وزارة التعليم العالي والبحث العلمي

جامعة الفرات الاوسط

المعهد التقني /السماوة

قسم تكنولوجيا المعلومات والاتصالات

مدرس المادة :م.م بيداء هادي محمد سعودي

المحاضرة السادسة

أمنية الحاسبات والبيانات

COMPUTER & DATA SECURITY

DATA ENCRYPTION: تشفير البيانات

مفهوم التشفير

التشفير (Encryption) : هي عملية تحويل النص أو البيانات إلى شكل غير مفهوم بغرض إخفاء هذه البيانات أو هو عملية تحويل من نص صريح (Plain Text)إلى نص مشفر غير صريح((Cipher text))
مصطلح التشفير (Cryptography)هو عملية يتم فيها إخفاء المعلومات عن طريق مفتاح سري وخوارزمية.
حيث ان الشخص الذي يعلم المفتاح ويعلم خوارزمية التشفير يمكنه فك الشفرة (أي استعادة المعلومات الأصلية)، يمكن ايضاً ان يقوم شخص لا يعرف خوارزمية التشفير ومفتاح التشفير بفك الشفرة ولكن تسمى العملية هنا عملية غير مخولة .

Plain text	*النص الأصلي قبل عملية التشفير*
Cipher text	*النص المشفر بعد عملية التشفير*
Encryption	*تحويل النص العادي إلى نص مشفر*
Decryption	*فك التشفير اي تحويل النص المشفر إلى نص عادي*

المفتاح(key) وهو عبارة عن كلمة السر المستخدمة في خوارزمية التشفير أو فك التشفير ويعتبر من أهم الأشياء التي يجب إخفائها حيث أنه يعتبر من الأشياء السرية التي لا يعرفها الا المخول لهم فك الشفرة1.

الخوارزمية (Algorithm):

الخوارزمية هي عبارة عن الخطوات اللازمة لحل مسألة ما,قد تكتب هذه الخوارزمية باللغة العربية أو الإنجليزية أو قد يعبر عنها برسم أشكال هندسية معينة .

أهداف التشفير

يوجد أربعة أهداف رئيسية وراء استخدام علم التشفير وهي كالتالي:

السرية أو الخصوصية (Confidentiality):هي خدمة تستخدم لحفظ محتوى المعلومات من جميع الأشخاص ما عدا الذي قد صرح لهم الاطلاع عليها.

تكامل البيانات (Integrity):وهي خدمة تستخدم لحفظ المعلومات من التغيير (حذف أو إضافة أو تعديل) من قبل الأشخاص الغير مصرح لهم بذلك.

3. إثبات الهوية (Authentication):وهي خدمة تستخدم لاثبات هوية التعامل مع البيانات (المصرح لهم .)

4. عدم الجحود Non-repudiation : وهي خدمة تستخدم لمنع الشخص من إنكاره القيام بعمل ما، أو اثبات عمل قام به فعالً فلا يستطيع انكاره أو التملص منه، فالتشفير يوفر الاثبات من خلال استخدامه في التوقيع الرقمي Digital Signature، والتوقيع الرقمي هو التوقيع الذي يستخدم تقنيات التشفير والذي يمتلك المفتاح العام والمفتاح الخاص والشهادة الرقمية.

إذاً الهدف الأساسي من التشفير هو توفير هذه الخدمات لأشخاص ليتم الحفاظ على أمن معلومات .

عناصر التشفير:

1-الخوارزمية .
2-مفتاح التشفير .
3-النص الأصلي .
4- نص المشفر .
5- ملاحظة -:معرفة أي ثلاثة عناصر من العناصر المذكورة سوف يؤدي إلى استنتاج العنصر الرابع.

يشير مصطلح كلمة تشفير إلى تحويل النص العاديPlaintext من شكل مقروء، بواسطة خوارزميات التشفير ومفاتيح Keys التشفير ، إلى هيئة نص مرمز (Ciphertext)وغير مقروءة ،ثم إعادة فك الترميز((Decryption)) هذا واعادة النص إلى أصله بواسطة الخوارزميات أيضا ومن قبل الاشخاص المسموح لهم بذلك الذين يملكون أدوات فك التشفير.

