الوحدة الرابعة

أمن المعلومات

و

التشفير

الفصل الأول : أمن المعلومات

١) علل / يعد أمن المعلومات من أهم الركائز التي تعتمد عليها الدول والمؤسسات والأفراد؟
من أجل الحفاظ على موقفها العالمي سياسيا وماليا ومع التطور الهائل الذي حصل في مجالي الإنترنت والبرمجيات أصبح تناقل المعلومات والحصول عليها أمرا سهلا .

٢) علل / وجب الاهتمام بكل ما يخص المعلومة من أجهزة تخزين ومعالجة والاهتمام بالكادر البشري الذي يتعامل معها بالإضافة إلى الحفاظ على المعلومات نفسها .
بسبب وجود المخترقين والمتطفلين بشكل كبير

٣) علل : أصبح تناقل المعلومات والحصول عليها أمرا سهلا .
بسبب التطور الهائل الذي حصل في مجالي الإنترنت والبرمجيات

٤) بسبب وجود المخترقين والمتطفلين بشكل كبير فقد وجب الاهتمام بكل ما يخص المعلومة . ما هي الأشياء التي تخص المعلومات .
١. أجهزة تخزين ومعالجة
٢. الاهتمام بالكادر البشري الذي يتعامل معها
٣. بالإضافة إلى الحفاظ على المعلومات نفسها

أولاً : مقدمة فى أنظمة المعلومات

١- مفهوم أمن المعلومات

١) ما المقصود بـ (أمن المعلومات) ؟
هو العلم الذي يعمل على حماية المعلومات والمعدات المستخدمة لتخزينها ومعالجتها ونقلها من السرقة أو التطفل أو من الكوارث الطبيعية أو غيرها من المخاطر ويعمل على إبقاءها متاحة للأفراد المصرح لهم باستخدامها

٢) بماذا تستخدم المعدات (ما علاقة المعدات بالمعلومات) .
١. تخزين المعلومات
٢. معالجتها
٣. نقلها

٣) ما هي المخاطر التي تهدد المعلومات .

١. السرقة
٢. التطفل
٣. الكوارث الطبيعية

٤) علل: ظهور أمن المعلومات .

- لحماية المعلومات والمعدات المستخدمة
- إبقاءها متاحة للأفراد المصرح لهم باستخدامها

٥) اذكر الخصائص الأساسية لأمن المعلومات ؟

١.السرية

٢.السلامة

٣.توافر المعلومات

٦)ما الهدف من أمن المعلومات ؟

الحفاظ على (السرية و السلامة و توافر المعلومات)

أ- السرية (confidentiality)

١) ما المقصود بـ (السرية / سرية المعلومات) ؟

وتعني أن الشخص المخول هو الوحيد القادر على الوصول إلى المعلومات والاطلاع عليها. / عدم القدرة على الحصول على المعلومات إلا من قبل الأشخاص المخول لهم ذلك .

٢) إن مصطلح السرية مرادف لعدة مفاهيم . أذكر هذه المفاهيم .

الأمن والخصوصية .

٣) أعط أمثلة على سرية المعلومات ./ أعط أمثلة على بيانات يعتمد أمنها على مقدار الحفاظ على سريتها .

- المعلومات الشخصية
- الموقف المالي لشركة ما قبل إعلانه
- المعلومات العسكرية بيانات يعتمد أمنها على مقدار الحفاظ على سريتها

ب- السلامة (integrity)

١) ما المقصود بـ (السلامة / سلامة المعلومات) ؟

تعني حماية الرسائل أو المعلومات التي تم تداولها والتأكد بأنها لم تتعرض لأي عملية تعديل سواء : بالإضافة أم الاستبدال أم حذف جزء منها .

٢) كيف يتم تعديل المعلومات ./ ما هي طرق تعديل المعلومات .

١. بالإضافة
٢. الاستبدال
٣. حذف جزء منها

٣) أعط مثالاً على سلامة المعلومات .

