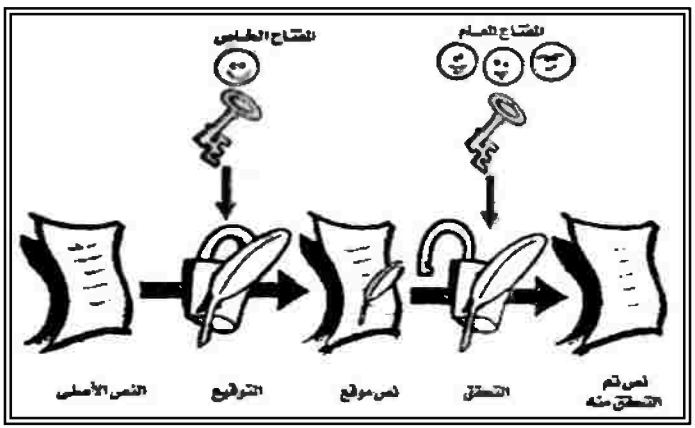
الفصل الخامس

(٤) التشفيـــر Cryptography

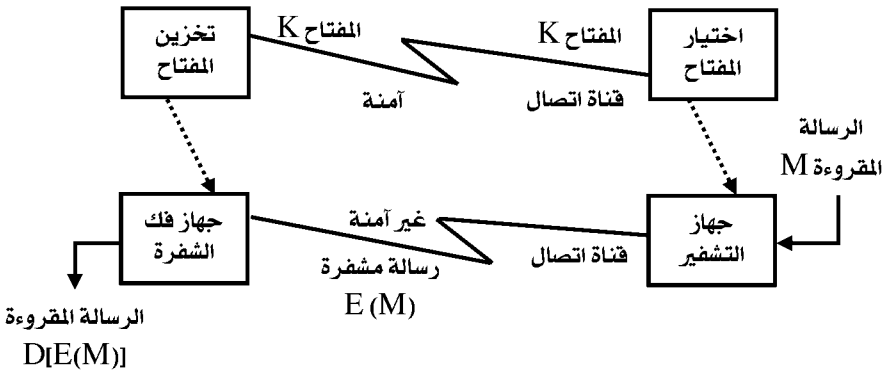


يقصد بالتشفير القيام بمزج المعلومات الحقيقية بمعلومات وهمية ينتج عنها توليد معلومات جديدة لا يمكن معرفة المعلومات الحقيقية فيها. دون معرفة طريقة التشفير المتبعة والمفتاح السري المستخدم في ذلك، وهذا المفتاح يتم الاتفاق عليه بين طرفي عملية التراسل (المرسل المستقبل)، ويستخدمه كل طرف من أجل تغيير شكل البيانات الحقيقية عن الإرسال، ويعيد البيانات إلى مضمونها الحقيقي بإزالة البيانات الوهمية عند الاستلام وهو ما يسمى بفك التشفير **Decryption**.

يوضح الشكل التالي نظام التشفير حيث يتم تحويل الرسالة المقروءة **M** إلى رسالة مشفرة **E(M)** وتتكون عملية التشفير أو فك الشفرة من خوارزم التشفير **(E)** أو فك الشفرة **(D)** ومفتاح التشفير **(K)**. ويتحكم المفتاح **(K)** في خوارزم التشفير. ويقوم

المستخدم بفك الشفرة للحصول على الرسالة باستخدام خوارزم فك الشفرة (D)، أي أن [1]

$$M = D[E(M)]$$



وتتألف عملية التشفير من ثلاث عناصر هي:

١- المعلومات التي سيتم تشفيرها فقد تكون رسالة نصية أو ملفات مهمة أو إشارات كهربائية مشفرة – كإشارة البث التلفزيوني الرقمي – ومنها في نطاق التجارة الإلكترونية، تشفير بيانات عروض صفقة من الصفقات التجارية عبر الإنترنت، أو المفاوضات السرية السابقة لهذا العقد.

٢- خوارزمية التشفير التي ستطبق على المعلومات، وذلك لتحويلها إلى بيانات مبهمة، وخوارزمية فك التشفير التي تعيد هذه البيانات إلى حالتها المفهومة الأصلية، وهناك خوارزميات عديدة متبعة في عمليات التشفير عبر إنترنت منها PGP و RSA و DES.

[1] د. محمد فهمي طلبه وآخرون، فيروسات الحاسب وأمن المعلومات، موسوعة دلتا للكمبيوتر، ١٩٩٢، ص ٢٤٧ وما بعدها٩.

٣- المفتاح، وهو سلسلة أو أكثر من الرموز تتسلمها الخوارزميات المتبعة، وتطبقها على البيانات لتشفيرها أو فك التشفير عنها[١] .

وهناك أسلوبين للتشفير حسب المفاتيح المستخدمة هما:

١- تشفير المفتاح السري أو المتماثل :

ويستخدم هذا النظام، المفتاح ذاته في عمليتي التشفير وفك التشفير .

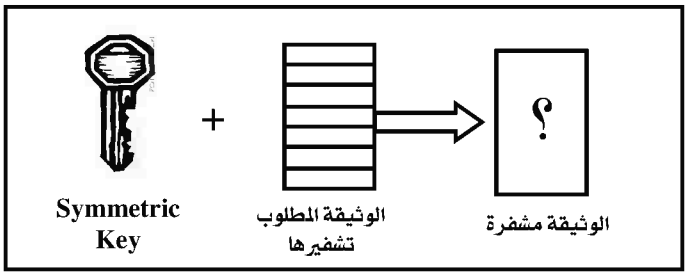
وهذا النوع يعتمد على اتفاق الطرفين – المرسل والمستقبل للمعلومات المشفرة – على مفتاح سري واحد. والأمان في هذا النوع أضعف من عوامل الأمان في تشفير المفتاح العام – الذي يرد ذكرها لاحقاً – حيث يمكن لشخص ما أن يتطفل على عملية تبادل المعلومات، والتي يتم خلالها الاتفاق على المفتاح السري، ويمكنه من خلال عملية التبادل أن يتعرف على هذا المفتاح.

وهذا النوع من التشفير يسمى التشفير المتناظر، ويعتبر نظام Des data encryption standard أشهر الأنظمة التي تعتمد على هذا النوع من التشفير، وقد طورته شركة IBM .

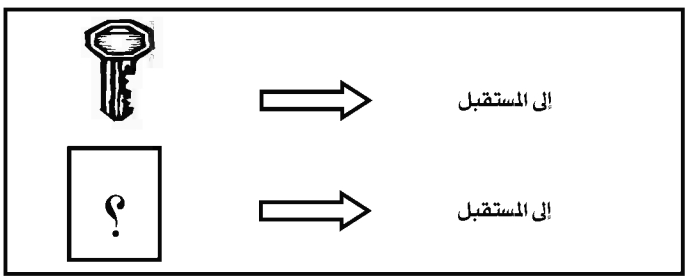
هذا وتتم خطوات التشفير هنا وفقاً للخطوات التي توضحها الأشكال التالية:

---

[١] راجع أ. فادي سالم، تشفير البيانات في إنترنت، دراسة في مجلة إنترنت العالم العربي، عدد أغسطس وسبتمبر ١٩٩٩، على موقع www.jawmay.com.ae .



