ترجمة العرض التقديمي: التشفير

# مقدمة إلى التشفير

# خطة الفصل:

مقدمة - التاريخ - التشفير الكلاسيكي - التشفير الحديث - التشفير المتماثل - التشفير غير المتماثل - الشهادات الإلكترونية

# مفاهيم أساسية:

علم التشفير، التشفير، فك التشفير، الرسالة الأصلية، الرسالة المشفرة، المفتاح، نظام التشفير

# أهداف التشفير:

السرية - التوثيق - سلامة البيانات - عدم التنصل

# تاريخ التشفير:

العصر اليدوي - العصر التقني - العصر المتناقض

# التشفير الكلاسيكي:

التشفير بالاستبدال - التشفير بالإزاحة (قيصر) - التشفير بالتبديل - التشفير بسكة الحديد

# تحليل الشفرات:

الهجوم بالقوة الغاشمة - الهجوم بالقاموس - التحليل الإحصائي

# التشفير الحديث:

DES، AES، خصائص التشفير - طرق التشغيل (ECB, CBC, CFB, OFB, CTR)

# التشفير غير المتماثل:

RSA، Diffie-Hellman، التوقيع الرقمي، الشهادات الإلكترونية

# الوظائف الهاشية:

MD5، SHA-1، SHA-256، خصائص الأمان

# البنية التحتية للمفاتيح العامة (PKI):

إدارة الشهادات، التحقق من الشهادات، تسلسل الثقة

# مشاريع مصغرة:

تحليل التشفير - إنشاء PKI باستخدام OpenSSL