

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

جامعة كرري

كلية الهندسة

أمن الاتصالات

د عثمان محمد دفع الله  
أستاذ مشارك جامعة كرري

# المحاضرة الأولى

## مقدمة عن أمن الاتصالات

د عثمان محمد دفع الله  
أستاذ مشارك جامعة كرري

## مقدمة

- ان استخدام الاتصالات السرية بواسطة رسائل مرمزة كان التطبيق العملي عبر التاريخ القديم والحديث
- تتضمن الرسائل المكتوبة بواسطة الرموز سلسلة من الأرقام لغرض إرسال المعلومات المجمعة عن الجهات المعادية لضمان عدم تسرب المعلومات
- بالإضافة للاستخدامات العسكرية والجهات الأمنية الأخرى للتشفير هنالك تطبيقات مدنية مثل البنوك والاتصالات
- عدد كبير من الاتصالات التجارية ترسل عن طريق علي رموز لتقليل التكلفة

## مقدمة

- في معظم المحلات التجارية الكبيرة لبيع الأغذية مواد كثيرة معلبة معظم هذه المواد تحمل رموز تاريخ تعلبيها
- كل رمز يعطي الشهر واليوم والسنة لموعد تعلبيها
- عند كتابة العنوان علي الرسائل من المفضل كتابة رمز الكود
- مثل هذا الرمز يمثل الموقع الجغرافي المحدد وهو يساعد في سهولة فرز ومعاملة أكياس البريد التي تحمل هذا الرمز

# المصطلحات والمفاهيم الأساسية

- الهجوم الأمني وهو عبارة عن أي عمل يعرض أمن المعلومات المملوكة لجهة معينة للخطر
- الآلية الأمنية هي عبارة عن آلية تصمم لعملية منع أو كشف الهجوم الأمني لأي منظومة اتصال
- الخدمة الأمنية هي خدمة تحسن أمن أنظمة البيانات وعملية تبادل المعلومات لأي دائرة أو جهة ذات طبيعة خاصة

# أنواع الخدمة الأمنية

- خدمة خصوصية هذا النوع من الخدمة يسمح لأشخاص وجهات مخولة فقط بالإطلاع علي المعلومات في أنظمة الحاسوب وكذلك عملية إرسال المعلومات
- خدمة موثوقة هذا النوع من الخدمة يعطي رسائل أو ملفات الكترونية أصلية وصحيحة وله طريقة معينة للتأكد علي صحة البيانات أو الرسالة
- خدمة متكاملة في هذه الخدمة الجهات والأشخاص المخولين فقط هم الذين يستطيعون أن يعدلوا في أنظمة الحاسوب ويرسلون المعلومات

# أنواع الخدمة الأمنية

- النص الصريح وهو عبارة عن الرسالة الأصلية التي يمكن قراءتها
- الترميز هو طريقة لتحويل الرسائل إلى صيغة سرية باستعمال كلمات أو رموز تمثل كلمات الرسالة
- الشفرة هي طريقة لتحويل الرسالة إلى صيغة سرية باستعمال حروف تعويضية محل الحروف الأصلية أو بواسطة تبديل موضع حروف الرسالة الأصلية
- الكتابة المشفرة هي الرسالة المزمرة أو المشفرة

# أنواع الخدمة الأمنية

- التشفير هو عبارة عن تشفير النص الصريح للحصول علي الكتابة المشفرة
- فك الشفرة هي عملية حل الشفرة وتحويلها إلي صيغة مفهومة للاستفادة منها
- تحليل الشفرة هي عملية حل أو كسر الرموز أو الشفرة دون معرفة المفتاح
- علم التشفير هو عبارة عن مصطلح يطلق علي التشفير وتحليل الشفرة



# أنواع الهجوم الأمني

- تعويقي هذا النوع يؤدي إلى تدمير وإعاقة منظومة الاتصال وجعلها غير قادرة علي أداء دورها بالصورة الصحيحة
- تعرضي وهنا يمكن لجهات غير مخولة الدخول علي المنظومة والاستفادة منها والحصول علي معلومات منها
- تعديلي وهنا يتم الدخول علي المنظومة بواسطة جهات غير مسموح لها بذلك وإعادة تشكيل وتبديل المعلومات الموجودة
- تصنيعي وهنا يتم إرسال معلومات مختلفة تماما عن المعلومات الأصلية

# لتصميم أي منظومة خدمة أمنية لا بدأ من الأتي

- تصميم لوغر ثم رياضي لأداء عملية التحويل التي تؤمن المنظومة
- توليد معلومات سرية لاستخدامها مع اللوغرثم الرياضي
- تطوير طرق وتغنيان لعملية توزيع والمشاركة بالنسبة للمعلومات السرية
- تحديد برتوكول معين واستخدامه بين الجانبين اللذين يقومان بتبادل المعلومات مع اللوغرثم الرياضي لتحقيق الخدمة الأمنية