وزارة التعليم العالي والبحث العملي

جامعة بابل /كلية العلوم للبنات

قسم الحاسبات

بحث لاستكمال متطلبات درجة البكالوريوس في علوم الحاسب الآلي

التشفير باستخدام خوارزمية Advanced Encryption Standard

إعداد

زهراء سليم عبدالله

إشراف

د.سيف محمود خلف العلاق

١٤٤٤هـ ٢٠٢٣م

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

﴿وَمَا أُوتِيتُمْ مِنَ الْعِلْمِ إِلَّا قَلِيلًا﴾

صدق الله العلي العظيم

سورة الأسراء الآية (٨٥)

جدول المحتويات

قائمة المختصرات

المختصر	**الدلالة**
AES	Advanced Encryption Standard
ECB	Electronic code book
CBC	Cipher Block Chaining
CFB	Cipher Feed Back
OFB	Output Feed Back

قائمة الاشكال

الأهداء

بِسْمِ ٱللَّهِ ٱلرَّحْمَٰنِ ٱلرَّحِيمِ

(قل إعملوا فسيرى الله عملكم ورسوله والمؤمنون)

إلهي لايطيب الليل إلا بشكرك ولايطيب النهار إلى بطاعتك .. ولاتطيب اللحظات إلا بذكرك .. ولا تطيب الآخرة إلا بعفوك .. ولا تطيب الجنة إلا برؤيتك الله ﷻ إلى من بلغ الرسالة وأدى الأمانة .. ونصح الأمة .. إلى نبي الرحمة ونور العالمين ..سيدنا محمد ﷺ إلى من كلله الله بالهيبة والوقار .. إلى من علمني العطاء بدون انتظار .. إلى من أحمل أسمه بكل افتخار .. أرجو من الله أن يمد في عمرك لترى ثماراً قد حان قطافها بعد طول انتظار وستبقى كلماتك نجوم أهتدي بها اليوم وفي الغد وإلى الأبد ..والدي العزيز)إلى ملاكي في الحياة .. إلى معنى الحب وإلى معنى الحنان والتفاني .. إلى بسمة الحياة وسر الوجود إلى من كان دعائها سر نجاحي وحنانها بلسم جراحي إلى أغلى الحبايب امي الحبيبة.

وكذلك نشكر كل من ساعد على إتمام هذا البحث وقدم لنا العون ومد لنا يد المساعدة وزودنا بالمعلومات اللازمة لإتمام هذا البحث ونخص بالذكر: د.سيف محمود خلف العلاق

الملخص

ان انتشار واستخدام المعلومات الرقمية في مختلف مجالات الحياة زاد من اهمية الاهتمام بأمنية البيانات التي تنتقل عبر شبكات الحاسوب. ولذلك تم استخدام طرق مختلفة لتأمين البيانات في شبكات الحاسوب ومن هذه الطرق هي طرق تشفير البيانات. يوجد نوعين رئيسين من طرق التشفير وهما طريقة التشفير المتناظر(Symmetric) الذي يعتمد على استخدام مفتاح واحد لغرض التشفير وفك الشفرة. وهناك نوع اخر من طرق التشفير وهي الغير متناظرة (Asymmetric) التي تستخدم مفتاح معلن لغرض التشفير ومفتاح سري لغرض فك الشفرة. من اهم طرق التشفير المتناظر هي طريقة (AES Advanced Encryption Standard) وهي تستخدم في تطبيقات مختلفة.

خوارزمية (AES) لها ثلاث اطوار مختلفة تستخدم فيهم احجام مفاتيح مختلفة هي ١٢٨، ١٩٢،٢٥٦ بت ويكون حجم البلوك فيها ١٢٨ بت.

في هذا المشروع تم حساب وقت التشفير باستخدام خوارزمية (AES) لثلاث ملفات مختلفة الحجم (١٧٤٧٠٤, ١٥٧٢٢٥٦,٥٢٤٠٩٦) وتم حساب وقت التشفير (٣.٤,٧.٨٤,١٥.٣٦) لنفس الملفات ثم تم مقارنة النتائج مع وقت فك الشفرة (٢.٣٢,٥.٤٨,١١.٨٨). وكان وقت التشفير وفك التشفير يزداد بازدياد حجم الملف ووجدنا ان وقت التشفير هو اكبر من وقت فك التشفير لملفات الاختبار. تم اجراء الاختبارات باستخدام لغة برمجة جافا (NetBean) و على حاسوب من نوع ايسر بمعالج (corei7) وذاكرة (8GB).

