تأمين البيانات باستخدام تقنية الـPGP

علي شائف محمد شعفل

مدرس بقسم تقنية المعلومات، كلية الهندسة وتقنية المعلومات، جامعة السعيد– تعز، اليمن

عمر عبد العزيز محمد أبو دابي

قسم علوم الحاسوب، كلية علوم الحاسوب وتقنية المعلومات، جامعة النيلين، الخرطوم، السودان

مها أبو يوسف

أستاذ مساعد، كلية علوم الحاسوب وتقنية المعلومات – جامعة النيلين، الخرطوم – السودان

تاريخ التسليم: ٣١ /١٢/ ٢٠١٧م تاريخ القبول: ٧ /١/ ٢٠١٨م

الملخص:

يُعد هذا البحث محاولة متواضعة لإثراء تشفير البيانات وتأمينها باستخدام تقنية الـ (PGP)، وقد استخدم الباحثون في الجانب العملي لغة برمجة (Java Netbeans) فهي شائعة الاستخدام لما تتمتع به من خصائص جميلة وأكثر سهولة بما فيها إنشاء الواجهات، وتم الدمج بين مجموعة خوارزميات في خوارزمية واحدة لزيادة تعقيد فهم البيانات المشفرة وحماية البيانات وزيادة تعقيد التشفير بحيث يصمد النظام أمام المعتدين الخارجيين والسيطرة على المفتاح وحمايته وكذا إدارته بطرق غاية في الدقة والأمان، وقد توصل البحث إلى النتائج التالية:

– تحقيق ثلاثة من أهداف التشفير ومتطلباته، هي:

* الوثوقية باستخدام خوارزمية تشفير متناظر من خلال (DES، TripleDES، AES، Blowfish).

* التكاملية باستخدام خوارزمية MD5.

* اثبات الشخصية وعدم الإنكار باستخدام خوارزمية المفتاح العام RSA.

– لم يتوفق الباحثون في استخدام خوارزميه لضغط النص.

الكلمات المفتاحية: تأمين البينات، الحماية، التشفير، فك التشفير، المفتاح العام، المفتاح الخاص، الدوال الهاشية، PGP.

Abstract:

This research is a modest attempt to enrich the data encryption and secure using PGP technology. In the practical side, the researchers used the Java Netbeans programming language, which is commonly used for its more beautiful and intuitive features including the creation of interfaces. One algorithm to increase the complexity of understanding encrypted data and data protection and increase the complexity of encryption so that the system is in front of external aggressors and control and protection of the key and management in a very accurate and safe manner, and the search results in the following:

- Achieve three of the objectives of encryption and its requirements:

* Reliability using symmetric encryption algorithm through (DES, TripleDES, AES, Blowfish).

* Integrity using the MD5 algorithm.

* Prove personal and non-denial using the RSA public key algorithm.

- Researchers have not been able to use the algorithm to compress text.

Keywords: data security, security, encryption, decryption, public key, private key, paging functions, PGP

١. المقدمـة:

إن الحاجة إلى أمنية المعلومات هي حاجة قديمة بقدم الحضارة نفسها، في ضرورة تناقل العبارات العسكرية والدبلوماسية، فاستخدام الاتصالات السرية بواسطة رسائل مرمزة كان موضوع التطبيق عبر التاريخ القديم والحديث، لذلك كان من الضروري إيجاد وسيلة يتم من خلالها التراسل بصورة آمنة وموثوقة، هذه الوسيلة تحققت عند المصريين القدماء منذ حوالي ٤٠٠٠ سنة باستخدام التشفير، والأسبان القدماء مثلًا شفروا عباراتهم العسكرية، وأما بالنسبة للصينيين فأنه يكفي فقط كتابة العبارات بلغتهم المعروفة والتي تعتبر لغة خاصة وذلك لأن القليل من الناس يستطيعوا قراءة الكلمات الصينية.

في الزمن القديم كانت قنوات الاتصال بسيطة تعتمد في تأمين السرية على استخدام مراسلين موثوقين، وهكذا أخذ التطور والاهتمام باستخدام التشفير لحماية الرسائل السرية، وبلغ هذا الاستخدام ذروته في فترات الحروب خوفًا من وقوع الرسائل الحساسة في يد العدو.