تشفير الوثيقة



إرسال الوثيقة المشفرة ومفتاح التشفير

حيث يتم تشفير الرسالة (المعاملة) لدى المرسل باستخدام مفتاح خاص لينتج منها رسالة مشفرة كما هو موضح بالشكل عاليه.

يقوم المرسل بإرسال الرسالة المشفرة إلى المستقبل باستخدام وسائل الاتصال العادية ويقوم بإرسال المفتاح باستخدام وسيلة مؤمنة كما هو موضح بالشكل.

يقوم المستقبل بعد تلقي الرسالة المشفرة والحصول على المفتاح بحل الشفرة والحصول على الرسالة الأصلية كما هو موضح بالشكل.

نلاحظ على هذا الأسلوب ما يأتي:

ضرورة إرسال المفتاح باستخدام وسيلة مؤمنة وبالتالي فإذا كانت هناك وسيلة مؤمنة فإن إرسال الرسالة بها قد يعد الأسلوب الأسهل.

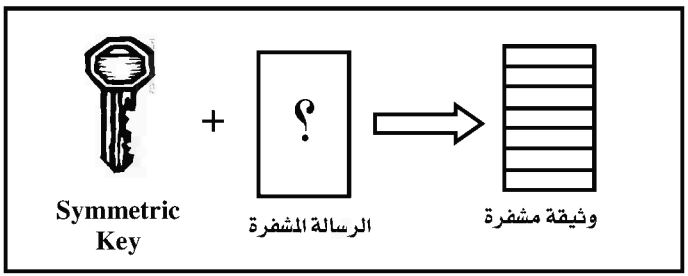
٢- نظام التشفير باستخدام المفتاح العام :

وهذا النظام يستخدم زوجاً من المفاتيح، أحدهما يسمى **المفتاح العام**، ويتم الإعلان عنه لجميع الجهات التي تتبادل المعلومات، وهو المفتاح المستخدم لتشفير البيانات، والآخر يدعى المفتاح الخاص، وهو المستخدم لفك التشفير، ويبقى هذا المفتاح سراً عند الجهة المستقبلة، فتزول بذلك ضرورة تبادل المرسل والمستقبل للمفتاح.

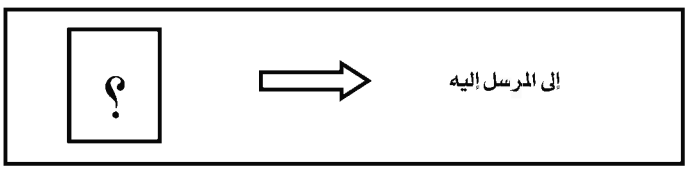
تتم العملية على النحو التالي:

- يرغب المرسل في إرسال رسالة مشفرة إلى المرسل إليه فيقوم باستخدام المفتاح العام للمرسل إليه ويقوم بتشفير الرسالة كما هو موضح بالشكل.
- يقوم بإرسال الرسالة المشفرة باستخدام وسائل وقنوات الاتصال العادية كما هو موضح بالشكل.
- يقوم المرسل إليه بتلقي الرسالة وباستخدامه مفتاحه الخاص يمكنه أن يقوم بحل الشفرة واستعادة الرسالة الأصلية كما هو موضح بالشكل.
- إذا تلقى أي شخص الرسالة المشفرة فإنه لا يستطيع أن يحل هذه الشفرة.

وذلك على النحو الذي توضحه الأشكال التالية:



التشفير بالمفتاح العام



إرسال الرسالة المشفرة

ويمكن توضيح طريقة المفتاح العام من خلال المثال التالي:

إذا أراد "زيد" أن يرسل إلى "عمرو" رسالة باستخدام نظام المفتاح العام، فعليه أن يطلب المفتاح العام العائد للمدعو عمرو، من أي جهة توفر المفاتيح العامة، وهذا المفتاح يشبه عنوان بريد إلكتروني يعرفه الجميع، وهو خاص بشخص واحد فقط، وعندما يستقبل عمرو الرسالة المشفرة، يستخدم المفتاح الخاص لفتحها، فلا يمكن من ثم لأي شخص كان أن يتطفل عليهما خلال إرسال هذه الرسالة

ويعد نظامي RSA, DSA (Digital Signature Algorithm) من أشهر الأنظمة التي تعتمد على هذا النوع من التشفير[1] .

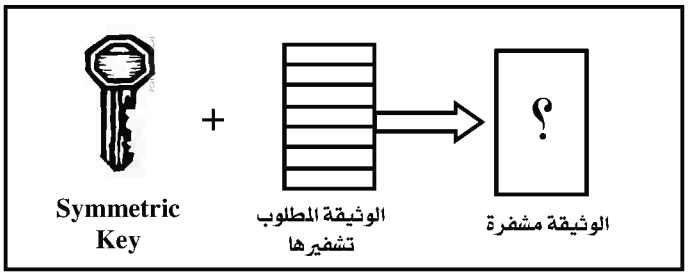
٣- التشفير من خلال المزج بين نظام المفتاح المتماثل والمفتاح العام :

- إذا كان نظام المفتاح المتماثل بسيطاً في درجة تشفيره، وبالتالي لا يحتاج إلى قوة حاسبات كبيرة ولا إلى وقت طويل في فك شفرته، فإن ما يعيبه هو طريقة إرسال المفتاح الخاص والتي تحتاج إلى قناة اتصال مؤمنة.
- وإذا كانت درجة التعقيد الموجودة في نظام المفتاح العام وما تحتاجه من قوة حساب عالية ووقت في التشفير وفي حل الشفرة تعد ميزة إضافية في توفير درجة أمان عالية وعيب بالنسبة لمتطلبات وتكلفة تنفيذ عملية التشفير .

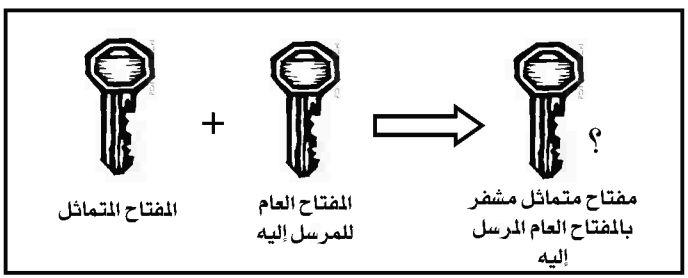
فإن المزج بين النظامين يوفر وسيلة لتحقيق درجة تأمين مناسبة في أقل وقت دون استخدام القدرات الكبيرة للحاسبات لتحقيق درجة التشفير المطلوبة وتتم الخطوات على النحو التالي:

