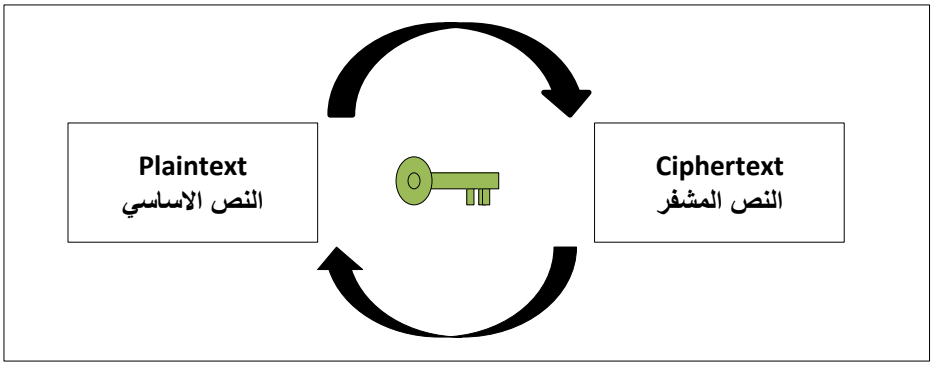
التشفير

يمكن تعريف التشفير على انه عملية تحويل النص الاساسي للرسالة الى شكل اخر لا يمكن قراءته الا من خلال الاشخاص المصرح لهم بذلك ، و تكون هذه الصلاحيات في قراءة والتعامل مع هذه الرسالة المشفرة من خلال ما يسمى بالمفتاح.

يمثل المفتاح في علم التشفير معادلة رياضية معقدة تستخدم في عملية التشفير و ايضا في عملية فك التشفير، و تعتمد قوة التشفير بناء على قوة هذا المفتاح و اقصد بالقوة هنا أي عدد البت (Bit) المستخدمة ، فكلما زادت عدد البت المستخدمة كلما كان التشفير قوياً وأخذ وقتاً اطول في كسر هذا التشفير، و في الشكل رقم (1) صورة توضيحية لعملية استخدام المفتاح في عملية التشفير وفك التشفير.



شكل رقم (1): استخدام مفتاح للتشفير و فك التشفير

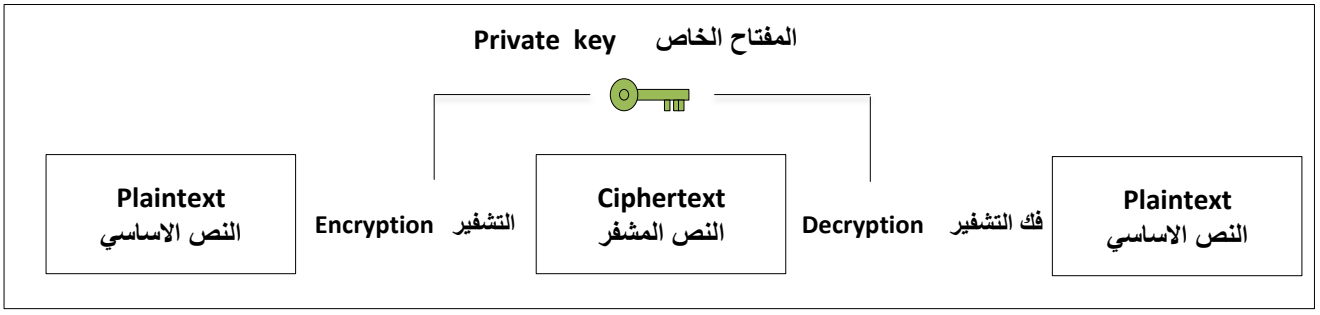
وهنا بعض المصلحات المهمة في علم التشفير:

المصطلح	تعريفه
Encryption	عملية التشفير.
Decryption	عملية فك التشفير.
Plaintext	وهو نص الرسالة الاساسي قبل عملية التشفير.
Ciphertext	ويمثل نص الرسالة بعد عملية التشفير.
Key	وهو المفتاح الذي يستخدم في عملية التشفير وفك التشفير و يمثل هذا المفتاح صيغة رياضية معقدة تسمى Algorithm.

و كما ذكرنا سابقا بان التشفير يتعمد على نوع المفتاح المستخدم نستعرض هنا انواع التشفير بناء على نوع المفتاح وهي كما يلي:

النوع الاول: التشفير باستخدام المفتاح المتماثل Symmetric

وفي هذا النوع يتم استخدام مفتاح واحد في عملية تشفير الرسالة وايضا يتم استخدام نفس المفتاح في عملية فك تشفير الرسالة و لذلك يطلق على هذا النوع بالمتماثل لأنه يتم استخدام نفس المفتاح، و يفضل الكثير استخدام هذا النوع لسهولته و لكن يعيبه ان نقل المفتاح المستخدم في التشفير في الشبكة يكون بشكل غير آمن ، و يوضح الرسم التالي عملية استخدام نفس المفتاح في علمية التشفير وايضا في عملية فك التشفير.