- عند نشر نتائج طلبة الثانوية العامة يجب الحفاظ على سلامة هذه النتائج من أي تعديلات
- عند صدور قوائم القبول الموحد للجامعات الأردنية والتخصصات التي قبل الطلبة فيها فلا بد من العمل على حماية هذه القوائم من أي تعديل أو حذف أو تبديل أو تغيير

جـ- توافر المعلومات (availability) :

١) ما المقصود بمفهوم توافر المعلومات ؟

قدرة الشخص المخول الحصول على المعلومات في الوقت الذي يشاء ، دون وجود عوائق .

٢) بالرغم من وجود سرية المعلومات و سلامتها إلا أنها في بعض الأحيان تكون بلا فائدة . متى تكون المعلومات بلا فائدة .

- إذا لم تكن متاحة للأشخاص المصرح لهم بالتعامل معها
- أو أن الوصول إليها يحتاج إلى وقت كبير

٣) ما هي الوسائل التي يقوم بها المخترقون لجعل المعلومات غير متاحة .

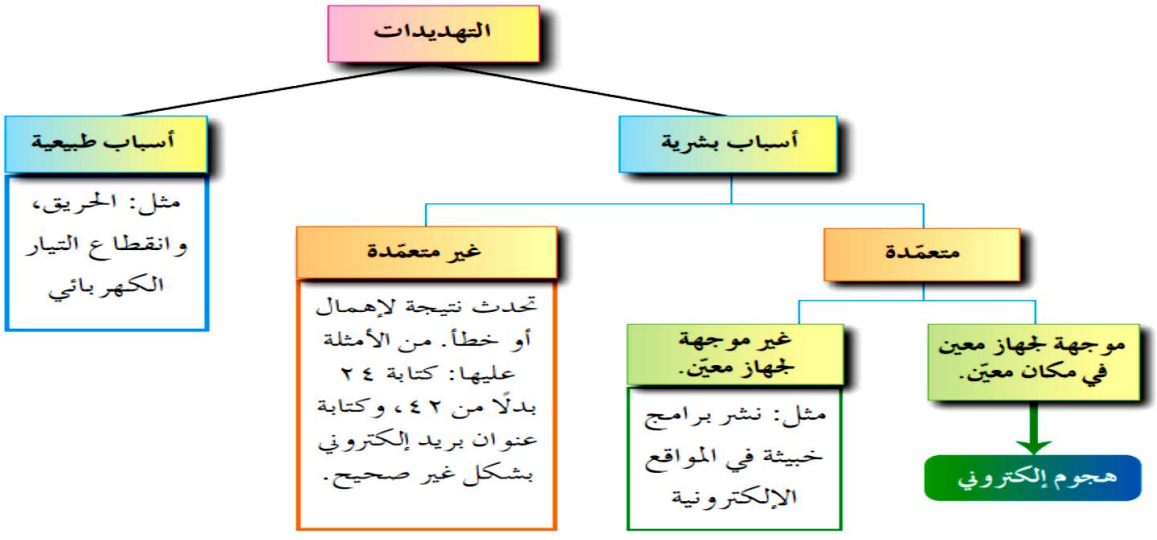
- إما بحذفها
- أو الاعتداء على الأجهزة التي تخزن فيها هذه المعلومات

٢- المخاطر التي تهدد أمن المعلومات

١) اذكر المخاطر الرئيسية التي تهدد أمن المعلومات ؟

تقسم المخاطر التي تهدد أمن المعلومات إلى نوعين رئيسين هما:

- التهديدات
- الثغرات .



أ- **التهديدات (threats)** :

١) اذكر الأسباب التي تحدث التهديدات ؟

١. **الأسباب الطبيعية :** مثل حدوث حريق أو انقطاع التيار الكهربائي ما يؤدي إلى فقدان المعلومات

٢. **الأسباب البشرية :** و تقسم إلى نوعين:

أ. أن تكون غير متعمدة وتحدث نتيجة لإهمال أو خطأ مثل : كتابة عنوان بريد إلكتروني بشكل غير صحيح

ب. أن تكون متعمدة وتقسم إلى قسمين

١.غير موجهة لجهاز معين كأن ينشر فيروس

٢. موجهة لجهاز معين وهذا ما يسمى **الهجوم الإلكتروني** ،أو **الاعتداء الإلكتروني**

٢) تقسم الأسباب البشرية (الأخطاء البشرية) إلى نوعين . أذكرهما .