---

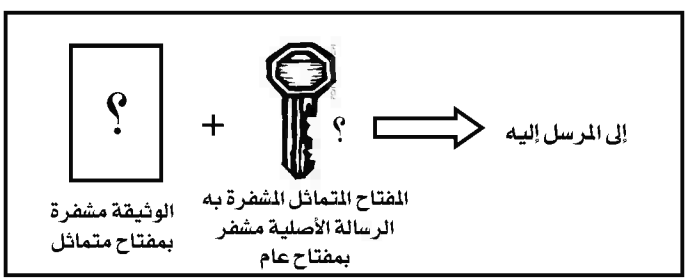
[1] تتحدد قوة نظام التشفير بناء على الخوارزمية المتبعة وطول المفتاح المستخدم، ويقصد بطول المفتاح عدد – البتات – التي يتكون منها المفتاح، ويزداد عامل الأمان كلما ازدادت، ويمكن تشبيه مفتاح التشفير بمفتاح الباب العادي، فكلما ازدادت عدد أسنان المفتاح العادي صعبت عملية تقليده، أو فتح القفل المرافق له. وتتراوح أطوال المفاتيح المستخدمة في عمليات التشفير ما بين ٤٠ إلى ٢٠٤٨ بت، مع العلم أن المفتاح لا يعتبر عامل أمان مرتفع حسب التقنيات الموجودة الآن، إلا إذا كان طوله يساوي أو يزيد على (١٢٨) حيث تحسب الاحتمالات الممكنة في هذه الحالة من العلاقة (٢ مرفوع للقوة ١٢٨) وتساوي (٤٥٦ و ٢١١ و ٧٦٨ و ٤٣١ و ٦٠٧ و ٣٧٤ و ٤٦٣ و ٩٣٨ و ٩٢٠ و ٣٦٦ و ٢٨٢ و ٣٤٠) احتمال.
فلو أراد شخص أن يخمن للوصول إلى المفتاح السري، فعليه أن يجرب كل هذا العدد من الاحتمالات، ولنا أن نتخيل عدد الاحتمالات متى كان طول المفتاح (٢٠٤٨) بت.



تشفير الوثيقة الأصلية بالمفتاح المتماثل



تشفير الوثيقة الأصلية بالمفتاح المتماثل



إرسال الوثيقة والمفتاح

٤- طريقة الطبقة الآمنة :

وتهدف هذه الطريقة إلى تحقيق أهداف معينة هي:

١- التشفير للرسائل.

٢- ضمان عدم تحوير محتوى الرسالة وضمان سلامتها.

٣- التحقق من الطرف الآخر.

وتقوم هذه الطريقة بضغط أو اختزال الرسالة أولاً بأحد الدوال المتخصصة في هذا المجال والتي ينتج عنها ما يسمى **Message Authentication Code (MAC)** رسالة موثقة مختزلة ثم يقوم المرسل بتشفيرها مع نص الرسالة الأصلي بالمفتاح العام للمرسل إليه ويرسل النتائج إلى المرسل إليه.

ويقوم المرسل إليه باستخدامه مفتاحه الخاص في فك الرسالة المشفرة ليحصل على نص الرسالة الأصلي مقروء بالإضافة إلى الرسالة الموثقة المختزلة.

يطبق المرسل إليه برنامج الضغط أو الاختزال الذي استخدمه المرسل على نص الرسالة الأصلي المقروء فيحصل على رسالة موثقة مختزلة جديدة ويقارنها بالمناظر لها الذي حصل عليه من المرسل فإذا تطابقا فإن هذا يعني أن الرسالة لم تحور أو تستبدل وإنها أرسلت من المرسل الأصلي نفسه.

٥- طريقة تكنولوجيا الاتصالات الخاصة :

وهذه الطريقة تشبه طريقة الطبقة الآمنة، إلا أنها تستخدم مفاتيح أكثر لزيادة درجة الأمان بالإضافة إلى أنها تستخدم مكونات أقل من الجزء الأول من طريقة **SSL**

والتي تسمى بروتوكول المصافحة الذي يشتمل على معلومات الهوية والمفتاح العمومي لكل من المرسل والمرسل إليه وبعض المعلومات الأخرى والإضافية.

٦- طريقة أمن الطبقة الناقلة:

وهذه الطريقة نسخة معدلة من طريقة الطبقة الآمنة وتستخدم لمقارنة الطرق الأخرى التي تستخدم في شبكة الإنترنت.

٧- طريقة تأمين التعاملات الإلكترونية:

وهذه الطريقة تم تطويرها بمعرفة شركة فيزا وماستر كارد لتأمين المعاملات المالية لبطاقات الائتمان خلال شبكة الإنترنت والتي تتعرض كثيراً لحالات القرصنة والسرقة.

حيث كان كل من الشركتين نظامها الخاص للتشفير إلا أن تعاونهما أسفر عن هذه الطريقة التي تتميز بدرجة عالية من الأمان حيث تصدر بصمة رقمية تستخدم في التأكد من صحة محتوى الرسالة وتمكن من التأكد من هوية صاحب البطاقة دون إظهار رقم ائتمانه.

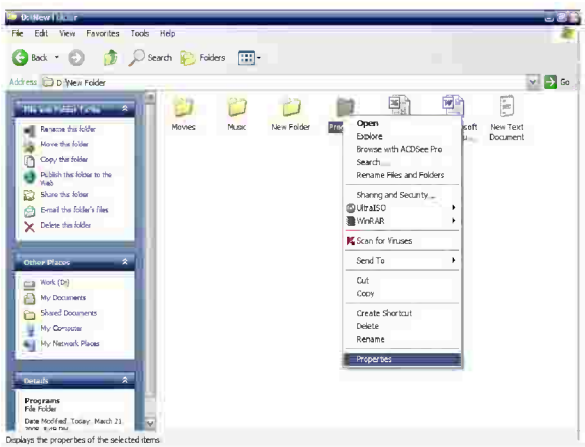
تشفيـر الملفـات :

مـن الممكـن أن تجعـل ملفاتـك الشخصـية تبـدو (كطلاسـم) للمـتطفلين ولصـوص المعلومات فبإمكانك أن تقوم بتشفير أحـد المستندات أو الملفـات الصـوتية أو أحـد أفـلام الفيديو كليب، بمعنى غلق الباب أمام أي شخص لفتح هذه الملفات إلا أنت. ولتنفيذ ذلك لابد أن تجعل لك حساباً شخصياً على الكمبيوتر، ثم تقوم بتشفير الملفات التي تريـدها، تأكد أن أحداً لن يستطيع فتح هذه الملفات رغم أنها ظاهرة أمامه إلا إذا عرف كلمة السر الخاصة بحسابك الشخصي وقام بتشغيل الكمبيوتر وفق هذا الحساب... وتجنباً للتعقيد هيا بنا لنتعرف على ذلك تفصيلياً وفق الخطوات التالية[1] :

١- قم بتشغيل الكمبيوتر، وادخل إلى حسابك الشخصي.

٢- اذهب إلى الملف – أو المجلد الذي تريد تشفيره.

