تهديدات وإجراءات مواجهة أمن المعلومات ①

النقاط الرئيسية

أ. أمن المعلومات

(1) **أمن المعلومات** (Information security) : هو عملية إدارة المعلومات بشكل صحيح والحفاظ عليها آمنة.

(2) العناصر الأساسية الثلاثة لأمن المعلومات هي:

[1] **السرية** (Confidentiality) : هي الحالة التي يمكن فيها فقط للأفراد المصرّح لهم الوصول إلى المعلومات.

[2] **السلامة** (Integrity) : هي الحالة التي لم يتم فيها تدمير المعلومات أو العبث بها أو محوها.

[3] **التوافرية** (Availability) : هي الحالة التي يمكن فيها الوصول إلى المعلومات في أي وقت عند الحاجة.

ب. تهديدات متنوعة لأمن المعلومات

(1) **الوصول غير المصرّح به** (Unauthorized access) : هو الوصول إلى نظام بشكل غير قانوني للتلاعب بالبيانات أو محوها أو سرقتها.

(2) **الاختراق** (Cracking) : هو الوصول إلى نظام بشكل غير قانوني للتلاعب بالبيانات أو محوها أو سرقتها.
ويُطلق على الشخص الذي يرتكب هذه الأفعال اسم المخترق (**cracker**).

(3) **البرمجيات الخبيثة** (Malware) : مصطلح عام للبرامج الضارة المصممة لإلحاق الضرر بأجهزة الكمبيوتر.
يمكن أن تحدث الإصابة عبر مواقع الويب، أو مرفقات البريد الإلكتروني، أو محركات أقراص USB، أو الشبكات.

[1] **فيروس الكمبيوتر** (Computer virus) : برنامج مصمم لإحداث ضرر بشكل مُتعمد، مثل تدمير البيانات أو البرامج.

[2] **حصان طروادة** (Trojan horse) : برنامج متنكر على أنه برنامج شرعي، يتسلل إلى النظام ويبدأ الهجمات بهدوء.

[3] **الدودة** (Worm) : برنامج ينسخ نفسه وينتشر عبر الإنترنت مثل الدودة، مما يؤدي إلى توسيع نطاق الإصابة.

[4] **برنامج التجسس** (Spyware) : برنامج يجمع المعلومات الشخصية دون علم المستخدم ويرسلها إلى أطراف ثالثة.

- **مسجل لوحة المفاتيح** (Keylogger) : برنامج يراقب ويسجل ضغطات المفاتيح.
- **برنامج الإعلانات** (Adware) : برنامج يعرض إعلانات غير مرغوب فيها دون موافقة المستخدم.

[5] **برنامج الفدية** (Ransomware) : برنامج يجعل البيانات غير قابلة للوصول ويطالب بفدية لاستعادة الوصول للبيانات.

(4) **الجريمة الإلكترونية** (Cybercrime) : أفعال إجرامية تُرتكب عبر شبكات الكمبيوتر.

[1] انتهاك قانون الوصول غير المصرّح به للكمبيوتر : الوصول غير القانوني إلى كمبيوتر باستخدام هوية مستخدم أو كلمة مرور الخاصة بشخص آخر.

[2] جرائم تتضمن الكمبيوتر أو السجلات الإلكترونية: جرائم تتضمن العبث بالبيانات المخزنة أو التلاعب غير المصرّح به بالأجهزة.

[3] جرائم قائمة على الشبكة: جرائم تُرتكب باستخدام الشبكات، مثل الاحتيال أو التشهير أو انتهاك حقوق المؤلف.

تحدى معلوماتك

أجب عن الأسئلة التالية.

(1) من بين الخيارات من أ إلى ت ، اختر الخيار الذي تكون فيه التوافرية (Availability) معرضة للخطر من حيث أمن المعلومات.

(أ) تسبب هجوم إلكتروني في تعطيل موقع ويب.

(ب) تم إدخال بيانات غير صحيحة بسبب خطأ في الكتابة.

(ت) تم تسريب معلومات شخصية بسبب إصابة ببرنامج خبيث على الكمبيوتر.

(2) من الخيارات أ إلى **ث** أدناه، اختر جميع الإجراءات التي تشكل انتهاكًا لقانون الوصول غير المصرح به إلى الكمبيوتر.

(أ) استخدام هوية مستخدم وكلمة مرور شخص آخر بشكل غير قانوني للوصول إلى كمبيوتر.

(ب) تخزين كلمة مرور تم الحصول عليها بشكل غير قانوني على كمبيوتر.

(ت) مشاركة هوية مستخدم وكلمة مرور صديق مع شخص آخر دون إذن الصديق.

(ث) نشر موقع ويب يبيع أدوية شبه قانونية أو يحتوي على محتوى غير قانوني وغير لائق.

الشرح

(1) يتكون أمن المعلومات من ثلاثة عناصر: السلامة والسرية والتوافر.

1. عندما تصبح المعلومات غير متوفرة، يتعرض التوافر للخطر.
2. عندما لم تعد المعلومات دقيقة، تتعرض السلامة للخطر.
3. عندما يتمكن أفراد غير مصرح لهم من عرض المعلومات، تتعرض السلامة للخطر.

لذلك، الإجابة الصحيحة هي أ.

(2)

1. استخدام جهاز كمبيوتر دون الحصول على حقوق وصول يشكل وصولاً غير مصرح به وهو محظور بموجب قانون الوصول غير المصرح به إلى الكمبيوتر.
2. تخزين كلمة مرور تم الحصول عليها بشكل غير قانوني لغرض الوصول غير المصرح به محظور بموجب قانون الوصول غير المصرح به إلى الكمبيوتر.
3. مشاركة كلمة مرور شخص آخر مع طرف ثالث دون سبب وجيه أو إذن يروج للوصول غير المصرح به وهو محظور أيضًا بموجب القانون.
4. قد يندرج نشر المحتوى غير القانوني تحت فئة الجرائم المتعلقة بالشبكة.

لذلك، الإجابات الصحيحة هي أ, **ب**, **ت**.

جرب بنفسك

1 هناك ثلاثة عناصر لأمن المعلومات: السلامة (Integrity)، والسرية (Confidentiality)، والتوفر (Availability). لكل من هذه العناصر، اختر الإجراء الأنسب من الخيارات التالية 1 إلى 3.

1. السرية 2. السلامة 3.التوفر

1. أبلغ مسؤول الشبكة بوصولك إلى العمل.
2. تعامل مع البيانات الخاصة مثل أرقام الهوية الشخصية في غرفة يُسمح بدخولها فقط للموظفين المصرح لهم.

3. احتفظ بسجلات الوصول إلى البيانات والتعديلات التي تتم عليها لتمكين إمكانية التتبع.
4. قم بتركيب إمدادات طاقة احتياطية لجميع الأجهزة المتعلقة بأنظمة المعلومات الحيوية استعدادًا لانقطاع التيار الكهربائي.
5. قم بتشغيل برامج ضارة لتتمكن دائمًا من الوصول إلى المعلومات الهامة.

2 عندما يستخدم طرف ثالث ليس لديه حقوق وصول إلى الشبكة هوية (ID) وكلمة مرور شخص آخر للدخول بشكل غير قانوني إلى نظام كمبيوتر، يسمى ذلك [(1) .....]. وقعت حوادث قام فيها أفراد يُعرفون بالمتسللين (hackers) أو [(2) .....] بتدمير الأنظمة
البرامج التي تدمر البيانات الداخلية للكمبيوتر أو تسبب عمليات غير طبيعية تسمى [(3) .....]. ومن بين هذه البرامج يوجد [(4) .....] ، التي تتنكر كبرامج شرعية وتتسرب بصمت إلى الأنظمة لتنفيذ الهجمات، و [(5) .....] ، التي تنسخ نفسها وتنتشر عبر الإنترنت مثل الديدان لزيادة الإصابات.

