الامن السيبراني وشبكات الحاسوب

م.م. مصطفى مشتاق محمد

المقدمة

الأمن السيبراني هو عملية حماية شبكات الحاسوب وأنظمة التشغيل والبرامج والبيانات ضد الهجمات الرقمية. تهدف هذه الهجمات إلى الوصول إلى معلومات مهمة ومحاولة تغييرها أو تدميرها او للاستفادة منها لأغراض معينة، مثل الاستيلاء على معلومات المستخدمين وعملاء المصارف للحصول على المال أو لاستلاء على بيانات شخصية للمستخدمين لأغراض الابتزاز وغيرها. يمثل تنفيذ تدابير الأمن السيبراني تحديًا كبيرًا اليوم نظرًا لوجود عدد أجهزة يفوق أعداد الأشخاص كما أصبح المهاجمون أكثر ابتكارًا.

شبكات الحاسوب (Computer Networks):

عبارة عن مجموعة من الأجهزة المتصلة مع بعضها البعض مثل (الحاسبات والطابعات والهواتف الذكية وأجهزة ربط الشبكات) ويتم استخدام البرمجيات للسيطرة على عمل الشبكات من ناحية إدارة المستخدمين ومشاركة الموارد:

- البيانات (Data): مثل تبادل البيانات عن طريق البريد الالكتروني.
- البرامج (Software): مثل تحميل البرامج الخدمية والعلمية.
- الأجهزة (Hardware): مثل الطابعات والكاميرات.

امن الشبكات (Networks Security):

تشمل حماية المعلومات والأجهزة المرتبطة بالشبكة من الاختراق والدخول غير المصرح به، وذلك عن طريق استخدام خوارزميات تشفير البيانات بالنسبة للمعلومات واستخدام برامج الحماية من الفيروسات والاختراق بالنسبة لأجهزة الشبكة.

أنواع الشبكات (Network Types)

تقسم الشبكات حسب المساحة الجغرافية الى:

الشبكات المحلية (Local Area Network LAN)

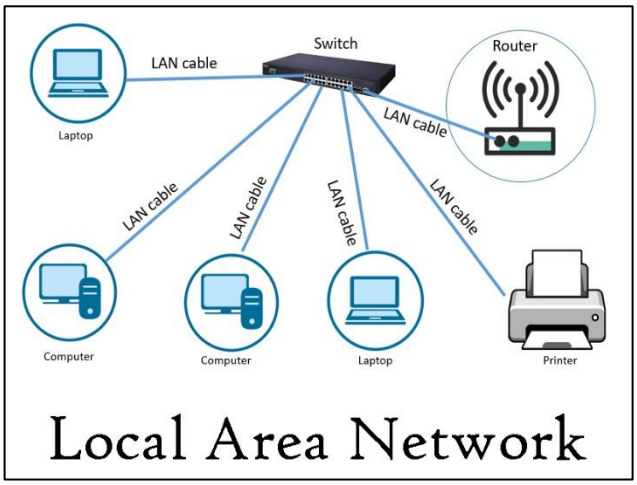
الشبكات الواسعة (Wide Area Network WAN)

ويمكن تقسيم شبكات الحاسوب أيضا بالاعتماد على نوع الربط بين الأجهزة الى:

الشبكات السلكية (Wired Networks)

الشبكات اللاسلكية (Wireless Networks)

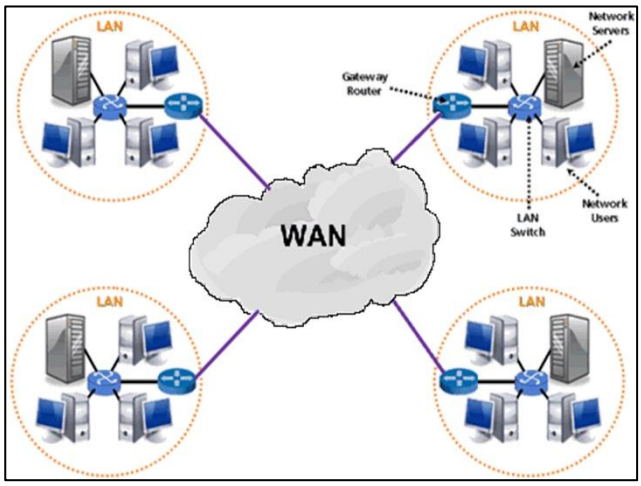
شبكات LAN:



