Journal of Insights in Basic and Applied Sciences
مجلة رؤى في العلوم الأساسية والتطبيقية
ISSN: 3106-1737
Volume 2, Issue 3, 2026, Pages: 823-837
Journal homepage: https://jibas.com.ly/index.php/jibas/en

Digital File Encryption Using The Advanced Encryption Standard (AES) in Gcm Mode: A Vb.Net Implementation with Nist Security and Performance Evaluation

Noura M. Alkurri[1] , Ali Salam Alatrsh[2], Noureddin Y. S. Elhaj[3], Amal Algohoul[4], Mahad Alshantah[5], Taqwi Altlaieiyah[6]
[1,4,5,6] Computer Science Department, Faculty of Science Assaba, University of Ghryan, Libya
[2] Department Electric and Electronic, College of Engineering, Nalut University, jado, Libya
[3] Higher Institute of Science and Technology Alrhebat, Alrhebat, Libya

تشفير الملفات الرقمية باستخدام خوارزمية معيار التشفير المتقدم (AES) في وضع GCM: تنفيذ بلغة VB.NET وتقييم أمني وأدائي وفق اختباراتNIST

نورا محمد الكري[1]*, علي سالم الاطرش[2], نورالدين يوسف الحاج[3], امل الغول[4], مهاد الشنطة[5],تقوي الطليعية[6]
[1، 4، 5، 6] قسم الحاسب الألى، جامعة غريان، كلية العلوم الأصابعة، ليبيا
[2] قسم الهندسة الكهربائية والإلكترونية، كلية الهندسة جادو، جامعة نالوت، ليبيا
[3] قسم تقنية المعلومات، المعهد العالي للعلوم والتقنية، الرحيبات، ليبيا

*Corresponding author: nouraalkorry@gmail.com

Received: June 27, 2026	Accepted: August 25, 2026	Published: September 22, 2026

Abstract:
This research presents the design of an integrated software system for data encryption and the protection of digital files against unauthorized access. The system utilizes the Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM) with a 128-bit key, implemented in Visual Basic .NET via an interface that supports both encryption and decryption with full content recovery. The random components used for key and initialization vector generation were subjected to the NIST statistical test suite—comprising 14 tests with an acceptance threshold of $p > 0.01$—and successfully passed all tests, maintaining values well below the 0.2 failure threshold. The system features a key space of 2^{128} and an exhaustive search time of 5×10^{21} years (at a rate of 50 billion keys per second). It recorded encryption and decryption times of 1.6 seconds and 1.1 seconds, respectively—compared to 3 and 1 seconds for DES, and 7.3 and 4.9 seconds for RSA—while ensuring complete data integrity without significant file size expansion. The results confirm the system's suitability for protecting stored files and recommend its broader adoption.

Keywords: Data Encryption; Digital File Protection; Advanced Encryption Standard (AES); VB.NET; NIST.

الملخص:
يعرض هذا البحث تصميم نظام برمجي متكامل لتشفير البيانات وتأمين الملفات الرقمية من الوصول غير المصرح به، اعتماداً على معيار التشفير المتقدم (AES) العامل بوضع Galois/Counter Mode بمفتاح 128 بت، منفذاً بلغة Visual Basic .NET عبر واجهة تدعم التشفير وفكّه مع استعادة كاملة للمحتوى. خضعت المكوّنات العشوائية لتوليد المفاتيح ومتجهات التهيئة لمجموعة اختبارات NIST الإحصائية المكوّنة من 14 اختباراً بحد قبول $p > 0.01$، فحققت اجتيازاً كاملاً وبقيت قيمها دون خط الفشل 0.2. بلغت مساحة المفاتيح 2^{128} وزمن الفحص الشامل 5×10^{21} سنة عند 50 مليار مفتاح/ثانية، وسجّل النظام زمن تشفير 1.6 ثانية وفك 1.1 ثانية مقابل 3 و1 ثانية لـ DES و7.3 و4.9 ثانية

لـRSA، مع سلامة كاملة للبيانات ودون زيادة جوهرية في حجم الملفات. تؤكد النتائج صلاحية النظام لحماية الملفات المخزنة، وتوصي بتوسيع اعتماده.

الكلمات المفتاحية: تشفير البيانات؛ حماية الملفات الرقمية؛ معيار التشفير المتقدم (AES) ؛VB.NET ؛.NIST.

1.المقدمة

1.1.خلفية الدراسة وأهمية تشفير الملفات الرقمية

ظلّ أمن الاتصالات وتكنولوجيا المعلومات حتى عقد قريب نسبياً محصوراً في مجالات محددة كالأعمال المصرفية والقضاء والتطبيقات العسكرية. لكن سرعة النمو والانتشار في استعمال اتصالات البيانات، وفي مقدمتها شبكة الإنترنت، جعلا الأمن مسألة تهمّ كل المستخدمين؛ فمع تضاعف الحواسب المتصلة تضاعف معها خطر الفيروسات والديدان والمتسللين وما يهدد خصوصية الموظفين [1, 3]. وتتعامل الحواسب اليوم مع شريحة معتبرة من الحياة اليومية، ما يستوجب اعتماد وسائل لحماية البيانات أثبتت جدواها في ضمان السرية والسلامة.

من المعتقد على نطاق واسع أن الأمن ينبغي أن يدخل في صميم بناء الأنظمة منذ التصور الأول، لا أن يُضاف تحديثات لاحقة؛ إذ يُعدّ الأمن بلا حماية من أخطر أخطاء الخدمة، ويستدعي ذلك دورة حياة منهجية للنظام تبدأ من التصور وتنتهي بمراجعة تصميم المشروع، وهي عصب كل نظم الملفات بشتى أنواعها. ومن الخوارزميات المستخدمة في التشفير، التي تختلف باختلاف طريقة التشفير، تأتي خوارزمية AES بوصفها من أهم خوارزميات هذا المجال؛ وينبع أهمية هذه الدراسة من أهمية الملفات وأهمية تحقيق السرية لها والتأكد من خصوصيتها وسلامة محتواها [2, 3]. ويتقصّر أي نقص في الحاجة الأمنية إلى انتهاك خصوصية النظم [5, 6].

2.1.مشكلة البحث ودوافعه

اعتمدت دراسة Thakur و Kumar (2011) منهجاً مقارناً لخوارزميات DES و AES و Blowfish من منظور الأداء، وتخصصت في الجانب التحليلي للخوارزميات، وخلصت إلى أن Blowfish حققت أفضل أداء من حيث سرعة المعالجة، وأن AES أسرع من DES و3DESفي عدد من مؤشرات الأداء [11]. غير أن هذه الدراسة توقفت عند المقارنة المحاكاتية دون بناء أداة تشفير ملفات مُقيَّمة إحصائياً.

أما دراسة زينب محمد حسين (2014) فقد تناولت تطوير تقنيتي التشفير الانسيابي والكتلي، واقترحت تعديلات على خوارزمية RC4 الانسيابية عبر مفتاح واحد وتدفقات متعددة بأطوال متغيرة وعملية XORثنائية الاتجاه، وبيّنت أن تعديل المقاربة الافتراضية يرفع زمن كسر الشفرة ويُصعّب مهام كسر الشفرات، بما يعزز مستوى أمان النظام [3, 13]. بقي العمل، مع ذلك، قائماً على إعادة تصميم خوارزمية انسيابية بدل تقييم نظام تشفير ملفات متكامل مع التحقق الإحصائي من عشوائية مكوناته.

