

الدرس 4

الوحدة 2

تشفير البيانات



وصف الدرس

الغرض العام من هذا الدرس هو أن يتعلم الطلبة أنواع التشفير وأن يتعلم كيفية تشفير وفك تشفير عرض **Microsoft PowerPoint** ورسالة بريد إلكتروني.

ما سيتعلمه الطالب

< التشفير، وأنواعه، وأمثلة استخدامه.

نتائج التعلم

< كيفية تشفير البيانات.

المصطلحات

اللغة الإنجليزية	اللغة العربية
Encryption	التشفير
Symmetric encryption	التشفير المتماثل
Assymetric encryption	التشفير غير المتماثل
Hard disk encryption	تشفير القرص الصلب
Email encryption	تشفير البريد الإلكتروني
Decryption	فك التشفير

اللغة العربية	اللغة الإنجليزية
المفتاح الخاص	Private key
المفتاح العام	Public key



التحديات المتوقعة



< قد يجد الطلبة صعوبة في فهم الفرق بين التشفير المتماثل وغير المتماثل. وضح لهم أن التشفير غير المتماثل يجبر كل شخص مشارك في عملية الاتصال أن يقوم مسبقاً بتبادل نفس المفتاح المستخدم لتشفير البيانات قبل أن يتم فك تشفيرها.

< لإرسال البيانات بشكل خاص باستخدام التشفير غير المتماثل - المعروف أيضاً باسم تشفير المفتاح العام - تحتاج إلى زوج من المفاتيح. الشخص الذي يستلمها له مفتاحان خاصان به أيضاً. على

سبيل المثال، المفتاح العام يشبه رقم الحساب المصرفي والمفتاح الخاص يشبه رقم التعريف الشخصي لجهاز الصراف الآلي.

< يمكنك مشاركة حسابك المصرفي مع أي شخص، ولكن لا يجب عليك أبداً مشاركة رقم التعريف الشخصي. يمكنك استخدام رقم التعريف الشخصي لجهاز الصراف الآلي لإرسال الأموال إلى أشخاص آخرين بشكل آمن إذا كان لديك رقم حسابهم المصرفي. بعد ذلك، سيستخدمون رقم التعريف الشخصي للتحقق من الوصول إلى رقم حسابهم عندما يذهبون إلى ماكينة الصراف الآلي؛ سيعرفون مصدر الأموال لأنهم سيرون رقم حسابك المصرفي في المعاملة. والعكس صحيحاً تماماً.

< عند تسجيل أي نوع من المعلومات باستخدام مفتاحك الخاص ويكون قد تم تشفيرها باستخدام المفتاح العام للمستلم، ستحقق ثلاثة أشياء: أنت تضمن أن المستلم المقصود فقط يمكنه قراءتها عن طريق فك تشفيرها بمفتاحه الخاص. سيضمن المستلم أنك أنت من أرسل الرسالة. ستعرفان أنت والمستلم أن الرسالة لم تعدل من قبل أي شخص آخر.

< قد يحتاج الطلبة إلى المساعدة في فهم نقطة التشفير. اشرح لهم أننا نستخدم التشفير للحفاظ على سرية بياناتنا، حتى لا تتمكن من رؤيتها أعين المتطفلين غير المصرح لهم بالوصول إليها. فقط أولئك المصرح لهم بالوصول إلى البيانات يمتلكون مفتاح فك التشفير. يساعد تشفير البيانات للاتصالات من طرف إلى طرف أيضاً على ضمان تكامل البيانات - أنه لم يتم العبث بها أبداً.



التمهيد

< ناقش مع الطلبة آلية جمع البيانات والتحقق من صحتها.

< ابدأ بطرح أسئلة عليهم مثل:

- هل سمعت من قبل عن مصطلحات التشفير وفك التشفير بالإضافة إلى المفاتيح العامة والخاصة؟

- هل يمكنك معرفة حالات استخدام التشفير؟

- ما هو التشفير وفك التشفير؟

- ما هو الفرق في رأيك بين المفتاح العام والمفتاح الخاص؟



التلميحات الخاصة بالتنفيذ

< لقد تم استخدام الكتابة السرية طوال فترة وجود الكتابة. تم استخدام الرموز طوال التاريخ كلما أراد الأشخاص الحفاظ على خصوصية الرسائل. منذ فترة طويلة يستخدم التشفير من قبل الحكومات والجيش والشركات والمؤسسات لحماية رسائلهم. اليوم، يتم استخدام التشفير لحماية تخزين البيانات والمعاملات بين أجهزة الحاسوب.

