

محاضرة: مقدمة في التشفير

مادة الحاسوب - المرحلة الثانية - قسم القانون

أهداف المحاضرة:

1. فهم مفهوم التشفير وأهميته.
2. التعرف على أنواع التشفير.
3. معرفة الفرق بين التشفير المتماثل وغير المتماثل.
4. تسليط الضوء على الاستخدامات القانونية للتشفير.
5. مناقشة الجوانب القانونية والأخلاقية المتعلقة بالتشفير.

أولاً: ما هو التشفير؟

التشفير هو عملية تحويل البيانات من شكلها المفهوم إلى شكل غير مفهوم لحمايتها من الوصول غير المصرح به.

يستخدم في حماية المعلومات الحساسة (البيانات الشخصية، كلمات المرور، المعلومات البنكية...).

ثانياً: أهمية التشفير في عالم اليوم

حماية الخصوصية والبيانات.

تأمين الاتصالات الإلكترونية (مثل رسائل البريد الإلكتروني).

يستخدم في الخدمات المصرفية، التجارة الإلكترونية، وحتى في تطبيقات المراسلة مثل واتساب وتيليغرام.

ثالثاً: أنواع التشفير

1. التشفير المتماثل (Symmetric Encryption):

نفس المفتاح يُستخدم للتشفير وفك التشفير.

سريع لكنه يتطلب طريقة آمنة لتبادل المفتاح.

مثال: خوارزمية AES.

2. التشفير غير المتماثل (Asymmetric Encryption):

يستخدم مفتاحين: مفتاح عام وآخر خاص.

المفتاح العام لتشفير البيانات، والمفتاح الخاص لفكها.

أكثر أماناً ويُستخدم في التوقيعات الرقمية.

مثال: خوارزمية RSA.

رابعاً: مفاهيم أساسية في التشفير

النص الصريح (Plaintext): المعلومات الأصلية قبل التشفير.

النص المُشَفَّر (Ciphertext): المعلومات بعد التشفير.

المفتاح (Key): العنصر المستخدم للتحكم في عملية التشفير أو فك التشفير.

خامساً: التشفير والقانون

التشفير يُستخدم لحماية البيانات القانونية والشخصية.

بعض القوانين تُلزم المؤسسات باستخدام التشفير لحماية معلومات المواطنين.

في المقابل، قد يُستخدم التشفير لإخفاء جرائم إلكترونية (مثل تهريب الأموال أو المواد المحظورة)، مما يخلق تحدياً قانونياً.

سادساً: هل التشفير قانوني دائماً؟

في أغلب الدول: نعم، التشفير مسموح.

بعض الدول تفرض قيوداً على قوة التشفير أو تطلب حق الوصول من الجهات الأمنية (Backdoors).

النقاش مستمر بين حماية الخصوصية والأمن القومي.

سابعاً: تطبيقات التشفير القانونية

حماية سجلات المحاكم.

تأمين المراسلات القانونية بين المحامين والموكلين.

توقيعات رقمية للعقود الإلكترونية.