❖ تشفير البيانات Data Encryption

يشير مصطلح "تشفير" إلى تحويل النص العادي(Plaintext) من شكل مقروء إلى هيئة نص مرمز (Ciphertext) وغير مقروءة بواسطة خوارزميات التشفير ومفاتيح التشفير ,ثم إعادة فك الترميز(Decryption) وإعادة النص إلى أصله بواسطة الخوارزميات أيضا ومن قبل الأشخاص المسموح لهم بذلك (الذين يملكون أدوات فك التشفير).

أنواع التشفير Encryption Types

يمكن تصنيف التشفير بناءً على المفاتيح المستخدمة في التشفير وفك التشفير إلى نوعين:

- **تشفير متماثل Symmetric Encryption**
- **تشفير غير متماثل Asymmetric Encryption**
-

- **تشفير متماثل Symmetric Encryption:**

يعرف أيضا بتشفير المفتاح الخاص حيث يستخدم فيه نفس المفتاح لتشفير الرسالة ولفك التشفير.يجب أن يتفق الطرفان على مفتاح التشفير مما يسبب مشكلة خاصة عند إرسال المفتاح عبر الشبكات فربما يحدث التقاط لهذا المفتاح وبالتالي كشف المراسلات بين الطرفين لذلك يجب تبادل المفاتيح بطريقة تضمن سريتها.

- **تشفير غير متماثل Asymmetric Encryption**

يعرف أيضا بتشفير المفتاح العام حيث يستخدم فيه زوج من المفاتيح أحدهما لتشفير الرسالة والآخر لفك التشفير.

- **خوارزميات التشفير Encryption Algorithm**

هي عبارة عن صيغ رياضية تستخدم لتحويل الرسالة العادية إلى مكونات مشفرة Ciphered ويمكن وصف العمليتين رياضيا بالآتي :

من أمثلة خوارزميات التشفير:

- **خوارزمية الإحلال Substitution :**

يتم فيها استبدال لمكونات الرسالة الأصلية بتبديل قيمة محل الأخرى مثلا تبديل الحرف الأول بالثالث كما في المثال التالي:

Plaintext=ABCDEFGHJKLMNOPQRSTUVWXYZ

Ciphertext=DEFGHIJKLMNOPQRSTUVWXYZABC

- **خوارزمية الخط المتعرج (Zig_Zag): في هذه الخوارزمية يقسم النص الواضح الى أطوال ثابتة ويتم توزيع الأحرف بالشكل التالي :**

١. **حدد عدد الصفوف التي ستستخدم لتشفير النص حيث أن عدد الصفوف يعد مفتاح التشفير ولا يلزمنا معرفة عدد الأعمدة .**
٢. **إملأ الفراغ في النص الأصلي بمثلث مقلوب (ملاحظة: استخدام المثلث المقلوب بديلا للفراغ لتسهيل الحل فقط).**
٣. **انشئ جدولا يعتمد على عدد الصفوف (مفتاح التشفير).**
٤. **وزع أحرف النص المراد تشفيره بشكل قطري**
٥. **اضف مثلث مقلوب لتساوي الاطوال**

<u>مثال</u> : شفر النص التالي :

I love my country

علما بأن مفتاح التشفير =٢ (صفين).

I		L		v		▼		y		c		u		t		y	
	▼		o		e		m		▼		o		n		r		▼

هنالك انواع اخرى كثيرة لخوارزميات التشفير منها خوارزمية الإزاحة Transportation وغيرها RSA,DES.

❖ برمجيات كشف ومقاومة الفيروسات Antivirus

يقصد بها البرمجيات التي تستخدم لمكافحة البرامج الخبيثة وتسميتها بمضادات الفيروسات لا يجعلها قاصرة على مكافحة الفيروسات فقط بل هو اصطلاح يطلق على هذا النوع من البرمجيات بغض النظر عما إذا كان فيروس فعلاً أو دودة أو Trojan horse أو أي نوع آخر من أنواع البرامج الخبيثة. ومن اشهر البرامج المضادة للفيروسات (McAfee , Norton, Kaspersky) ويجب تحميل النسخة الأصلية وذلك لأن هذه البرامج تقوم بالتأكد من عدم وجود الفيروسات المعروفة، وتكون عديمة الفائدة في مواجهة الفيروسات الجديدة إلا إذا تم تحديث البرنامج من موقع الشركة المنتجة أو المصنعة له على شبكة الإنترنت، ولا يتم التحديث بشكل صحيح إلا إذا كان البرنامج أصلياً.

❖ الجدران النارية Firewall

هي عبارة عن أجهزة hardware وبرامج Software تعمل على أسلوب فلترة وتصفية حركة البيانات الواردة والصادرة من والى الشبكة اعتمادا على قوانين ومعاملات بسيطة. تطورت الجدران النارية بشكل سريع منذ نشأتها وحتى الآن .كانت مثل هذه الجدران النارية توضع في مواقع بين الشبكات للحد من انتشار المشاكل التي يواجهها جزء من الشبكة إلى الأجزاء الأخرى . ظهرت أول الجدران النارية للشبكات في عام ١٩٨٠ وكانت عبارة عن موجهات Routers تستخدم في تقسيم هذه الشبكات إلى شبكات محلية (LAN) صغيرة .

❖ النسخ الاحتياطي Backup

النسخ الاحتياطي عملية اساسية يجب القيام بها بشكل دوري ومنتظم حسب أهمية الملفات، هذا ينطبق على المستخدم المنزلي والملفات على أجهزة الحاسوب في الشركات والمدارس إلى الملفات الحساسة . بسبب عواقب فقدان الملفات نتيجة حادث مثل حريق أو فيضانات، أو تلف أحد مكونات الحاسوب مثل القرص الصلب الحامل للملفات، أو تعرض الحاسوب إلى السرقة أو تخريب متعمد كأن يخترق من قبل قراصنة حاسوب . يصعب على صاحب الملفات استرجاعها وإعادة إنشائها خاصة اذا كانت كبيرة الحجم ومهمة، فيتم عمل نسخ احتياطية من تلك الملفات على وسائط خارجية مثل قرص مضغوط (DVD) أو قرص صلب خارجي ويتم تكرار العملية حسب إستراتيجية تحددها أهمية الملفات وحجمها وتوفر وسائط التخزين الخارجية .