الفصل الاول

الجزء النظري

١ـ ١ مقدمة

يتضمن هذا الفصل لمحه عن علم التشفير وانواعه واهدافه، سيشمل هذا الفصل ايضاً إيضاح خوارزمية موضوع البحث من حيث تحليل وتحديد الجوانب الايجابية والسلبية والمستوى الامني الخاص بها

يُشار عادةً إلى علم التشفير باسم "دراسة السر". التشفير هي عملية تحويل النص العادي إلى نموذج غير قابل للقراءة. فك التشفير عملية تحويل النص المشفر إلى نص عادي في شكل مقروء ، فإن نظام

عملية التشفير التقليدية كما هو محدد في RFC 2828 (RFC2828) التشفير هو "مجموعة من خوارزميات التشفير جنبًا إلى جنب مع عمليات الإدارة الرئيسية التي دعم استخدام الخوارزميات في بعض سياق التطبيق. " التعريف يعطي الآلية الكاملة التي توفر المستوى الضروري من الأمان

تتألف من بروتوكولات الشبكة وخوارزميات تشفير البيانات[١]

١ـ٢ علم التشفير وانواعه

ان الأصل اللغوي لمفردة التشفير (Cryptography) إغريقي حيث تتكون المفردة من جزئيين

الأول "Crypto " وتعني سري والثاني "graphy "وتعني كتابة (Writing) ولذلك فإن

المصطلح (Cryptography) الكتابة السرية للنص الواضح حيث تم استخدامها منذ قديم الزمان

بشكل بسيط مثل (شيفرة القيصر)، أما في الوقت الحالي فيتم استخدامها بشكل معقد جداً وأكثر

تطوراً بسبب تزايد حاجة الإنسان لها في الوقت الحاضر. [2]

إذا نستطيع القول إن علم التشفير Cryptography هو جزء من علم أمن المعلومات

security information وهو علم وفن حماية البيانات والمعلومات وعلم سرية الرسالة، حيث

تعد عملية إخفاء معنى الرسالة هي أحد أهم الأهداف الأساسية لعلم التشفير، والذي يتضمن التخزين

والإرسال والاستقبال للمعلومات والبيانات بشكل آمن عبر وسائط نقل وتخزين غير محمية وغير

آمنة مثل شبكة الانترنت أو الشبكات اللاسلكية أو عبر السحابة ويتم ذلك بتشفير البيانات المعلومات

النصية أو الصور او غيرها من أنواع المعلومات المختلفة ليصبح شكلها غير مفهوم أو مقروه وذلك

بمساعدة العديد من خوارزميات التشفير[٣]

١-٢-١ /لتشفير المتماثل (Symmetric Encryption)

التشفير بشكل عام هو عملية الحفاظ على سرية المعلومات (الثابت منها و المتحرك) باستخدام برامج لها القدرة على تحويل وترجمة تلك المعلومات الى رموز بحيث إذا ما تم الوصول إليها من قبل أشخاص غير مخول لهم بذلك لا يستطيعون فهم أي شي لأن ما يظهر لهم هو خليط من الرموز والأرقام و الحروف الغير مفهومة، يتم تشفير الملف وفك التشفير عن طريق كلمة السر، التي يجب ان تكون معروفة للطرفين (المرسل والمستقبل) وهذا ما يسمى بالتشفير المتماثل. ويسمى أيضًا باسم تشفير المفتاح الفردي. يستخدم مفتاح واحد. في هذا التشفير عملية المتلقي والمرسل يجب أن يتفق على واحد مفتاح سري (مشترك). إعطاء رسالة (تسمى نص عادي) والمفتاح ،ينتج عن التشفير بيانات غير مفهومة ، وهي بنفس طول ملفات كان النص الصريح. فك التشفير هو عكس التشفير ، ويستخدم الامتداد نفس مفتاح التشفير. اشهر طرق التشفير المتماثل (Blowfish, Digital Encryption Standard (DES), TinyEncryption Algorithm, Triple DES, and (International Data Encryption

قوة التشفير: تعتمد قوة وفعالية التشفير على عاملين اساسين: الخوارزمية، وطول مفتاح البت، كل ما زاد البت، زادت نسبة الامان وصعوبة فك التشفير. الطريق الصحيحة لتشفير الملف: ١-ضغط الملف.٢- ومن ثم تشفيره.

١-٢-٢ التشفير غير متماثل (Asymmetric Encryption)

مع ازدياد الاعتماد على البريد الالكتروني أحد أهم وسائل الاتصال في قطاع الأعمال يزداد القلق من مخاطر استخدام البريد الالكتروني على سرية المراسلات ومن إساءة استخدامه عن قصد. وخاصة بعد انكشاف منظومات تجسس عملاقة تديرها حكومة الولايات المتحدة الأمريكية وحلفاؤها في بريطانيا وأستراليا. ومؤخرا أقرت الولايات المتحدة قانونا يبيح التجسس

على مراسلات الأفراد بدون إذن قانوني، مما يزيد المخاوف من عمليات تجسس مستمرة على المراسلات الشخصية للأفراد والشركات.

يقصد بالتشفير الغير متناظر، اي وجود مفتاحين لإتمام عملية التشفير وفك التشفير، وليس مفتاح واحد كما في التشفير المتناظر. يتكون التشفير الغير متماثل من مفتاحين وهما:

١- المفتاح العام الذي يستخدم لتشفير الرسالة، ويتم ارساله لمن تريد (شخص، مجموعة)

٢- المفتاح الخاص الذي يستخدم لفك التشفير، تحتفظ به في جهازك الخاص ، لا احد يعرف كلمة سر المفتاح الخاص، ولا يمكن فك الشيفرة عن الرسالة الا عن طريق المفتاح الخاص فقط، فإذا ضاع المفتاح الخاص فلا يمكنك فك التشفير عن الرسالة.