أنواع التشفير: Encryption Types

اولا:التشفير باتجاهين

تستخدم هذه الطريقة من التشفير عندما نكون بحاجة لاستعادة المعلومات التي قمنا بتشفيرها أي إعادتها للنص الاصل ويمتلك هذا النوع من التشفير خمسة أجزاء، وهي:

1. **النص الصريح**
2. **خوارزمية التشفير**
3. **المفتاح السري**
4. **النص المشفر**
5. **خوارزمية فك التشفير**

يمكن تصنيف التشفير بناءً على المفاتيح المستخدمة في التشفير وفك التشفير إلى نوعين تشفير متماثل Symmetric Encryption وتشفير غير متماثل :Asymmetric Encryption

أنواع التشفير باتجاهين:

1-التشفير المتماثل sy mmetric encryption: وعرف أيضاً بالتشفير بالمفتاح العام، وهو يستخدم مفتاح واحدً لعملية التشفير وفك التشفير للبيانات. ويعتمد هذا النوع من التشفير على سرية المفتاح المستخدَم. حيث أن الشخص الذي يملك المفتاح بإمكانه فك التشفير وقراءة محتوى الرسائل أو الملفات. من أمثلة هذا النوع: شفيرة قيصر، تشفير البيانات القياسي (DES، AES, IDEA, ,3DES, blowfish) وهي أنظمة حديثة ومتطورة وأثبتت جدواها في عصرنا الحالي في مجال التشفير .

يمكن تصنيف التشفير بناءً على المفاتيح المستخدمة في التشفير وفك التشفير إلى نوعين تشفير متماثل Symmetric Encryption وتشفير غير متماثل :Asymmetric Encryption

2-التشفير الغير متماثل: ويعتمد في مبدأه على وجود مفتاحين وهما المفتاح العام Public key والمفتاح الخاص Privet key، حيث أن المفتاح العام هو لتشفير الرسائل والمفتاح الخاص لفك تشفير الرسائل. ومن الأنظمة التي تستخدم هذا النوع من التشفير :

PGP, DSA, Deffie-Hellman, Elgamal, RSA

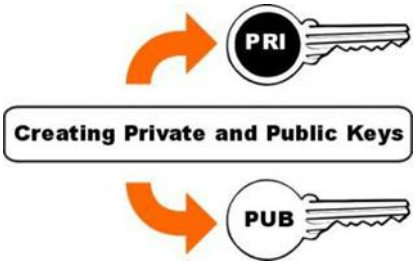
مزايا وعيوب التشفير المتماثل وغير المتماثل:

1-التشفير المتماثل أسرع بكثير باستخدام أنظمة الكمبيوتر الحديثة، ولكنه يستخدم مفتاح واحد فقط. فهو عرضة أكثر لاختراقات.

2-أما تشفير غير المتماثل فيستخدم مفتاحين في عملية التشفير وفك التشفير، وهو أقوى وأقل عرضة لاختراقات، ولكنه أبطأ من التشفير التقليدي .

وتعتمد قوة التشفير في هذا النوع على عاملين أساسيين، هما:

- ✓ **قوة خوارزمية التشفير**
- ✓ **وسرية المفتاح**



ثانياً :التشفير باتجاه واحد :

عملية يتم بموجبها تشفير المعلومات باستخدام خوارزمية التشفير ولكن لا يوجد خوارزمية فك تشفير الرسالة .

لماذا نستخدم هذه الطريقة إن كنا غير قادرين على استعادة النص الأصلي؟

وقد تتسائل عن الحاجة لتشفير البيانات إذا لم تكن قادرا بعد ذلك على فك تشفيرها، لكن هذا الأسلوب من أساليب التشفير هو في الواقع أكثر الأساليب استخداما، وهو 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.