اختر المصطلحات الصحيحة من الخيارات التالية من أ إلى د لملء الفراغات من [1] إلى [5] في النص التالي، اختر الحروف المناسبة التالية للإجابة المقابلة.

(أ) دودة	**(ب)** مخترق	**(ت)** الوصول غير المصرح به
(ث) حصان طروادة	**(ج)** فيروس الكمبيوتر	**(ح)** برامج الإعلانات المتسللة
(خ) مسجل لوحة المفاتيح	**(د)** انتحال شخصية	

3 **أجب عن الأسئلة التالية.**

(1) اختر جميع العناصر من 1 إلى 4 التالية والتي تمثل خطرًا من الإصابة بفيروسات الكمبيوتر:

1. مرفق بريد إلكتروني مُرسل من جهاز كمبيوتر مصاب بفيروس.
2. الاتصال بشبكة مصابة بفيروس.
3. ذاكرة فلاش (USB) تم استخدامها على جهاز كمبيوتر مصاب بفيروس.
4. قرص DVD لفيلم تم تشغيله على جهاز كمبيوتر مصاب بفيروس.

(2) جملة أو فعلًا واحدًا من 1 إلى 4 من التالي ويشكل انتهاكًا لقانون الوصول غير المصرح به للكمبيوتر:

1. تقديم معلومات شخصية لطرف ثالث دون موافقة الفرد.
2. التقاط صورة لصفحة مجلة بهاتف ذكي وتحميلها على وسائل التواصل الاجتماعي.
3. الحصول على فيروس كمبيوتر قادر على التسلل التلقائي إلى الشبكات.
4. استخدام هوية مستخدم (ID) وكلمة مرور شخص آخر دون إذن لشراء منتجات عبر التسوق عبر الإنترنت.

تمرين

1 **أجب على الأسئلة التالية.**

(1) لكل عنصر من عناصر أمن المعلومات الثلاثة، حدد:

- الوصف الأنسب من <مجموعة أ> من (1 - 3) لكل عنصر.
- الأضرار المحتملة القابلة للتطبيق من <مجموعة ب> من (أ - ح) التي قد تحدث إذا لم يتم تأمين هذا العنصر

1. السرية 2. التكامل 3. التوفر

<مجموعة أ>

1. ضمان الوصول غير المنقطع إلى المعلومات عند الحاجة.
2. ضمان أن الأفراد المصرح لهم فقط يمكنهم الوصول إلى المعلومات.
3. ضمان أن المعلومات لم يتم تدميرها، أو التلاعب بها، أو حذفها.

<مجموعة ب>

(أ) التنصت على الشبكة

(ب) انقطاع الخدمة مثل توقف النظام

(ت) تسرب كلمة المرور

(ث) التلاعب بالمعلومات أو تدميرها

(ج) تسرب المعلومات

(ح) الاستخدام غير المصرح به لأجهزة الكمبيوتر أو الشبكات

2 أجب عن الأسئلة التالية.

(1) اختر المصطلح الصحيح من الخيارات أ إلى خ لملء كل فراغ . أجب باستخدام الحرف المقابل.

[1] الفيروس الذي يعرض إعلانات لم يقصد المستخدم رؤيتها يسمى. ( ).

[2] فعل التسلل غير القانوني إلى جهاز كمبيوتر للتلاعب بالبيانات أو محوها أو سرقتها يسمى . ( ).

[3] البرنامج الذي يسرب البيانات المخزنة على جهاز الكمبيوتر إلى الخارج يسمى. ( ).

[4] البرامج الضارة التي تشمل فيروسات الكمبيوتر وحصان طروادة يشار إليها مجتمعة باسم. ( ).

الخيارات: **(أ)** برامج ضارة **(ب)** مسجل لوحة المفاتيح **(ت)** برامج الإعلانات

(ث) قرصنة (Cracking) **(ج)** اختراق (Hacking) **(ح)** تصيد (Phishing)

(خ) برامج تجسس (Spyware)

(2) اختر عبارة واحدة صحيحة من 1 إلى 4 الخاصة بإصابة الفيروسات الكمبيوتر.

1. طالما أن الكمبيوتر متصل بالشبكة، فهناك دائمًا خطر الإصابة بفيروس كمبيوتر.
2. إذا لم تتصل بجهاز كمبيوتر أو شبكة وقمت فقط بنقل البيانات باستخدام ذاكرة فلاش (USB)، فلن تحدث الإصابة.
3. إذا تجنبت الدخول إلى المواقع الضارة أو غير القانونية، فلن تصاب بالفيروس.
4. طالما أنك لا تفتح رسائل البريد الإلكتروني، فأنت في أمان من الإصابة، لذا فإن توخي الحذر مع رسائل البريد الإلكتروني يكفي.

التهديدات والتدابير المضادة في أمن المعلومات ②

النقاط الرئيسية

أ. كلمات المرور والمصادقة

(1) **كلمة المرور** (**Password**): سلسلة من الأحرف تُستخدم للتحقق من هوية المستخدم وانه هو صاحب الحساب الشرعي.

(2) إرشادات لإنشاء كلمات المرور:

- استخدم سلسلة أحرف (**طويلة**) قدر الإمكان.
- (**اجمع**) بين الأحرف الكبيرة والصغيرة والأرقام والرموز.
- لا تستخدم معلومات شخصية مثل تاريخ ميلادك أو عنوان بريدك الإلكتروني أو معرف المستخدم.
- لا تُعد استخدام كلمات المرور المستخدمة في خدمات أخرى.

(3) **كلمة المرور لمرة واحدة** (**One-time-password**) : كلمة مرور تتغير على فترات منتظمة ولا يمكن استخدامها إلا مرة واحدة.

(4) **المصادقة** (**Authentication**) : عملية التحقق من هوية المستخدم على كمبيوتر أو شبكة.

(5) أنواع المصادقة:

الاسم	الطريقة	أمثلة
أ. **المصادقة القائمة على المعرفة** (**Knowledge-based authentication**)	المصادقة باستخدام معلومات يعرفها الفرد فقط.	معرف المستخدم وكلمة المرور، رمز PIN
ب. **المصادقة البيومترية** (**Biometric authentication (Biometrics)**)	المصادقة باستخدام الخصائص الفيزيائية أو السلوكية للفرد.	بصمة الإصبع، القزحية، نمط الوريد، الخط اليد
ت. **المصادقة القائمة على الحيازة** (**Possession-based authentication**)	المصادقة باستخدام عنصر يمتلكه الفرد.	بطاقة ذكية، كلمة مرور لمرة واحدة، التحقق من الرسائل النصية القصيرة
ث. **المصادقة الثنائية باستخدام عاملين مختلفين** (**Two-factor authentication**)	طريقة تجمع بين نوعين مختلفين من العوامل مثل التحقق بالمعرفة والحيازة	مثل رقم PIN ورمز عبر SMS
ج. **المصادقة متعددة الخطوات** (**Two - step authentication**)	طريقة تقوم بالمصادقة على خطوتين باستخدام معلومتين من نفس نوع العامل	كلمة المرور + سؤال سري

ب. إجراءات أمن المعلومات

(1) **التحكم في الوصول** (**Access control**) : طريقة للحد من الوصول إلى أنظمة الكمبيوتر أو البيانات بحيث يُسمح فقط لمستخدمين محددين، ويتم التحقق منهم من خلال استخدام المصادقة.

(2) **جدار الحماية** (**Firewall**) : نظام مُثبت عند نقاط دخول الشبكة لمنع (**الوصول غير المصرح به**) من الخارج ولمنع (**تسرّب البيانات**) من الداخل.