آلية عمل هذه التقنية: بعد القيام بتكوين المفتاحين، تقوم بإرسال المفتاح العام لمن تريد (شخص، مجموعة..)، مهمة المفتاح العام هي عمل تشفير للرسالة فقط وليس فك التشفير، الطرف المستقبل يقوم بتشفير الرسالة عن طريق استخدام مفتاحك العام الذي تم ارساله اليه، بعد ذلك يقوم الطرف المستقبل بإرسال الرسالة المشفرة الى المرسل الأصلي الذي قام بإرسال المفتاح العام له، عند استلام المرسل الرسالة المشفرة فإنه يقوم بفك التشفير عن طريق المفتاح الخاص فقط ، هو الوحيد الذي يستطيع فك التشفير عن ذلك الملف.

١-٣ تطبيقات علم التشفير وفوائده

فوائد التشفير: الغرض الأساسي من التشفير هو حماية سرية البيانات الرقمية المخزنة على أنظمة الكمبيوتر أو المنقولة عبر الإنترنت أو المنقولة عبر الانترنيت او أي شبكة كمبيوتر اخرى. بالإضافة إلى الأمان، غالبًا ما يكون اعتماد التشفير مدفوعًا بالحاجة إلى تلبية لوائح الامتثال. يوصي عدد من المؤسسات والهيئات المعنية بالمعايير أو تتطلب تشفير البيانات الحساسة من أجل منع الأطراف الثالثة غير المصرح لها أو الجهات الفاعلة التي تهدد من الوصول إلى البيانات. على سبيل المثال ،

يتطلب معيار أمان بيانات صناعة بطاقة الدفع من التجار تشفير بيانات بطاقة الدفع الخاصة بالزبائن عندما يتم تخزينها بالراحة ونقلها عبر الشبكات العام. [٤] 2011 Journal Anu Book

١- ٤ خوارزمية Advanced Encryption Standard (AES)

تنقسم خوارزمية التشفير إلى تشفير أحادي الاتجاه وتشفير ثنائي الاتجاه التشفير احادي التجاه لا يمكن التراجع عن خوارزمية التشفير أحادية الاتجاه ، أي أنه لا يمكن استعادة البيانات المشفرة إلى البيانات الأصلية ما لم يتم اعتماد هجوم التصادم والأساليب الشاملة. مثل تخزين كلمات مرور الحساب المصرفي، يتم اعتماد طريقة التشفير أحادية الاتجاه بشكل عام.

تشفير ثنائي الاتجاه إنه قابل للانعكاس ، وهناك مفتاح للنص المشفر ، ويمكن للطرف الذي يحمل النص المشفر فك تشفير النص العادي الأصلي وفقًا للمفتاح ، والذي يُستخدم بشكل عام عندما يتمكن كل من المرسل والمستقبل من الحصول على النص العادي من خلال المفتاح. يتضمن التشفير ثنائي الاتجاه التشفير المتماثل والتشفير غير المتماثل. يشمل التشفير المتماثل (DES) و (AES) إلخ. يشمل التشفير غير المتماثل (RSA) و (ECC).

خوارزمية ال(AES) هي اختصار لل (Advanced Encryption Standard). والمفهوم الاساسي لـ (AES)،حيث يجب ان نفهم اولا ثلاث مفاهيم اساسية لتعلم الخوارزمية (AES) هم المفتاح والحشو والوضع.

اولا: مفتاح التشفير

تدرك الخوارزمية أساسيات التشفير وفك التشفير. خوارزميات التشفير المتماثل متناظرة لأنها تتطلب نفس المفتاح لتشفير وفك تشفير النص العادي لخوارزمية تدعم ثلاثة أطوال رئيسية هم: 128 بت ، ١٩٢ بت ، ٢٥٦ بت. المفاتيح ذات اطوال مختلفة من منظور الامن (AES128)، (AES192)، (AES256) يشير في الواقع إلى استخدام خوارزمية AES عادة ما قال الجميع ان لمفاتيح ذات أطوال مختلفة. ، فإن (AES256) لديها أعلى أمان. من وجهة نظر الأداء ، تتمتع AES128بأعلى أداء. السبب الأساسي هو أن لديهم جولات معالجة تشفير مختلف

ثانيا: الحشوة (Padding)

عند تشفير النص العادي ، لا تقوم خوارزمية بتشفير النص العادي بالكاملASE لفهم مفهوم الحشو، يجب ان نفهم ميزة تشفير كتلة إلى نص مشفر بالكامل ، ولكنها تقسم النص العادي إلى كتل نص عادي مستقلة ، يبلغ طول كل منها ١٢٨ بت ولكن هنا تنطوي على

مشكلة:

إذا كان طول قطعة من النص العادي ١٩٢ بت ، إذا تم تقسيمه وفقًا لكتلة نص عادي كل ١٢٨ بت ، فإن كتلة النص العادي هي ٦٤ بت فقط ، أقل من ١٢٨ بت. ماذا تفعل في هذا الوقت؟ تحتاج إلى حشو كتل النص العادي. تحتوي AES على العديد من خوارزميات الحشو المختلفة في تطبيقات اللغات المختلفة ، وسنقدم فقط قائمة بالحشو النموذجي لتقديمه (No Padding). لا يلزم الحشو ، ولكن يجب أن يكون النص العادي عددًا صحيحًا مضاعفًا لـ ١٦ بايت. افتراضي (PKCS5Padding): إذا كانت كتلة النص العادي أقل من ١٦ بايت (١٢٨ بت) ، فسيتم إضافة العدد المقابل من الأحرف في نهاية كتلة النص العادي ، وتساوي قيمة كل بايت عدد الأحرف المفقودة .