وفي 2017 صمم Usop وزملاؤه تطبيقاً لتأمين الملفات المنقولة باستخدام AES عبر تطبيق جافا (Beans Net)لنقل الملفات بين الأطراف المتفقة، فضمن سرية الملفات أثناء النقل وحمايتها من الوصول غير المصرح به أثناء القراءة [12]. ظلّ نطاقه محصوراً في سيناريو النقل الشبكي. تتقاطع الدراسات الثلاث عند نتيجة واحدة وهي ان AES الأكثر فعالية وأمناً بين الخوارزميات المدروسة. لكن الفجوة المسكوت عنها تتحدد كمّياً في أربع نقاط لم تجمعها أي من هذه الأعمال معاً, (1) بناء خط أنابيب كامل بمفتاح 128 بت يخدم سبع فئات من الملفات؛ (2) إخضاع المكوّنات العشوائية للمجموعة الكاملة من 14 اختباراً إحصائياً بحد قبول $p > 0.01$ ؛ (3) قياس زمني مباشر مقابل DES وRSA؛ (4) التحقق من الاسترجاع الكامل بلا فقدان أو تشويه على ملف ملموس بحجم 59.83 كيلوبايت وأبعاد 720×901 بكسل.

3.1.أهداف الدراسة ومساهماتها العلمية

1.**صمّمنا وبنينا**: نظاماً برمجياً متكاملاً بلغة VB.NET لتشفير وفك تشفير الملفات الرقمية وفق معيار AES [4]بوضع GCM [14]، بمفتاح 128 بت وكتلة 128 بت وعشر جولات، عبر مسار تنفيذي من ست خطوات يدعم ملفات Word و Excel و Access و PowerPointوالصوتية والمرئية و PDFوسائر الملفات .

2.**قيّمنا**: المكوّنات العشوائية لتوليد المفاتيح ومتجهات التهيئة عبر مجموعة الاختبارات الإحصائية لمعهد NIST (SP 800-22)المكوّنة من 14 اختباراً بحد قبول $p > 0.01$ [10]، فحقق النظام اجتيازاً كاملاً (14/14) مع بقاء جميع القيم دون خط المؤشر الفاشل 0.2.

3.**أجرينا**: تقييماً مقارناً كمّياً أظهر مساحة مفاتيح (2^{128} مقابل 2^{56} لـ DES و2^{112} أو 2^{168} لـ3 DES)، وزمن فحص شامل 5×10^{21} سنة لمفتاح 128 بت عند 50 مليار مفتاح/ثانية مقابل 400 يوم لـ DES و800 يوم لمفتاح 3 DES بطول 112 بت، وأزمنة تشفير/فك 1.1/1.6 ثانية مقابل 1/3 لـ DESو4.9/7.3 لـ RSA.

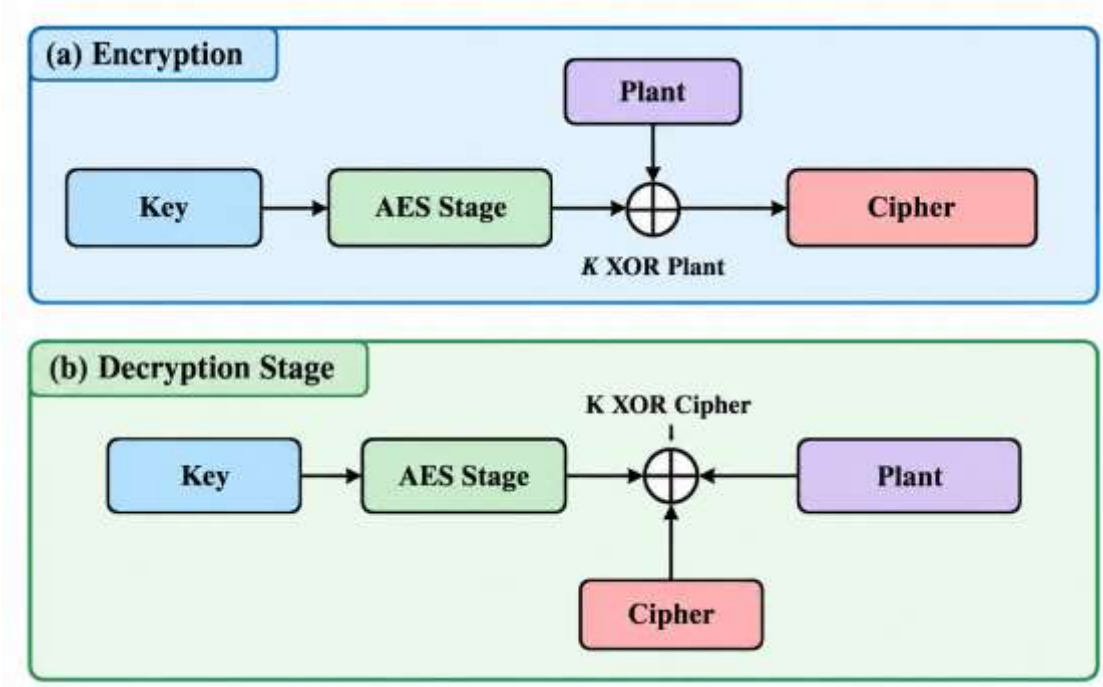
4.1. منهجية الدراسة وهيكل الورقة

يغطي القسم الثاني المنهجية المقترحة وبنية النظام التشفيري وجدولة المفاتيح وخط أنابيب التطبيق وإطار التقييم الإحصائي. يعرض القسم الثالث النتائج الرقمية وجداول المقارنة ونتائج الاختبارات. يناقش القسم الرابع الأسباب التقنية وموقع النظام من الأدبيات ويعلن القيود صراحة. يخلص القسم الخامس إلى الإنجازات ويقترح مسارين للتطوير. تختتم الورقة بقائمة المراجع.

2. الأساس النظري والتقني

1.2. أساسيات تشفير الملفات الرقمية

يقوم النموذج الأساسي على مرحلتين متناظرتين (الشكل 1): في مرحلة التشفير يمرّ المفتاح عبر مرحلة AESلتوليد تدفق المفتاح K، ثم يُدمج مع النص الصريح ببوابة (XOR) عملية (K XOR Plant) لإنتاج النص المشفر؛ وفي مرحلة فك التشفير يُولَّد التدفق ذاته ويُدمج مع النص المشفر (K XOR Cipher) لإعادة النص الصريح. يشفّر التطبيق الملفات بمراحل عديدة، يُقرأ الملف، ويُولَّد مفتاح التشفير عبر AES ، ويُنفَّذ التشفير، ثم تُحوَّل أجزاء الملف التالية وفق مفتاح التشفير وخطوات الخوارزمية، مع شرط إلزامي بإضافة مفتاح التشفير قبل عملية AES ويعمل النظام بوضع Galois/Counter Mode (GCM)الذي يوفر التشفير والتحقق الموثّق من سلامة البيانات في عملية واحدة، تتيح كشف أي تعديل غير مصرح به أو تلاعب بالمحتوى المشفر [14].



الشكل :1 المخطط المعماري لخط أنابيب التشفير وفك التشفير.

في سياق التخزين، تعتمد البيانات نظام ملفات قياسياً [7] تُخزَّن فيه الملفات بصيغة ثنائية على أقراص مغناطيسية متعددة الأسطح (Platters)، مع إمكان الوصول عبر بروتوكولات الشبكة واعتماد الربط

(Mapping) بين الملفات الافتراضية والمخزون الحقيقي [8] (Backing store])، وهو ما يبرر استهداف الدراسة للملفات المخزنة على القرص الصلب.