(3) إجراءات مواجهة فيروسات الكمبيوتر:

- قم بتثبيت (**برنامج مكافحة الفيروسات**) لإزالة الفيروسات أو عزلها، واحرص على تحديث تعريفات الفيروسات داخل البرنامج.
- احتفظ دائمًا بنظام التشغيل (OS) وبرنامج التطبيق (**محدثًا لمنع الثغرات الأمنية**) في البرنامج.
- أنشئ (**نسخًا احتياطية**) لبياناتك بانتظام.

تحدى معلوماتك

أجب عن الأسئلة التالية.

(1) من الخيارات من أ إلى ث ، اختر العبارة غير الصحيحة بخصوص أفضل الممارسات لكلمة المرور. أجب بتحديد الحرف المقابل.

(أ) لا تُعد استخدام نفس كلمة المرور عبر خدمات متعددة.

(ب) من الأفضل الاستمرار في استخدام كلمة المرور الافتراضية التي تم تعيينها في البداية.

(ت) اجمع بين الأحرف والأرقام والرموز عند إنشاء كلمة مرور.

(ث) تجنب استخدام معلومات يمكن تخمينها بسهولة مثل اسمك أو تاريخ ميلادك.

(2) من الخيارات من أ إلى ث ، اختر جميع العبارات الصحيحة حول كلمات المرور لمرة واحدة.

(أ) إذا تم تسريب كلمة مرور لمرة واحدة، فقد يؤدي ذلك بسهولة إلى وصول غير مصرّح به.

(ب) استخدام كلمة مرور لمرة واحدة يقوّي الأمان بشكل عام.

(ت) كلمة المرور لمرة واحدة لها وقت استخدام محدود وتصبح غير صالحة بعد انتهاء الصلاحية.

(ث) يمكنها منع الوصول غير المصرّح به باستخدام كلمات مرور مسرّبة.

(3) من الخيارات من أ إلى ث ، اختر المثال الصحيح للمصادقة البيومترية.

(أ) المصادقة باستخدام هوية مستخدم وكلمة مرور مُخصصة لكل فرد.

(ب) المصادقة باستخدام رسالة SMS مُرسلة إلى هاتف ذكي.

(ت) المصادقة عن طريق مسح بصمة الإصبع على جهاز الاستشعار.

(ث) المصادقة باستخدام كلمة مرور لمرة واحدة.

(4) إذا كان يمكن في كلمة المرور استخدام الأرقام من 0 إلى 9 والأحرف الصغيرة من a إلى z، فكم عدد التركيبات المختلفة لكلمة مرور مكونة من 3 أحرف؟ أعط إجابتك في صورة رقمية.

الحل

(1) إذا تم تعيين كلمة مرور أولية عبر البريد الإلكتروني أو مذكرة، فهناك احتمال أن تكون كلمة المرور قد تسربت إلى طرف ثالث. لذلك، يجب تغيير كلمة المرور الأولية. الإجابة الصحيحة هي **ب**.

(2) كلمة المرور لمرة واحدة هي كلمة مرور تتغير على فترات زمنية ثابتة ولا يمكن استخدامها إلا مرة واحدة. هذا يعزز الأمان. الإجابات الصحيحة هي **ب – ت – ث**.

(3) المصادقة البيومترية تشير إلى استخدام الخصائص الجسدية أو السلوكية للفرد للتحقق. تشمل الأمثلة المصادقة بالبصمة أو قزحية العين أو الوريد أو خط اليد. الإجابة الصحيحة هي **ت**.

ملاحظة: (أ) هي مصادقة قائمة على المعرفة، (ب) هي مصادقة قائمة على الامتلاك، و ث هي أيضًا مصادقة قائمة على الامتلاك.

(4) يوجد 10 أرقام (0-9) و 26 حرفًا (a-z)، مما يجعل المجموع 36 حرفًا محتملاً. نظرًا لأن كل حرف في كلمة المرور يمكن أن يكون أيًا من الـ 36، فإن فإن إجمالي عدد التركيبات لكلمة مرور مكونة من 3 أحرف هو $36^3=36\times36\times36$ مجموعة.

جرب بنفسك

(1) من الخيارات 1 إلى 4 ، اختر العبارة غير الصحيحة فيما يتعلق بأفضل ممارسات كلمة المرور. أجب باستخدام الرقم المقابل.

1. لا تستخدم معلومات مثل أرقام الهواتف أو أعياد الميلاد أو عناوين البريد الإلكتروني أو معرفات المستخدم (user IDs).

2. من الأفضل الاستمرار في استخدام كلمة المرور الأولية دون تغييرها.

3. لا تعيد استخدام نفس كلمة المرور عبر الخدمات المختلفة.

4. استخدم مزيجًا من الأحرف الكبيرة والصغيرة والأرقام والرموز.

(2) من الخيارات 1 إلى 4 ، اختر الشيء الذي يمكن منعه باستخدام كلمة مرور لمرة واحدة (one-time password). أجب باستخدام الرقم المقابل.

1. سرقة كلمة المرور أثناء الإرسال عبر الشبكة.

2. التلاعب بالملفات السرية بعد الوصول غير المصرح به.

3. الإصابة بفيروس من خلال البرامج الضارة.

4. الوصول غير المصرح به باستخدام كلمة مرور مسربة.

(3) من الخيارات 1 إلى 4 ، اختر المثال الصحيح للمصادقة البيومترية. أجب باستخدام الرقم المقابل.

1. المصادقة باستخدام شكل بصمة الإصبع أو نمط الوريد.

2. المصادقة باستخدام شهادة رقمية.

3. المصادقة بناءً على ما إذا كان المستخدم يمكنه قراءة نص مشوه في صورة بشكل صحيح.

4. المصادقة باستخدام كلمة مرور لمرة واحدة.

(4) اختر الكلمات الصحيحة لملء الفراغات من [1] إلى [4] في الجملة من الخيارات أ إلى ح

لحماية أجهزة الكمبيوتر والشبكات من التهديدات مثل الوصول غير المصرح به وفيروسات الكمبيوتر، من الضروري تنفيذ تدابير أمنية متنوعة. على سبيل المثال، تحديد ما إذا كان الشخص مصرحًا له بالوصول إلى جهاز كمبيوتر أو شبكة يسمى [(1) .....] . كإجراءات مضادة لفيروسات الكمبيوتر، هناك إدخال [(2) .....] و [(3) .....] للأجهزة وأنظمة التشغيل. علاوة على ذلك، يسمى النظام الذي يخفي أجهزة الكمبيوتر الموجودة في الشبكة المحلية (LAN) الداخلية عن الشبكات الخارجية ويمنع الوصول غير المصرح به بـ [(4) .....].

(أ) جدار الحماية (Firewall)

(ب) برنامج مضاد للفيروسات (Antivirus software)

(ت) تشفير (Encryption)

(ث) مصادقة (Authentication)

(ج) تحديث (Update)

(ح) ثغرة أمنية (Security hole)

(5) ما هو المصطلح الذي يطلق على تقييد الوصول بحيث لا يمكن إلا لمستخدمين محددين تشغيل نظام كمبيوتر أو شبكة؟

(6) إذا كانت كلمة المرور تستخدم 26 حرفًا (من A إلى Z)، فكم مرة يزيد الحد الأقصى لعدد محاولات القوة الغاشمة (brute-force) المطلوبة لكسر كلمة المرور عند زيادة الطول من 4 أحرف إلى 6 أحرف؟

تمرين

1 **أجب عن الأسئلة التالية.**

(1) من الخيارات 1 إلى 4 ، اختر العبارة غير الصحيحة فيما يتعلق بإنشاء كلمة المرور. أجب بالحرف المقابل.