وبسبب اكتشاف أنظمة الحاسبات واستخدام شبكات الحاسوب الواسعة بين الدول في القرن العشرين فإن مفهوم الحماية قد تغير بصورة ملحوظة. ففي الحاسبات المبكرة (الأولى)، كانت الأمنية الفيزيائية ومعها سياسة الاختيار الملائم للكادر كافيان لتوفير الأمنية، لكن هذا المفهوم أصبح غير كافٍ بعد اكتشاف أنظمة حاسبات المشاركة الزمنية (Computers Timesharing) والتي تتألف من عدة محطات طرفية موزعة على مساحة جغرافية واسعة.

بعد التزايد الواضح في أجهزة الحاسوب وأنظمة الاتصال واستخدامها في شتى مجالات الحياة المدنية والعسكرية أصبح من الضروري توفير وسائل لحماية المعلومات، لذلك تم بذل مزيد من الجهد في بداية السبعينات حيث تم تطوير طرق تشفير معتمدة مثل (TripleDES، DES) وفي عام ١٩٨٥م تم إيجاد صنف من التشفير يتمتع بقوة كبيرة معتمدًا في ذلك على فكرة المفتاح العام (Public Key) والذي نبع منه استخدام التوقيعات الرقمية.

هذه التقنيات وتقنيات أخرى وفرت حماية كبيرة ضد الانتهاكات والخروق من المتطفلين وفي مقدمتهم هواة تحليل الشفرة. لذلك فإن طرق التشفير معرضة للكسر والانتهاك، فكلما تعرضت طرق التشفير للانتهاك يجد المصممون أنفسهم في تطوير طرق تشفير جديدة، ولهذا فقد جرت العديد من المحاولات لتوفير الحماية للبيانات.

٢. المنهجيـة:

طُوّرت تقنيات التشفير لتستخدم في الأغراض العسكرية والحربية. وبقيت التقنيات المتقدمة في التشفير حصرًا على الحكومات والمؤسسات الكبيرة، حتى كتب المبرمج فيليب زيمرمان Philip Zimmermann في العام ١٩٩١ برنامج (Pretty Good Privacy, PGP) أي (الخصوصية الجميلة)، وهو برنامج تشفير يستخدم ١٢٨- بت، لاستخدامه في تشفير البريد الإلكتروني والملفات الشخصية. وتؤدي زيادة عدد البتات في طول مفتاح التشفير، إلى زيادة صعوبة كسر المفتاح، وتزيد في الوقت ذاته الزمن اللازم لفك التشفير. فخوارزمية مثلًا، تعمل على ٤١-بت، تستهلك ضعف الزمن اللازم لفك تشفير خوارزمية ٤٠-بت، وتستهلك خوارزمية ٤٢-بت ضعف الزمن اللازم لفك تشفير خوارزمية ٤١-بت. ولا يمكن كسر تشفير خوارزمية بطول ١٢٨-بت على حواسيب هذه الأيام. وضع فيليب زيمرمان برنامجه PGP في رحاب الإنترنت. فأصبح بإمكان الأشخاص العاديين استخدام تقنية تشفير قوية جدًا في كل أنحاء العالم.

- **تحليل تقنية الـ PGP:**

إن PGP هي اختصار للعبارة pretty good privacy ولعلَّ هذا الأسلوب عالي الجودة في التشفير، وهو من الطرق الدارجة كثيرًا، خاصّة لما يتمتّع به من صمود غريب أمام أي محاولة لكسر نظام التشفير، ويتمتع بإدارة رئيسية ممتازة ومرنة، والعديد من الخوارزميّات

المُشفَّرة، وتكمن قوته في الـ PGP الذي اكتسبَ شهرة عالمية، جعلته واحدًا من أشهر الأساليب في المراسلة الإلكترونية المُشَفَّرَة والآمنة في نفس الوقت.

إنَّ الـ cryptosystems التقليديّ، هو عبارة عن مفتاح مزدوج الوظيفة، فهو يقوم بالتشفير وكذلك يقوم بفك الشيفرة نفسها ... ومن الشروط الأولى لضمان السرّيّة في عدم اكتشاف هذا المفتاح السرّي secret key ، هو إرساله إلى الطرف الآخر بالوسائل الآمنة، لأن أي شخص يتمكن من الحصول على نسخة من هذا المفتاح secret key السرّي، يستطيع حينها فكّ الشيفرة والاطلاع على كافة الكتابات .. إذًا المهمّة الأولى هي وجود المفتاح السرّي secret key لدى أطراف المُكاتَبة في مكانٍ آمن وحريز .. ثم تأتي بعدها المهمة الثانية وهي المفتاح العام public key الذي يستعمله الجمهور لتشفير الرسائل التي يُرسِلونَها إليك.