2.2.خوارزمية التشفير المتقدم AES

خوارزمية AES هي نسخة معيارية من Rijndael؛ وهي خوارزمية تشفير كتلي متناظر (Symmetric Block Cipher)تدعم أطوال مفاتيح وكتل 128 أو 192 أو 256 بت، اختيرت عام 2000 واستُصدرت بمعيار FIPS 197 عام 2001 بابتكار Daemen وRijmen [4, 5]. تمثَّل الخوارزمية بثلاث مصفوفات, مفتاح التشفير $\underline{k}$ ذو البعدين $4 \times N_k$ حيث $N_k = 4,6,8$ (بموافقة أطوال 128 و192 و256 بت)، والنص المرمّز $\underline{x}$ ذو البعدين $4 \times N_b$، ومفاتيح الجولة $\underline{\omega}$ بذات البعدين؛ وجميع العناصر $k_{i,j}$ و$x_{i,j}$ و$\omega_{i,j}$ أعداد صحيحة من 8 بت (من 0 إلى 255) في المجموعة Z_{256}يولّد طول المفتاح 128 بت 44 كلمة إجمالية، كل كلمة 32 بت (4 بايت)، تُوزَّع على الجولات من $W[0:3]$ حتى$W[40:43]$ ، ويُرتَّب النص كمصفوفة حالة (State) يبلغ طول أعمدتها 4 بايت. يبين جدول 1 عدد الجولات N_r وفق أطوال المفتاح والكتلة [5]؛ ويشغل تكوين المنفَّذ في هذه الدراسة مفتاح 128 بت وكتلة 128 بت، أي ($N_k = N_b = 4$) عشر جولات.

جدول 1:عدد جولات Rijndael N_r وفق أطوال المفتاح N_k والكتلةN_b .

	$N_b = 4$	$N_b = 6$	$N_b = 8$
$N_k = 4$	10	12	14
$N_k = 6$	12	12	14
$N_k = 8$	14	14	14

الجولة الأولى T_0 هي عملية XOR بين النص (الحالة الابتدائية) ومفتاح التشفير :

$$T_0(\underline{x}) = \begin{pmatrix} k_{0,0} & k_{0,1} & \cdots & k_{0,N_k-1} \\ k_{1,0} & k_{1,1} & \cdots & k_{1,N_k-1} \\ k_{2,0} & k_{2,1} & \cdots & k_{2,N_k-1} \\ k_{3,0} & k_{3,1} & \cdots & k_{3,N_k-1} \end{pmatrix} \oplus \begin{pmatrix} x_{0,0} & x_{0,1} & \cdots & x_{0,N_b-1} \\ x_{1,0} & x_{1,1} & \cdots & x_{1,N_b-1} \\ x_{2,0} & x_{2,1} & \cdots & x_{2,N_b-1} \\ x_{3,0} & x_{3,1} & \cdots & x_{3,N_b-1} \end{pmatrix} \qquad (1)$$

وتتكون الخوارزمية الكاملة من تركيب التحويلات (Transformations) على ضعيات [5]. Rijndael

$$RIJ(\underline{x}) = \underline{y} = \left(T_{N_r} \circ T_{N_r-1} \circ \cdots \circ T_{N_1} \circ T_{N_0}\right) \qquad (2)$$

3.2.نمط التشفير الموثقGCM

تقوم كل جولة (ما عدا الأخيرة التي تُلغى فيها عملية الخلط الخطي) على ثلاث عمليات موضحة في الشكل 2:

(أ) الاستبدال غير الخطي ByteSub: يستخدم صندوق الاستبدال (S-box) المعرّف كمصفوفة word8 S[256]تبدأ قيمها بالمتتالية: 99، 124، 119، 123، 242، 107، 111، 197، 48، 1، 103، 43، 254، 215، 171، 118، 202، 130، 201، 125، 250، 89، 71، 240، 173، 212، 162، 175، 156، 164، 114، 192، ... وقد ورد في المستند المصدر مثالٌ كان فيه العدد المطلوب استبداله 19 بالنظام العشري، فكانت النتيجة وفق الجدول x4d1 أي 212 (حسب القاعدة 11).

(ب) إزاحة الأسطر ShiftRows: ترجيع الصفوف بإزاحة دائرية

$$SR:\ w = \begin{pmatrix} w_{0,0} & w_{0,1} & w_{0,2} & w_{0,3} \\ w_{1,0} & w_{1,1} & w_{1,2} & w_{1,3} \\ w_{2,0} & w_{2,1} & w_{2,2} & w_{2,3} \\ w_{3,0} & w_{3,1} & w_{3,2} & w_{3,3} \end{pmatrix} \rightarrow \begin{pmatrix} w_{0,0} & w_{0,1} & w_{0,2} & w_{0,3} \\ w_{1,1} & w_{1,2} & w_{1,3} & w_{1,0} \\ w_{2,2} & w_{2,3} & w_{2,0} & w_{2,1} \\ w_{3,3} & w_{3,0} & w_{3,1} & w_{3,2} \end{pmatrix} \quad (3)$$

(ج) خلط الأعمدة MixColumns: معرفة على الحقل $GF(2^8)$ بمتعدد الحدود غير القابل للاختزال

$$m(x) = x^8 + x^4 + x^3 + x + 1 \quad (4)$$

$$\begin{bmatrix} s'_0 \\ s'_1 \\ s'_2 \\ s'_3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix} \quad (5)$$

وتتيح طريقة تنفيذ بديلة عبر الدوال :

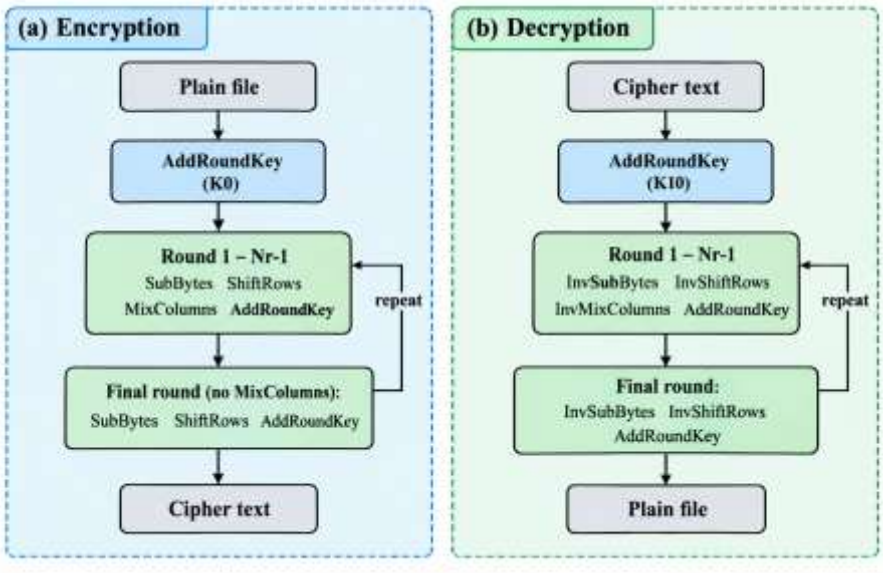
$$f(a_0, a_1, a_2, a_3) = (a_1 \oplus a_2 \oplus a_3) \oplus g\big((a_0 \oplus a_1) \ll 1\big) \quad (6)$$

$$g(x) = \begin{cases} x \oplus 11B_x, & \text{إذا كان } x \wedge 100_x \text{ صحيحاً} \\ x, & \text{غير ذلك} \end{cases} \quad (7)$$

$$\begin{aligned} d_1(a_0, a_1, a_2, a_3) &= a_0 \oplus a_1 \oplus a_2 \oplus a_3 \\ d_2(a_0, a_1, a_2, a_3) &= g(d_1 \ll 1) \oplus (a_0 \oplus a_2) \\ d_3(a_0, a_1, a_2, a_3) &= g(d_2 \ll 1) \oplus (a_0 \oplus a_1) \end{aligned} \quad (8)$$

(د) إضافة مفتاح الجولة AddRoundKey: تجمع الحالة مع مفتاح الجولة ω_i بعملية XOR عنصراً بعنصر. وبذلك يتسلسل التشفير: تصنيف مفتاح الجولة الأول K_0 ، ثم N دورات تضم الاستبدال وإزاحة الأسطر وخلط الأعمدة (ما عدا الجولة الأخيرة)، ثم إضافة مفتاح الجولة K_i حتى نهاية التشفير ويكون فك التشفير معكوس التركيب.

$$RIJ^{-1}(\underline{y}) = \underline{x} = \left(T_{N_0}^{-1} \circ T_{N_1}^{-1} \circ \cdots \circ T_{N_{r-1}}^{-1} \circ T_{N_r}^{-1}\right) \quad (9)$$



الشكل 2: بنية جولات AES للتشفير وفك التشفير بمفتاح 128 بت (عشر جولات).