1. استخدم أقصر سلسلة ممكنة لتكون سهلة التذكر.
2. لا تعيد استخدام كلمات المرور المستخدمة في خدمات أخرى.
3. لا تدون كلمات المرور في دفتر ملاحظات أو على أوراق لاصقة.
4. اجمع بين الأحرف الكبيرة والصغيرة والأرقام والرموز.

(2) من الخيارات 1 إلى 4 ، اختر التهديد الذي يمكن منعه باستخدام كلمة مرور لمرة واحدة. أجب بالحرف المقابل.

1. سرقة هوية المستخدم (user ID) عبر الهندسة الاجتماعية.
2. الوصول غير المصرح به من خلال هجمات القوة الغاشمة (brute-force attacks).
3. الوصول غير المصرح به باستخدام كلمة مرور مسربة.
4. الإصابة بالفيروس من خلال ثغرة أمنية.

(3) من الخيارات 1 إلى 4 ، اختر المثال الصحيح للمصادقة البيومترية. أجب بالحرف المقابل.

1. المصادقة باستخدام هوية شخصية أو كلمة مرور.
2. المصادقة باستخدام الخصائص الفيزيائية مثل بصمات الأصابع أو قزحية العين.
3. المصادقة بناءً على قدرة الفرد على حل المشكلات.
4. المصادقة باستخدام الأداء البدني مثل قوة القبضة أو المرونة.

(4) املأ الفراغات من [1] إلى [5] في الجملة التالية باستخدام المصطلحات المناسبة من الخيارات أ إلى ح.

يجب على مديري الأنظمة تنفيذ تدابير مثل تثبيت [(1) .....] لمنع الوصول غير المصرح به من خارج النظام وتقليل التلاعب بالبيانات أو تسربها قدر الإمكان. من أجل التعامل مع الظهور المستمر لـ [(2) .....] جديدة، من الضروري إدخال [(3) .....] وتصحيح [(4) .....] . لمنع الوصول غير المصرح به، يعد [(5) .....] مفيدًا لتقييد استخدام النظام أو الشبكة على مستخدمين محددين فقط.

(أ) جدار الحماية (Firewall)
(ب) برنامج مضاد للفيروسات (Antivirus software)
(ت) الأمان (Security)
(ث) التحكم في الوصول (Access control)
(ج) فيروس الكمبيوتر (Computer virus)
(ح) ثغرة أمنية (Security hole)

(5) ما اسم طريقة المصادقة التي تجمع بين عنصرين مختلفين من "المعرفة"، "البيومترية"، و "الحيازة"؟

(6) إذا كان يمكن استخدام الأرقام من 0 إلى 9 والحروف الصغيرة من a إلى z في كلمة المرور، فكم عدد التركيبات الممكنة لكلمة مرور مكونة من ٤ أحرف؟ اكتب إجابتك في صورة a^n.

التهديدات والتدابير المضادة فى أمن المعلومات ③

النقاط الرئيسية

أ. الاحتيال بالفواتير

(1) **فاتورة احتيالية** (**Fraudulent billing**): احتيال يتم فيها إصدار فاتورة لشخص ما مقابل خدمة وهمية لم يستخدمها أبدًا، بهدف الحصول على المال بشكل احتيالي.

(2) **الاحتيال بنقرة واحدة** (**One-click fraud**): احتيال يؤدي فيه النقر على رابط (URL) في موقع ويب أو بريد إلكتروني تلقائيًا إلى رسالة تدّعي أنه تم إبرام عقد، يليها طلب دفع مبالغ فيه.

ب. الحصول غير المصرح به على المعلومات

(1) **التصيّد** (**Phishing**) : احتيال يستخدم مواقع ويب مزيفة متنكرة على أنها مؤسسات مالية أو هيئات عامة لسرقة المعلومات الشخصية مثل رموز PIN أو تفاصيل الحساب.

(2) **الهندسة الاجتماعية** (**Social engineering**) : طريقة للحصول على المعلومات بشكل احتيالي عن طريق استغلال علم النفس البشري أو الإهمال قلة الوعي.

[1] **انتحال الشخصية** (**Impersonation**) : هو التظاهر بأنك شخص آخر - مثل إجراء مكالمة هاتفية باسم الشخص الآخر - للحصول على معلومات.

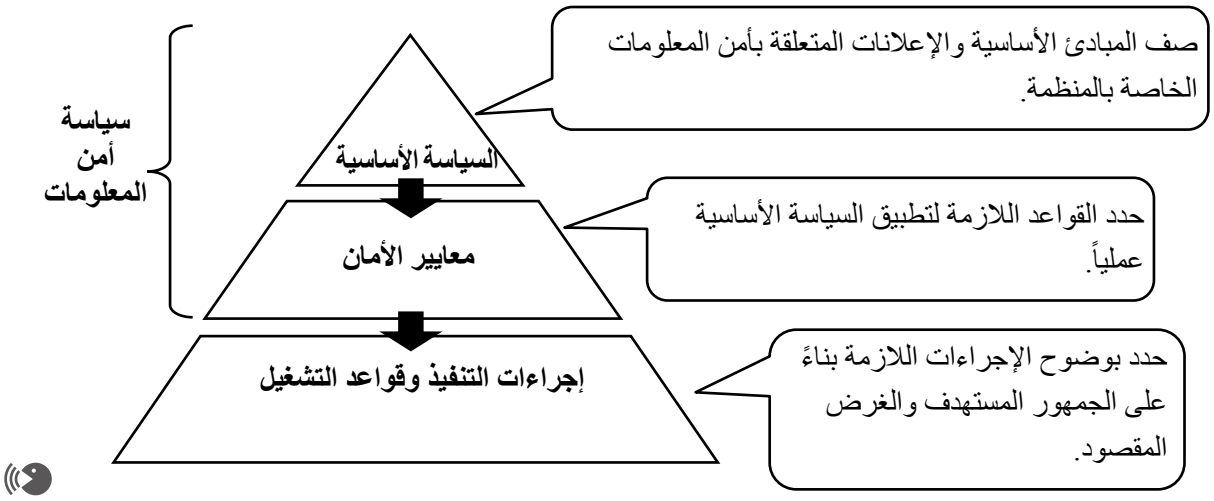
[2] **التجسس المباشر** (**Shoulder surfing**) : التلصص على الشاشة أو لوحة مفاتيح شخص لسرقة كلمات المرور أو رموز PIN.

[3] **البحث فى المهملات** (**Dumper diving**) : البحث في المهملات للحصول على معلومات سرية تم التخلص منها.

(3) **التزوير** (**Skimming**) : هو استخراج البيانات بشكل غير قانوني من بطاقة ائتمان أو خصم خاصة بشخص ما واستخدام البيانات لإنشاء بطاقة مزورة.

ت. سياسة أمن المعلومات

سياسة أمن المعلومات (**Information Security Policy**) : مجموعة من القواعد والإرشادات الأساسية التي تضعها شركة أو منظمة للحفاظ على أمن المعلومات وحمايته.



تحدى معلوماتك

أجب عن الأسئلة التالية.

(1) من بين الخيارات أ إلى ث، اختر الخيار الذي يصف بشكل صحيح التصيّد.

(أ) برنامج يسرق المعلومات الشخصية من داخل كمبيوتر دون علم المستخدم ويرسلها إلى طرف ثالث.

(ب) التظاهر بأنه بريد إلكتروني من مؤسسة مالية لإغراء شخص ما بالدخول إلى موقع ويب مزيف والحصول بشكل غير قانوني على رمز PIN أو رقم بطاقة الائتمان الخاصة به.

(ت) النقر فوق رابط (URL) مرة واحدة في موقع ويب أو بريد إلكتروني يؤدي إلى إعلان زائف عن عقد وطلب دفع كبير.

(ث) يتم فوترتك مقابل خدمة لا تعترف بها ويتم الاحتيال عليك للحصول على المال.