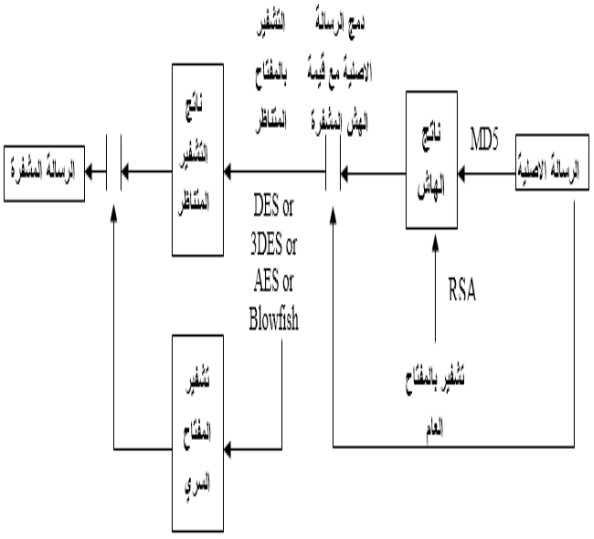
إن" فيليب زيميرمان " Philip Zimmermann مُخترع الـ PGP يعتمد في اختراعه على مفتاحين، العام والخاص، فالمفتاح الخاص، تستطيع بواسطته إنشاء رسائل مُشفَّرَة وفك رموزها، فيما المفتاح العام هو الذي يتداوله الجمهور الذي تختاره أنت، فبواسطة المفتاح الخاص تستطيع فكّ أيّ شيفرة رسالة مُشفَّرَة بواسطة المفتاح العام، فيما الذي يحمل المفتاح العام يستطيع فقط إرسال رسائل مُشَفرَة إليك، ولكنه لا يستطيع فك الشيفرة إطلاقًا، حتى أن كاتب الرسالة نفسه وبعد أن يقوم بتشفيرها – بواسطة المفتاح العام – لا يستطيع فكّ شيفرَتها، لِأَنَّهُ لا يملك المفتاح الخاص الذي تملكه أنت.

وحينَ تمتلك المفتاح العام تستطيع تشفير أيّة رسالة وترسلها سواءً بالبريد الإلكتروني، أو حتى تنشرها في صفحات WEB ومن ثمّ ترسل عنوان هذه الصفحات إلى مالِكي المفاتيح الخاصة، فيستطيعون هم فقط فكّ تشفيرها والاطلاع عليها دون غيرهم حتمًا، لأنَّ فك الشيفرة لا يتمّ إلاّ بواسطة المفتاح الخاص، كما أسلفنا سابقًا.

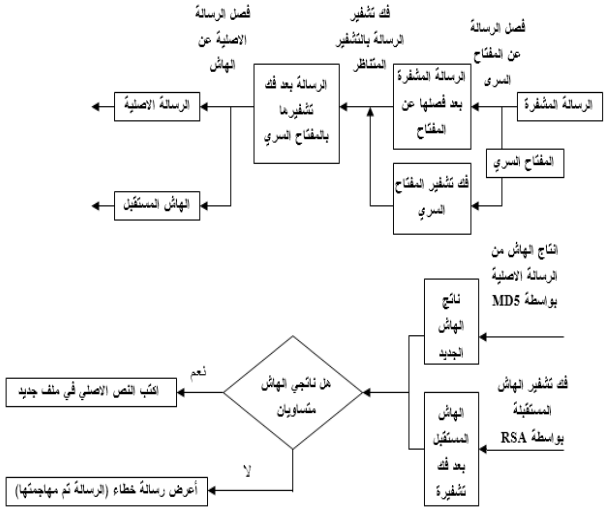
- **تحليل مكونات خوارزمية PGP:-**

ما يميز خوارزمية الـPGP هو انها تتكون من أكثر من خوارزمية تتساند معًا لتعطي تشفير عالي الجودة، ونحن بصدد استخدام هذه التقنية لما تتميز به من مميزات قوية وفعالة لتشفير الملفات النصية واضفاء ميزة التواقيع الرقمية واثبات الهوية.