هي مجموعة من أجهزة الكمبيوتر والأجهزة الأخرى مثل الطابعات والكاميرات المتصلة ببعضها عبر الشبكة، وكلها في نفس الموقع عادةً داخل مبنى واحد مثل المكتب أو المنزل او داخل قسم من اقسام الكليات في الجامعة.

شبكات LAN لا تحتاج الى حاسوب مركزي (Server) لإدارة الشبكة. يمكن لهذه الأجهزة مشاركة اتصال إنترنت ومشاركة الملفات مع بعضها البعض والطباعة إلى الطابعات المشتركة.

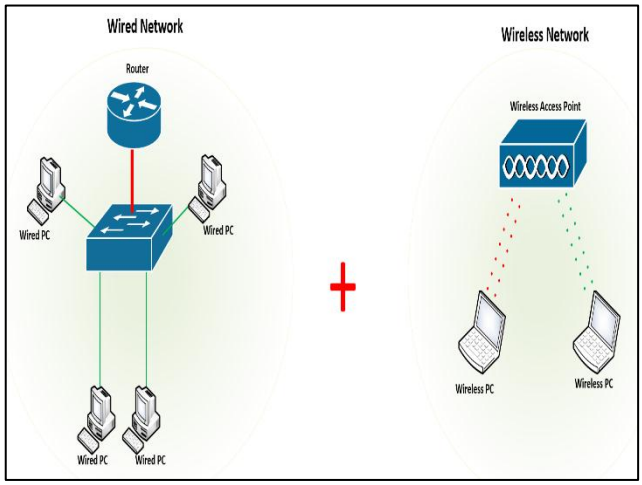
شبكات WAN:



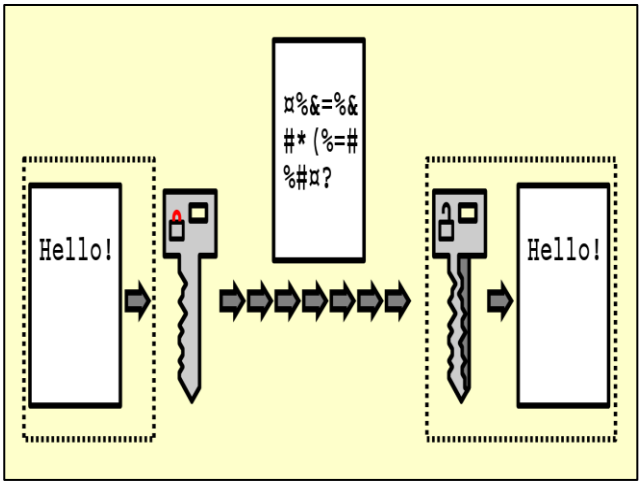
هي مجموعة من شبكات LAN المتصلة مع بعضها ضمن مساحات واسعة مثل شبكة الانترنيت التي تربط الأقسام والكليات مع مركز الحاسبة في الجامعة.

شبكات WAN تحتاج الى حاسوب مركزي (Servers) لإدارة موارد الشبكة مثل مشاركة الملفات عن طريق البريد الالكتروني (Gmail, yahoo mail) او استخدام برامج الاتصالات والتواصل الاجتماعي مثل (Viber, Facebook).