ثالثا: الطور (Security Mode):

ينعكس وضع عمل هذه الخوارزمية في عملية تشفير كتلة نص عادي الى كتلة نص مشفر. توفر هذه الخوارزمية خمسة اوضاع مختلفة:

١- وضع دفتر الكود الإلكتروني (ECB)
٢- وضع سلسلة (CBC) ويعني (Cipher Block Chaining).
٣- وضع نسبة النقر إلى الظهور:CFB (Cipher Feed Back).
٤- وضع:OFB وضع تعليقات الإخراج (Output Feed Back)

١- ٤- ١ ميزات خوارزمية (AES)

توجد عدة مميزات لهذه الخوارزمية:

١- الحماية :تمتلك خوارزمية AES القدرة على مقاومة الهجمات بشكل أفضل من خوارزميات التشفير الأخرى.

٢- التكلفة:تشمل هذه الخوارزمية نطاق عالمي غير محدود وخالي من حقوق الملكية.

٣- التنفيذ :تتميز خوارزمية AES بالمرونة وهي مناسبة تمامًا عند تنفيذها في الأجهزة والبرامج.

١- ٤- ٢ أمن خوارزمية (AES)

يؤكد خبراء الأمن أن خوارزمية التشفير المتقدم AES آمنة عند تنفيذها بشكلٍ صحيحٍ. مع ذلك، يجب حماية مفاتيح تشفير .AES حتى أكثر أنظمة التشفير انتشارًا يمكن أن تكون عرضة للخطر إذا تمكن أحد المتطفلين من الوصول إلى مفتاح التشفير. يعد استخدام كلمات مرور قوية ومصادقة متعددة العوامل (MFA) وجدران الحماية وبرامج [5]

الفصل الثاني

الجزء العملي

٢ـ ١ مقدمة

يأتي لابتوب ايسر اسباير ٣ A315-54 ماركة ايسر من السلسلة (Aspire Acer), بشاشة مقاس ١٥.٦", ونظام تشغيل أساسي Windows 10, سعة تخزين الجهاز ١ TB HDD و 4 جيجابايت رام, أما المعالج فهو من نوع (Intel Core i5-10210U 10th Gen), وكرت الشاشة (UHD Intel Graphics 620), بسعر تقريبي ٥٥٠ دولار أمريكي.

(NetBeans) هو نظام أساسي لتطوير البرامج ، معظمه لـ Java ، يوفر معالجات وقوالب لمساعدة المطورين على إنشاء التطبيقات بسرعة وسهولة. وهي تتضمن مكونات معيارية عبر مجموعة واسعة من الأدوات وتتميز ببيئة تطوير متكاملة (IDE) تسمح للمطورين بإنشاء تطبيقات باستخدام واجهة المستخدم الرسومية. بينما يعد (NetBeans) أداة أساسية لمطوري جافا ، فإنه يدعم أيضًا(HTML5, C++, C, PHP). تاريخ (NetBeans) نشأت أصول (NetBeans) من مشروع جامعي في جامعة تشارلز في براغ في جمهورية التشيك في عام ١٩٩٦. أطلق عليه اسم IDE(Zelfi) لجافا (وهو اقلاع عن لغة البرمجة دلفي) ، وكان (NetBeans)أول جافا (IDE)من أي وقت مضى. كان الطلاب متحمسين حول هذا الموضوع وعملوا على تحويله إلى منتج تجاري. في أواخر التسعينات ، تم الحصول عليها من قبل شركة صن مايكروسيستمز التي دمجتها في مجموعة أدوات جافا الخاصة بها ، ثم حولتها إلى المصدر المفتوح. بحلول يونيو ٢٠٠٠ ، تم إطلاق موقع (netbeans)الأصلي.

٢ـ ٢ الاختبارات المقترحة في البحث

في هذا البحث تم انجاز اختبارين وهما اختبار التشفير واختبار فك التشفير. في كلا الاختبارين تم حساب الوقت المستغرق لإتمام الاختبار. تم اجراء الاختبارين على ثلاث عينات مختلفة من حيث

الحجم كما موضح بالجدول رقم (٢-١). ويجب الاشارة الى ان الوقت تم حساب المعدل له حيث تم حساب الوقت ١٠٠ مرة وحساب المعدل له لتقليل نسبة الاخطاء.