١. **أن تكون غير متعمدة وتحدث نتيجة لإهمال أو خطأ** مثل : كتابة عنوان بريد إلكتروني بشكل غير صحيح

٢. **أن تكون متعمدة . وتقسم إلى قسمين:**

أ.غير موجهة لجهاز معين كأن ينشر فيروس

ب. موجهة لجهاز معين وهذا ما يسمى **الهجوم الإلكتروني** ،أو **الاعتداء الإلكتروني**

٣) وضح المقصود بـ (الهجوم الالكتروني / الإعتداء الإلكتروني) .

نوع من التهديدات ضمن الأسباب البشرية المتعمدة و التي تكون موجهة لجهاز معين ، بقصد الإضرار به.

٤) اذكر أمثلة على الهجوم الإلكتروني ،أو الاعتداء الإلكتروني ؟

١. سرقة جهاز الحاسوب أو إحدى المعدات التي تحفظ المعلومات .
٢. التعديل على ملف أو حذفه .
٣. الكشف عن بيانات سرية .
٤. منع الوصول إلى المعلومات .

٥) يعد الاعتداء الإلكتروني من أخطر أنواع التهديدات ويعتمد نجاح هذا الهجوم على ثلاثة عوامل رئيسة ، اذكر هذه العوامل ؟

١. الدافع ٢. الطريقة ٣. فرصة النجاح

(يجب أخذ هذه العوامل في الحسبان لتقييم التهديد الذي يتعرض له النظام)

٦) علل: يجب الأخذ بالحسبان في العوامل (الدافع / الطريقة / فرصة النجاح) عند التعرض للتهديد .

لتقييم التهديد الذي يتعرض له النظام .

٧) اذكر دوافع الأفراد لتنفيذ هجوم إلكتروني . / ما هي دوافع الأفرد لتنفيذ هجوم الكتروني .

١. الرغبة في الحصول على المال .

٢. محاولة لإثبات القدرات التقنية .

٣. بقصد الإضرار بالآخرين .

٨) اذكر الأمور التي تتضمنها / على ماذا تعتمد الطريقة في الهجوم الالكتروني ؟

١.المهارات التي يتميز بها المعتدي الإلكتروني .

٢. قدراته على توفير المعدات والبرمجيات الحاسوبية التي يحتاج إليها .

٣. معرفته بتصميم النظام وآلية عمله

٤. ومعرفة نقاط القوة والضعف لهذا النظام .

٩) بماذا تتمثل / على ماذا تعتمد فرصة نجاح الهجوم الإلكتروني؟

١. تحديد الوقت المناسب للتنفيذ ٢. كيفية الوصول إلى الأجهزة

١٠) اذكر أنواع الاعتداءات الإلكترونية؟ / تتعرض المعلومات إلى أربعة أنواع من الاعتداءات الإلكترونية. اذكرها .

١. التنصت على المعلومات

٢. التعديل على المحتوى

٣. الإيقاف

٤. الهجوم المزور أو المفبرك

١١) ما هدف التنصت على المعلومات .

والهدف منه الحصول على المعلومات السرية حيث يتم الإخلال بسريتها

١٢) وضح المقصود بـ التعديل على المحتوى / كيف يتم التعديل على المحتوى / أذكر خطوات تعديل محتوى المعلومات / وضح آلية التعديل على محتوى المعلومات .

- يتم اعتراض المعلومات
- وتغيير محتواها
- وإعادة إرسالها للمستقبل من دون أن يعلم بتغيير محتواها
- وفي هذا النوع يكون الإخلال بسلامة المعلومات

١٣) وضح المقصود بـ الإيقاف . / كيف يتم إيقاف المعلومات / أذكر خطوات إيقاف المعلومات / وضح آلية إيقاف المعلومات .

- يتم قطع قناة الاتصال
- ومن ثم منع المعلومات من الوصول إلى المستقبل
- وفي هذه الحالة تصبح المعلومات غير متوافرة

١٤) وضح المقصود بالهجوم المزور أو المفبرك / كيف يتم الهجوم المفبرك / أذكر خطوات الهجوم المفبرك / وضح آلية الهجوم المفبرك .