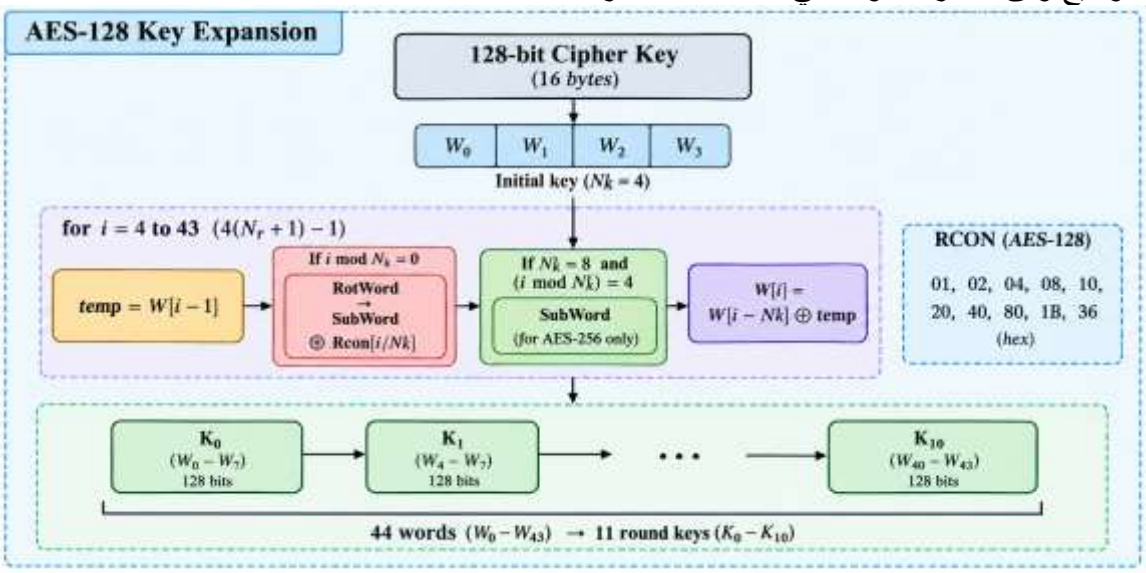
تمنح هذه البنية الخوارزمية خصائص أمنية موثقة [5] لا توجد مفاتيح ضعيفة (صفة الشكل) كما في DES، وأمان الخوارزمية كله متعقل باختيار الحد الأقصى وليس خطياً أو تافهاً.

$$AES_k(x) \neq AES_{k^{-1}}(\overline{x}), \qquad S[i] + S[j] \neq S[i+j] \qquad (10)$$

فإذا كانت S مصفوفة تافهة, فان نتيجة التأثير تكون كلها تافهاً وكان كسرها بسهولة ممكناً. وتقتصر أفضل الهجمات الموثقة [6] على نسخ مخففة من الجولات (7 جولات للمفتاح 128 بت و8 جولات للأطوال الأعلى)، ولا يوجد هجوم فعّال على كامل الجولات، إذ يبقى زمن الكسر الكامل مقيداً بمساحة المفتاح 2^{128} [5] .

4.2.جدولة المفاتيح (Key Expansion)

الخوارزمية مبنية على مفتاح رئيسي واحد؛ إن لم يستخدم المفتاح نفسه مرتين فيكون الناتج جديداً كل مرة. تُنشأ المفاتيح الفرعية من مصفوفة المفتاح ذي البعد N_k (كل كلمة 32 بت) بحيث يحصل التشفير على مفتاح الجولة $(N_r + 1)$، وتُعرف الكلمات القديمة بالمصفوف، $W[4(N_r + 1)]$ حيث تشكّل الكلمات الأربع الأولى مفتاح الجولة الأولى والأربع التالية مفتاح الجولة الثانية وهكذا (الشكل 3). ويولَّد التوسيع وفق الشفرة الموثقة في المستند المصدر:



الشكل 3: توسيع المفتاح 128 بت إلى أحد عشر مفتاح جولة ($W[0:3]$ حتى $W[40:43]$)

5.2.الجداول العشوائية والديناميكية

ناقشت الدراسة جدول التبديل العشوائي (Random S-boxes) بهدف ألا تكون عملية الاستبدال معتمدة على معلومات ثابتة، بحيث تُولَّد القيم بشكل عشوائي بالاعتماد على خوارزمية Knuth لتوليد جدول عشوائي كامل يعتمد على المفتاح المشفر [10, 9] .

```
For I = 1 to 256: S_box[I] = I /* جدول التبديل الابتدائي */
For i = 1 to 256: J = RandomInRange(I, 256)
Swap(S_box[i], S_box[J]) End for
```

أثبتت الدراسة أن توليد الجداول العشوائية يجبر المهاجمين على الاعتماد على الجداول المولدة بدلاً من الجداول التقليدية للمخططات السابقة [2, 9]. أما جداول التبديل الديناميكية فتعتمد على إعداد عشوائياً يتغير ترتيب القيم داخلها بناءً على المفتاح، وتختلف عن البناء السابق وفق Knuth في أنها لا تشتمل على كامل محتويات جدول التبديل بل على بعض عناصره [9] .

6.2.خط أنابيب التطبيق وواجهة المستخدم

صُمم النظام بأداة VB.net في تصميم المراحل المختلفة لتشفير الملف عبر خطوات AES ، مع تحليل نتائج التطبيق عبر برنامج NIST المشهور في اختبارات التشفير، وهي أرقام عشوائية لاختبار نتائج تشفير الخوارزميات (الشاشة الثالثة الرئيسية للنموذج المطبق داخل تجربة التشفير). ويمكن وصف النموذج التطبيقي وفقاً للآتي:

1.اختيار مكان تخزين الملف في الذاكرة المعينة (Select a file).

2.إدخال مفتاح التشفير (Enter PassWord).

3.التعديل في طول مفتاح التشفير حتى يساوي 128 بت، ويُحوَّل المدخل إلى Hexadecimal ومن ثم إلى BITs.

4.تقسيم الملف المدخل إلى كتل معينة وتحويله إلى Hexadecimal ثم إلى BITs، وتوزيع بتات الملف على المصفوفات حتى تتم عملية الاستبدال والإزاحة على هيئة خوارزمية AES ، ثم إضافة مفتاح الجولة المولد من المفتاح الأساسي لكل دورة وفق البوابة المنطقية XOR ، بما ينتج نصاً مشفراً أو ملفاً مشفراً (محفوظاً في ثنائيات الملف) .

5.تجميع الكتل المشفرة على حسب خوارزمية AES ومفتاح التشفير، وتخزين الملف المشفر .