شبكات السلكية واللاسلكية:



امن الشبكات (Network Security) بالنسبة لشبكات (Wireless Network) تكون أضعف من شبكات (Wired Network) لان عملية اختراق الشبكة تعتمد على قوة (Router Password) بينما شبكات (Wired Network) تحتاج الى ربط الجهاز بالشبكة فيزيائياً ليتم اختراقها.



تشفير البيانات(Data Encryption) :

عملية تشفير البينات هي عملية تحويل البيانات من صورتها الحالية الى صورة مشفرة غير قابلة للتفسير وعملية فك التشفير هي عملية معاكسة تماماً اذ يتم استرجاع البيانات الاصلية من الصورة المشفرة للبيانات، كما في الشكل المقابل.

تتم عملية تشفير البيانات باستخدام احدى خوارزميات التشفير المعتمدة مثل (AES , 3DES) مع مفتاح رقمي (digital key) عبارة عن ارقام ورموز تتراوح اعدادها من (8 - 64) رقم ورمز بالاعتماد على نوع الخوارزمية المستخدمة.

قوة تشفير البيانات تعتمد عدد الأرقام والرموز المستخدمة من قبل خوارزمية التشفير:

Super-computer speed= $33.86*2^{52}$ operations per second. (china's super-computer)

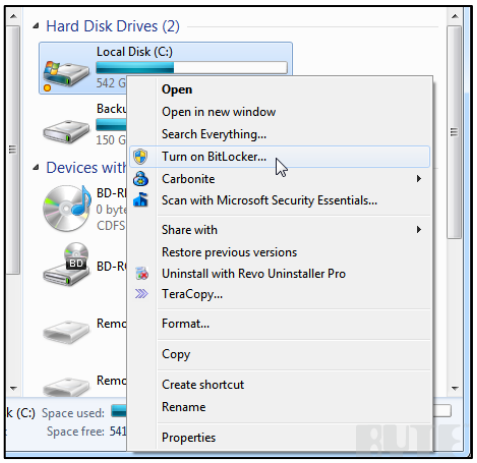
Encryption Key length=16 digits… each digit is 8 bits in the computer world !!, key length is 16*8=128 bits.

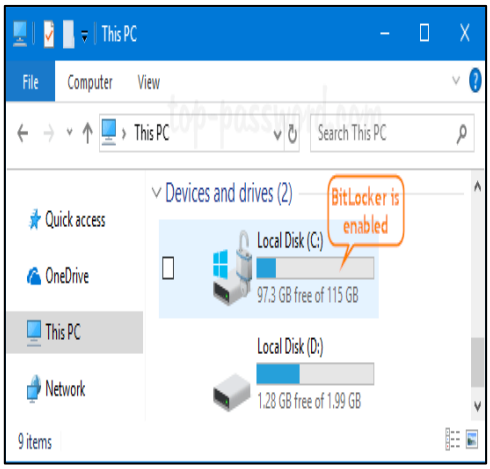
So, the number of possibilities to guess the encryption key= 2^{128}

Time to crack the encryption key = $\frac{2128}{(365*24*60*60)*33.86*252}$ =$2.83*10^{14}$ years!!

تشفير البيانات الثابتة:

تمثل عملية تشفير البيانات المخزونة في وحدات الخزن مثل القرص الصلب وذاكرة الفلاش المستخدمة في أجهزة الحاسوب، حيث يمكن استخدام أداة التشفير التي يوفرها نظام التشغيل (BitLocker Drive Encryption) لتشفير البيانات المخزونة في أجزاء من القرص الصلب، حيث ان الوقت اللازم للتشفير يعتمد على حجم البيانات في وحدة التخزين.





