المقالات العلمية

الكتابة المشفرة (Cryptography)

الكاتب : طالب من طلاب كلية علوم الحاسب والمعلومات. جامعة الملك سعود

المراجع: خالد الرويلي

ماجد الربيعان

النسخة : الأولى

تنبيه:

تعتبر هذه الممقالة مشاركة من كاتبها في زيادة التوعية والمحتوى الخاص بأمن المعلومات، وقد راجعها مراجع واحد على الأقل، ولا يتحمل مركز التميز لأمن المعلومات أي تبعات لهذه المقالة، ولا أي معلومات تطرح في هذه المقالة ولايضمن دقة المعلومة وصحتها.

كل شخص منا لديه أسرار وتتفاوت أهمية هذه الأسرار من شخص لآخر، وعندما يصبح من الضروري إرسال هذه الأسرار من مكان إلى آخر فمن المهم حماية هذه المعلومات عند نقلها، وتقدم الكتابة المشفرة المسماة بال(Cryptography) هذه الحماية باستخدام أساليب وطرق التشفير المتعددة التي سوف نتحدث عنها لاحقاً.

في مجتمعنا المعلوماتي اليوم، الكتابة المشفرة أَصبحت إحدى الأدوات الرئيسية لضمان السرية ، الثقة، التحكم في دخول المستخدمين، التسديد الإلكتروني، أمن الشركات، ومجالات أخرى لاتحصى..إن إستعمال الكتابة المشفرة لم يعد حكراً على الحكومات والإختصاصيين الماهرين جداً، بل أصبح متوفراً لكل فرد يريد استخدامه.

على مدى التاريخ قلة السرية في الاتصالات الحكومية كلفت العديد من الأرواح، وسببت حروب، وأسقطت حكومات. وكالات حكومية كاملة أنشئت للمساعدة على ضمان السرية، وثروات صرفت محاولةً لحماية الأسرار الوطنية وكذلك محاولةً لتعلم أسرار البلدان الأخرى. ولقد شهدت أسواق برامج التشفير انتعاشاً مذهلاً بعد أن سمحت السلطات الأمريكية للشركات التجارية المتخصصة ببيع هذه التقنية للجمهور و عامة الناس بعدما كانت محصورة للاستخدامات العسكرية والحكومية لسنوات طويلة ولقد اتخذت الحكومة الأمريكية هذا القرار في سبيل دعم الجانب الأمني لمجال التجارة الإلكترونية علما بأنها وحتى وقت قريب جدا لم تسمح بتصدير هذه التكنولوجيا إلى خارج الولايات المتحدة، خاصة للتي تزيد قوة تشفيرها عن 56 بت.

تناقش هذه الورقة الأقسام المختلفة للكتابة المشفرة وكيف تستعمل في مجال الحاسوب. إن معلوماتك الخاصة وبياناتك يجب أن تحصن من الوصول الغير مصرح به والاستغلال، إن الطريقة الأساسية لحماية بياناتك من العيون المحدقة بها هي الكتابة المشفرة. وفي هذه الورقة سنتناول كل مايتعلق بالCryptography من نشأته وأقسامه وخوارزمياته وكيفية عملها وفوائده وماهو الPKI و بعض الهجمات التي ربما تتعرض إليها الأنظمة المشفرة.

نشأته

التشفير هو أسلوب قديم استخدمه البشر منذ القدم وأول مجهود بشري للتشفير سجله التاريخ حدث قبل 4000 سنة فقد استخدم قديماً في الحضارات القديمة لإخفاء المعلومات والمراسلات مثل الحضارة الفرعونية والدولة الرومانية (انظر الشكل-1-). ولكن التشفير كعلم مؤسس منظم يدين بولادته ونشأته للعلماء الرياضيين واللغويين العرب إبان العصر الذهبي للحضارة الإسلامية ومن أشهرهم الفراهيدي والكندي، وقد ألف هؤلاء العلماء مفاهيم رياضية متقدمة من أهمها التوافيق والتباديل. وكذلك استخدم الكندي ومن تبعه مفاهيم الإحصاء والاحتمالات في كسر الشفرة.

