File Transfer in Cloud Through Double Encryption Using AES and RSA Algorithm**, IEEE.
10. Sk Al Mamun, Md.Ashiq Mahmood and Md Ashiqul Amin. (2021). **Ensuring Security of Encrypted Information by Hybrid AES and RSA Algorithm with Third-Party Confirmation**, IEEE.
11. Sidharth S Prakash and Visakha K. (2021). **Ensemble of AES –RSA Cryptographic Model for Securing Sensitive Laptop Data**, IEEE.
12. Ridwan B. Marqas, Saman M. Almufti and Rasheed Rebar Ihsan. (2020) **. Comparing Symmetric and Asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms**. Xi'an University of Architecture & Technology, Vol 12, No 3, Page: 3110– 3116. ISSN: 1006-7930.
13. K. Sujatha, A Arjuna Rao, P V Nageswara Rao and L V Rajesh. (2016). **Renowned Information Security Algorithms:A Comparative Study.** International Journal of Engineering Research & Technology, Vol 5, No 02, Page: 216– 224. ISSN: 2278-0181.
14. Achi Harrisson Thiziers, Haba Cisse Théodore, Jérémie T. Zoueu and Babri Michel4. (2019). **Enhanced, Modified and Secured RSA Cryptosystem based on n Prime Numbers and Offline Storage for Medical Data Transmission via Mobile Phone.** International Journal of Advanced Computer Science and Applications, Vol 10, No 10, Page:353– 360.
15. Neha Mishra, Shahid Siddiqui and Jitesh P. Tripathi. (2014). **A Compendium Over Cloud Computing Cryptographic Algorithms and Security Issues**. BIJIT - BVICAM's International Journal of Information Technology, Vol 7, No 01, Page:810– 814. ISSN 0973 – 5658.

16. Xinmiao Zhang ; Parhi, K.K., **Implementation approaches for the Advanced Encryption Standard algorithm,** Circuits and Systems Magazine, IEEE , Vol 2,Issue: 4 , pp 24 – 46
17. KAK A ., (2020) **Computer and Network Security. Purdue University,** Page:3 – 18.
18. Shaheen Ayyub and Praveen Kaushik, (2019), **Secure Searchable Image Encryption in Cloud Using Hyper Chaos**, The International Arab Journal of Information Technology, Vol. 16, No. 2.

19. ملوك وضاح (2019)، **تصميم نموذج لحماية البيانات بدمج خوارزميتي AESو RSA**، مجلة جامعة دمشق للعلوم الهندسية.

20. Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, **Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm (Hyper Image Encryption Algorithm)**, International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3. ISSN 2249-6343.