جدول (٢-١): حجم ملفات الاختبار

اسم الملف	حجم الملف
الملف الاول	**١٧٤٧٠٤ بايت**
الملف الثاني	**٥٢٤٠٩٦بايت**
الملف الثالث	**١٥٧٢٢٥٦بايت**

٢- ٢- ١ الاختبار الاول (التشفير)

في هذا الاختبار تم تشفير العينات (الملفات) ذات الاحجام المختلفة باستخدام خوارزمية تشفير متناظرة (وكما موضح في المخطط الانسيابي بالشكل (٢-١) والخوارزمية (٢-٢). حيث نقوم بادخال حجم الملف ومفتاح طالما قيمة له اصغر من حجم الفايل i,j,encryption time =0 الاخراج هو وقت التشفير اعطاء قيم ابتدائية $block_j$ نقوم بقراءة ١٦ بايت من الملف في

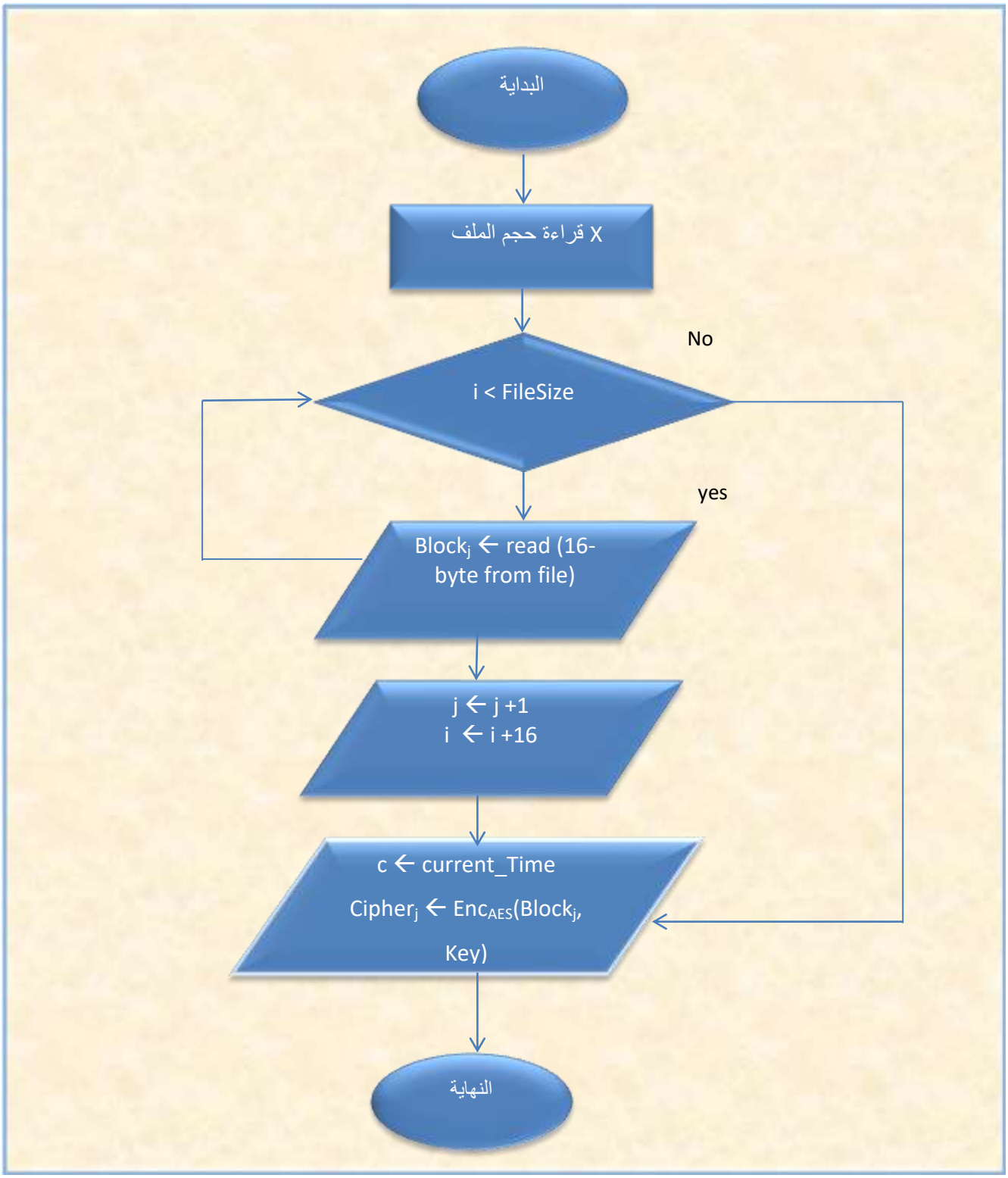
نقوم بزيادة ال I بمقدار ١ وال j بمقدار ١٦ C=current time