في البداية يتم قراءة الملف المراد تشفيره، ثم يتم استخدامه لإنتاج قيمة الهاش بإحدى خوارزميات انتاج الـHash، ونحن هنا نستخدم خوارزمية الـMD5، ثم يتم تشفير قيمة الهاش بواسطة إحدى خوارزميات المفتاح العام، وهنا نستخدم خوارزمية RSA، ثم نقوم بدمج قيمة الهاش المشفرة ١٢٨–بت مع النص الأصلي للملف المراد تشفيره، وفي الخطوة الأخيرة يتم تشفير النص بإحدى خوارزميات المفتاح المتناظر (وهنا يتم تخيير المستخدم بإحدى الخوارزميات التالية وهي DES ، TripleDES ، AES ، Blowfish)، بعدها يتم كتابة النص المشفر في ملف جديد في نفس مسار الملف الأصلي. أما عند عمل فك تشفير ملف فإنه يتم بنفس الخوارزميات السابقة ولكن بعكس الترتيب. ويوضح الشكلان التاليان تسلسل عملية التشفير وفك التشفير بواسطة الـPGP .



شكل (١) تسلسل عملية التشفير بواسطة خوارزمية PGP



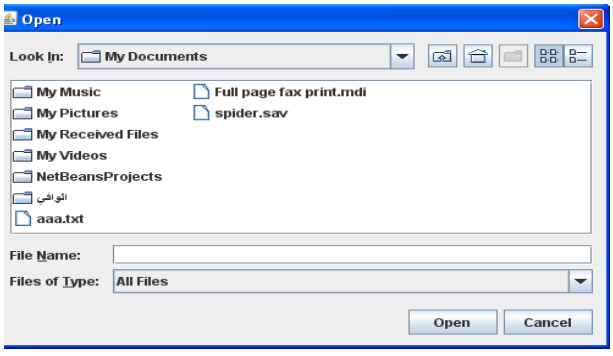
شكل (٢) تسلسل عملية فك التشفير بواسطة خوارزمية PGP

٣. النتائج:

الشاشة التالية هي الشاشة الرئيسة للبرنامج، تتكون من ثلاث قوائم وزر أمر Browser لتحديد مسار الملف المراد تشفيره أو فك تشفيره، إضافة إلى مربع نص يستقبل مسار الملف.

شكل (٣) شاشة تنفيذ البرنامج الرئيسة

عند الضغط على زر Browser يتم فتح النافذة التالية، حيث يقوم المستخدم بتحديد مسار الملف المراد تشفيره أو فك تشفيره ثم يضغط على Open.

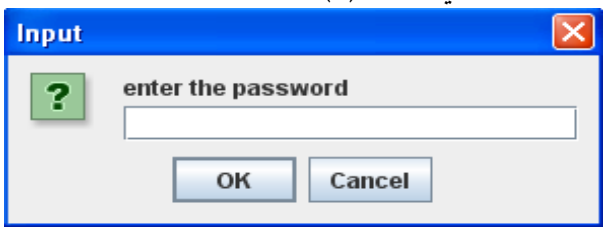


شكل (٤) نافذة تحديد مسار الملف

بعد تحديد الملف، وعند اختيار القائمة Encryption تظهر الخيارات الأربعة المتاحة للتشفير (باختلاف خوارزميات التشفير المتناظر) كما في الشكل(٥) مع وجود مفاتيح اختصار لتحديد الخوارزميات التي تستخدم.

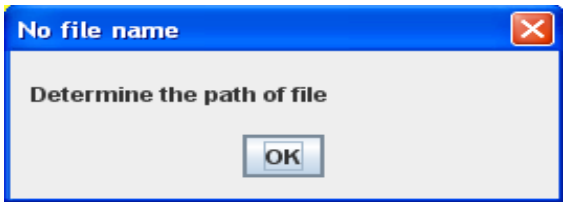
شكل (٥) القائمة Encryption

بعد أن يحدد المستخدم أحد الخيارات من قائمة Encryption يظهر مربع يطلب من المستخدم إدخال كلمة سر كما في الشكل (٦).



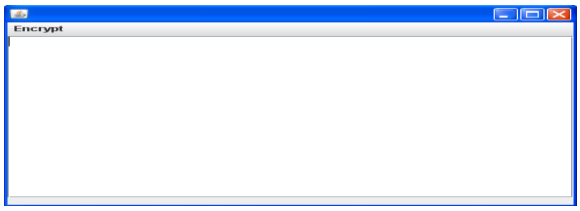
شكل (٦) شاشة ادخال كلمة المرور

إذا قام المستخدم بتحديد أحد الخيارات في قائمة Encryption او Decryption دون أن يحدد مسار الملف المراد تشفيره أو فك تشفيره، فإن البرنامج يقوم بإظهار الرسالة التالية.