وفي هذا النوع من التشفير التشفير باتجاه واحد عادتا يتم استخدام دالة الاختزال أو الـ (Hash Function)وهي عبارة عن عملية تحويل الرسالة أو البيانات إلى قيمة عددية (numeric hash)

(Value).ودالة الهاش تعتبر إما أحادية الاتجاه أو 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

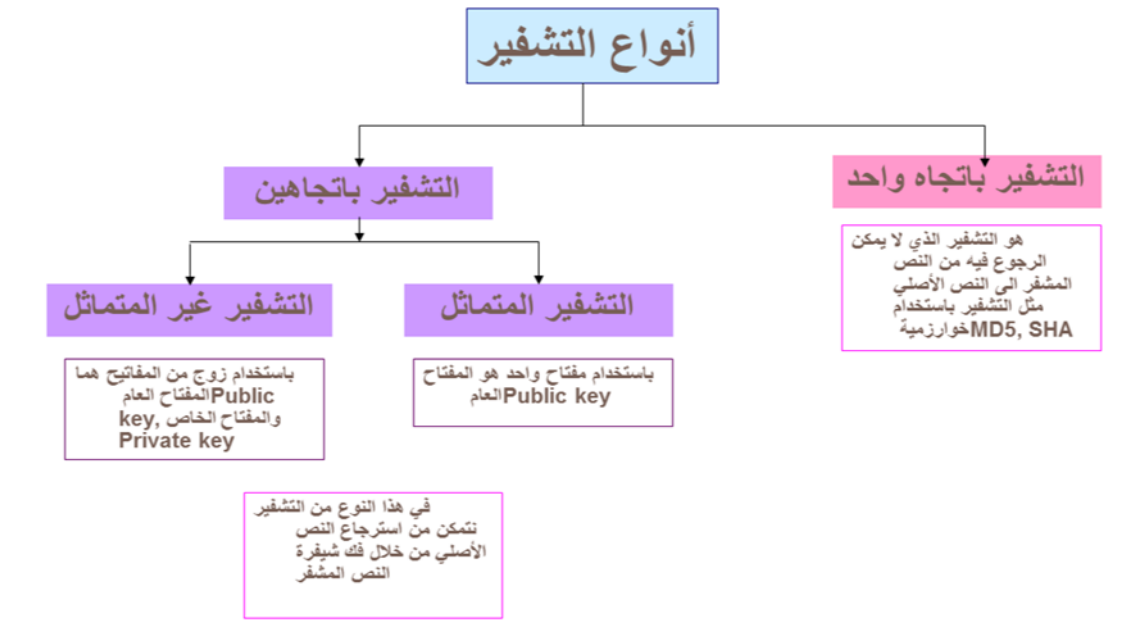
وفي الأغلب أكثر دالات الهاش أحادية الاتجاه أي يستحيل فهم النص المشفر أو العودة منه للنص الأصلي

التأكد من عدم التلاعب ببيانات ما

واحدة من استخدامات نظام التشفير باتجاه واحد أيضا هو للتحقق من عدم التلاعب ببيانات أو ملفات ما، فإذا قمت مثلا بالحصول على برنامج ما من أحد الزملاء، فإن هنالك احتمالا بأن هذا البرنامج قد يكون قد تم التلاعب به عمدا أو أنه أصيب بفيروس ما أو أنه حدث به تغيير غير متعمد أثناء تنزيله من الإنترنت مثلا 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 البرنامج الأصلي الذي تنتجه بنظام md5 وsha1 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 أية 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 ولملفات الأساسية في النظام وتخزين مفاتيح تشفيرها في قاعدة بيانات محفوظة، ومع تكرار هذه العملية دوريا يقوم النظام بالتأكد من أن مفاتيح التشفير للبرامج لم تتغير، وإذا حدث تغير ما فإن النظام يقوم باصدار التحذيرات الأمنية المطلوبة إلى مدير النظام، وهذا النظام مفيد جدا 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 جدا من الأمان أو بطباعتها على الورق وأرشفتها.



أوجه القصور في عملية التشفير:

تنقسم أوجه القصور في عملية التشفير إلى ثالثة أنواع:

1. **الأخطاء البشرية.**
2. **أوجه الخلل في الشفرة ذاتها.**
3. **عمليات الهجوم غير المنطقية.**