الوحدة 2 | الدرس 4

تشفير البيانات

وصف الدرس

الغرض العام من هذا الدرس هو أن يتعلم الطلبة أنواع التشفير المختلفة وكيفية تشفير وفك تشفير عرض **Microsoft PowerPoint** ورسالة بريد إلكتروني. سيتعلمون أيضًا تشفير البيانات باستخدام **Python**.

ما سيتعلمه الطالب

> التشفير، وأنواعه، وأمثلة استخدامه.

نتاجات التعلم

> كيفية تشفير البيانات.

المصطلحات

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

اللغة العربية	اللغة الإنجليزية
فك التشفير	Decryption
المفتاح الخاص	Private key
المفتاح العام	Public key

التحديات المتوقعة

> قد يجد الطلبة صعوبة في تحديد الاختلاف بين التشفير المتماثل (**symmetric**) وغير المتماثل (**asymmetric**). وضِّح للطلبة أن الاختلاف يكمن في أن التشفير المتماثل يفرض على جميع المشتركين في عملية الاتصال التبادل المسبق للمفتاح المستخدم لتشفير البيانات قبل أن يتم فك تشفيرها.

> لإرسال الأشياء بصورة خاصة باستخدام التشفير غير المتماثل - المعروف أيضًا باسم تشفير المفتاح العام – يكون هناك حاجة إلى وجود زوج من المفاتيح، فيتوافر لدى المستلم مفتاحان. فعلى سبيل المثال، يشبه المفتاح العام رقم الحساب المصرفي، ويشبه المفتاح الخاص رقم التعريف الشخصي لجهاز الصراف الآلي.

> على الطلبة معرفة أنه يمكنهم مشاركة رقم الحساب المصرفي مع أي شخص، ولكن لا ينبغي أبدًا مشاركة رقم التعريف الشخصي (**PIN**) الخاص بهم، حيث يستخدم هذا الرقم لاستخدام جهاز الصراف الآلي (**ATM**) لسحب وإيداع النقود، وكذلك لإرسال الأموال بشكل آمن إلى الآخرين في حال معرفة المستخدم لرقم حسابهم المصرفي. بعد ذلك، سيستخدم المستلمون رقم التعريف الشخصي بهم للتحقق من صحة الوصول إلى رقم حسابهم عند ذهابهم إلى ماكينة الصراف الآلي؛ كما وسيعرفون مصدر الأموال، لأن بإمكانهم مشاهدة رقم الحساب المصرفي الخاص بالمُرسل في المعاملة.

> بصورة مماثلة، عند التوقيع على أي نوع من المعلومات باستخدام المفتاح الخاص ثم تشفيره بالمفتاح العام الخاص بالمستلم، يتم التحقق من ثلاثة أشياء: اولًا يتم التأكد من أن المستلم المقصود فقط هو من سيكون قادرًا على قراءة المعلومات عن طريق فك تشفيرها بمفتاحه الخاص، وسيحصل المستلم على ضمان أن الرسالة تم إرسالها،

وسيكون المرسل والمستلم على يقين بأن الرسالة لم يتم تعديلها من قبل أي شخص آخر.

> قد يحتاج الطلبة إلى مساعدة لإدراك مفاهيم بالتشفير. اشرح لهم أننا نستخدم التشفير للحفاظ على سرية بياناتنا كي لا يتمكن الآخرون غير المصرح لهم من الوصول إليها، حيث يقتصر الوصول إلى تلك البيانات على من يمتلكون مفتاح فك التشفير. يساعد تشفير بيانات الاتصالات من طرف لطرف أيضًا على ضمان تكامل البيانات - بحيث لا يتم العبث بالبيانات أثناء انتقالها بين الأطراف المختلفة.

التمهيد

> استخدم استراتيجية الحوار والمناقشة حول طرق جمع البيانات وطرق التحقق من صحة البيانات.

> قم بطرح بعض الأسئلة على الطلبة مثل:

- عرِّف المصطلحات التالية: التشفير وفك التشفير، والمفاتيح العامة والخاصة؟
- هل يمكنكم التفكير في استخدامات التشفير؟
- ما هو المقصود بالتشفير وفك التشفير؟
- ما هو الفرق بين المفتاح العام والمفتاح الخاص؟

> قم بطرح إحدى المشكلات حول موضوع التشفير وأدر النقاش مع الطلبة حول آرائهم بخصوص الحاجة للتشفير وأهمية تشفير البيانات لحمايتها من الأشخاص غير المصرح لهم بالوصول إليها.