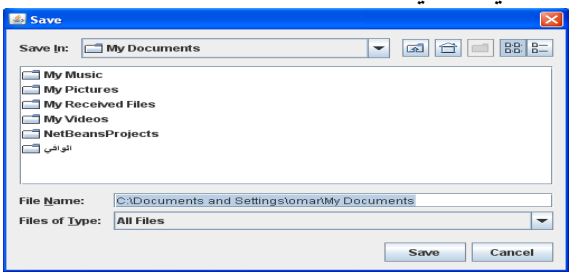
شكل (٧) شاشة توجيه (حدد مسار الملف)

كذلك يستطيع المستخدم أن يقوم بتشفير نص يقوم هو بإدخاله وذلك من خلال الضغط على Text من القائمة Encryption فتظهر له النافذة التالية ويكتب النص الذي يريد تشفيره ثم يختار من القائمة Encrypt أحد الخيارات المتاحة للتشفير.

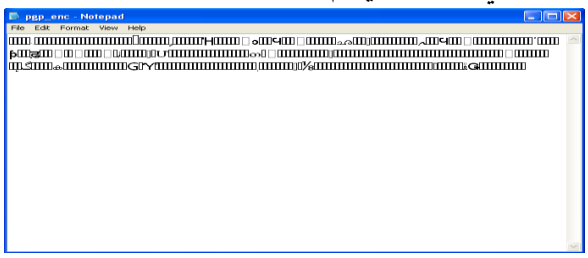


شكل (٨) شاشة ادخال نص

بعد أن يقوم المستخدم بتحديد أحد الخيارات السابقة تظهر له نافذة لتحديد اسم الملف الذي يريد حفظ النص فيه وهي كالتالي.



شكل (٩) شاشة تحديد مسار خزن النص المدخل يتم إنشاء ملف النص المشفر في نفس المسار الموجود فيه الملف الأصلي، والشكل (١٠) يظهر شكل النص المشفر في الملف الذي تم إنشاؤه.



شكل (١٠) النص المشفر في ملف التشفير

عند فك التشفير نتبع نفس الخطوات السابقة، فنحدد مسار الملف المراد فك تشفيره ثم نحدد أحد الخيارات الموجودة في القائمة Decryption والخاصة بفك التشفير (لابد أن يكون الخيار المقابل لنفس الخيار المستخدم عند التشفير).

شكل (١١) القائمة Decryption

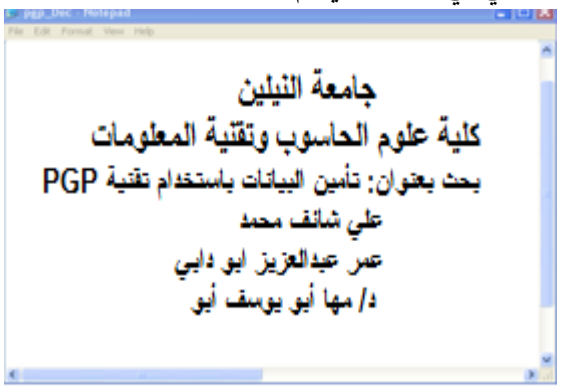
وعند فك تشفير ملف تظهر الرسالة الخاصة بإدخال كلمة المرور والمبينة بالشكل(١٢) ويجب إدخال نفس الكلمة التي تم إدخالها عندما شفرنا نفس الملف، مالم فان الرسالة التالي تظهر للدلالة على أن كلمة المرور خطأ.

شكل (١٢) شاشة تحذيرية (كلمة المرور خطاء)

عند فك تشفير ملف حدث فيه تغيير من قبل أي شخص من اضافة أو حذف يقوم البرنامج بعرض الرسالة التالية والتي تخبر المستخدم بأن الملف قد تمت مهاجمته (أي حدث فيه تغيير).

شكل (١٣) شاشة تحذيرية (الملف تمت مهاجمته)

بعد فك التشفير يتم إنشاء الملف الذي يحوي النص بعد فك تشفيره (النص الأصلي) في نفس المسار الموجود فيه الملف المشفر، والشكل (١٤) يظهر شكل النص الاصلي في الملف الذي تم إنشاؤه.



شكل (١٤) شاشة النص الاصلي في الملف بعد فك تشفيره

في القائمة Help يوجد خيارين احدهما About program للتعريف بالبرنامج كما في الشكل (١٥).

شكل (١٥) شاشة (About_program)

الخيار الثاني من قائمة Help هو (Hot To UseProgram) لشرح عمل البرنامج (كيفية الاستخدام) كما في الشكل (١٦).