< في العصور القديمة عندما تم نقل الرسائل سيراً على الأقدام لأميال، كان الملوك والحكام يشفرون الرسائل التي يرسلونها إلى الحلفاء. وقد ساعد ذلك على حماية سرية الرسالة في حال سرقتها. في التاريخ الأمريكي المبكر، حتى جورج واشنطن أرسل رسائل مشفرة إلى زملائه الجنود. وبالمثل، قام أعضاء الكونغرس بترميز مستنداتهم أيضاً. عندما تم اختراع التلغراف، تم استخدام "مورس كود" لإرسال رسائل مفهومة عبر أنماط الصوت.

< واليوم، يقوم مستخدمو الحاسوب بتشفير المستندات ومساحة الشبكة ورسائل البريد الإلكتروني كوسيلة لحماية سرية رسائلهم. الأنواع الجديدة من التشفير متقدمة جداً وأحياناً معقدة، لكن المهارة الأساسية تظل مرتبطة بالطرق القديمة!

< ساعد الطلبة على فهم أن كلمة المرور في **Microsoft PowerPoint** تساعد على منع الآخرين من فتح عرض تقديمي أو تعديله. عند إنشاء كلمة مرور للعرض التقديمي، قم بتسجيل كلمة المرور واحتفظ بها في مكان آمن. إذا فقدت كلمة المرور، فلا يمكن استردادها ولن يتمكنوا من فتح العرض التقديمي أو الوصول إليه. حماية كلمة المرور غير مدعومة في **PowerPoint** لملفات **ODP Open Document Presentation**. تعد إزالة كلمة المرور من مستند عملية بسيطة، ولكن يجب على الطلبة معرفة كلمة المرور الأصلية. إذا حاولوا فتح ملف محمي بكلمة مرور يعمل عليه شخص آخر بالوقت نفسه،

فسيتمكنون من فتحه، لكنهم لن يتمكنوا من تحريره. سوف يرون الملف في وضع القراءة فقط.



استراتيجيات غلق الدرس

في نهاية الدرس تأكد من تحقيق الطلبة لجميع أهداف الدرس وتقييم معرفتهم من خلال أسئلة على سبيل المثال لا الحصر:

< هل تستطيع أن تتذكر:

- ما هو التشفير وأنواعه.

- كيفية حماية وتشفير العرض التقديمي أو البريد الإلكتروني.

< ذكر الطلبة بالمصطلحات الهامة وكرّرها معهم.

< يمكنك الاستعانة بتدريبات الكتاب ضمن الاستراتيجيات التي ستستخدمها لغلق الدرس.

التدريبات المقترحة لخلق الدرس

يمكنك استخدام التمرين الرابع ضمن استراتيجية خلق الدرس للتأكد من أن الطلبة يمكنهم تطبيق المهارات التي تعلموها في هذا الدرس.

الصف الحادي عشر | المسار العلمي ومسار الإنسانيات

الفصل الأول | كتاب الطالب | الصفحة 143



الفروق الفردية

تمارين إضافية للطلبة ذوي التحصيل المرتفع

< بعد الانتهاء من التمرين الرابع في هذا الدرس، اطلب من الطلبة إنشاء عرض تقديمي يتضمن مقترحات لعكس تغير المناخ، على سبيل المثال ترميم الغابات الاستوائية. ثم اطلب منهم تشفير عرضهم التقديمي وإرساله إلى زملائهم. اطلب من المستلمين فتحه واطلب من المرسلين الكشف عن كلمة المرور. اطلب من المستلمين محاولة فتح العرض التقديمي مرة أخرى وقراءة الاقتراحات للحد من تغير المناخ.

التعامل مع التشفير:

على افتراض أنك تريد إنشاء عرض تقديمي باستخدام PowerPoint، وذلك بخصوص التغير المناخي في قطر، ومن ثم حفظه في حاسوبك.