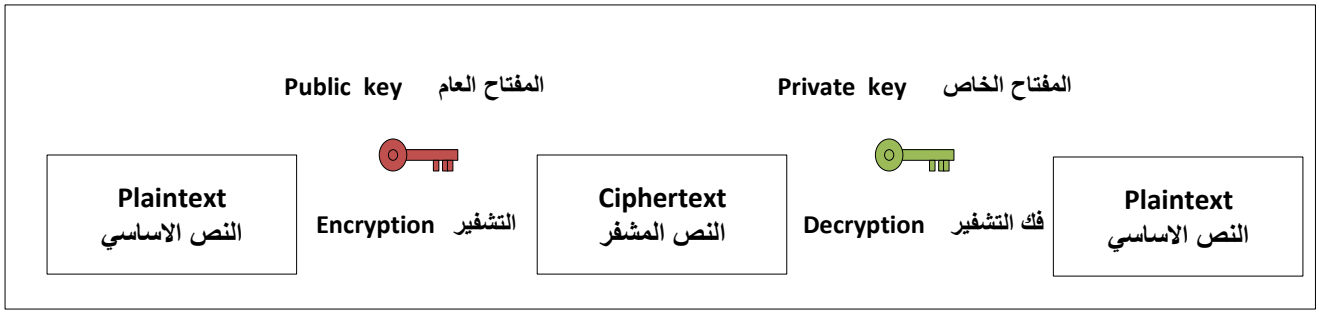


شكل رقم (2): التشفير من النوع المتماثل Symmetric

و كمثال على هذا النوع Data Encryption Standard DES والذي يستخدم مفتاح واحد بطول 56 بت ، و لكن المشكل في هذا النوع ان المرسل والمستقبل يستخدمان نفس المفتاح والذي قد يكون عرضه للسرقة عند أرساله من خلال الشبكة .

النوع الثاني: التشفير باستخدام المفتاح الغير متماثل Asymmetric

وهنا يتم استخدام مفتاح لتشفير الرسالة يسمى المفتاح العام (Public key) و استخدام مفتاح اخر في عملية فك التشفير يسمى المفتاح الخاص (Private key)، و بالنسبة للمفتاح العام فيكون متوفر مع الكل بينما المفتاح الخاص يكون مع شخص واحد فقط وهو المسئول عن فك التشفير ، والرسم التالي يوضح التشفير باستخدام المفتاح الغير متماثل.



شكل رقم (3): التشفير من النوع الغير المتماثل Asymmetric

ونذكر هنا التشفير باستخدام Pretty Good Privacy PGP وهو من افضل انواع التشفير واكثرها استخداماً و ذلك لأنه يحتوي على نسخه تجارية و اخرى مجانية ، ويستخدم هذا النوع تشفير بمفتاح لا يقل عن 128 بت.

و كخدمة ممتازة في انظمة التشغيل سواء الخاصة بالاستخدام الشخصي مثل ويندوز XP او حتى انظمة الشبكات مثل ويندوز سيرفر 2003 ، فان اداة التشفير مضمنة مع النظام ، حيث يمكن للمستخدم ان يقوم بعملية تشفير الملفات بكل سهولة ، و سوف اعرض هنا الخطوات الخاص بشفير مجلد في نظام الويندوز XP :

1-تحديد المجلد المراد تطبيق التشفير عليه و لنفرض ان هذا المجلد هو CISP .

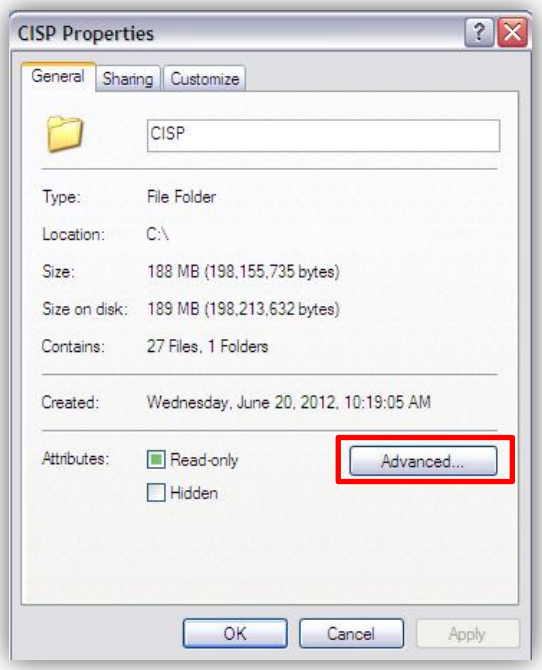
شكل رقم (4):المجلد المراد تشفيره

2-الضغط على هذا المجلد بالزر الايمن للفارة لتظهر القائمة التالية.

شكل رقم (5):قائمة اوامر المجلد

3-نختار من القائمة الامر خصائص.

4-تظهر شاشة الخصائص الخاصة بهذا المجلد نقوم بالضغط على زر خصائص متقدمة.



شكل رقم (6):خصائص المجلد

5-تظهر شاشة تحتوي على اختيار لإجراء عملية التشفير Encrypt contents to secure data نقوم بوضع علمه الصح عليه (√) ثم نضغط على زر الموافقة.

شكل رقم (7):اختيار تشفير المجلد