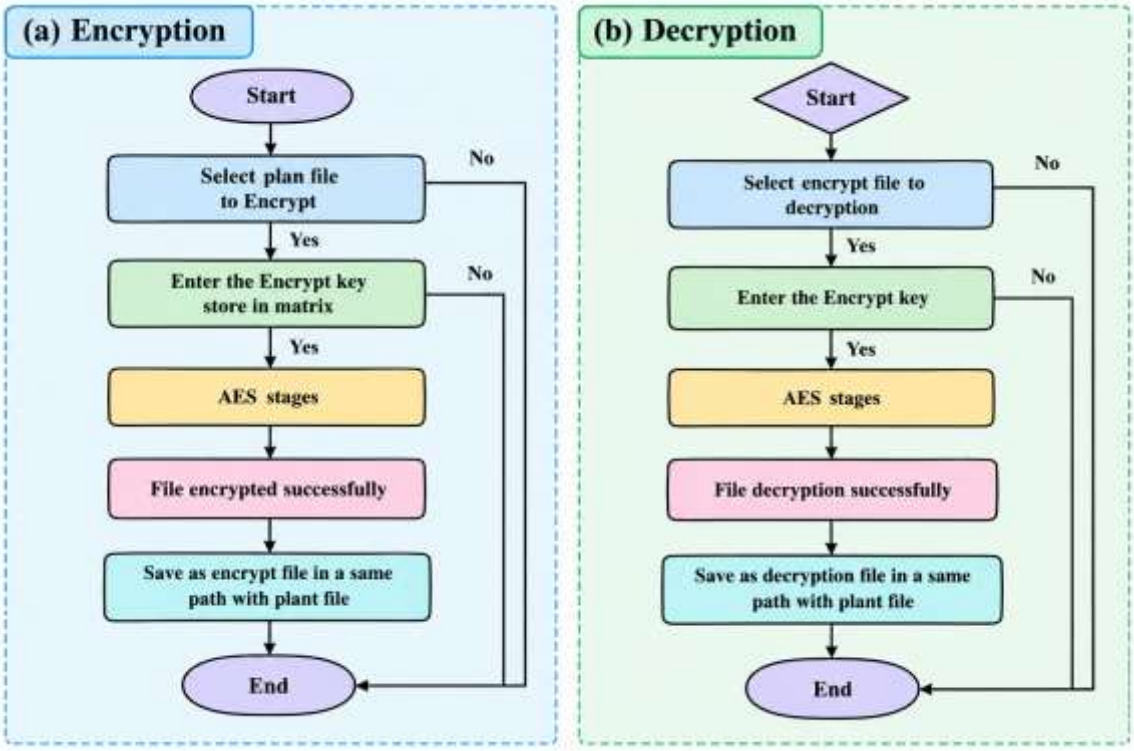
6.منع التعامل مع الملف إلا من خلال مفتاح التشفير الذي شُفِّر به .

ويتبع مسار التشفير ومسار فك التشفير التسلسلين الموثقين في الشكل 4. وتتيح الواجهة الرسومية العناصر Add File Encryptica :و Browse File وEnter PassWord وزرّي Encrypt و Decryptوزر العودة إلى الشاشة الرئيسية، مع تحديد صريح بأن الملفات المشفرة تشمل Word : files, Excel files, Access files, PowerPoint files, audio files, video/visual files, PDF files, and all other files mentioned above—everything.

ولأغراض التأسيس المقارن، وُصف كذلك التشفير الانسيابي RC4 الذي يولِّد مفتاحه لكل جلسة عبر علاقة التبديل, بمفتاح متغير الطول بين 1 و251 بايت وجدول توليد 251 بايت، وطورين تشغيليين هما الإعداد الرئيسي (جدولة المفتاح، وهي المرحلة الأكثر حساسية) وطور توليد النص المشفر [3].

$$[\,K\,] \rightarrow [\,\text{Keystream}\,]\ \text{XOR}\ \text{planttext} \rightarrow \text{encrypttext} \qquad (11)$$

ويبقى التحدي الأساسي في جعل المرسل والمستقبل يتفقان على المفتاح السري دون أن يعرفه أو يخدعه أي شخص آخر، وهو ما يعرف بإدارة المفتاح (Key Management) [13]. كما يُستخدم AES في تطبيقات برمجية واسعة في برنامج ضغط الملفات (WINZIP) عندما يطلب المستخدم تشفير البيانات بعد ضغطها، وفي بروتوكول TLS لإنشاء اتصال آمن، وفي بروتوكول IPsec لضمان الأمان في الاتصالات العاملة بوساطة IP عبر الإنترنت [14].



الشكل 4: خطوات تشفير الملف وفك تشفيره في النموذج المطبق.

7.2. إطار التقييم الإحصائي (مجموعة NIST)

خضعت مخرجات الخوارزمية إلى الاختبارات الأربعة عشر لمجموعة (1) Frequency (monobit) NIST [10].لتحديد ما إذا كان عدد الأحاد والأصفار في المتتالية معقولاً؛ Frequency within a Block (2)لتحديد تكرار الواحدات في رزمة M بنسبة متوقعة$M/2$ ؛ (3) Runs لعدد الجولات من الأحاد والأصفار بأطوال مختلفة؛ (4) Longest run of ones in a Block لطول جولة الواحدات في المتتالية؛ (5) Binary matrix Rank لفحص التبعية الخطية بين متتاليات جزئية ذات أطوال ثابتة؛ (6) Discrete Fourier transform لتحديد الأنماط الدورية والانحرافات عن العشوائية؛ (7) Non-overlapping template matchingلعدد مرات تحقق أنماط محددة سلفاً دون تداخل؛ (8) الاختبار الثامن (بنفس التسمية كما وردت في المصدر) مع السماح بتداخل الأنماط من الموضع الثاني؛ (9) Maurer's universal statisticalلإمكانية ضغط المتتالية دون ضياع معلومات؛ Linear complexity (10)لما إذا كانت المتتالية معقدة كفاية لتُعدّ عشوائية؛ (11) Approximate entropy لمقارنة تكرار الأنماط المتداخلة بطولي m و$(m + 1)$؛ (12) Cumulative sums (Cusums) لما إذا كانت المجاميع الجزئية صغيرة جداً أو كبيرة جداً بالنسبة إلى التصفّر المتوقع؛ (13) Random excursions variantلعدد مرات تحقق عدة نماذج وانحرافها؛ (14) Random Excursions المشابه للسابق لكن بتركيزه على نموذج واحد فقط [10].

ويتم توليد البيانات عبر نماذج مخصصة منها: (1) Key Avalanche توليد كتلة نصية معماة من نص ثابت بمجموعة مفاتيح يختلف كل منها عن الآخر ببت واحد فقط, (2) Plaintext Avalanche مجموعة نصوص معماة كل واحدة من نص واحد فقط وبمفتاح التعمية الخاص بها، (3) Plaintext/Ciphertext Correlation توليد نصوص معماة من مجموعة نصوص واضحة ودراسة الارتباط بين أزواج النصوص، (4) Cipher block chaining mode توليد النصوص وفق النظام السلسلي بإدخال الجزء الأول في المرحلة الثانية، (5) Random Plaintext/Random 128-Bit Keys دراسة عشوائية النص الصريح، (6) Low Density 128-bit keys مفاتيح بتاتها أصفار

غالباً تختلف ببت واحد، (7) High Density 128-bit keys مفاتيح بتاتها واحدان غالباً تختلف ببت واحد.
يتلخص منطق القبول في الآتي: بتُحوَّل الأحاد والأصفار في المتتالية إلى $+1$ أو -1 ثم يُؤخذ المجموع S_n، وتُحسب القيمة الإحصائية .

$$S_{obs} = \frac{|S_n|}{\sqrt{n}} \quad (12)$$

$$P = \text{erfc}\left(\frac{S_{obs}}{\sqrt{2}}\right) \quad (13)$$

تُعدّ المتتالية عشوائية عندما يكون $p > 0.01$ (بالنسبة لاختبار التردد النسبي)، وتختلف الخطوات والقيم المحسوبة من اختبار إلى آخر بحسب طبيعة الاختبار وهدفه. وتعني عتبة القبول 0.01 نظرياً ألا يتجاوز عدد المتتاليات المرفوضة واحداً لكل 111 مجموعة بيانات مختبرة، إذ يجب أن تتجاوز القيمة النظرية المتكررة لكل اختبار عتبة القبول المحددة، ويُحسب الحد الأدنى لعدد المتتاليات المرفوضة وفق الصيغة الواردة حرفياً في الوثيقة المصدر :

$$s\left(\alpha \mid 3\sqrt{\frac{\alpha(1-\alpha)}{s}}\right) \quad (14)$$

حيث s هي حجم المجموعة وα هي عتبة قبول المقالة. وبعد تطبيق الاختبارات المطبقة على نتائج التشفير باستخدام أنماط مختلفة، تبين أن الخوارزمية ذات ثقة عالية.