تشفير البيانات المرسلة:

عملية تشفير البيانات المرسلة عبر الانترنيت تتم بطريقتين:

- تشفير البيانات بأجهزة الحواسيب والهواتف الذكية باستخدام خوارزميات التشفير، حيث يتم تشفير البيانات قبل ارسالها الى (servers) ومنه الى مستلم البيانات، مثل تطبيق (WhatsApp) الذي يستخدم طريقة (end to end encryption) بين المرسل والمستلم عند تبادل البيانات.
- تشفير البيانات بأجهزة (servers) الخاصة بمجهز الخدمة مثل خدمات البريد الالكتروني (G-mail) حيث تشفر البيانات عند استلامها ثم تخزن في وحدات الخزن الخاصة بشركة (Google) وترسل نسخة من هذه البيانات الى المستلم.

امن الشبكات (Network Security)

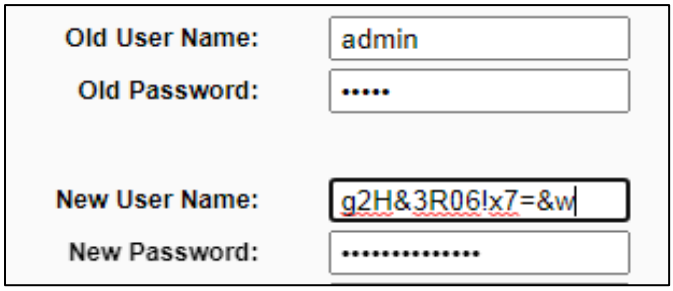
ثلاث خطوات مهمة لأمن الشبكات اللاسلكية يمكن تطبيقها في أجهزة الراوتر (Router):

- (PIN code):

ينصح بتغيير الرمز الخاصة براوتر الشبكة واستخدام رمز جديد يتم توليده من قبل الراوتر، حيث ان هذه الخطوة هي الخطوة الأولى لحماية الشبكة من الاختراق.

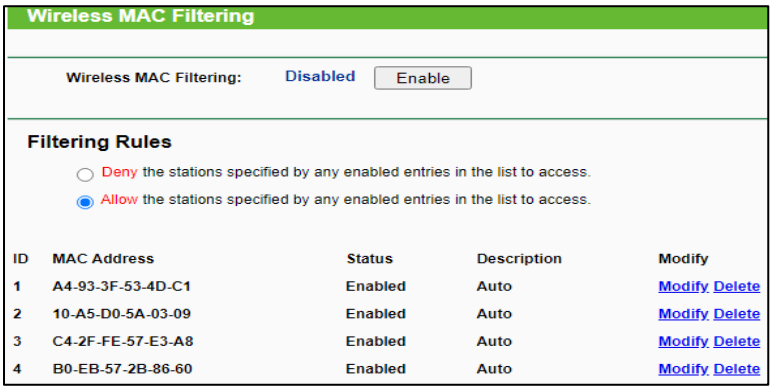
- (user name and password):

ينصح باستخدام اسم مستخدم وكلمة مرور صعبة التخمين، واستخدام الأرقام والرموز بما لا يقل عن 14 رقم ورمز بالنسبة لكلمة المرور.



- (MAC filter):

استخدام قائمة الفلتر الخاص بالراوتر لتسجيل عناوين الأجهزة الموجودة بالشبكة والمعروفة من قبل مدير الشبكة، حيث ان الأجهزة غير المسجلة بالقائمة لا تتمكن من دخول الشبكة حتى لو استخدمت (PIN code) الخاصة بالراوتر.



الجدار الناري (Firewall):

هو إنشاء حاجز لحركة مرور البيانات بين شبكة الداخلية مثل المكتب أو المنزل والشبكة الخارجية (مثل شبكة الإنترنت الخارجي) من أجل منع الملفات والبيانات الضارة مثل الفيروسات وبرامج التجسس والاختراق من المرور إلى الحاسوب، الجدار الناري ممكن أن يكون جهاز (Hardware) أو برنامج (Software) يتم تثبيته على جهاز الكمبيوتر او يكون مدمج مع نظام التشغيل. لذا ينصح دائما بتحديث نظام التشغيل وبرامج الحماية وبشكل دوري.