وقد شاع في أيامنا استخدام مصطلح "التشفير" ليدل على إخفاء المعلومات. ولكن كلمة" التشفير" وافدة من اللغات الأوربية (Cipher) وهذه بدورها جاءت أصلا من اللغة العربية ولكن بمعنى آخر لكلمة "الصفر". فكما هو معلوم أن العرب قد تبنوا مفهوم الصفر والخانات العشرية واستخدموه في الحساب، وهو ما لم يكن الأوربيون يعرفونه في القرون

الوسطى . وكان مفهوم الصفر جديداً وغريباً لدرجة أنهم أخذوه بنفس الاسم فأسموه"Cipher" ولأن مفهوم الصفر الجديد كان في منتهى التعقيد والغموض فقد صاروا يستخدمون كلمة "Cipher"للدلالة على الأشياء المبهمة وغير الواضحة.

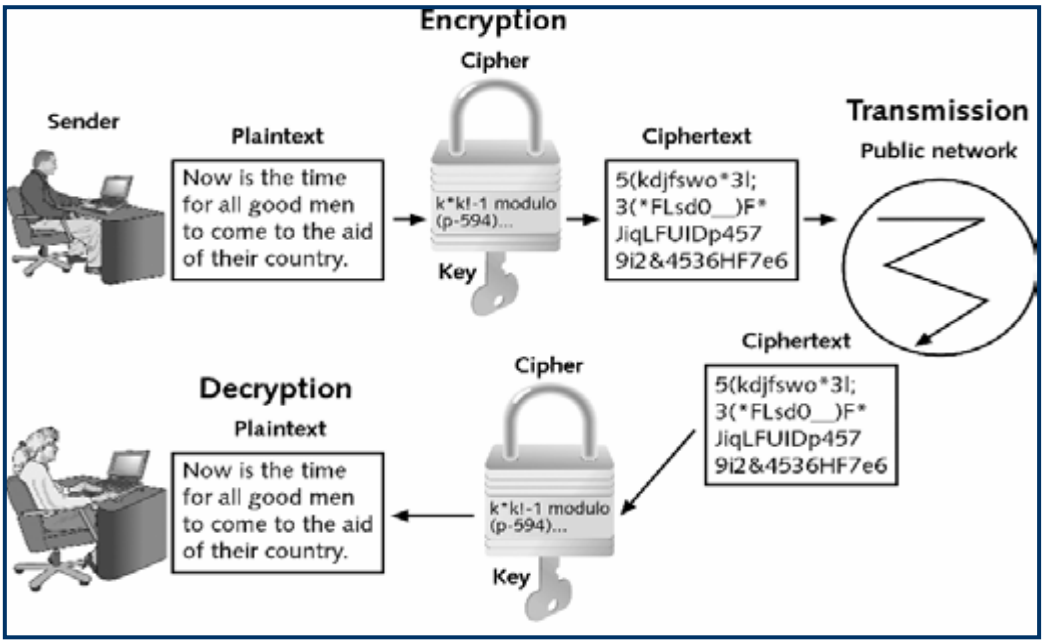
شكل 1: توضح الصورة إحدى أدوات التشفير التي استخدمت في الحضارة اليونانية

ماهو ال Cryptography؟

علم التشفير أو الكتابة المشفرة المسماة بال (Cryptography) هو فن أو علم إخفاء المعلومات بحيث تكون بأمان عند إرسالها أو تخزينها، ويعتبر مجال ذو أهمية كبيرة للحكومات، والشركات الخاصة، و مع ثورة الإنترنت وازدياد مستخدميه ازدادت أهميته للأفراد. فالأفراد يحتاجون للخصوصية عندما يتعلق الأمر بالمعلومات الشخصية والحساسة، الشركات كذلك تريد حماية سجلاتها المالية، وأسرارها التجارية، ومعلومات عملائها وموظفيها وغيرها من المعلومات المهمة والخاصة. تستعمل الحكومة الكتابة المشفرة للمساعدة على ضمان الأمان والاستقرار لمواطنيها.

التشفير Encryption **:** هو عملية تحويل المعلومات المهمة أو التي لا تريد أن يطلع عليها أحد (Plaintext) إلى نص مخفي لا يمكن فهمه (Cipher text) عند نقلها خلال قناة غير آمنة وذلك باستخدام الكتابة المشفرة، أما عملية فك التشفيرDecryption فهي العملية العكسية للتشفير(انظر الشكل-2-)

© CoEIA



شكل 2: توضح الصورة عملية التشفير وفكه

الأفراد الذين يَتخصّصون في تطوير وعمل الرموز يطلق عليهم مشفرين(Cryptographers). أما الأفراد الذين بتخصّصون في كسر الرموز وتحليلها فيطلق عليهم محللي التشفير (Cryptanalysts). العديد من هؤلاء المحترفين عباقرة ولديهم خلفية قوية في الرياضيات وعلم الحاسبات. هم يعيشون في عالمهم الخاص، و لا يستطيعون أن يتحدثوا عما يعملون.