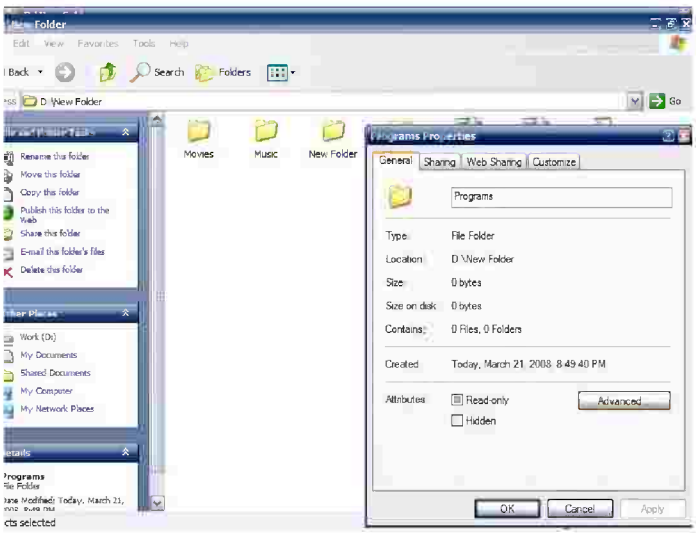
٣- انقر بمفتاح الماوس الأيمن فوق هـذا الملـف أو المجلـد: لتظهـر لـك النافـذة المختصـرة التالية:



[1] لاحظ أن الملفات الموجودة بالأجزاء Partitions المهيئة وفق نظام NTIS هي فقط التي يمكن تشفيرها، أما الملفات الموجودة في الأجزاء المهيئة وفق النظام Fat or Fat 32 فلا يمكن تشفيرها.

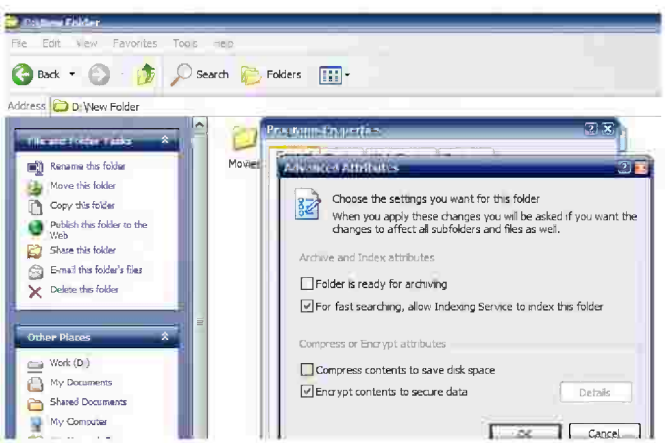
٤- اختر Properties من تلك القائمة.

ولاحظ .. ظهور النافذة التالية:



٥- اختر Advanced من تلك القائمة.

ولاحظ.. ظهور النافذة التالية:



٦- أنقر Click فوق مربع تنشيط الخيار Encrypt Contents to secure date فهو الخاص بتشفير الملف.

٧- أنقر Click فوق Ok، ثم انقر مرة أخرى فوق Ok من نافذة الخصائص الرئيسية.

٨- انتظر قليلاً حتى تتم عملية التشفير، وبعد انتهاء تلك العملية ستجد أن اسم الملف قد تحول لونه إلى الأخضر، وهذا دليل على أن الملف قد تم تشفيره.

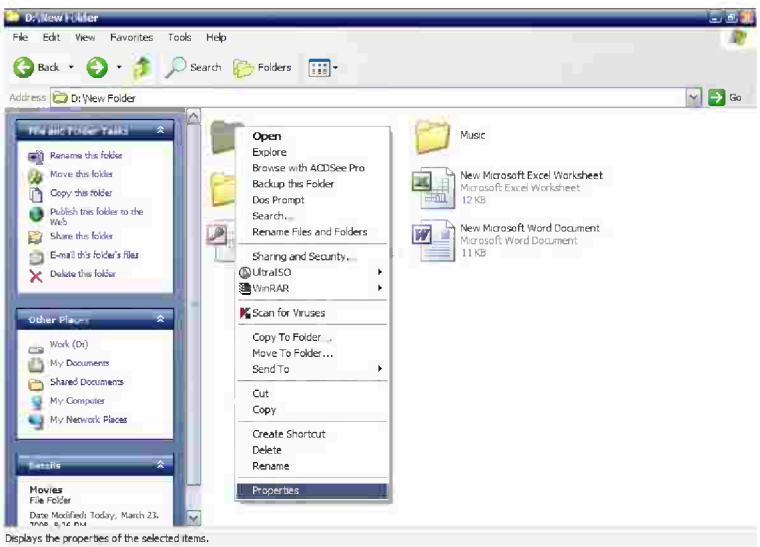
والآن ... إذا حاولت تشغيل الملف من داخل حسابك فستتم هذه العملية على أكمل وجه، أما إذا قام أحدهم بتشغيل الكمبيوتر وفق أي حساب آخر؛ فسيرى الملف دون أن يبدو عليه أي تغيير، فإذا حاول تشغيله فستظهر له رسالة توحي بأن هذا الملف تالف ولا يمكن تشيله بأي حال من الأحوال.

إخفاء الملفـــات:

يمكنك أن تقوم بإخفاء ملفاتك الهامة لتكون بعيدة عن متناول اللصوص، فإذا قام أحدهم باستعراض محتويات اسطوانتك الصلبة فستظهر كافة الملفات عدا تلك الملفات التي أخفيتها، ولتنفيذ تلك عليك إتباع الخطوات التالية:

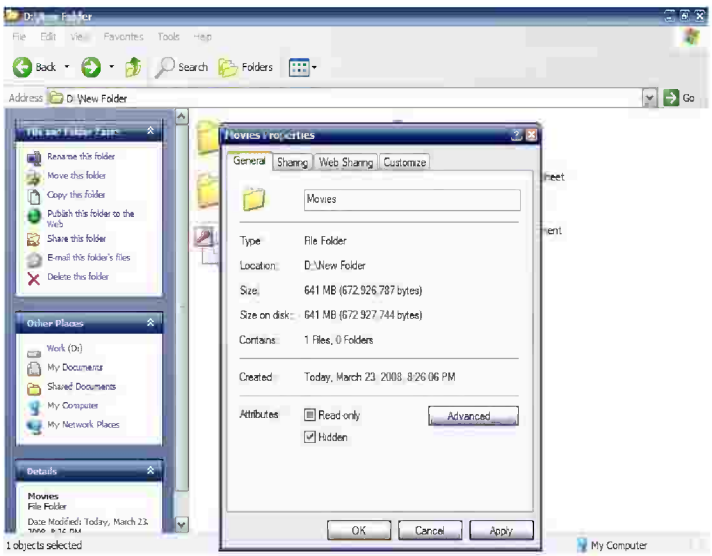
١- اذهب إلى الملف أو المجلد الذي تريد إخفاؤه.

٢- انقر بمفتاح الماوس الأيمن فوق هذا الملف أو المجلد لتظهر لك النافذة المختصرة التالية:



٣- اختر Properties من تلك القائمة.

ولاحظ .. ظهور النافذة التالية:



٤- انقر Click داخل مربع تنشيط الخيار Hidden، فهو الخاص بإخفاء الملف.

٥- انقر Click فوق OK.