(2) من بين الخيارات أ إلى ث، حدد كل ما يتوافق مع الهندسة الاجتماعية.

(أ) تعطيل الوصول إلى البيانات على كمبيوتر والمطالبة بفدية لاستعادتها.

(ب) إنشاء موقع ويب مزيف يتظاهر بأنه بنك لسرقة رمز PIN لحساب بنكي.

(ت) التنصت على المحادثات مع مستخدمين آخرين.

(ث) البحث في المهملات للحصول على معلومات سرية تم التخلص منها.

الشرح

(1) (أ) هو برنامج تجسس، (ت) هو احتيال بنقرة واحدة، و(ث) هو فاتورة احتيالية. الإجابة: **(ب)**

(2) (أ) هو برنامج فدية (ransomware)، (ب) هو تصيد (phishing). الإجابات: **(ت، ث)**

جرب بنفسك

اقرأ الفقرة التالية وأجب عن الأسئلة التي تليها.

مع ازدياد عدد مستخدمي الإنترنت، تتزايد أيضًا حالات الاحتيال التي تتضمن إساءة استخدام أجهزة الكمبيوتر والهواتف الذكية. على سبيل المثال، هناك عمليات احتيال يتم فيها اعتبار مجرد النقر على رابط URL على موقع ويب بمثابة موافقة على عقد خدمة، ويُطلب مبلغ مالي كبير [(1)] ، أو رسائل بريد إلكتروني تتظاهر بأنها من مؤسسات مالية تقود المستخدمين إلى مواقع ويب مزيفة لسرقة أرقام التعريف الشخصي (PINs) أو أرقام بطاقات الائتمان [(2)] . توجد طرق خداعية مختلفة. بالإضافة إلى ذلك، فإن (أ) **استغلال الثغرات في النفس البشرية أو الإهمال يمكن أن يؤدي أيضًا إلى الاستحواذ غير المصرح به على المعلومات**.

(1) اكتب المصطلحات التي تناسب الفراغين [1] و [2] بشكل أفضل.

(2) ما هو المصطلح المستخدم لوصف نوع النشاط المذكور في الجزء الذي تحته خط (أ)؟

(3) من بين الخيارات من 1 إلى 4 ، اختر كل ما يتعلق بالإجابة في (2). اكتب الأحرف المقابلة.

1. يمكن للأفراد التواصل مع بعضهم البعض عبر الإنترنت.
2. يتم منع الوصول إلى البيانات الموجودة على جهاز الكمبيوتر، ويُطلب فدية لاستعادتها.
3. التنصت على المحادثات مع المستخدمين الآخرين.
4. التلصص أثناء قيام شخص ما بإدخال هوية المستخدم أو كلمة المرور الخاصة به.

تمرين

1 أجب عن الأسئلة التالية.

(1) لكل وصف من الأوصاف التالية، اختر العنصر المناسب من أ إلى ج وأجب بالحرف المقابل.

[1] أن يتم فرض رسوم استخدام عليك بمجرد النقر على رابط، كما لو كنت قد انضممت أو وقعت عقدًا.

[2] التظاهر بأنك مؤسسة مالية لخداع المستخدمين وجعلهم يدخلون هوية المستخدم وكلمة المرور الخاصة بهم، والتي يتم إساءة استخدامها بعد ذلك.

[3] سياسة أساسية تضعها شركة أو مؤسسة للحفاظ على أمن المعلومات.

[4] الاستخراج غير القانوني للمعلومات من بطاقة ائتمان أو بطاقة بنكية لشخص آخر.

(أ) التصيد (Phishing) **(ب)** الاحتيال بنقرة واحدة (One-click fraud)

(ت) التزوير (Skimming) **(ث)** سياسة أمن المعلومات (Information security policy)

(ج) الهندسة الاجتماعية (Social engineering)

(2) من بين الخيارات 1 إلى 4، اختر كل ما يندرج تحت الهندسة الاجتماعية.

1. الاتصال من الخارج مع التظاهر بأنك موظف، من أجل استخلاص معلومات داخلية سرية.
2. أن يتم مطالبتك بدفع فاتورة لخدمة وهمية لا تعرفها ويتم الاحتيال عليك وسرقة أموالك.
3. البحث في القمامة للحصول على معلومات سرية تم التخلص منها.
4. تشغيل برنامج يتسبب في تحميل برامج ضارة دون علم المستخدم.

تقنيات المعلومات للسلامة ④

النقاط الرئيسية

فهم مبادئ وأساليب التشفير، وتصوّر الحالات التي يُستخدم فيها.

أ. التشفير (Encryption)

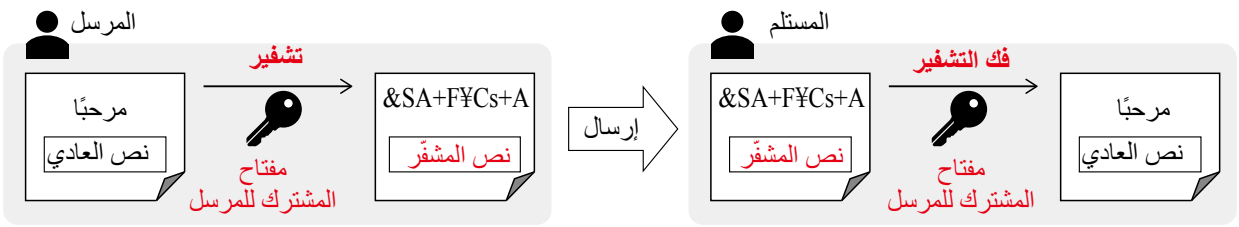
(1) **التشفير** (Encryption) : طريقة تُستخدم عند إرسال المعلومات لمنع اعتراضها من قبل أي شخص آخر غير المستلم المقصود. يُطلق على النص المشفر اسم **النص المشفر** (ciphertext)، ويُطلق على النص الأصلي غير المشفر اسم **النص العادي** (plaintext).

(2) **فك التشفير** (Decryption) : عملية تحويل النص المشفر مرة أخرى إلى شكله الأصلي كنص عادي.

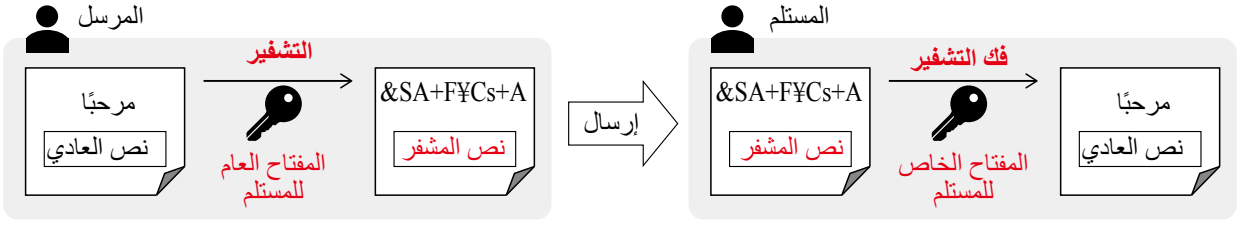
(3) **المفتاح** (Key) : الإجراء أو البيانات المحددة المستخدمة للتشفير وفك التشفير.

ب. أنواع التشفير

(1) **التشفير بالمفتاح المتناظر** (Symmetric key encryption) : طريقة تشفير حيث يتم استخدام نفس **المفتاح المشترك** (shared key) لكل من التشفير وفك التشفير. يتم تشفير الرسالة باستخدام مفتاح المرسل المشترك وفك تشفيرها باستخدام مفتاح المرسل المشترك الذي تم إرساله مسبقًا من قبل المرسل.