3.النتائج التجريبية والتقييم المعياري

1.3.المقارنة البنيوية الأمنية

يعرض الجدول 2 مقارنة بنيوية كاملة **أمنية بين AES وDES3 وDES.**

جدول 2: مقارنة بنيوية أمنية بين AES وDES3 وDES.

العامل	AES	3DES	DES
طول المفتاح	128 أو 192 أو 256 بت	168 بت (k_1, k_2, k_3) أو 112 بت $(k_1 = k_2)$	56 بت
نوع التشفير	كتلي متناظر	كتلي متناظر	كتلي متناظر
حجم الكتلة	128 أو 192 أو 256 بت	64 بت	64 بت
مقاومة التحليل المشفر	قوي ضد هجمات التمييز التفاضلي والخطي والاستيفاء والمربع	عرضة للتمييز التفاضلي؛ مهاجم القوة الغاشمة، تحليل النص الصريح	عرضة للتمييز التفاضلي والخطي؛ جداول استبدال ضعيفة
الحالة الأمنية	يُعدّ آمناً	ضعف واحد فقط موروث من DES	ثبت عدم كفايته
المفاتيح الممكنة	2^{128} أو 2^{192} أو 2^{256}	2^{112} أو 2^{168}	2^{56}
مفاتيح ASCII قابلة للطباعة	95^{16} أو 95^{24} أو 95^{32}	95^{14} أو 95^{21}	95^{7}
زمن فحص كل المفاتيح عند 50 مليار مفتاح/ثانية	مفتاح 128 بت: 5×10^{21} سنة	مفتاح 112 بت: 800 يوم	مفتاح 56 بت: 400 يوم

يوضح الجدول الأساس الكمي لتفوق AES : رفع مساحة المفاتيح من 2^{56} إلى 2^{128} يحوّل كلفة البحث الشامل من 400 يوم إلى 5×10^{21} سنة في ظل معدل فحص قياسي قدره 50 مليار مفتاح/ثانية، وهو تحوّل يُخرج الهجوم الغاشم عملياً من نطاق الجدوى. وقد تقرر هذا الاختيار عبر سلسلة وثائق FIPS-PUBالمؤسسية التي تصدرها مؤسسة NIST لاختيار مجموعة واسعة من أدوات ونتائج التشفير، وبعد اجتياز الاختبارات اللازمة لتحديد مستوى الأمان الذي تقدمه المؤسسات المعيارية والبروتوكولات [4].

2.3.الأداء الزمني

جدول 3: التعقيد الزمني لخوارزميات AES و DES وRSA

الخوارزمية	زمن التشفير (ثانية)	زمن فك التشفير (ثانية)
DES	3	1
AES	1.6	1.1
RSA	7.3	4.9

سجّل AES زمن تشفير 1.6 ثانية، أقل من DES (3 ثوانٍ) و RSA (7.3 ثانية)، وزمن فك تشفير 1.1 ثانية يقارب زمن DES (1 ثانية) ويبقى أدنى بكثير من RSA (4.9 ثانية)، كما يوضح الشكل 5 هذا التوازن بين الزمن والتأمين، أي الكفاءة الزمنية من الدرجة الأولى مع القوة الأمنية الأعلى بين الأساليب المعروفة لتكسير الخوارزميات، كان معياراً حاكماً في اختيار[4] AES ، ويتوافق مع نتائج الدراسة السابقة التي وجدت AES أسرع من DES و3 DES في أغلب مؤشرات الأداء [11].

الشكل 5: مقارنة أزمنة التشفير وفك التشفير بين DES و AES و RSA.

3.3.نتائج الاختبارات الإحصائية الأربعة عشر(NIST)

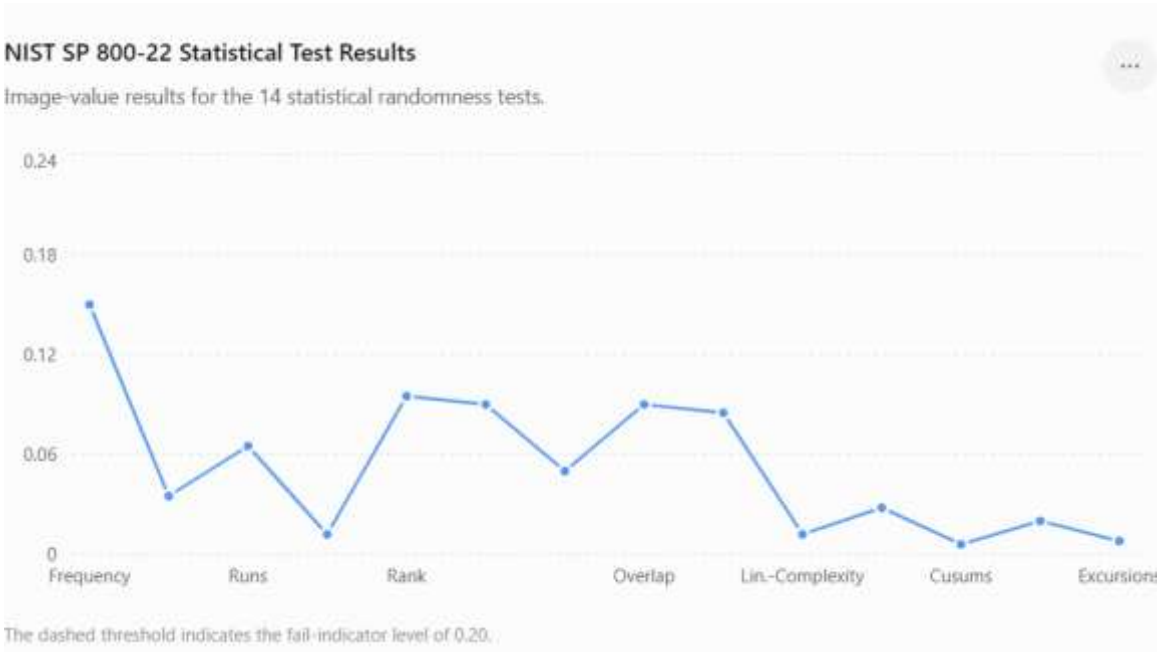
جدول 4: نتائج الاختبارات لنجاح عينة الملف المشفر الخارجية.

#	الاختبار	النتيجة
1	The Frequency (monobit)	ناجح
	Frequency test within a Block	ناجح

ناجح	The Runs	
ناجح	For the longest–run of one’s a Block	
ناجح	The binary matrix Rank	
ناجح	The discrete Fourier transform	
ناجح	The non-overlapping template matching	
ناجح	The non-overlapping template matching (بالتسمية الواردة في المصدر)	
ناجح	Maurer’s “universal statistical”	
ناجح	The linear complexity	
ناجح	The approximate entropy	
ناجح	The cumulative sums (Cusums)	
ناجح	The random excursions variant	
ناجح	The random Excursions	

حققت جميع الاختبارات الأربعة عشر نتيجة "ناجح" (الجدول 4)، وفي مخطط قيم الاختبارات العشوائية (الشكل 6) بقيت جميع القيم المقاسة دون خط المؤشر الفاشل (Fail indicator) البالغ 0.2، بما يطابق معيار القبول $p > 0.01$ المعمول به في المجموعة [10]. أثبتت هذه النتائج موثوقية المكوّنات العشوائية المستخدمة، مما يرسّخ الثقة في المتانة الأمنية للنظام

.



الشكل 6: قيم اختبارات العشوائية الأربعة عشر مقابل حد الفشل 0.2.