> قم بالإشارة إلى أن التشفير ليس أمرًا حديثًا، بل أنه وُجد منذ العصور القديمة، ويُقال أن يوليوس قيصر استخدم نوعًا من التشفير لحماية رسائله.

التلميحات الخاصة بالتنفيذ

> تم استخدام الكتابة السرية منذ ظهور عملية الكتابة، فقد تم استخدام الرموز عبر التاريخ للحفاظ على سرية الرسائل. تم استخدام علم التشفير لفترة طويلة من قبل الحكومات والجيوش والشركات والمؤسسات لحماية رسائلهم. يُستخدم التشفير في يومنا هذا لحماية البيانات المخزنة والمعاملات بين أجهزة الحاسوب.

> عندما كانت الرسائل تُحمل سيرًا على الأقدام لمسافاتٍ طويلة في العصور القديمة، كان الملوك والحكام يشفرون الرسائل التي يرسلونها إلى حلفائهم للحفاظ على سرية الرسائل

في حال تم الاستيلاء عليها. يذكر التاريخ الأمريكي الحديث أن جورج واشنطن استخدم الرسائل المشفرة في مخاطباته مع جنوده، وكذلك قام أعضاء الكونغرس أيضًا بتشفير وثائقهم. تم استخدام "شيفرة مورس" لإرسال رسائل يمكن ترجمتها من خلال الأنماط الصوتية عندما تم اختراع التلغراف.

> يقوم مستخدمو الحاسوب بتشفير المستندات واتصالات الشبكات ورسائل البريد الإلكتروني كطريقة للحفاظ على سرية بياناتهم. تعدُّ أنواع التشفير الجديدة متطورة للغاية وقد تكون معقدة أحيانًا، ولكنها ما زالت تعتمد على ذات المبدأ الذي تم استخدامه قديمًا.

> ساعد الطلبة على فهم أن استخدام كلمة المرور في **Microsoft PowerPoint** يساعد في منع الأشخاص غير المصرح لهم من فتح العرض تقديمي أو تعديله. يجب تسجيل كلمة المرور تلك والاحتفاظ بها في مكان آمن، حيث إن فقدان كلمة المرور يعني عدم التمكن من فتح العرض التقديمي أو الوصول إليه. تجدر الإشارة إلى أن **PowerPoint** لا تدعم تلك الحماية للملفات بصيغة **ODP**.

> يمكن للمستخدم إزالة كلمة المرور لملف بشرط معرفة كلمة المرور الأصلية. يمكن لمستخدم فتح ملف محمي بكلمة مرور يعمل عليه شخص آخر حاليًا في وضع القراءة فقط.

> استخدم الأسئلة الشفوية كاستراتيجية تعليمية لاستكشاف الأفكار والافتراضات غير الصحيحة.

> اطرح بعض الأسئلة على الطلبة على سبيل المثال:

- هل يتاح التشفير فقط في مصنفات **Microsoft Excel**؟
- ما هي التطبيقات الأخرى التي يمكن تشفير بياناتها؟

> استمر بالشرح بتوضيح آلية عمل شيفرة القيصر لتشفير البيانات واعرض التعليمات البرمجية بلغة **Python** التي تنفذ هذا النوع من التشفير.

> في النهاية قم بعرض برنامج **Python** يستخدم مفتاحًا مُدخلًا لتشفير البيانات. امنح الطلبة الوقت الكافي لتجريب البرنامج بإدخال بيانات مختلفة وباستخدام مفتاح مختلف كل مرة.

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 وما هي أنواعه؟
- كيف يمكن حماية وتشفير عرض تقديمي أو بريد إلكتروني؟
- كيف يمكن استخدام **Python** في تشفير البيانات؟

> ذكّر الطلبة بالمصطلحات الهامة وكرّرها معهم.

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

التدريبات المقترحة لغلق الدرس

يمكنك استخدام التمرين الرابع ضمن استراتيجية غلق الدرس لتقييم وتعزيز قدرة الطلاب على تطبيق المهارات المقدمة في هذا الدرس.