أقسام الCryptography

ينقسم علم التشفير إلى **ثلاثة** أقسام هي :

1. الكتابة المشفرة الطبيعية (Physical Cryptography)

تتضمن الكتابة المشفَرة الطبيعية أنواع مختلفة من الطرق، والطرق الأكثر شيوعاً تستخدم الإحلال أو تبديل الحروف أو الكلمات، ومن الطرق الطبيعية أيضاً طريقة التشفيرالمسماة بفن الاختزال (Steganography) ، وهي لإختفاء المعلومات ضمن معلوماتِ أخرى، كصورة مثلاً. عموماً تشيرالكتابة المشفرةالطبيعية إلى أي طريقة لا تعدّل القيمة بإستعمال عملية رياضية.

هناك ثلاثة أنواعِ رئيسية من الكتابة المشفرة أَو التشفير، صفر cipher هي طريقة تستعمل لتشفير الحروف وذلك لإخفاء قيمتها. أما التَشفير Ciphering هي عمليةُ إستعمال الصفر لتشفيررسالة. النموذج الهجين hybrid model يسخدم طريقة واحد أَو أكثر للتشفير.

2. الكتابة المشفرة الرياضية (Mathematical Cryptography)

تتعامل الكتابة المشفرة الرياضية مع القضايا المتعلقة بإستعمال العمليات الرياضية على الحروف أَو الرسالةِ. الأكثر شيوعاً هي دالة تسمى الهاش (Hashing) وهي عبارة عن عملية حسابية تتم على الرسالة وتحولها إلى قيمة عددية (numeric hash value).

كما هو ملحوظ هذه قيمة عددية (numeric hash value) هي فقط عدد وحيد. و لا يمكن أن تستعمل لإشتقاق معنى الرسالة. هذا العددِ يمكن أأن يرسل بالرسالة إلى المستلم. الطَرف الآخر يمكن أن يستعمل نفس دالة الهاش لتقرير أن الرسالةِ موثوق بها. إذا قيمةِ الهاش مختلفة، فهذا يدل على أن الرسالة عُدّلت بطريقةٍ ما. هذه العملية معروفة كذلك بحساب المجموع (checksum).

3. الكتابة المشفَرة الكمية (Quantum Cryptography)

الكتابة المشفَرة الكَمية هي طريقة جديدة نسبياً من التشفيرِ. قبل 2002، تطبيقها كان محدوداً على عمل المختبر وربما بعض التطبيقات الحكومية السرية. هذه الطريقة تعتمد على خصائص أصغر جزيئات عُرفت. من الممكن الآن صنع شفرات مستحيلة الكسر باستخدام الطرق الكمية.

أسطورة الرموزِ مستحيلة الكسر

إذا الزمان علمنا أي شيئ فهو علمنا أن الناس كثيراً يعملون أشياء يعتقد أناس آخرين أنها مستحيلة. ففي كل مرة يخترع رمز أَو عملية جديدة، يأتي شخص آخر بطريقة لكسره.

هناك طرق كثيرة لكسر الشفرات أو الرموز وهي:

1. تحليل التكرار (Frequency Analysis)

يتضمن النظر إلى كتل (Blocks) الرسالة المشفرة لتحديد وجود أي نمط متكرر، فعلى سبيل المثال في اللغة الإنجليزية يتكرر الحرفين T, E فمثلاً الكلمات That, the, and, i هي كلمات شائعة جداً و محلل التشفير يبحث عن هذه الأنواع من الأنماط ومع مرور الوقت، قد يكون قادراً على استنتاج الدالة التي استعملت لتشفير البيانات. هذه العملية يمكن أن تكون بسيطة جداً أحياناً، أَو ربما قد تأخذ الكثير من الجهد.

2. أخطاء خوارزمية (Algorithm Errors)

© CoEIA

الخوارزمية هي عملية أو مجموعة من الأوامر لأداء مهمة أو أمر. في عالم الحاسبات، الخوارزميات **تستخدم للقيام بعمليات تكرارية. الخوارزميات المعقدة تعطي أحياناً نتائج غير متوقعة، وهذه النتائج عند اكتشافها يمكن أن تسبب إلى كشف كل خوارزمية التسفير.**

3. هجمات القوة العنيفة (Brute Force Attacks)

يمكن القيام بها بتَطبيق كل مجموعة محتملة من الحروف التي يمكن أم تكون المفتاح. إذا على سبيل المثال، تعرف بأن المتاح يتكون من ثلاثة حروف، ومنه يمكن أن تعرف بأن هناك عدد محدود من الاحتمالات التي يمكن أن تكون هي المفتاح. على الرغم من أنه قد يأخذ وقت طويل لإيجاد المفتاح، فالمفتاح يمكن أن يوجد.