(2) **التشفير بالمفتاح العام** (Public key encryption) : طريقة تشفير تستخدم مفتاح تشفير مشترك بشكل علني **المفتاح العام** (public key) ومفتاح تشفير خاص **المفتاح الخاص** (private key). يتم تشفير الرسالة باستخدام المفتاح العام للمستلم، الذي تم إرساله مسبقًا، وفك تشفيرها باستخدام المفتاح الخاص للمستلم، الذي يمتلكه المستلم فقط.



(3) خصائص التشفير بالمفتاح المتماثل والتشفير بالمفتاح العام

	التشفير بالمفتاح المتماثل	التشفير بالمفتاح العام
المزايا	(السرعة) معالجة التشفير وفك التشفير أسرع مقارنة بتشفير المفتاح العام.	نظرًا لأن أي شخص لديه المفتاح يمكنه فك تشفير البيانات، فإن كل مرسل يحتاج إلى مفتاح مشترك مختلف.
العيب	نظرًا لأن المفتاح العام يمكن مشاركته بحرية، فإن إدارة المفاتيح أسهل.	سرعة معالجة تشفير وفك تشفير أبطأ مقارنة بتشفير المفتاح المتماثل

(4) **طريقة المفتاح المؤقت** (**Session key method**): طريقة تشفير تجمع بين التشفير بالمفتاح المتماثل والتشفير بالمفتاح العام.

التشفير بالمفتاح المتماثل هو طريقة يتشارك فيها الطرفان ويستخدمان نفس "المفتاح السري" لتبادل المعلومات.
أما التشفير بالمفتاح العام (Public-key cryptography)، فهو يشبه استخدام قفل تم توزيعه على الجميع؛ إذ يمكن لأي شخص استخدام القفل لإغلاق الصندوق، ولكن وحده المستلم يمتلك المفتاح الفريد لفتحه.

تحدى معلوماتك

أجب عن الأسئلة التالية.

(1) املأ الفراغات [1] إلى [4] في الجمل بالمصطلحات المناسبة.

عند إرسال المعلومات، فإن التكنولوجيا المستخدمة لمنع تسربها أو العبث بها من قبل أي شخص آخر غير المستلم المقصود تسمى ([1]). البيانات الأصلية قبل التشفير تسمى ([2])، وفعل تحويل النص المشفر مرة أخرى إلى نص عادي يسمى ([3]). أيضًا، خلال كل من ([1]) و([3])، يتم استخدام شيء يسمى ([4]).

(2) لكل من العناصر من أ إلى ث، اكتب "A" إذا كانت العبارة تشير إلى التشفير بالمفتاح المتماثل ، أو "B" إذا كانت تشير إلى التشفير بالمفتاح العام.
(أ) يتم جعل مفتاح التشفير عامًا، ويتم التشفير باستخدام المفتاح العام بينما يتم فك التشفير بالمفتاح الخاص.
(ب) يستخدم التشفير مفاتيح منفصلة يحتفظ بها المستلم - واحد للتشفير وواحد لفك التشفير.
(ت) مقارنةً بالطريقة الأخرى، فإن سرعة معالجة التشفير وفك التشفير أسرع.
(ث) مقارنةً بالطريقة الأخرى، فإن تبادل المفتاح أكثر صعوبة.

(3) ما هو اسم طريقة التشفير المختلطة التي تجمع بين التشفير بالمفتاح المتماثل والتشفير بالمفتاح العام؟

الحل

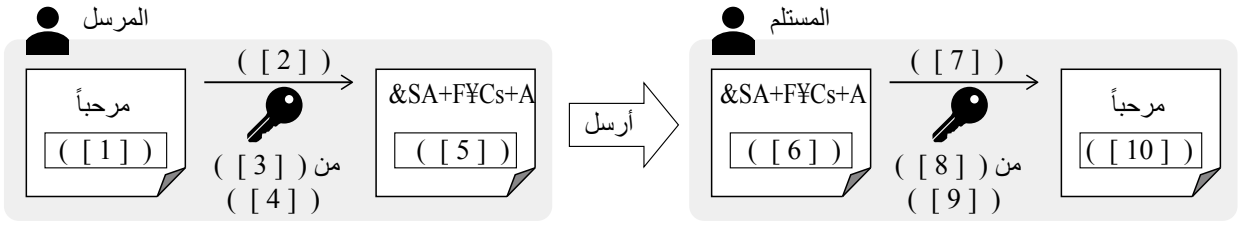
(1) [1] التشفير [2] النص العادي [3] فك التشفير [4] المفتاح
(2) **(أ)** و **(ب)**: الطريقة التي يتم فيها إجراء التشفير باستخدام المفتاح العام للمستلم وفك التشفير باستخدام المفتاح الخاص للمستلم تسمى التشفير بالمفتاح العام.
(ت) و **(ث)**: التشفير بالمفتاح المتماثل أسرع من التشفير بالمفتاح العام، ولكن نظرًا لأنه يستخدم نفس المفتاح لكل من التشفير وفك التشفير، توجد مشكلة كيفية مشاركة المفتاح بشكل آمن مع المستلم.
لذا، (أ) (ب) (ب) (ب)، (ت) (أ)، (ث) (أ)

(3) طريقة المفتاح المؤقتس

جرب بنفسك

1 أجب عن السؤال التالي.

(1) يوضح الرسم البياني سير عملية التشفير بالمفتاح العام. بالنسبة للفراغات من [1] إلى [10]، اختر المصطلحات المناسبة من الخيارات من أ إلى ر . لاحظ أنه يمكن استخدام نفس الخيار أكثر من مرة.



(أ) نص عادي (ب) نص مشفر (ت) فك التشفير (ث) تشفير (ج) ترميز

(ح) مفتاح مشترك (خ) مفتاح عام (د) مفتاح خاص (ذ) المرسل (ر) المستلم

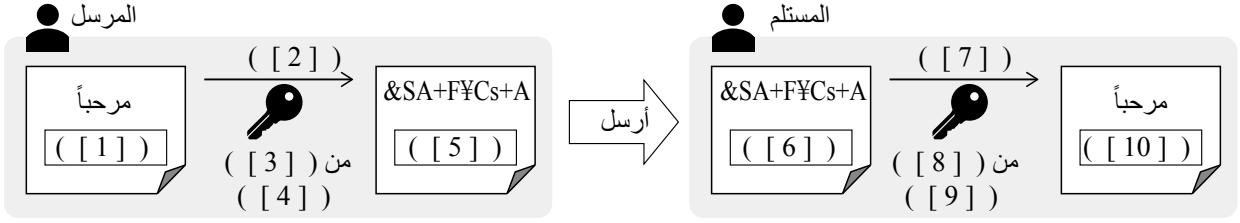
(2) من بين الخيارات 1إلى 4 ، اختر العبارة التي تصف بشكل أفضل إحدى خصائص التشفير بالمفتاح المتماثل (symmetric key encryption) عند مقارنته بـ التشفير بالمفتاح العام (public key encryption) .

1. يجب إعداد مفتاح منفصل لكل مرسل.
2. يتم استخدام نفس المفتاح من قبل المرسل لكل من التشفير وفك التشفير.
3. التشفير وفك التشفير أبطأ مقارنة بالطريقة الأخرى.
4. تبادل المفتاح أسهل مقارنة بالطريقة الأخرى.

تمرين

1 أجب على الأسئلة التالية.

(1) يوضح الرسم البياني سير عملية التشفير بالمفتاح العام. بالنسبة للفراغات من [1] إلى [10]، اختر المصطلحات المناسبة من الخيارات من أ إلى ر . لاحظ أنه يمكن استخدام نفس الخيار أكثر من مرة.