الصف الحادي عشر | الفصل الأول | كتاب الطالب | صفحة 233

الفروق الفردية

تمارين إضافية للطلبة ذوي التحصيل المرتفع

> بعد الانتهاء من التمرين الرابع لهذا الدرس ، اطلب من الطلاب إنشاء عرض تقديمي يتضمن بعض الاقتراحات للتخفيف من تغير المناخ ، مثل إعادة تشجير الغابات الاستوائية. يجب على الطلاب تشفير العرض التقديمي قبل إرساله إلى زملائهم في الفصل ، حيث سيحاول المستلمون فتح هذا العرض التقديمي. اطلب من المرسلين تحرير كلمة المرور وإخبار المستلمين بها ، حيث يجب عليهم محاولة فتح العرض التقديمي مرة أخرى والاطلاع على المقترحات الخاصة بالتخفيف من تغير المناخ.

4 التعامل مع التشفير:

على افتراض أنك تريد إنشاء عرض تقديمي باستخدام Microsoft PowerPoint، وذلك بخصوص التغير المناخي في قطر، ومن ثمّ 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 نعني 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.

233

الإجابات النموذجية للتدريبات:

1 اختر الإجابة الصحيحة:

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

2 تحقق من الجمل التالية هل هي صحيحة أم خطأ.

.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 قِبل 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 قابلًا للقراءة من قِبل الأشخاص المعنيين فقط.	✓
.5	تشفير رسالة بريد إلكتروني في Outlook أو Outlook Web App، يعني تحويلها من نص عادي يمكن قراءته إلى تسجيل صوتي.	✗

3 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 قِبل الشخص الذي يملك مفتاحًا خاصًا بفك التشفير لتلك البيانات ويعتبر مفتاح التشفير عنصرًا أساسيا في فك التشفير.

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

4 التعامل مع التشفير:

على افتراض أنك تريد إنشاء عرض تقديمي باستخدام PowerPoint، وذلك بخصوص التغير المناخي في قطر، ومن ثمَ 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؟

ستظهر نافذة Password (كلمة المرور)، حيث سنقوم بإدخال كتابة كلمة المرور لنتمكن من فتح العرض التقديمي وتعديله.

> ماذا نعني بالتشفير؟

هي عملية تحويل المعلومات أو البيانات إلى رموز غير مفهومة لمنع الوصول غير المصرح به.

> قم بإعطاء المفتاح السري لزملائك.

> اطلب منهم محاولة فتح ملف Microsoft PowerPoint مرة أخرى.

> ماذا تلاحظون؟

يمكننا فتح وتعديل العرض التقديمي.

> هل هناك فرق بين التشفير المتماثل والتشفير غير المتماثل؟

يستخدم التشفير المتماثل مفتاحًا واحدًا يجب مشاركته بين الأشخاص الذين سيتلقون الرسالة، بينما يستخدم التشفير غير المتماثل زوجًا من المفاتيح، مفتاحًا عامًا وآخر خاصًا لتشفير الرسائل وفك تشفيرها عند الاتصال.

إن التشفير المتماثل هو تقنية قديمة على عكس التشفير غير المتماثل، والذي يُعدُّ تقنية حديثة نسبيًا. تم تقديم التشفير غير المتماثل لتجاوز المشكلة المتمثلة في الحاجة إلى مشاركة المفتاح في نموذج التشفير المتماثل، مما يلغي الحاجة إلى مشاركة المفتاح 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 في حماية المعلومات الخاصة والبيانات الحساسة، كما أنه يعزز أمان الاتصالات بين تطبيقات العملاء والخوادم. فعندما يتم تشفير بياناتك، لن يتمكن أي شخص أو كيان غير مصرح بقراءة البيانات حتى إن تسنى لهم الوصول إلى تلك البيانات.

> أغلق العرض التقديمي.
> قم بإغلاق البرنامج.

5

لقد تم تشفير الكلمة التالية باستخدام شفرة القيصر، إذا علمت أن مقدار الإزاحة هو خمسة أحرف إلى الخلف. حاول فك التشفير والتعرف على الكلمة الصحيحة.

M	F	U	U	D
↓	↓	↓	↓	↓
H	A	P	P	Y

6

استخدم شفرة القيصر لتشفير اسمك.

> قم بعمل التشفير على ورقة.

> تحقق من النتيجة باستخدام Python.

تلميح:

هذه الخوارزمية، يتم استبدال كل حرف داخل النص بحرف آخر وفق ترتيب عددي ثابت. استعن بصفحة 223 من الكتاب.

استخدم برنامج Python في صفحة 224 للتحقق من النتائج.