3. الخطأ البشري (Human Error)

أحد الأسباب الرئيسية لنقاط ضعف التشفير. إذا أرسل بريد الكتروني باستعمال التشفيروشخص آخر أرسله بدون تشفير، وإذا عثر محلل التشفير على هذه الرسالتين فهذا يسهل عليه ترجمة الرسائل المستقبلية.

4. الهندسة الاجتماعية (Social Engineering)

هذه الحالة يمكن أن تكون نتيجة خطأ أو يمكن أن يكون سببها الحوافز الشخصية مثل الطمع. المال والمعتقدات السياسية دافعان قويان. الناس يمكن أن يرشوا لإعطاء معلومات. إذا موظف ما أعطى المفاتيح لشخص آخر، أنت لا تَعرف بالضرورة أن هذا حدث. المهاجم يمكن أن يَستعمل المفاتيحَ لفك تشفيرالرسائل واستغلال المعلومات التي تحتويها.

خوارزميات ال Cryptography

الخوارزميات المشفرة تستعمل لتشفيرالرسالة الواضحة أو غير المشفرة إلى رسالة مشفرةِ. وهنالك ثلاثة خوارزميات أساسية وهي:

1.الهاش (Hashing)

الهاش (Hashing) وهي عبارة عن عملية تحويل الرسالة أو البيانات إلى قيمة عددية (numeric hash value). ودالة الهاش تعتبر إما أحادية الإتجاه أَو مزدوجة. فإذا كانت الدالة أحادية الاتجاه فلا تسمح للرسالة بأن تعود إلى قيمتها

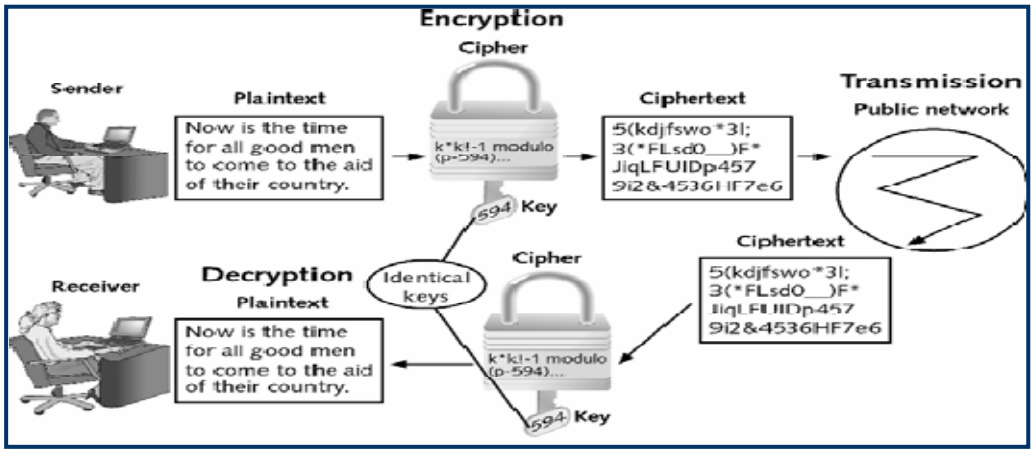
الأصلية‘ ، أما في حالة الدالة المزدوجة فيسمح للرسالة بأن يعاد بناءها من الهاش، وفي الغلب أكثر دالات الهاش أحادية الاتجاه.

يوجد معياران أساسيان يستخدمان دالة الهاش للتشفير وهما:SHA, MD.

2.التشفير المتناظر (Symmetric Algorithms)

يتم بتشفير الرسالة أو المعلومات باستخدام رقم واحد يسمى الرقم العام وكذلك في نفس الوقت يتم فك الشفرة و ترجمة المعلومات إلى وضعها الأصلي بإستخدام نفس الرقم العام. ولذلك لو حصل و أن شخص اخر يعرف هذا الرقم أو حصل عليه من الدليل العام فإنه قادر على فك الشفرة و قراءة تلك الرسالة أو المعلومة(انظرالشكل-3-).