- يتمثل هذا النوع بإرسال المعتدي الالكتروني رسالة إلى أحد الأشخاص على الشبكة
- يخبره فيها بأنه صديقه ويحتاج إلى معلومات أو كلمات سرية خاصة
- تتأثر بهذه الطريقة سرية المعلومات وقد تتأثر أيضا سلامتها

ب- الثغرات (vulnerability) :

١) ما المقصود بمفهوم الثغرات .

يقصد بها نقطة الضعف في النظام سواء أكانت في الإجراءات المتبعة مثل عدم تحديد صلاحيات الوصول إلى المعلومات ، أم مشكلة في تصميم النظام ، كما أن عدم كفاية الحماية المادية للأجهزة والمعلومات تعد من نقاط الضعف التي قد تتسبب في فقدان المعلومات أو هدم النظام أو تجعله عرضة للاعتداء الإلكتروني .

٢) أين توجد الثغرات (نقاط الضعف) .

- في الإجراءات المتبعة :مثل عدم تحديد صلاحيات الوصول إلى المعلومات ، أم مشكلة في تصميم النظام .
- كما أن عدم كفاية الحماية المادية للأجهزة والمعلومات تعد من نقاط الضعف التي قد تتسبب في فقدان المعلومات أو هدم النظام أو تجعله عرضة للاعتداء الإلكتروني .

٣) ما أثر عدم كفاية الحماية المادية للأجهزة والمعلومات التي تعد من نقاط الضعف .

تتسبب في فقدان المعلومات أو هدم النظام أو تجعله عرضة للاعتداء الإلكتروني .

٢- الحد من مخاطر أمن المعلومات

١) يرى المختصون في مجال أمن المعلومات بأن الحفاظ على المعلومات وأمنها ينبع من عدة أمور. اذكرها .

- التوازن بين تكلفة الحماية وفعالية الرقابة من جهة .
- مع احتمالية الخطر من جهة أخرى .

٢) علل : قام المختصون في أمن المعلومات بوضع مجموعة من الضوابط.

لتقليل المخاطر التي تتعرض لها المعلومات والحد منها .

٣) قام المختصون في أمن المعلومات بوضع مجموعة من الضوابط لتقليل المخاطر التي تتعرض لها المعلومات والحد منها . أذكر هذه الضوابط .

١. الضوابط المادية .
٢. الضوابط الإدارية .
٣. الضوابط التقنية .

أ- الضوابط المادية :

١) وضح المقصود بمفهوم الضوابط المادية .

مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها باستخدام الجدران والأسوار واستخدام الأقفال ووجود حراس الأمن وغيرها من أجهزة لإطفاء الحريق .

٢) كيف يمكن مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية . / أعط أمثلة على الضوابط المادية .

- الجدران والأسوار
- واستخدام الأقفال
- و وجود حراس الأمن
- أجهزة لإطفاء الحريق .

ب- الضوابط الإدارية :

١) وضح المقصود بمفهوم الضوابط الإدارية .

استخدام مجموعة من الأوامر والإجراءات المتفق عليها مثل : القوانين واللوائح والسياسات والإجراءات التوجيهية وحقوق النشر وبراءات الاختراع والعقود والاتفاقيات .

٢) اذكر الأوامر والإجراءات المتفق عليها في الضوابط الإدارية .

القوانين واللوائح والسياسات والإجراءات التوجيهية وحقوق النشر وبراءات الاختراع والعقود والاتفاقيات .

جـ- الضوابط التقنية :

١) وضح المقصود بمفهوم الضوابط التقنية ؟

وهي الحماية التي تعتمد على التقنيات المستخدمة سواء أكانت معدات (hardware) أو برمجيات (software) وتتضمن كلمات المرور ومنح صلاحيات الوصول و بروتوكولات الشبكات والجدر النارية والتشفير وتنظيم تدفق المعلومات في الشبكة .

٢) ما هي التقنيات التي يتم وضع الضوابط المادية عليها .

- معدات (hardware)
- أو برمجيات (software)

٣) تعتمد الضوابط المادية على التقنيات المستخدمة سواء أكانت معدات (hardware) أو برمجيات (software) ، حيث تتضمن هذه الضوابط عدة أمور . أذكرها .