(أ) نص عادي (ب) نص مشفر (ت) فك التشفير (ث) تشفير (ج) ترميز

(ح) مفتاح مشترك (خ) مفتاح عام (د) مفتاح خاص (ذ) المرسل (ر) المستلم

(2) من بين الخيارات 1إلى 3 ، اختر العبارة التي تصف بشكل أفضل إحدى خصائص التشفير بالمفتاح المتماثل (symmetric key encryption) عند مقارنته بـ التشفير بالمفتاح العام (public key encryption) .

يستخدم مفاتيح مختلفة للتشفير وفك التشفير.

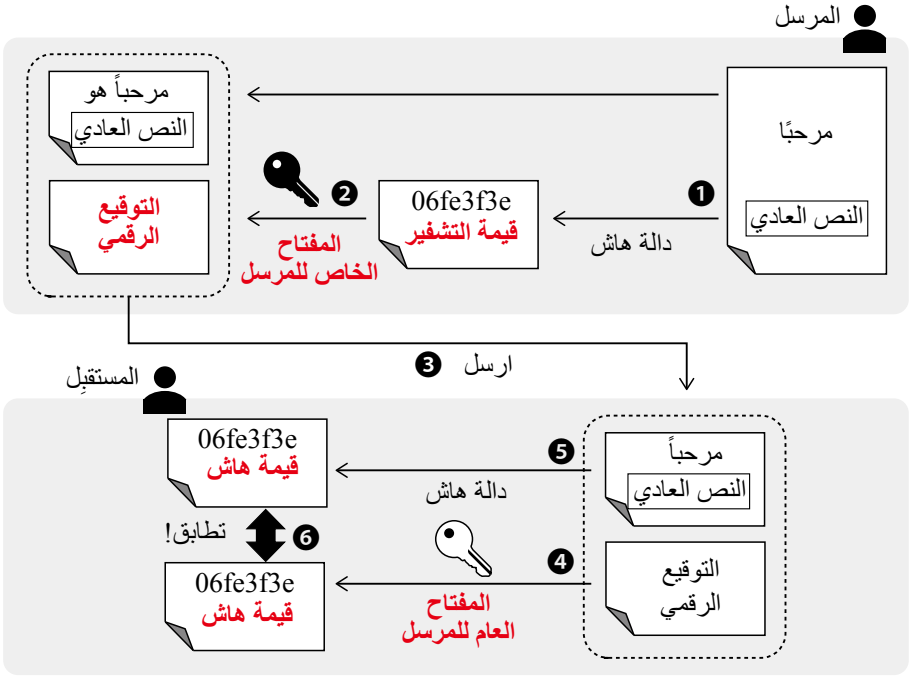
1. يسمح بالتشفير وفك التشفير بسرعة.
2. يتيح توزيع المفاتيح بشكل أكثر أمانًا.
3. يجعل إدارة المفاتيح أسهل حتى عند التواصل مع العديد من الأطراف المختلفة.

النقاط الرئيسية

أ. التوقيع الرقمي (Digital Signature)

(1) **دالة التجزئة** (**Hash function**) : دالة تحسب قيمة فريدة بناءً على بيانات الإدخال. القيمة الناتجة عن دالة التجزئة تسمى **قيمة التجزئة** (**hash value**). ليس من الممكن استعادة البيانات الأصلية من قيمة التجزئة.

(2) **التوقيع الرقمي** (**Digital signature (Electronic signature)**) : تقنية تستخدم التشفير بالمفتاح العام وقيم التجزئة لإثبات أن البيانات المرسلة هي من المرسل ولم يتم العبث بها.



【إجراءات المرسل】

1. تستخدم دالة تجزئة لتوليد قيمة تجزئة من النص العادي المراد إرساله.
2. تشفر قيمة التجزئة باستخدام المفتاح الخاص للمرسل. هذا التشفير يسمى التوقيع الرقمي.
3. يرسل كل من النص العادي والتوقيع الرقمي إلى المستلم.

【إجراءات المستلم】

1. يستخدم المفتاح العام للمرسل لفك تشفير التوقيع الرقمي المستلم واسترداد قيمة التجزئة الأصلية.
2. تستخدم دالة التجزئة نفسها المستخدمة في الخطوة 1 لتوليد قيمة تجزئة جديدة من النص العادي المستلم.
3. تقارن قيمتي التجزئة من الخطوتين 4 و 5. إذا تطابقت، فإنه يثبت أن الرسالة من المرسل ولم يتم العبث بها.

(3) **جهة التصديق** (**Certification authority (CA)**) : منظمة طرف ثالث موثوقة تتحقق مما إذا كان المفتاح العام ينتمي حقًا إلى المالك المطروح. تُصدر (**الشهادة الرقمية**) التي تتضمن المفتاح العام ومعلومات تعريف صاحب المفتاح.

ب. SSL / TLS

(**SSL/TLS**) : تقنية تُستخدم لتشفير الاتصال بين خادم الويب ومتصفح الويب. يتم استخدام طريقة مفتاح الجلسة (**Session Key**) في هذا التشفير. يبدأ رابط URL لصفحة ويب مشفرة بـ "**https**)://...")

* تم تقديم TLS (أمان طبقة النقل - Transport Layer Security) كإصدار أكثر أمانًا من SSL (طبقة المقابس الآمنة - Secure Sockets Layer) المستخدمة في الأصل. ومع ذلك، نظرًا لأن مصطلح "SSL" أصبح معترفًا به على نطاق واسع، غالبًا ما يتم استخدام المصطلح المجمع SSL/TLS.

تحدى معلوماتك

أجب عن الأسئلة التالية.

(1) لكل من العبارات من أ إلى ث حول قيم التجزئة، اكتب "صحيح" إذا كان البيان صحيحًا، أو "خطأ" إذا كان غير صحيح.

(أ) إذا تم تغيير حرف واحد في البيانات الأصلية، فإن حرفًا واحدًا فقط في قيمة التجزئة الناتجة سيتغير.

(ب) يتم إنشاء التوقيع الرقمي عن طريق تشفير قيمة التجزئة للمستند المراد إرساله بمفتاح خاص.

(ت) من الصعب استعادة الرسالة الأصلية من قيمة التجزئة الخاصة بها.

(ث) حتى إذا كانت المستندات المرسلة مختلفة، فإن قيم التجزئة التي تم الحصول عليها من دالة التجزئة نفسها ستكون دائمًا نفسها.

(2) تصف الجمل التالية خطوات إنشاء توقيع رقمي. املأ الفراغات [1] إلى [4] بالمصطلحات المناسبة.

يقوم المرسل بتوليد ([1]) بناءً على البيانات التي يريد إرسالها ويقوم بتشفيرها باستخدام ([2]). هذا يسمى ([3])، ويرسل المرسل كل من البيانات والتوقيع الرقمي إلى المستلم. يقوم المستلم بفك تشفير ([3]) المستلم باستخدام ([4]) لاستعادة ([1]) الأصلية. يقوم المستلم أيضًا بتوليد ([1]) من البيانات المستلمة باستخدام دالة التجزئة نفسها. إذا تطابقت قيمتا ([1])، فإنه يثبت أن البيانات من المرسل ولم يتم العبث بها.

(3) ما هو اسم التكنولوجيا المستخدمة لتشفير الاتصال بين خادم الويب ومتصفح الويب؟

الشرح

(1) **(أ)** إذا كان هناك حرف واحد فقط مختلف في الرسالة الأصلية، فإن قيمة الهاش الناتجة تصبح مختلفة تمامًا. لذلك: ✘

(ب) ✓

(ت) ✓

(ث) إذا كانت الرسالة المُرسلة مختلفة، فإن قيمة الهاش الناتجة ستكون مختلفة تمامًا حتى عند استخدام نفس دالة الهاش. لذلك: ✘

(2) [1] قيمة الهاش [2] المفتاح الخاص [3] التوقيع الرقمي (التوقيع الإلكتروني) [4] المفتاح العام

(3) SSL/TLS

جرب بنفسك

أجب عن السؤال التالي.