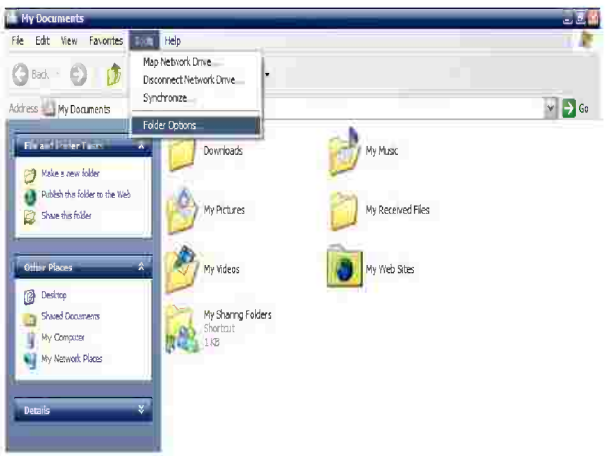
لاحظ .. أن الملف أصبح ملفاً مخفياً.

إظهار الملفات المخبأة:

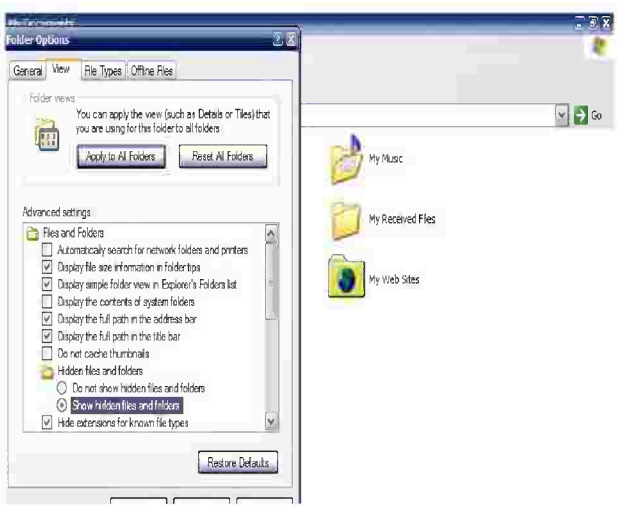
رغم أن فكرة إخفاء الملفات تبدو كأنها قد حلت المشكلة، إلا أن بعض اللصوص ذوي الخبرة البسيطة بالكمبيوتر يمكنهم أن يقوموا بإظهار كافة الملفات المخبأة الموجودة بالاسطوانة الصلبة، ويمكنك التأكد من تلك بإتباع الخطوات التالية:

١- افتح أحد نوافذ عرض الملفات، ولتكن نافذة My Documents .

٢- من قائمة Tools اختر Folder Option .



٣- اختر View من أعلى تلك النافذة لتظهر لك مجموعة الخيارات التالية:



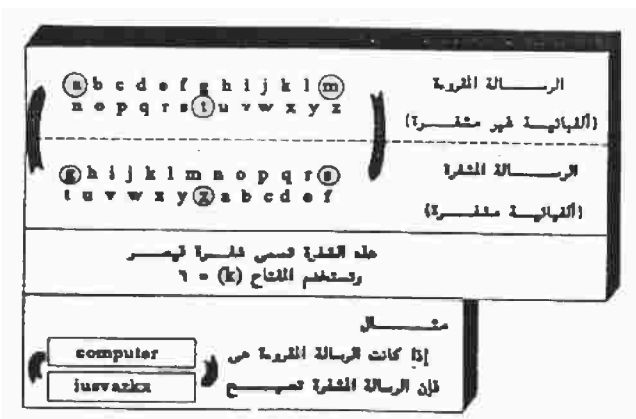
٤- انقر Click داخل مربع تنشيط الخيار Show Hidden File and Folder فهو خاص بإظهار كافة الملفات المخبأة.

نظم التشفير التقليدية

نظم التشفير:

يوجد نوعان أساسيان من نظم التشفير، أحدهما يستخدم التشفير بالإحلال والآخر يستخدم التشفير بالتبديل، كما يمكن دمجهما معاً وعمل نظام ثالث يسمى **بنظام التشفير المختلط**. ويعتبر النظامان الأساسيان (الإحلال والتبديل) غير كافيين حيث يمكن فكهما من قبل محلل النظم وباستخدام الكمبيوتر. أما النظام الثالث فيفي بالغرض إلى حد معقول.

تتم عملية التشفير بإحلال الحروف الموجودة بالرسالة المقروءة بالحروف المناظرة لها بكود الشفرة. ويوضح الشكل التالي أبسط طرق الإحلال حيث يتم الإحلال من أبجدية أحادية. وفي هذه الطريقة يتم بناء أبجدية مشفرة (X) لتشفير الرسالة (A)، بحيث يكون كل حرف في (A) له نظير وحيد في الأبجدية (X).



وهذا النوع من أنظم التشفير سهل الكشف لوجود خواص مميزة للغة، مثل تردد الحرف (e) كثيراً في اللغة الإنجليزية.

ويمكن تطوير هذا النوع من نظم التشفير باستخدام الإحلال من أبجديات متعددة لإخفاء الخواص المميزة للغة. ويتم هذا بوضع مجموعة (n) من الأبجديات المشفرة($X_1, X_2, X_3, \ldots\ldots X_n$) ثم يتم إحلال أول حرف بالرسالة المقروءة بنظيره في الأبجدية (X_1) ثم إحلال الحرف الثاني بالحرف المناظر له في الأبجدية (X_2) وهكذا حتى يتم إحلال الحرف (n) في الرسالة بالحرف المناظر له في الأبجدية (X_n)، ثم يعاد الإحلال من (X_1) مرة أخرى وتستمر هذه العملية حتى يتم تشفير الرسالة. وفي الحالتين يمكن إجراء عملية التشفير بإحلال حرف مكان حرف أو إحلال مجموعة من الحروف في نفس الوقت.

نظام التشفير القياسي:

أنتجت الهيئة القومية الأمريكية للقياسات في منتصف السبعينات خوارزم يقوم بالتشفير باستخدام طريقة الخلط وطرق أخرى غير خطية، وهذا الخوارزم تسمى بنظام التشفير القياسي للبيانات (Data Encryption Standard) ويختصر (DES) وفيه تقسم الرسالة إلى مجموعات كل منها يحتوي على ٦٤ خانة (64-bits)، وتطبق طريقة التشفير المستخدمة على كل مجموعة ١٦ مرة وبعد هذا نحصل على رسالة مشفرة مكونة أيضاً من مجموعات كل منها يحتوي على ٦٤ خانة. ويتكون المفتاح المستخدم من ٥٦ خانة مأخوذين من مفتاح مكون من ٦٤ خانة من ضمنهم ٨ خانات النوعية ويستخدم خوارزم الـ (DES) بالعكس لفك الرسالة المشفرة بنفس مفتاح التشفير.

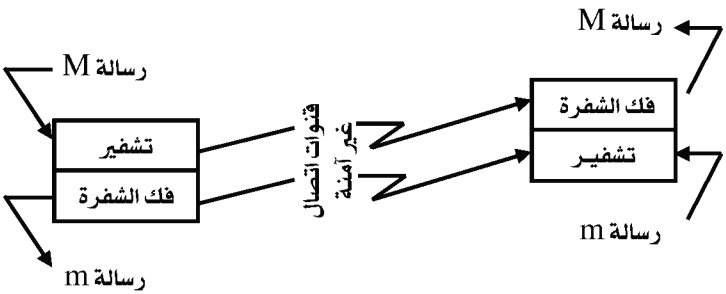
وتستخدم طريقة التشفير هذه في:

أ- حماية كلمة السر.