ومن أشهر طرق التشفير المتناظر: Blowfish, Digital Encryption Standard (DES), Tiny Encryption Algorithm(TEA), Triple DES, and International Data Encryption Algorithm (IDEA).



شكل3: توضح الصورة خوارزمية التشفير المتناظر

3. التشفير الغير متناظر (Asymmetric Algorithms)

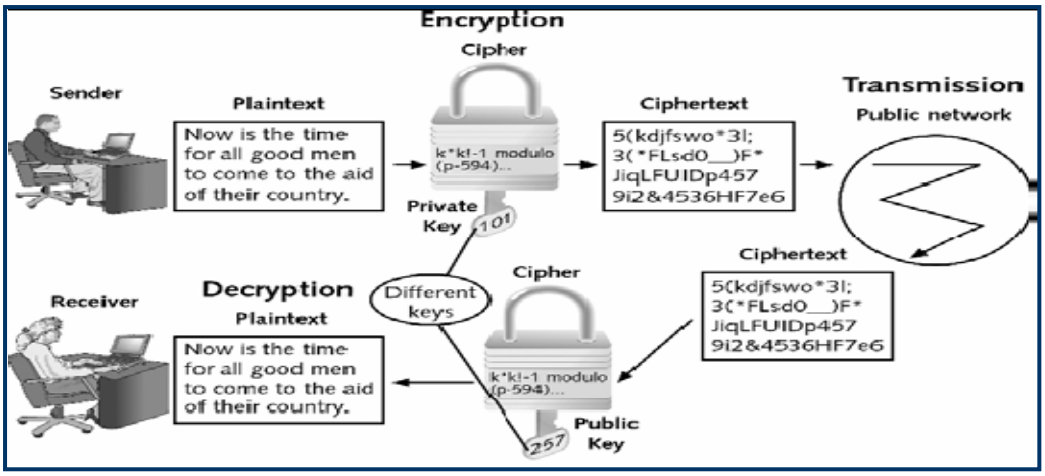
يتم تشفير المعلومات بالرقم العام ولكن لا يمكن فك الشفرة و الوصول إلى تلك المعلومات الا بالمفتاح الخاص لصاحب ذلك المفتاح العام الذي تم على أساسه عملية التشفير(انظرالشكل-4-).

ومن أشهر طرق التشفير الغير متناظر:

Pretty Good Privacy(PGP), Reivest, Shamir & Aselman (RSA)

ولنفهم الفرق بين التشفير المتناظر و الغير متناظر لنأخذ هذا المثال تخيل بأنك تقوم بالاتصال هاتفيا بأحد أصدقاءك وعندما تدخل رقم هاتفه (الرقم العام) ويبدأ هاتفه بالرنين ولكن ذلك الصديق لا يرد على مكالمتك فيرد

عليك جهاز إجابة و تترك له رسالة صوتية في ذلك الجهاز . و الان لنتخيل بأنك قمت بحماية (تشفير) تلك الرسالة برقم سري و لا يستطيع أحد الاستماع إلى تلك الرسالة إلا بإدخال ذلك الرقم السري. فإن كان صديقك هذا قد اتفق معك على اختيار الرقم السري هو نفس رقم هاتفك العام فهذا ما يسمى بطريقة التشفير المتناظر لأن المفتاح العام = الرقم السري أما لو قام ذلك الصديق ببرمجة التشفير لطلب الرقم السري الخاص بك (رقم اخر لا يعرفه أحد غيرك) فهذا مايعرف بالتشفير الغير متناظر لأن المفتاح العام لا يساوي الرقم السري.



شكل4: توضح الصورة خوارزمية التشفير الغير متناظر

فوائد الCryptography

النظام المشفر يضمن للمستخدم التالي:

أ. التحقق Authentication : عملية إثْبات هوية الشخص وذلك لإثبات أنه من يدعّي.

ب. سريّة Privacy/confidentiality: ضمان بأنّ لا أحد يمكنه أن يقرأ الرسالةَ ماعدا المستلمِ المقصود.

ج. سلامة البيانات Integrity: يضمن للمستلم بأن الرسالةَ المستلَمةَ لَم تعدل في أية حال من وأنها هي الرسالة الأصلية.

د. عدم الإنكار Non-repudiation : آلية لإثْبات أن المرسلِ أرسل هذه الرسالة حقاً.

ه. التحكم في الدخول Access control: هي الطرقِ، والعمليات، ووالآليات لمنع وصولِ الغير مخوّل لهم إلى الدخول إلى الأنظمة التي تقوم بالتشفير.