(1) للفراغات [1] إلى [6] في الجمل التالية، اختر الكلمات المناسبة من الخيارات أ إلى ر .

للسماح للمستلم بالتحقق من أن البيانات تم إنشاؤها بواسطة المرسل الفعلي ولم يتم العبث بها أثناء الإرسال، هناك تقنية تسمى ([1]). يتم إنشاء ([1]) عن طريق توليد ([2]) من النص العادي المراد إرساله باستخدام برنامج، ثم تشفيره بـ ([3]). يتم إرفاق هذا بالنص العادي وإرساله إلى المستلم. يقوم المستلم بفك تشفير ([1]) باستخدام ([4]). إذا تطابقت ([2]) الناتجة مع ([2]) التي تم إنشاؤها من النص العادي المستلم، فإنه يثبت أن البيانات تم إنشاؤها بواسطة المرسل ولم يتم تغييرها. ومع ذلك، هذا وحده لا يمكنه منع انتحال الشخصية. لذلك، تقوم منظمة طرف ثالث تسمى ([5]) بإصدار ([6]) لضمان أن المفتاح العام ينتمي حقًا إلى المرسل.

(أ) المفتاح الخاص للمرسل **(ب)** المفتاح العام للمرسل **(ت)** المفتاح المشترك للمرسل

(ث) المفتاح الخاص للمستلم **(ج)** المفتاح العام للمستلم **(ح)** المفتاح المشترك للمستلم

(خ) الشهادة الرقمية **(د)** التوقيع الرقمي **(ذ)** قيمة التجزئة

(ر) جهة التصديق (CA)

(2) للفراغات [1] و [2] في الجملة التالية، اختر الكلمات المناسبة من الخيارات أ إلى ث .

بخصوص دالة التجزئة المستخدمة في التوقيعات الرقمية: يتم دائمًا تحويل البيانات نفسها إلى ([1]) قيمة التجزئة، ومن ([2]) استعادة البيانات الأصلية من قيمة التجزئة المحولة.

(أ) مختلفة **(ب)** نفس **(ت)** ممكن **(ث)** المستحيل

(3) للفراغات [1] إلى [6] في الجملة التالية، اختر المصطلحات المناسبة من الخيارات أ إلى خ .

عندما يكون بداية رابط (URL) لصفحة ويب هو "https://:"، فهذا يعني أنه يتم إجراء تشفير باستخدام ([1]). في ([1])، يتم إجراء التشفير باستخدام ([4]) التي تجمع بين ([2]) و ([3]). بالإضافة إلى ذلك، فإن ([1]) تساعد أيضًا في منع التصيّد للتوجيه إلى موقع ويب مزيف عن طريق إرفاق ([6]) الصادرة عن ([5]).

(أ) التشفير المفتاح العام **(ب)** التشفير المفتاح المتناظر **(جـ)** طريقة المفتاح الجلسة

(د) الشهادة الرقمية **(هـ)** التوقيع الرقمي **(و)** SSL/TLS

(ز) سلطة التصديق (CA)

(4) من بين الخيارات التالية من أ إلى ث، اختر الخيار الذي يصف بشكل صحيح وظيفة SSL/TLS.

(أ) يولد كلمات مرور لمرة واحدة للمصادقة على مواقع الويب.

(ب) يشفر الاتصال بين متصفح الويب وخادم الويب.

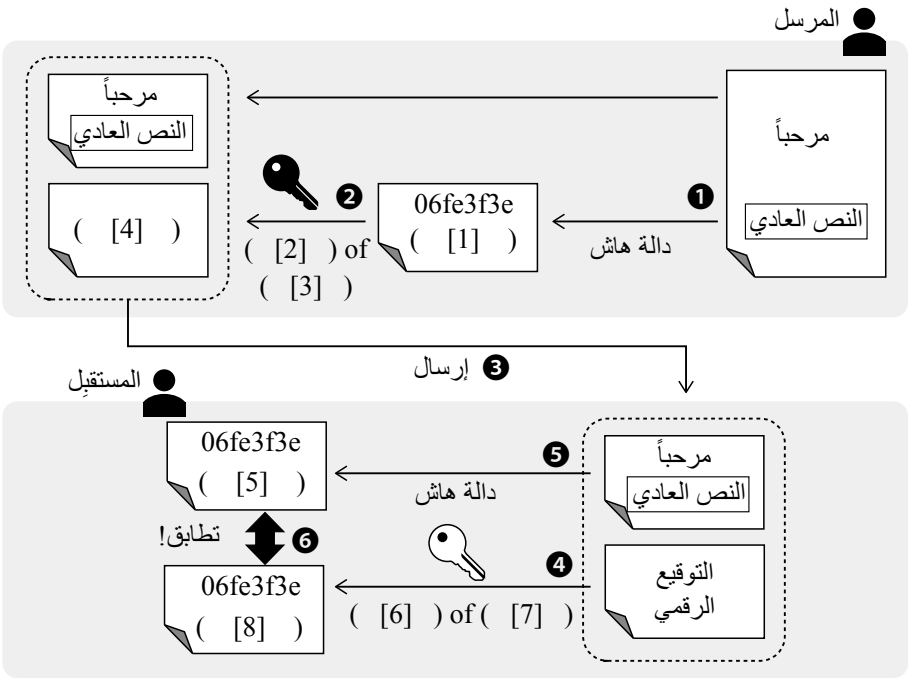
(ت) يرشح الاتصال إلى مواقع ويب غير مصرّح بها.

(ث) يكتشف الفيروسات التي تنتشر عبر الشبكات.

تمرين

1 أجب على الأسئلة التالية.

(1) يوضح الرسم البياني آلية التوقيع الرقمي. بالنسبة للفراغات من [1] إلى [8]، اختر المصطلحات المناسبة من الخيارات من أ إلى د وأجب باستخدام الأحرف المقابلة. (يمكن استخدام نفس الحرف أكثر من مرة).



【بنك الكلمات】 (أ) المرسل (ب) المستلم (ت) مفتاح المشترك (ث) مفتاح الخاص
(ج) مفتاح العام (ح) قيمة التجزئة (خ) توقيع الرقمي (د) المصادقة الإلكترونية

(2) من بين الخيارات أ إلى ث ، اختر العبارة التي تصف بشكل مناسب شيئًا يتعلق برسالة بريد إلكتروني تحمل توقيعًا رقميًا. أجب باستخدام الحرف المقابل.

(أ) من المرجح أن يحدث نص مشوش أثناء إرسال البريد الإلكتروني.

(ب) يسمح لك بالتأكد مما إذا كان البريد الإلكتروني قد أُرسل من المرسل الصحيح.

(ت) يمنع اعتراض محتويات البريد الإلكتروني أثناء الإرسال.

(ث) يمنع فقدان محتويات البريد الإلكتروني.

(3) من بين الخيارات أ إلى ت ، اختر كل ما يصف بشكل صحيح وظائف SSL/TLS. أجب باستخدام الأحرف المقابلة.

(أ) يُعتبر بروتوكول SSL سابقًا لبروتوكول TLS، وفي الوقت الحالي يُعدّ TLS هو المعيار الرئيسي المُستخدم.

(ب) هي وظيفة تقييد الوصول إلى المواقع الضارة أو غير القانونية بناءً على شروط معينة.

(ت) عناوين URL التي تبدأ بـ "http://..." تكون مشفرة باستخدام SSL/TLS.

(ث) SLS/TLS يشفر الاتصال باستخدام طريقة مفتاح الجلسة التي تجمع بين طرق التشفير بالمفتاح المتماثل والمفتاح العام.