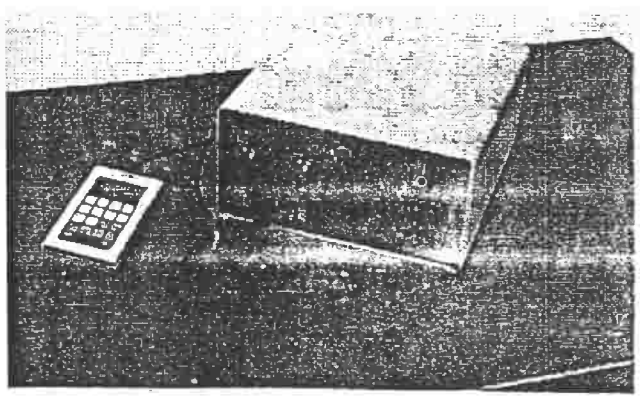
ب- التشفير بين طرفي نظم المعلومات.

ج- تشفير الملفات والبرامج لتخزينها على أوساط حرة النقل.

ويوضح الشكل التالي استخدام نظام (DES) في التشفير بين طرفي نظم المعلومات حيث يمكن إرسال الرسائل السرية عبر قنوات غير مؤمنة بعد تشفيرها.



ويتم الآن تصنيع دوائر إلكترونية تقوم بالتشفير بالـ DES ويوضح الشكل التالي جهاز التشفير الإلكتروني الذي يقوم بتحويل الرسالة المقروءة إلى رسالة مشفرة خلال قنوات الاتصال.



كفاءة الـ (DES) في الحماية من التهديدات:

في هذا الجزء سنرى مدى كفاءة طريقة التشفير بالخوارزم (DES)، بفرض أن مفتاح فك الشفرة غير معلوم. إذن يوجد ثلاث طرق أساسية لمحلل الشفرة لمهاجمة شفرة الـ (DES) وهي:

أ- مهاجمة الرسالة المشفرة حيث يحصل محلل الشفرة على الرسالة المشفرة فقط ولا يعرف أي شيء عن الرسالة الأصلية.

ب- مهاجمة الرسالة المقروءة حيث يحصل محلل الشفرة على الرسالة المشفرة والرسالة المقروءة المناظرة لها.

ج- مهاجمة رسالة مقروءة مختارة حيث يحصل محلل الشفرة على رسالة مقروءة معينة ويستطيع الحصول على الرسالة المشفرة المقابلة.

وفي أي من هذه الحالات يجب على محلل النظم إجراء محاولات عددها (٢)^{٥٦} أي (٧,٢×١٠^{١٦}) لكي يحصل على مفتاح فك الشفرة الخاص بالرسالة الموجودة. وإذا كانت كل محاولة تأخذ ميكرو ثانية على الكمبيوتر فإن هذه المحاولات ستأخذ (٧,٢×١٠^{١٠}) ثانية أي سيتم ذلك في (٢٣١٤٠٨ سنة) بالكمبيوتر.

وقد أوضح بعض الباحثين جدلاً أنه من المجدي اقتصادية بناء كمبيوتر متوازي عالي السرعة ليقوم بتنفيذ هذه العملية في (٧,٢×١٠^{٤}) ثاني أي في (٢٠ ساعة). لذلك اعتبر هؤلاء الباحثون أن الـ ٥٦ خانة المكونة لمفتاح الشفرة قليلة ويجب استخدام مفتاح مكون من (١٢٨ خانة) وهو ما يجعل فك هذه الشفرة ضرب من الخيال. **وكما أن نظام التشفير DES معروف تفصيلياً فإن أمن الشفرة بهذا النظام يعتمد على أمن مفاتيح فك الشفرة. لذلك يجب اتخاذ الإجراءات الأمنية الآتية:**

أ- تخزين مفاتيح فك الشفرة – ويجب أن يتم تشفير المفاتيح أيضاً.

ب- توزيع مفاتيح فك الشفرة – حيث يتم توزيعها من خلال رسول خاص أو من خلال شبكة اتصالات الحاسب.

ج- عدم توقع مفاتيح فك الشفرة – حيث يجب توليد المفتاح باستخدام الأرقام العشوائية بحيث يصعب تخمينها.

ونظام التشفير DES حول مشكلة حماية البيانات إلى مشكلة حماية مفتاح فك الشفرة أثناء تداوله أو استخدامه.

التشفير باستخدام المفتاح المتداول Public Key :

تختلف طريقة التشفير باستخدام مفتاح التشفير المتداول عن الطرق الأخرى في أنها:

١- طريقة غير متماثلة.

٢- مفتاح التشفير يعتبر معروفاً للعامة.

وفي هذه الطريقة يختلف مفتاح التشفير (Ke) عن مفتاح فك الشفرة (K_d)، ولكن يجب المحافظة على:

أ- تطبيق العلاقة $M = D[E(M)]$ لفك الشفرة.

ب- عدم القدرة على استنتاج (K_d) من (K_e) بما أنه معلوم.

وتعمل نظم التشفير في هذه الحالة بالطريقة الآتية:

أ- يقوم الشخص بتوليد زوج من المفاتيح (K_e , K_d).

ب- يتم تخزين مفتاح التشفير (K_e) في الفهرس الخاص به في الكمبيوتر.

ج- أي شخص أو هيئة تريد إرسال رسالة (M) لهذا الشخص تقوم باستعراض الفهرس الخاص به ومعرفة المفتاح (K_e) ثم إرسال الرسالة مشفرة ($E(M)$).

د- يستطيع المتطفل في هذه الحالة معرفة الرسالة المشفرة ($E(M)$) ومفتاح التشفير (K_e) ولكن تبقى أمامه مشكلة معرفة مفتاح فك الشفرة (K_d).

وتتم عملية التشفير في هذه الحالة في اتجاه واحد ولا يمكن استخدام الخوارزم بالعكس لفك الشفرة. ومصمم زوج المفاتيح في هذه الحالة يجب أن يعرف معلومات إضافية (سرية) والتي يمكنه بها تخليق مفتاح فك الشفرة (K_d) وتسمى هذه المعلومات (بالباب المسحور).

طريقة ريفيست للتشفير بالمفتاح المتداول:

تعتبر هذه الطريقة من أحسن الطرق المعروفة للتشفير بالمفتاح المتداول والتي تبني فكرتها على صعوبة تحليل عدد كبير من الأرقام الصحيحة إلى معاملاتها الأولية. وتتلخص الخطوات الرئيسية لهذه الطريقة في الآتي:

١- تمثل كل من الرسالة المقروءة (M) والرسالة المشفرة ($E(M)$، ومفتاحي التشفير وفك الشفرة (K_e, K_d)، وطريقتي التشفير وفك الشفرة بأعداد صحيحة موجبة.

٢- يتم توليد مفتاحي التشفير (K_e) وفك الشفرة (K_d) بالطريقة التالية:

أ- اختيار عددين عشوائيين أوليين(p) أو (q) كل منهما يتكون من أكثر من (مائة) رقم.