خوارزمية ال AES مدخلاتها ال BLOCK AND KEY الناتج بمتغير $cipher_j$

C=current time – c نقوم بطرح ال c من ال current time لتحصيل القيمة الجديدة

لتحصيل قيمة وقت التشفير الجديد نقوم بجمع حساب وقت التشفير القديم مع ال c

عند ال I الى اكبر من حجم الفايل نقوم بارجاع وقت التشفير

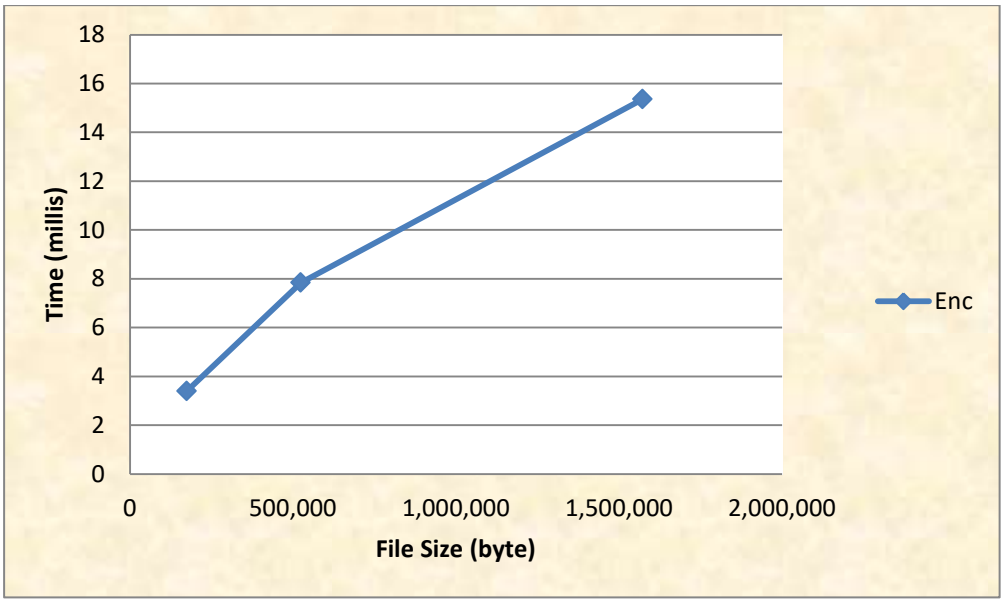


الشكل (٢-١) الاختبار الاول مخطط التشفير

Input: FileSize, Key
Output: Encryption_Time
Begin
1. i ← 0, j ← 0, Encryption_Time ←0
2. Do_While i < FileSize
3. $Block_j$ ← read (16-byte from file)
4. j ← j +1
5. i ← i +16
6. c ← current_Time
7. $Cipher_j$ ← $Enc_{AES}(Block_j, Key)$
8. c ← current_Time - c
9. Encryption_Time ← Encryption_Time + c
10. end_ Do_While
11. return Encryption_Time
12. End

شكل (٢-٢): خوارزمية حساب وقت تشفير (AES)

تشير النتائج المحسوبة في هذا الاختبار ان وقت التشفير يتزايد بشكل خطي مع زيادة حجم الملف المشفر كما هو موضح بالشكل (٢-٣). حيث ان الوقت المحسوب لتشفير ملف بحجم (١٧٤٧٠٤) وهو اقل ملف عينة البحث من جهة اخرى الوقت المحسوب لتشفير ملف بحجم (٥٢٤٠٩٦) بايت وهو اعلى ملف في عينة البحث كان (١٥٧٢٢٥٦).