< أنشئ العرض التقديمي باستخدام Microsoft PowerPoint.

< قم بتشفير العرض التقديمي.

< أرسل العرض التقديمي عبر البريد الإلكتروني إلى زملائك في الفصل.

< اطلب من زملائك القيام بفتح العرض التقديمي.

< ماذا تلاحظون؟

< ماذا تعني بالتشفير؟

< قم بإعطاء المفتاح السري لزملائك.

< اطلب منهم محاولة فتح ملف Microsoft PowerPoint مرة أخرى.

< ماذا تلاحظون؟

< هل هناك فرق بين التشفير المتماثل والتشفير غير المتماثل؟

ما هي أهمية استخدام التشفير في حماية البيانات؟

< أغلق العرض التقديمي.

< قم بإغلاق البرنامج.



اختر الإجابة الصحيحة:

<input type="radio"/> رسائل البريد الإلكتروني.	
<input type="radio"/> الملفات على القرص الصلب.	1. يمكن تشفير:
<input checked="" type="radio"/> جميع ما سبق.	
<input type="radio"/> المفتاح العام	2. يستخدم التشفير المتماثل
<input checked="" type="radio"/> نفس المفتاح	_____ لتشفير وفك
<input type="radio"/> المفتاح الخاص	تشفير ملف أو رسالة.
<input type="radio"/> أداة كلمة المرور السرية	3. التشفير غير المتماثل يُعرف أيضًا
<input type="radio"/> حماية البيانات	باسم _____.
<input checked="" type="radio"/> تشفير المفتاح العام	
<input type="radio"/> يتم رؤية بياناتك من الأشخاص غير المرغوب بهم.	4. في التشفير المتماثل:
<input checked="" type="radio"/> على المرسل والمستقبل معرفة المفتاح السري.	
<input type="radio"/> يُمكن لأي أحد الاطلاع على بياناتك أثناء نقلها.	



ضع علامة ✓ أمام العبارة الصحيحة وعلامة ✗ أمام العبارة الخطأ.

1.	تهدف عملية تشفير القرص الصلب إلى حماية نصف وحدة التخزين في حاسوبك. ✗
2.	يهدف تشفير البريد الإلكتروني إلى حماية المعلومات الحساسة المحتمل قراءتها من قبل أي شخص آخر غير المستلمين المعنيين. ✓
3.	يُمكن استخدام تشفير القرص الصلب مع وحدات التخزين الأخرى. ✓
4.	يمكنك استخدام تشفير البريد الإلكتروني للتأكد من أنه سيكون قابلاً للقراءة من قبل الأشخاص المعنيين فقط. ✓
5.	تشفير رسالة بريد إلكتروني في Outlook أو Outlook Web App، يعني تحويلها من نص عادي يمكن قراءته إلى تسجيل صوتي. ✗



وضح المقصود بعملية التشفير وما هي أنواعه؟

< التشفير هو وسيلة لحماية البيانات عن طريق إخفائها عن الأشخاص غير المرغوب بهم. لتحقيق هذا، يجب أن يتم تشفير البيانات بطريقة لا يمكن فكها إلا من قبل الشخص الذي يملك مفتاحًا خاصًا بفك التشفير لتلك البيانات ويعتبر مفتاح التشفير عنصراً أساسياً في فك التشفير.

< هناك نوعان رئيسيان من أنواع التشفير وهما، التشفير المتماثل والتشفير غير المتماثل.



على افتراض أنك تريد إنشاء عرض تقديمي باستخدام PowerPoint، وذلك بخصوص التغير المناخي في قطر، ومن ثم حفظه في حاسوبك.
 < أنشئ العرض التقديمي باستخدام Microsoft PowerPoint.
 < قم بحماية العرض التقديمي.
 < أرسل العرض التقديمي عبر البريد الإلكتروني إلى زملائك في الفصل.
 < اطلب من زملائك القيام بفتح العرض التقديمي.
 < ماذا تلاحظون؟

تظهر نافذة "كلمة المرور" وتتطلب منا كتابة كلمة مرور حتى نتمكن من فتح العرض التقديمي وتعديله.