ب- تكوين الكميتين:

$$n = pq$$

$$r = (p-1)(q-1)$$

ج- اختيار عدد (e) عشوائياً بحيث يكون ($e < r$) وليس عامل مشترك للعدد (r).

د- حساب رقم صحيح (d) من العلاقة:

$$Ed = 1 \bmod r = 1 \bmod (p-1)(q-1)$$

ه- عمل مفتاح التشفير (K_e) (المفتاح المتداول) من (e,n).

٣- تتمثل قوة هذه الطريقة في صعوبة التعرف على العدد (d) والذي يتطلب تحليل العدد n، حيث n هذا يتكون من مائتي رقم.

٤- تحويل الرسالة (M) إلى رسالة مشفرة (C) حيث:

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

٥- تسترجع الرسالة (M) من الرسالة المشفرة (C) عن طريق:

$$M^e \bmod (n) = M$$

مثال توضيحي:

باعتبار الحالة البسيطة التالية:

أ- العددان الأوليان هما:

$$P = 7, q = 11$$

ب- إذن العددان r,n هما:

$$n = pq = 7 \times 11 = 77$$

$$r = (p-1)(q-1) = 6 \times 10 = 60$$

ج- إذن العدد e المطابق للشروط يمكن أن يكون:

$$e = 37$$

د- يتم حساب العدد d من العلاقة:

$$37d - 1 \bmod 60$$

نجد أن:

$$d = 13$$

ه- في هذه الحالة يكون:

المفتاح (K_d)السري هو (13.77).

المفتاح (K_e) المتداول هو (37.77).

وهذا المثال بالطبع غير حقيقي ولكنه يوضح لنا كيفية استخدام هذه الطريقة، ويجب ملاحظة أنه يوجد قيم أخرى لكل من (e,d) لكل من n= 77، r =60. فمثلاً يمكن للقيمة (e=11) أن تفي بالشروط وباستخدامها نحصل على قيمة أخرى للعدد (d).

التشفير في اتجاه واحد :

التشفير في اتجاه واحد one way encryption هو أسلوب من أساليب التشفير تأخذ الرسالة المراد تشفيرها وتحورها لتخرج بشيء يسمى مفتاح الشفرة (Hash Key)، وأهم ما في هذا المفتاح هو أنه لا توجد طريقة فيه لفك التشفير والحصول على الرسالة الأصلية منه، ولهذا السبب سمى هذا الأسلوب بأسلوب التشفير باتجاه واحد.

ومن أشهر خوارزمياته المستخدمة حالياً md5، ويعتبر البعض خوارزمية sha1 خليفة الخوارزمية md5.

وقد تتساءل عن الحاجة لتشفير البيانات إذا لم تكن قادراً بعد ذلك على فك تشفيرها، لكن هذا الأسلوب من أساليب التشفير هو في الواقع أكثر الأساليب استخداماً. هو يستخدم في الأنظمة التي تحتاج فيها للتحقق من صحة معلومات ما دون الحاجة لمعرفة فحوى هذه المعلومات، وذلك لأن تشفير نفس الرسالة بنفس الخوارزمية ينتج مفتاح الشفرة نفسه في كل مرة.. وسنأخذ أمثلة عملية على ذلك...

تخزين كلمات المرور في ملف قابل للاختراق :

لنفرض أن لديك موقعاً على الإنترنت وكنت تريد تخزين كلمات المرور للمشتركين فيه، لكنك كنت قلقاً من أن يتمكن مخترق ما من الوصول إلى هذه المعلومات خاصة وإن الكثير من المستخدمين يستخدمون كلمات المرور نفسها في أكثر من مكان، وبالتالي قد يستخدم المخترق هذه المعلومات لاختراق صناديق البريد الإلكترونية للمشتركين في خدمتك عبر تجربة كلمة المرور نفسها، أو اختراق اشتراكاتهم في آية خدمات أخرى، مما سيعود عليك بسمعة سيئة جداً.

في هذه الحالة يمكنك أن تقوم بتشفير كلمات المرور باستخدام md5 مثلاً وتخزين مفتاح الشفرة في الملف، وهذا لن يتمكن المخترق أبداً من معرفة كلمة المرور حتى لو حصل على الملف الذي يحتوي على مفاتيح الشفرة لكلمات المرور.

وفي المقابل، فإنه عندما يقوم المستخدم الذي يعرف كلمة المرور الصحيحة الخاصة به بمحاولة الدخول على الخدمة، يمكن لبرنامج أن يقوم بتشفير كلمة المرور التي أدخلها المستخدم باستخدام md5 أيضاً وبعد ذلك مقارنة مفتاح الشفرة الناتجة بمفتاح الشفرة المخزن في ملف المستخدم، فإذا كان المستخدم قد أدخل كلمة المرور نفسها فإن مفتاح الشفرة الذي سينتج عن تشفيرها هو نفس مفتاح الشفرة المخزن بالملف وبالتالي نعلم بأن كلمة المرور صحيحة.

ولهذا السبب قلت في البداية أننا نستخدمها عندما نريد التحقق من صحة المعلومات دون الحاجة لأن نعرف فحوى المعلومات، فهناك مثلاً نريد التحقق من صحة كلمة المرور المدخلة دون أن يهمنا محتوى كلمة المرور نفسه.

إرسال كلمة المرور بصورة مشفرة على الشبكة:

في المثال السابق قلنا بأننا سنقوم بتشفير كلمة المرور في ملف المستخدم المخزن على السيرفر، وفي حال حدث اختراق فإن المخترق لن يتمكن من معرفة كلمة المرور الحقيقية، لكن هناك مشكلة أخرى، وهي أن البيانات في أغلب المواقع سترسل على الشبكة عبر اتصال غير آمن، وذلك يعني بأن من السهل معرفة كلمة المرور التي أرسلت عبر الشبكة عن طريق التصنت على الاتصال.

الحل الأفضل من الناحية الأمنية هو استخدام تقنية SSL لحماية الاتصال، لكن ذلك خيار غير عملي في أغلب المواقع بسبب تكاليف الحصول على شهادة SSL

وبسبب المتطلبات التقنية لاستخدام هذه التقنية على المزود، لذا فإننا مضطرون لإيجاد حل وسط.

يمكننا مبدئياً أن نقوم بتشفير كلمة المرور قبل إرسالها، ومقارنتها بالنسخة المشفرة عند وصول كلمة المرور إلى هناك، وهنا نكون قد تأكدنا من أن المتجسسين على الاتصال لن يعرفوا كلمة المرور، لكن المشكلة هي أن كلمة المرور المشفرة أصبحت الآن هي التي يتوقعها برنامج ليسمح لك بالدخول إلى النظام، وبالتالي فإن الكلمة المشفرة نفسها تصبح أمراً حساساً وسرياً في نظامك، وبالطبع لن يتمكن المخترق أو المتصنت من معرفة كلمة المرور. لكنه سيتمكن من الدخول إلى النظام باستخدام مفتاح الشفرة.