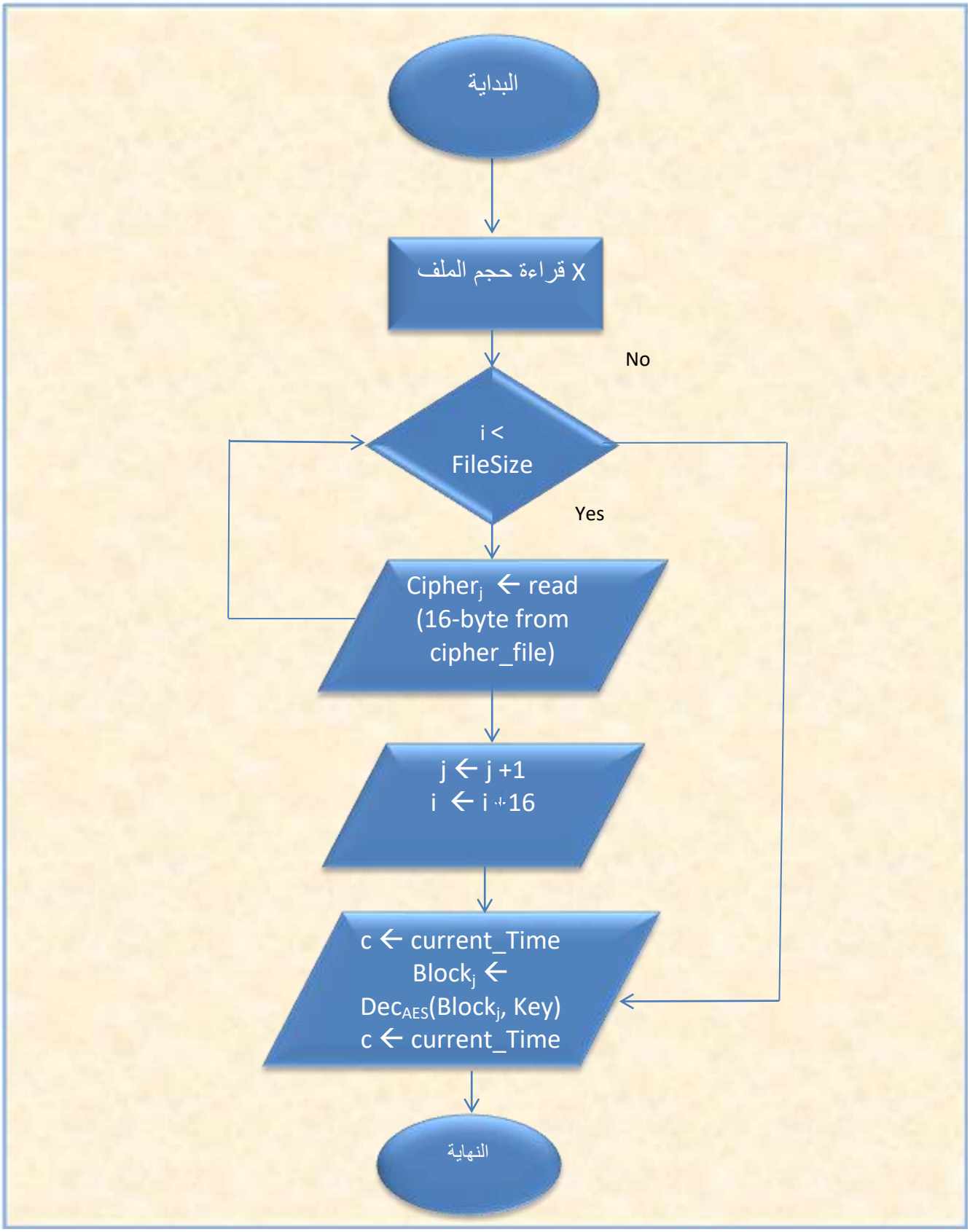
الشكل (٢-٣) نتائج وقت التشفير

٢-٢- ٢ الاختبار الثاني (فك التشفير)

كما موضح في هذا الاختبار تم فك تشفير العينات (الملفات) ذات الاحجام المختلفة باستخدام خوارزمية تشفير متناظرة (٢-٤) والخوارزمية (٢-٥). حيث نقوم بادخال حجم الملف ومفتاح طالما قيمة له اصغر من حجم الفايل i,j,decryption time =0 الاخراج هو وقت التشفير اعطاء قيم ابتدائية $block_j$نقوم بقراءة ١٦ بايت من الملف فيه نقوم بزيادة ال I بمقدار ١ وال j بمقدار١٦

C=current time خوارزمية ال AES مدخلاتها ال cipher AND KEY الناتج بمتغير BLOCk

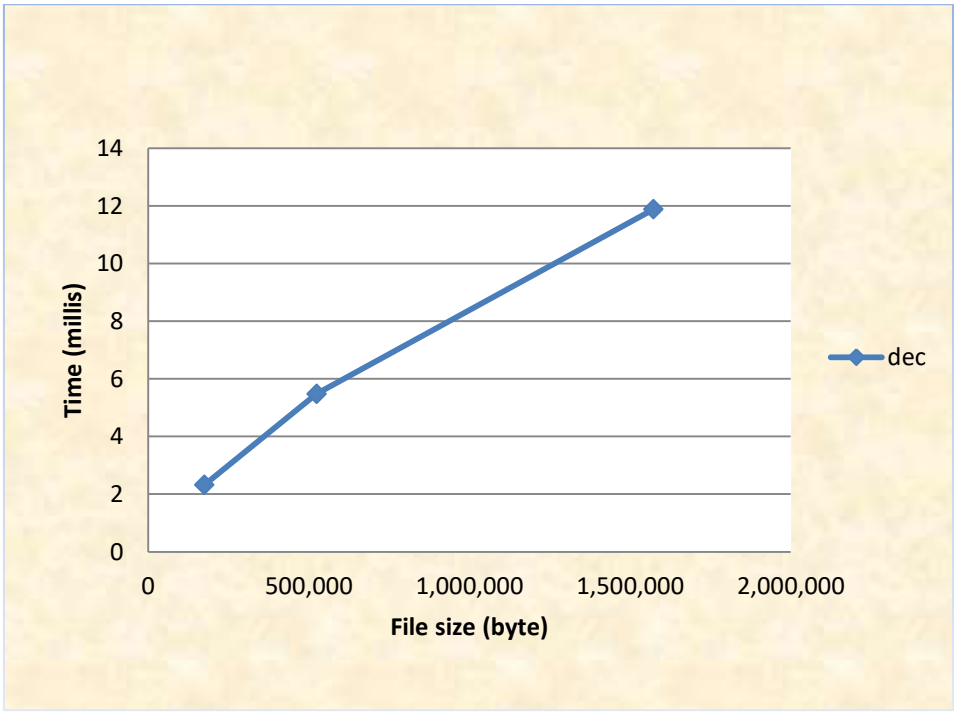
C=current time – c نقوم بطرح ال c من ال current time لتحصيل القيمة الجديدة لتحصيل قيمة وقت فك التشفير الجديد نقوم بجمع حساب وقت فك التشفير القديم مع ال cعند ال I الى اكبر من حجم الفايل نقوم بارجاع وقت فك التشفير