4.3. النتائج الوظيفية للتنفيذ

أظهر التنفيذ الفعلي سلوكاً وظيفياً مطابقاً للمواصفات فعند اختيار مسار الملف المراد تشفيره ظهرت رسالة "تم التشفير بنجاح"، وعرض الملف المشفر بوصفه غير قابل للعرض كصورة (not image)؛ وبعد إدخال مفتاح فك التشفير ظهرت رسالة "تم فك التشفير بنجاح" واستُعيد الملف الأصلي كاملاً (صورة JPEG بحجم 59.83 كيلوبايت وأبعاد 901×720 بكسل) دون أي فقدان أو تشويه. ووثّقت العينات النص الأصلي بالبتات وبنظام ASCII (بايتات على النمط 11111111)، ومفتاح التشفير المطبق المبدوء بالتسلسل: 15 15 17 15 12 13 13 17 11 19 11 11 11 11 11 11 41 49 1 e 2e 17 0f 2b 01 00 00 00 0e 00 0e 20 20 20 ... ff da 2 ... 17 15 17 15 15 15 15 18 60 baea 6e 04 40 08 59 25 b4 89 02 63 9e 00 3f 00 00 00، وعينة الملف المشفر بعد التمرير عبر النموذج المطبق.

5.3. النتائج الموجزة للنظام

توصّلت الدراسة عبر نتائجها إلى:

1. تفوق AES في الأداء والأمان مقارنة بالخوارزميات الأخرى RC4 و DES في تشفير البيانات، مما يجعله الخيار الأمثل لتطبيقات حماية الملفات .
2. نجاح الاختبارات العشوائية المطبقة (Randomize Tests) على الخوارزمية، مما يدل على درجة تعقيد عالية عند الهجمات الجبرية والفيزيائية والإلكترونية التي تستخدم للوصول إلى المحتوى الأصلي باستخدام مفتاح طوله 128 بت، وبما يجعل زمن الاختراق المحتمل يصل إلى 4 سنوات باستخدام المعالجات الحديثة كما ورد نصاً في النتائج .
3. إمكانية استخدام خوارزمية AES لتشفير الملفات المخزونة على القرص الصلب لتحقيق مستويات أمنية متعددة تشمل مستوى المستخدم ومستوى التطبيقات ومستوى نظام التشغيل .
4. إسهام واجهة المستخدم بتأكيد المفتاح بنفسه لضمان السرية في البيانات الشخصية، حيث يتمكن المستخدم من إدخال مفتاح التشفير بصورة صريحة .
5. زيادة تشفير الملف نفسه باستخدام مفاتيح مختلفة ترفع المستوى الأمني على الملف .
6. فعالية النظام في بيئات التشغيل المختلفة اختُبر على مجموعة متنوعة من الملفات (نصية، صورية، فيديو) وأظهرت نتائج منسجمة من حيث السرعة والدقة .
7. انخفاض استهلاك موارد النظام (الذاكرة والتخزين) أثناء تنفيذ عمليات التشفير، مما يجعله مناسباً للتشغيل على أجهزة ذات إمكانيات متوسطة .

---

4. المناقشة وبيان القيود

1.4. التفسير التقني للنتائج

تفسّر بنية الجولات التفوق الملحوظ في أولًا: الاستبدال غير الخطي ByteSub مع خلط الأعمدة على $GF(2^8)$(المعادلات 5–8) يكسر أي بنية خطية محتملة، ويدعم ذلك التحقق الرياضي في المعادلة 10 $S[i] + S[j] \neq S[i + j]$.ثانيًا: جدولة المفاتيح بثابتات RCON (قوى العدد 2 في الحقل) تضمن استقلالية مفاتيح الجولة وتمنع ظهور مفاتيح ضعيفة كما في DES [5]. ثالثًا: الاعتماد على عشر جولات بمفتاح 128 بت يبقي أفضل الهجمات الموثقة [6] محصورة في نسخ مخففة، بينما يبقى كسر النسخة الكاملة مقيداً بمساحة 2^{128} [5]، وهو ما ينعكس في زمن الفحص الشامل 5×10^{21} سنة. رابعًا: يضيف وضع GCM طبقة التحقق الموثق من السلامة ضمن العملية نفسها [14]، فلا يكتفي النظام بالسرية بل يكشف أي تعديل غير مصرح به، استيفاءً لأهداف التشفير من السرية وتكاملية البيانات وإثبات شخصية الكائنية وإثبات شخصية الرسالة وغيرها. خامسًا: التوفيق بين زمن تشفير منخفض (1.6 ثانية) واستهلاك موارد متوسط يجعل النظام عملياً على أجهزة ذات إمكانيات محدودة، وهو ما تؤكده نتيجة الاسترجاع الكامل لعينة 59.83 كيلوبايت دون زيادة جوهرية في الحجم.

2.4.موقع النظام من الأدبيات

مقارنةً بالأعمال السابقة، يتقدم هذا النظام على الدراسة المحاكاتية [11] ببناء أداة كاملة وتحليل نتائج التشفير بعد تطبيقها فعلياً على الملفات وفق معيارNIST، وعلى دراسة تعديل RC4 بمعالجة تشفير الملفات المخزنة على القرص الصلب عبر هيئة AES بدل التدفقات، وعلى نظام النقل الشبكي [12] بتغطية سيناريو التخزين المحلي مع تقييم عشوائية المكوّنات. ومع ذلك، يُلتزم هنا بعدم ادعاء الأسبقية المطلقة؛ فالمقارنة محصورة في الأدبيات المذكورة ضمن المستندات المصدرية، وعبارة "يُعدّ آمناً" في جدول المقارنة تعكس الحالة المعيارية لـ AES الموثقة في [4] FIPS 197 وليست ادعاء أمان مطلق أو برهاناً شكلياً.

3.4.القيود والفرضيات التشغيلية (Limitations)

تُعلن الدراسة بصراحة القيود الآتية دون تعويضها ببيانات مولَّدة :

مقاييس غير مقاسة رقمياً في بيانات المصدر: لم يوثَّق معدل الإنتاجية (MB/s) ؛ لم تُقس قيم الإنتروبيا عددية (اكتفى المصدر باختبار Approximate Entropy النوعي "ناجح")؛ لم تُقس نسب تأثير الانهيار الجليدي كمّياً (وُصفت نماذج Key Avalanche و Plaintext Avalancheكإطار اختبار دون قيم مئوية)؛ لم تتوفر معاملات ارتباط عددية (اختبار Plaintext/Ciphertext Correlation ورد نوعياً)؛ لم ترد مؤشراتNPCR/UACI ؛ ولم توثَّق البصمة الذاكرية الدقيقة (اكتُفي بنتيجة نوعية حول انخفاض استهلاك الموارد) .

تعارض ظاهري داخل بيانات المصدر: ذكر قسم النتائج زمن اختراق محتمل قدره "4 سنوات باستخدام المعالجات الحديثة" لمفتاح 128 بت، بينما قدّرت جداول المقارنة نفسها زمن الفحص الشامل بـ× 5 10^{21} سنة عند 50 مليار مفتاح/ثانية؛ لم تتيح بيانات المصدر تسوية هذا التعارض، فأُبقيت القيمتان موثقتين بموضعهما الأصلي .

سيناريوهات هجوم غير مُقيَّمة: لم تُنفَّذ ضمن هذه الدراسة تجارب هجوم النص الأصلي المختار (Chosen-Plaintext)، ولا الهجمات الجانبية(Side-Channel) ، ولا تحليلات التمييز التفاضلي/الخطي التجريبية؛ واكتُفي بمقاومة موثقة في المراجع [5, 6] وبنتائج الجداول المقارنة .

غياب إثبات أمان شكلي: لم يقدم المصدر برهاناً شكلياً للأمان؛ وتعابير مثل "لا يمكن كسرها بسهولة" تعكس وصفاً مقارناً لا ادعاء unbreakable أو provably secure.