شكل (١٦) شاشة كيفية الاستخدام البرنامج

٤. الاستنتاج:

تم التطرق في ثنايا البحث بشكل عام على أهم الخوارزميات المستخدمة في تشفير البيانات، وبشكل خاص على تقنية الـPGP والتي تتكون من أربع خوارزميات، حققنا من خلالها ثلاثة من أهداف التشفير ومتطلباته وهي:

–الموثوقية باستخدام خوارزمية تشفير متناظر واستخدمنا أربع منها (DES، TripleDES، AES، Blowfish).

–التكاملية باستخدام خوارزمية MD5.

–اثبات الشخصية وعدم الإنكار باستخدام خوارزمية المفتاح العام RSA.

–حاول البحث استخدام خوارزميه لضغط النص ولكن لم يوفق في ذلك.

كما استخدم البحث لغة الجافا (Java NetBeans) في بناء هذا النظام لما تتميز به من مواصفات جميلة إضافة لسهولة إنتاج الواجهات، ويتكون النظام من واجهةيستطيع المستخدم من خلالها تحديد مسار الملف النصي المراد تشفيره وكذلك فك تشفيره.

كما أن النظام يتطلب كلمة مرور عند تشفير أي ملف ويتم دمج هذه الكلمة مع الملف المشفر بعد تشفيرها مع النص الأصلي، وبالتالي فان النظام لن يقوم بفتح شفرة هذا الملف مالم يقوم المستخدم بإدخال كلمة المرور نفسها التي أدخلها عند التشفير.

٥. التوصيات:

لقد أصبح علم التشفير ذو أهمية بالغة، لاسيما في عصر أصبحت فيه المعلومة سلعة تباع وتشترى، ولاسيما ايضًا لجهات معينة تهتم بالسرية وترى في المعلومة سيف ذو حدين، يمكن الاستفادة منها مالم تقع في يد الغير، وعليه فقد جاء هذا البحث محاكيًا لهذه الفكرة، وفي محاولة متواضعة منا لتقديم أفضل ما نستطيع تقديمه، ولما كان الكمال ضربًا من ضروب الخيال، فإن البحث يوصي بالآتي.

– وضع هذا البرنامج كشفرة مفتوحة على الإنترنت لمن أراد الاستفادة منه او تطويره دون طلب أذن ولا حفظ للحقوق.

– تطبيق خوارزمية من خوارزميات ضغط النصوص على هذا البرنامج.

– في عملية الحشو في خوارزمية الـ MD5 استخدمنا الحشو بالبايت مع أن القياسي هو الحشو بواسطة البت.

– تطوير البرنامج ليشمل تشفير الصور وملفات الوسائط، كونه لا يُستخدم إلا لتشفير الملفات النصية.

– يمكن الاستفادة من هذا النظام لتطوير نظام تشفير آخر (خادم/عميل) للدمج بين مفهومي التشفير ونقل الملفات عبر الشبكة.

– إنشاء موقع أو منتدى في كل جامعة على شبكة الإنترنت للهواة والمهتمين بهذا المجال وإقامة المسابقات بين الطلاب لتحفيز قدراتهم.

– ضرورة اهتمام الجامعات العربية بالتعريب لمراجع الحاسوب، لخدمة العلم والباحثين والطلبة في تخصصات علوم الحاسوب وتقنية المعلومات.

٦. المراجع:

[1]أ.د عوض حاج علي أحمد، د. أمير حسين خلف ؛ طرق التشفير مطبعة جامعة النيلين ؛ الخرطوم؛ ٢٠٠٢.

[2] The Laws of Cryptography with Java Code by Neal R. Wagner;2003.

[3] Introduction to cryptography with Java applets, David Bishop.

[4] RSA Security's Official Guide to Cryptography, Steve Burnett and Stephen Paine.

[5] Beginning Cryptography in Java; by David Hook; Wrox Press © 2005 (480 pages).

[6] Applied Cryptography, Second Edition: Protocols, Algorthms, and Source Code in C (Publisher: John Wiley & Sons, Inc.).

[7] Cryptography: Theory and Practice by Douglas Stinson.

[8] Fundamental Data Compression by Ida Mengyi Pu.

[9] Malware: Fighting Malicious Code By Vapors in Presence of Carbon Particulates in Air. Bulletin of High Institute of Public Ed Skoudis, Lenny Zeltser Publisher: prentice Hall PTR ,Pub Date:November 21,2003.

[10] Nofal, F.H., Zakaria, A.M., 1997. Behavior Pattern of Some Organic Solvent Health, 27(1): 321-327.