البداية
X قراءة حجم الملف
No
i < FileSize
Yes
Cipher_j ← read (16-byte from cipher_file)
j ← j +1
i ← i +16
c ← current_Time
Block_j ← Dec_AES(Block_j, Key)
c ← current_Time
النهاية

```
Input: FileSize, Key
Output: Decryption_Time
1.  Begin
2.     i ← 0, j ← 0, Decryption _Time ←0
3.     _While i < FileSize
4.         Cipher_j  ← read (16-byte from cipher_file)
5.         j ← j +1
6.         i  ← i +16
7.         c ← current_Time
8.         Block_j ← Dec_AES(Block_j, Key)
9.         c ← current_Time - c
10.        Decryption _Time ← Decryption _Time + c
11.    end_ Do_While
12.    return Decryption _Time
13.  End
```

الشكل(٢-٥): خوارزمية حساب وقت فك تشفير (AES)

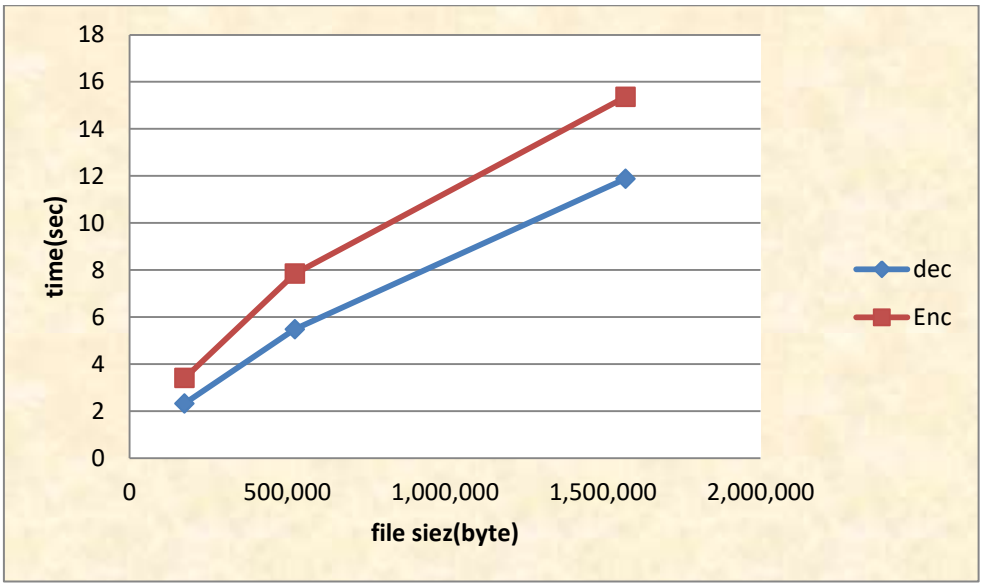
تشير النتائج المحسوبة في هذا الاختبار ان وقت فك التشفير يتزايد بشكل خطي مع زيادة حجم الملف المشفر كما هو موضح بالشكل (٢-٦). حيث ان الوقت المحسوب لفك تشفير ملف بحجم (١٧٤٧٠٤) وهو اقل ملف عينة البحث من جهة اخرى الوقت المحسوب لتشفير ملف بحجم (٥٢٤٠٩٦) بايت وهو اعلى ملف في عينة البحث كان .



الشكل(٢ -٦) نتائج فك التشفير

٢-٣ مقارنة بين التشفير وفك التشفير

عند الملف الاول الحجمه (١٧٤,٧٠٤) وقت التشفير في خوارزميةAES (٣.٤)بينما فك التشفير (٢.٣٢)والملف الثاني الحجمه(٥٢٤,٠٩٦) وقت التشفير(٧.٨٤)بينما فك التشفير (٥.٤٨) والملف الثالث الحجمه(١,٥٧٢,٢٥٦) وقت التشفي(١٥.٣٦)بينما فك التشفير (١١.٨٨)كما موضح في الشكل(٢-٧)



الشكل (٢-٧)مقارنة بين وقت التشفير ووقت فك التشفير

الاستنتاج

١-كلما يزداد حجم الملف يزداد وقت التشفير

٢- وقت فك التشفير يزداد مع زيادة حجم الملف

٣- وقت التشفير يكون اكبر من وقت فك التشفير

References

١. Nagesh Kumar1 , Jawahar Thakur2 , Arvind Kalia3 2Associate Professor, 3Professo . 2011 Journal Anu Books

٢. Whitman, M. E., & Mattord, H. J. (2013). *Management of information security*. Cengage Learning.

٣. Stallings, W. (2017). C Ryptography and. Stallings, W., Brown, L., Bauer, M. D., & Howard, M. (2012)

٤. symmetric Encryption, asymmetric Encryption. Nagesh Kumar1 , Jawahar Thakur2 , Arvind Kalia3 2Associate Professor, 3Professo . 2011 Journal Anu Books https://studylib.net/doc/25479989/2fc41064a148cbd737af2ea1eb07ddb2-cryptography

٥. Advanced Encryption Standard , https://abouttechnology.com/%D8%AE%D9%88%D8%A7%D8%B1%D8%B2%D9%85%D9%8A%D8%A7%D9%84%D8%AA%D8%B4%D9%81%D9%8A%D8%B1%D8/%A7%D9%84%D9%85%D8%AA%D9%82%D8%AF%D9%85-aes