افتراضات إدارة المفاتيح: يُشتق المفتاح من كلمة مرور تُدخل عبر الواجهة (Enter PassWord)، ويُفترض توزيع آمن للمفاتيح وقبول المستخدم لمسؤولية إدخال مفتاح التشفير بصورة صريحة؛ آلية توليد متجهات التهيئة وضوابط منع إعادة استخدامها لم تُوثَّق تفصيلاً في المصدر .

بيئة القياس غير موصوفة: مواصفات العتاد وحجم المدخلة المرجعية التي قيست عليها أزمنة الجدول 3 غير مصرح بهما في المصدر، مما يحد من قابلية التعميم عبر المنصات .

الدلالة الإحصائية: لم تُطبق اختبارات دلالة عند مستوى $p < 0.05$ على فروق الأزمنة لعدم توفّر عينات قياس متعددة في بيانات المصدر؛ واعتمد التقييم الإحصائي للعشوائية معيار القبول $p > 0.01$ [10].

حجم عينة الاختبارات الوظيفية: اقتصر التوثيق الوظيفي على عينات معروضة (نص، صورة، مثال ملف 59.83 كيلوبايت) دون كيان اختباري واسع موثق .

تفاصيل تنفيذ GCM : ورد وضع GCM في ملخص الدراسة ومتطلباتها وفي مرجع التوصية [14]، دون عرض كود مفصل لإدارة العداد ومتجه التهيئة في بيانات المصدر .

---

1. الخاتمة والأعمال المستقبلية

1.5. الخاتمة

توصّلت الدراسة إلى تصميم وتطوير نظام تطبيقي فعّال لتشفير الملفات وفك تشفيرها باستخدام خوارزمية AES، وذلك ضمن بيئة تطويرVisual Basic .NET ، بما يتلاءم مع سهولة الاستخدام والموثوقية العالية. تمكّن النظام المقترح من إنجاز عمليات التشفير من البداية حتى النهاية (End-to-

End) عبر مراحل متسلسلة، بدءاً من إدخال النص الواضح (Plaintext) ، مروراً بتطبيق خوارزمية التشفير مع إدارة مفاتيح التشفير، وصولاً إلى إنتاج ملف مشفر يُحفظ في الموقع الذي يحدده المستخدم، مع إمكانية فك التشفير واستعادة المحتوى الأصلي بدقة تامة ودون أي زيادة ملحوظة في حجم الملفات المعالجة. كما خضع النظام لاختبارات المولدات العشوائية (Random Number Tests) لتقييم جودة المكوّنات العشوائية المستخدمة في عملية التشفير، وأثبتت النتائج مطابقتها للمعايير المطلوبة، مما يعزز متانة النظام وقدرته على مقاومة الهجمات التي تهدف إلى استنتاج النص الواضح أو اختراق البيانات المشفرة.

2.5. الأعمال المستقبلية

يقترح مساران واقعيين للتطوير:

المسار الأول — تعزيز هيكلي وتطبيقي: (1) تطوير خوارزميات التشفير عموماً، لا AES فقط، من خلال الدمج البيني بين خوارزميات الذكاء الاصطناعي لزيادة مستوى الحماية؛ (2) تطوير التطبيق ليعمل على منصات متعددة (Web Application) و (Mobile Application)وتوجيه الواجهة ليتيسر الوصول إليها بكل سهولة لمختلف فئات المستخدمين؛ (3) دمج طبقات مصادقة إضافية (كمصادقة ثنائية أو كلمات مرور) مع النظام لرفع مستوى الحماية ومنع الوصول غير المصرح به حتى في حالة تسريب المفاتيح؛ (4) توثيق عملية التشفير من خلال سجلات (Logs) لتتبع المسؤولين عن عمليات التشفير وفك التشفير لأغراض التدقيق الأمني؛ (5) اعتماد النظام في المؤسسات الحكومية والقطاعات الحيوية كالصحة والتعليم والمالية، بما يوفر مستوى حماية معتبراً وبكلفة منخفضة.

المسار الثاني — التحقق الشكلي وتحليلات أعمق: (1) قياس إمكانية هجوم خوارزمية AES من خلال الهجمات الجبرية ودراسة إمكانية زيادة زمن الوصول إلى النص الواضح مع تطور أجهزة المعالجة؛ (2) تنفيذ القياسات الكمية الغائبة (الإنتاجية MB/s) على بيانات معيارية موصوفة، الإنتروبيا، نسب الانهيار الجليدي، معاملات الارتباط، NPCR/UACI، البصمة الذاكرية مع توثيق بيئة القياس؛ (3) مراجعة أمن الملفات على المستويات المتعددة (المستخدمين، التطبيقات، نظام التشغيل) قبل استخدام أي نظام مهما كانت درجة أمانه، لضمان الأمنية الكافية للخصوصية.

References

[1] C. Paar and J. Pelzl, *Understanding Cryptography: A Textbook for Students and Practitioners*. Berlin, Germany: Springer, 2009.

[2] National Institute of Standards and Technology (NIST), “Data Encryption Standard (DES),” Federal Information Processing Standards Publication 46-3, Gaithersburg, MD: National Institute of Standards and Technology, 1999.

[3] M. E. McKague, “Design and Analysis of RC4-like Stream Ciphers,” Master’s thesis, University of Waterloo, Waterloo, Ontario, Canada, 2005.

[4] National Institute of Standards and Technology (NIST), “Advanced Encryption Standard (AES),” Federal Information Processing Standards Publication 197, Gaithersburg, MD: National Institute of Standards and Technology, 2001.

[5] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*. Berlin, Germany: Springer, 2002.

[6] N. T. Courtois and J. Pieprzyk, “Cryptanalysis of block ciphers with overdefined systems of equations,” in *Advances in Cryptology—ASIACRYPT 2002*, Lecture Notes in Computer Science, vol. 2501, pp. 267–287. Springer, 2002.

[7] R. H. Arpaci-Dusseau and A. C. Arpaci-Dusseau, *File Systems*. Arpaci-Dusseau Books, 2014.

[8] R. H. Arpaci-Dusseau and A. C. Arpaci-Dusseau, *Network File Systems*. Arpaci-Dusseau Books, 2014.

[9] T. Ritter, “Substitution cipher with pseudo-random shuffling: The dynamic substitution combiner,” *Cryptologia*, vol. 14, no. 4, pp. 289–303, 1990.

[10] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, S. D. Leigh, M. Levenson, M. Vangel, D. L. Banks, N. A. Heckert, J. F. Dray, and S. Vo, "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," NIST Special Publication 800-22 Rev. 1a, Gaithersburg, MD: National Institute of Standards and Technology, 2010.
[11] J. Thakur and N. Kumar, "DES, AES and Blowfish: Symmetric key cryptography algorithms simulation based performance analysis," *International Journal of Emerging Technology and Advanced Engineering*, vol. 1, no. 2, pp. 6–12, 2011.
[12] N. S. M. Usop, A. F. Abidin, F. A. Wahab, and N. Udin@Kamaruddin, "Securing file transferring system by implementing AES algorithm," *World Applied Sciences Journal*, vol. 35, pp. 122–132, 2017.
[13] R. C. Merkle, "A Software Encryption Function," Xerox PARC, 1989.
[14] NIST, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," NIST Special Publication 800-38D, Gaithersburg, MD: National Institute of Standards and Technology, 2008.

[15] Abdulwahid A. Khalleefah, Omar G. Mrehel, & Abdurazaq Elbaz. (2026). Economic Load Dispatch Optimization Using the Jaya Algorithm: A Case Study on the Libyan Power Grid. International Journal of Computer Information Systems and Industrial Management Applications, 18(8s), 552–564. https://doi.org/10.70917/ijcisim-2026-3297.