< ماذا نعني بالتشفير؟

إنها عملية تحويل المعلومات أو البيانات إلى رمز، خاصة لمنع الوصول غير المصرح به.

< قم بإعطاء المفتاح السري لزملائك.

< اطلب منهم محاولة فتح ملف Microsoft PowerPoint مرة أخرى.

< ماذا تلاحظون؟

يمكننا فتح وتحرير العرض التقديمي.

< هل هناك فرق بين التشفير المتماثل والتشفير غير المتماثل؟

يستخدم التشفير المتماثل مفتاحًا واحدًا يجب مشاركته بين الأشخاص الذين يحتاجون إلى تلقي الرسالة بينما يستخدم التشفير غير المتماثل زوجًا من المفاتيح العام ومفتاحًا خاصًا لتشفير الرسائل وفك تشفيرها عند الاتصال. التشفير المتماثل تقنية قديمة بينما التشفير غير المتماثل جديد نسبيًا. تم إدخال التشفير غير المتماثل لتكملة المشكلة المتأصلة في الحاجة إلى مشاركة المفاتيح في نموذج التشفير المتماثل، مما يلغي الحاجة إلى مشاركة المفاتيح باستخدام زوج من المفاتيح العامة والخاصة. يستغرق التشفير غير المتماثل وقتًا أطول نسبيًا من التشفير المتماثل.

ما هي أهمية استخدام التشفير في حماية البيانات؟

يساعد التشفير على حماية المعلومات الخاصة والبيانات الحساسة ويمكن أن يعزز أمان الاتصال بين تطبيقات الزبون والخوادم. النقطة المهمة هي أنه عندما يتم تشفير بياناتك، حتى إذا تمكن شخص أو كيان غير مصرح له من الوصول إليها، فلن يتمكن من قراءتها.

< أغلق العرض التقديمي.

< قم بإغلاق البرنامج.

التلميحات وأفضل الممارسات

- < بالنسبة لهذا المشروع، يجب على الطلبة إنشاء ملف **Microsoft Excel** يحتوي على بيانات حول استهلاك الطاقة ومصادر الطاقة المتجددة. لهذا السبب، سيقومون بإجراء بحث على الإنترنت.
- < يمكن فصل الطلبة في مجموعات أصغر ويمكنك تعيين كل عضو من أعضاء الفريق لنوع مختلف من المهام.
- < حث الطلبة على البحث في الإنترنت عن مصادر الطاقة المتجددة.
- < اطلب من كل فريق رسم مسودة لورقة العمل وقواعد التحقق التي سيتم تطبيقها في كل عمود.
- < بعد أن يجمع الطلبة المعلومات التي يريدونها، يجب عليهم استيرادها في ملف **Microsoft Excel** واستخدام قواعد التحقق من صحة البيانات من أجل المستخدمين الآخرين للملف، لكتابة البيانات المقبولة والمسموح بها فقط.
- < أخيرًا، يجب على الطلبة إنشاء عرض تقديمي في **Microsoft PowerPoint** يتضمن حقائق من أبحاثهم. ثم يمكنهم تشفيرها وتبادلها مع زملائهم.
- < عندما يتمكنون أخيرًا من فتح ملف العرض التقديمي، يمكنهم مناقشة طرق أخرى مع زملائهم لتقليل استهلاك الطاقة وفقًا للعروض التقديمية.

تمارين إضافية للطلبة ذوي التحصيل المرتفع

< اطلب من الطلبة تجربة بعض المهارات المحددة لإكمال هذا النشاط:

- البحث باستخدام الإنترنت عن بيانات حول المصادر الرئيسة للطاقة المتجددة وكمية الطاقة التي يمكن أن توفرها لنا هذه المصادر.

- استيراد البيانات في ملف **Microsoft Excel** مع القواعد المناسبة للتحقق من صحة البيانات.

- ثم اطلب من الطلبة تضمين هذه البيانات الإضافية في **Microsoft PowerPoint**.

الكفايات الأساسية للمنهج التعليمي الوطني لدولة قطر

التعاون والمشاركة



التقصي والبحث



حل المشكلات



التفكير الإبداعي والتفكير الناقد



الكفاية اللغوية



الكفاية العددية



التواصل