- كلمات المرور
- منح صلاحيات الوصول
- بروتوكولات الشبكات
- الجدر النارية
- التشفير
- تنظيم تدفق المعلومات في الشبكة .

٤) كيف يتم الوصول إلى أفضل النتائج عند استخدام الضوابط التقنية .

تعمل الضوابط التقنية بشكل متكامل للحد من الأخطار التي تتعرض لها المعلومات .

ثانيا : الهندسة الاجتماعية

١) علل / يجب الاهتمام بالعنصر البشري .

- لان العنصر البشري من أهم مكونات الأنظمة
- للحفاظ على أمن المعلومات

٢) يعتمد اختيار الكادر البشري المسؤول عن حماية الأنظمة على عدة أمور . اذكرها .

١. كفايته العلمية .
٢. اختبارات شفوية و ورقية و مقابلات
٣. إخضاعهم إلى ضغوط نفسية كل حسب موقعهم للتأكد من قدرتهم على حماية النظام .

٣) ما أنواع الاختبارات التي يخضع لها الكادر البشري المسؤول عن حماية الأنظمة .

اختبارات شفوية و ورقية و مقابلات .

١- مفهوم الهندسة الاجتماعية

١) وضح المقصود بمفهوم الهندسة الاجتماعية .

هي الوسائل والأساليب التي يستخدمها المعتدي الإلكتروني لجعل مستخدم الحاسوب في النظام يعطي معلومات سرية أو يقوم بعمل ما يسهل عليه الوصول إلى أجهزة الحاسوب في النظام يعطي معلومات سرية .

٢) علل : استخدام المعتدي الالكتروني مجموعة من الوسائل في الهندسة الإجتماعية . / ما هدف الهندسة الإجتماعية .

- لجعل مستخدم الحاسوب في النظام يعطي معلومات سرية
- أو يقوم بعمل ما يسهل عليه الوصول إلى أجهزة الحاسوب في النظام يعطي معلومات سرية .

٣) علل : تعد الهندسة الاجتماعية من أنجح الوسائل وأسهلها التي تستخدم للحصول على معلومات غير مصرح بالاطلاع عليها .

- بسبب قلة اهتمام المتخصصين في مجال أمن المعلومات
- وعدم وعي مستخدمي الحاسوب بالمخاطر المترتبة عليها .

٢- مجالات الهندسة الاجتماعية

١) تتركز الهندسة الاجتماعية في مجالين ، اذكرهما ؟

١. البيئة المحيطة
٢. الجانب النفسي

أ- البيئة المحيطة :

١) اذكر الأمور التي تشتمل عليها البيئة المحيطة ؟

١. مكان العمل.
٢. الهاتف
٣. النفايات الورقية
٤. الإنترنت

٢) كيف يمكن أن يكون مكان العمل عامل مؤثر ضمن البيئة المحيطة في الهندسة الاجتماعية ؟

يكتب بعض الموظفين كلمات على أوراق ملصقة بشاشة الحاسوب وعند دخول الشخص غير المخول له الاستخدام كزبون أو حتى عامل نظافة أو عامل صيانة يستطيع معرفة كلمات المرور ومن ثم يتمكن من الدخول إلى النظام بسهولة ليحصل على المعلومات التي يريدها

٣) كيف يمكن أن يكون الهاتف عامل مؤثر ضمن البيئة المحيطة في الهندسة الاجتماعية ؟

يتصل الشخص غير المخول بمركز الدعم الفني هاتفيا ويطلب إليه بعض المعلومات الفنية ويستدرجه للحصول على كلمات المرور وغيرها من المعلومات ليستخدمها في ما بعد .

٤) كيف يمكن أن تكون النفايات الورقية عامل مؤثر ضمن البيئة المحيطة في الهندسة الاجتماعية ؟

يدخل الأشخاص غير المخولين إلى مكان العمل ويجمعون النفايات التي قد تحتوي على كلمات المرور ومعلومات تخص الموظفين وأرقام هواتفهم وبياناتهم الشخصية وقد تحتوي على تقويم العام السابق وكل ما يحتويه من معلومات يمكن استغلالها في تتبع أعمال الموظفين أو الحصول على المعلومات المرغوبة .