الحل لهذه المشكلة يكمن في أسلوب يدعى التحقق بالتحدي والرد authentication challenge- response، وفي هذا النظام يقوم المزود (السيرفر) بإرسال نص عشوائي للزبون فيقوم الزبون بأخذ كلمة المرور التي أدخلها المستخدم ويضيف إليها هذا النص العشوائي ويشفرهما معاً ويرسل مفتاح الشفرة الناتج عن هذه العملية إلى المزود، فيقوم المزود من جانبه بإضافة هذا النص العشوائي إلى كلمة المرور المخزنة في ملف المستخدم وتشفيرهما ومقارنة مفتاح الشفرة الناتج بمفتاح الشفرة الذي أرسله الزبون، وأهم نقطة في هذا النظام أن النص العشوائي الذي يرسل إلى الزبون يجب أن يتغير مع كل مرة يحاول فيها المستخدم الدخول.

وبهذه الطريقة، حتى إذا تمكن المتصنت من الحصول على مفتاح الشفرة الذي أرسله المستخدم إلى المزود، فإنه لن يتمكن من استخدامه مرة أخرى، لأن المزود سيرسل نصاً عشوائياً مختلفاً في كل مرة ولن يسمح للمتصنت باستخدام نفس النص العشوائي الذي استخدمه المستخدم من قبل.

هذه الطريقة قد لا تكون الطريقة التي تقرأ عنها عند قراءة الكتب المتخصصة تحت عنوان نظام التحدي والرد، ولكنها أقرب شيء لتحقيق الهدف نفسه بسهولة وفعالية باستخدام التشفير باتجاه واحد، أما أشهر الأمثلة على هذا النظام فهو بروتوكول كيربيروس الذي يستخدم في الشركات والذي يعتمد على خطة التشفير المتناظر.

التأكد من عدم التلاعب ببيانات ما:

واحدة من استخدامات نظام التشفير باتجاه واحد أيضاً هو للتحقق من عدم التلاعب ببيانات أو ملفات ما، فإذا قمت مثلاً بالحصول على برنامج ما من أحد الزملاء، فإن هناك احتمالاً بأن هذا البرنامج قد يكون قد تم التلاعب به عمداً أو أنه أصيب بفيروس ما أو أنه حدث به تغيير غير متعمد أثناء تنزيله من الإنترنت مثلاً بسبب عطل ما في الاتصال، فنحن بحاجة هنا لطريقة ما نتأكد فيها من تطابق نسخة البرنامج التي لدينا مع النسخة الأصلية للبرنامج.

لهذا السبب تقوم الكثير من مواقع البرامج مفتوحة المصدر وبعض الشركات بوضع مفتاح تشفير للبرنامج الأصلي الذي تتجه بنظام md5 و sha1 لتتمكن من تشفير نسخة الملف التي لديك لمقارنة مفتاح التشفير الناتج بمفتاح التشفير المنشور على موقع الشركة والتأكد بالتالي من أن البرنامج متطابق ولم تحدث عليه آية تغييرات.

كذلك فإن هذه الطريقة تستخدم ضمن الأجهزة كأسلوب أمني للتأكد من عدم حدوث تغييرات في الأجزاء الحساسة من النظام، فتقوم بعمل فحص دوري للبرامج وللملفات الأساسية في النظام وتخزين مفاتيح تشفيرها في قاعدة بيانات محفوظة، ومع تكرار هذه العملية دورياً يقوم النظام بالتأكد من أن مفاتيح التشفير للبرامج لم تتغير،

وإذا حدث تغير ما فإن النظام يقوم بإصدار التحذيرات الأمنية المطلوبة إلى مدير النظام، وهذا النظام مفيد جداً بعد اكتشاف حادثة اختراق للنظام لمعرفة ما إذا كان المخترق قد تلاعب بملفات النظام. بشرط أن يكون هنالك قاعدة بيانات تحتوي على مفاتيح التشفير لبرامج النظام قبل الحادثة وأن تكون قاعدة البيانات هذه محمية من التلاعب بحيث نعلم بأن المخترق لم يقم بالتلاعب حتى بقاعدة البيانات هذه، ويكون ذلك عادة بحفظ قاعدة البيانات بصفة دورية في جهاز منفصل يكون على درجة عالية جداً من الأمان أو بطباعتها على الورق وأرشفتها.

ضوابط ومستويات التشفير

أولاً: الضوابط

١- لا يوجد نص في القانون يحظر تشفير بيانات هذه التجارة الإلكترونية وذلك من خلال الوسائط الإلكترونية المتعددة.

٢- احترام سرية البيانات المشفرة والاعتراف بحق أصحابها في الخصوصية.

٣- أن استخدام التشفير كوسيلة يعتد بها القانون في شأن تحرير البيانات والمعلومات يكون بواسطة الجهات المختصة التي يحددها القانون أو لائحته التنفيذية في حالة الإحالة إليها.

ثانياً : مستويات التشفير

م	مستوى التشفير	ما يتم تشفيره	نماذج التطبيقات
١	تشفير وصلات الاتصالات Transmission level	تشفير كل ما يمر عبر وصلات الاتصالات عند نقطة الإرسال ويتم حلها عن نقطة الاستقبال	الشبكات الخاصة المؤمنة
٢	مستوى التصفح Session level	تشفير البيانات التي يتم تداولها بين برنامج تصفح البيانات وبين مقر المعلومات الذي يتم تصفحه	نظام نيتسكيب لتأمين المقابسsecure socket layer نظام التأمين secureبروتوكول الاتصال hyper text transport protocol (SHTTP)
٣	مستوى التطبيق المستخدم في تنفيذ المعاملة الإلكترونية Application layer	استخدام تطبيق خاص لتشفير البيانات ويتم استخدامه للتشفير الجزئي	نظام تأمين المعاملات الإلكترونية secure Electronic Transaction(SET) نظام محفظة سيبر كاش Cyber Cash Wallet
٤	مستوى الملفات	تشفير الملفات أو الرسائل التي يتم تبادلها.	نظام نورتل إنترنت Nurtel's Enterust نظام فيل زيمرمان للخصوصية Phil Zimmerman's pertly good privacy (PGP)

وأخيراً فإنه يجب التنبيه إلى أن هناك مجموعة من العقبات والصعوبات التي تواجه عملية التشفير منها ما يلي:

١- من الصعب فرض أسلوب تشفير معين أو الحد من استخدامه في إحدى الدول لأنه سيدفع شركات التشفير الأجنبية على زيادة نشاطها. فالمنافسة بين شركات الدول المتقدمة الصناعية في هذا المجال منافسة قوية.

٢- الضغط على الجهات التي تتبع أسلوب التشفير بأن تضع مفاتيح شفرتها لدى طرف ثالث هو أسلوب غير عملي لأنه يتعارض مع هدف التجارة الإلكترونية ذات الاقتصاد العالمي ويحتاج إلى تنسيق دولي فيما بين الدول في شكل اتفاقيات دولية أو متعددة الأطراف.

٣- للحكومات دور مهم في تشجيع نمو وانتشار التجارة الإلكترونية ولكن تمسكها بإجراءات ومتطلبات الأمن القومي سيفقدها ما أنفقته على تشجيع هذه التجارة.

ولكن على الرغم من كل هذه الاعتبارات فإن التشفير دوراً مهماً جداً في التسويق عبر الإنترنت.