ماهو الPKI؟

على اختلاف أنواع و أشكال البرامج المتخصصة في هذا المجال إلا أنها جميعا تتشارك في القاعدة أو الأساس وهي مبنية على مفهوم بسيط جدا وهو أن كل رقم أو معلومة مشفرة تحتاج لفكها و إعادتها الى وضعها الأصلي الى ثلاث عناصر مجتمعة مع بعضها البعض و لنفرض انها (س ، ص ، ع) أما في حالة معرفة قيمة واحدة فقط من هذه العناصر و بقاء الاثنتين الباقيتين مجهولتين فإنك سوف تجد نفسك في دوامة الاحتمالات والتخمين للوصول إلى القيم الصحيحة لهذين العنصرين المجهولين اللازمين لاكمال الحلقة و فك الشفرة وعلى هذا الأساس علينا التعرف على ثلاث مصطلحات لفهم هذه التكنولوجيا : المفتاح العام ، المفتاح الخاص ، و الرقم الأساس حيث أن أي معلومة يتم تشفيرها لا يمكن الاطلاع عليها صحيحة وكاملة إلا بوجود هذه المفاتيح الثلاثة مجتمعة.

يتم إصدار رقم الأساس عن طريق البرنامج المتخصص أو احد الهيئات المستقلة و المتخصصة في إصدار هذه الأرقام وهو مايعرف ب Certificate Authority (CA) بحيث يكون لكل مستخدم رقم أساس وهو (ع) و يتم تقسيم هذا الرقم الى مجموعتين (س) و هو ما يعرف بالمفتاح العام و (ص) هو ما يعرف بالمفتاح الخاص ، بحيث اذا قمنا بعملية ضرب س في ص يكون الناتج هو (ع) الرقم الأساس وهو الرقم اللازم لإعادة الملفات و المعلومات الى وضعها الأصلي قبل التشفير وطبعا هذا الرقم محمي ومشفر بقوة ولا يمكن الوصول اليه بسهولة.

المفتاح العام (Public Key):

الرقم الذي يتم تداولة و نشره بين بقية المستخدمين لتشفير أي معلومات أو رسالة الكترونية مخصصة لك و يعتبر رقمك العام اساس عملية التشفير و لا يستطيع أحد فك رموز تلك المعلومة غيرك انت لأنها تحتاج الى الرقم السري و ليكن هو المفتاح الخاص بك لإكمال العملية الحسابية والوصول الى الرقم الأساس وبالتالي فتح الملفات مرة أخرى.

المفتاح الخاص (Private Key) :

هو النصف الآخر المكمل للمفتاح العام للوصول الى الرقم الأساس واعادة المعلومات المشفرة الى وضعها الطبيعي قبل التشفير ، و هذا المفتاح هو الذي يميز كل شخص عن غيره من المستخدمين ويكون بمثابة هوية الكترونية تمكن صاحبها من فك أي معلومة مشفرة مرسله اليه على أساس رقمه العام ولذلك يجب عليك الاحتفاظ بالمفتاح الخاص سرا وهذ ما يعرف ب Private Key

و بهذه الطريقة لا يستطيع أحد فك الشفرات وقراءة المعلومات المحمية بهذه الطريقة دون اكتمال الحلقة و التي لا تتم إلا بمعرفة القيمة الصحيحة للمفتاح العام و المفتاح الخاص.

المراجع والمصادر:

النشرات العلمية:

[1] D. B. Johnson and S. M. Matyas, "Asymmetric Encryption: Evolution and Enhancements", *Crypto Bytes RSA Laboratories*, vol. 2, no. 1, pp. 2-15, Spring 1996.

] Hans , Dobbertin, "The Status of MD5 after a Recent Attack", *Crypto Bytes RSA* 2[*Laboratories*, vol. 2, no. 2, pp. 2-15, Summer 1996.

الكتب:

[3] Eric, Cole, *"Network Security Bible"*, 1St Edition, Indianapolis, Wiley Publishing, 2005.

[4] Michael, Pastore, *"Security+ Study Guide (Exam SYO-101)"*, 1St Edition, Sybex, 2003.

مواقع الإنترنت:

[4] www.garykessler.net/library/crypto.html#intro

[5] www.wisegeek.com/what-is-cryptography.htm

[6] www.ssh.com/support/cryptography/algorithms/

[7] en.wikipedia.org/wiki/Cryptography#Cryptographic_primitives

[8] www.unixwiz.net/techtips/iguide-crypto-hashes.html#whatis