٥) كيف يمكن أن يكون الانترنت عامل مؤثر ضمن البيئة المحيطة في الهندسة الاجتماعية ؟

من خلال استخدام الموظفين أو مستخدمي الحاسوب عادة كلمة المرور نفسها للتطبيقات جميعها حيث ينشئ المعتدي الإلكتروني موقعا على الشبكة يقدم خدمات معينة ويشترط التسجيل فيه للحصول على هذه الخدمات يتطلب التسجيل في الموقع اسم مستخدم وكلمة المرور وهي كلمة المرور نفسها التي يستخدمها الشخص عادة وبهذه الطريقة يتمكن المعتدي الإلكتروني من الحصول عليها .

٦) علل : يعتبر الإنترنت من أكثر الوسائل شيوعاً ضمن البيئة المحيطة في الهندسة الاجتماعية .
بسبب استخدام الموظفين أو مستخدمي الحاسوب عادة كلمة المرور نفسها للتطبيقات .

ب-**الجانب النفسي :**

١) **من أجل التأثير على الجانب النفسي للمستخدم يسعى المعتدي الالكتروني للقيام بعدة امور** . أذكرها.
- كسب ثقة مستخدم الحاسوب
- ومن ثم الحصول على المعلومات التي يرغب بها

٢) اذكر الأساليب التي يستخدمها المعتدي الإلكتروني هنا لكسب ثقة مستخدم الحاسوب ومن ثم الحصول على المعلومات ؟
١. **الإقناع.**
٢. **انتحال الشخصية والمداهنة**
٣. **مسايرة الركب**

٣) يستخدم المعتدي طريقتين في الإقناع ، اذكرهما ؟
يستطيع المعتدي إقناع الموظف أو مستخدم الحاسوب
أ. بطريقة مباشرة : بحيث يقدم الحجج المنطقية والبراهين .
ب.بطريقة غير مباشرة :
- بحيث يتعمد إلى تقديم إيحاءات نفسية تحث المستخدم على قبول المبررات من دون تحليلها أو التفكير فيها
- إظهار نفسه بمظهر صاحب السلطة
- إغراء المستخدم بامتلاك خدمة نادرة حيث يقدم له عرضا معينا من خلال موقعه الإلكتروني لمدة محددة يمكنه ذلك من الحصول على كلمة المرور .
- قد يلجأ المعتدي الالكتروني إلى إبراز أوجه التشابه مع الشخص المستهدف لإقناعه بأنه يحمل الصفات والاهتمامات نفسها فيصبح الشخص أكثر ارتياحا وأقل حذرا للتعامل معه فيقدم له ما يريد من معلومات .

٤) علل : قد يلجأ المعتدي الالكتروني إلى إبراز أوجه التشابه مع الشخص المستهدف .
لإقناعه بأنه يحمل الصفات والاهتمامات نفسها فيصبح الشخص أكثر ارتياحا وأقل حذرا للتعامل معه فيقدم له ما يريد من معلومات .

٥) وضح كيف تتم عملية انتحال الشخصية والمداهنة ؟
- حيث يتقمص شخص شخصية أخرى
- وهذا الشخص قد يكون شخصا حقيقيا أو وهميا
- فقد ينتحل شخصية فني صيانة معدات الحاسوب أو عامل نظافة أو حتى المدير أو السكرتير
- وبما أن الشخصية المنتحلة غالبا تكون ذات سلطة يبدي أغلب الموظفين خدماتهم ولن يترددوا بتقديم أي معلومات لهذا الشخص المسؤول .

٦) أعط مثالاً على انتحال الشخصية .
انتحالل شخصية فني صيانة معدات الحاسوب أو عامل نظافة أو حتى المدير أو السكرتير

٧) علل : عند انتحال الشخصية يبدي أغلب الموظفين خدماتهم ولن يترددوا بتقديم أي معلومات لهذا الشخص المسؤول .

لأن الشخصية المنتحلة غالبا تكون ذات سلطة

٨) وضح كيف تتم مسايرة الركب؟

- حيث يرى الموظف بأنه إذا قام زملاؤه جمعيهم بأمر ما فمن غير اللائق أن يأخذ هو موقفا مغايرا
- فعندما يقدم شخص نفسه على أنه إداري من فريق الدعم الفني ويرغب بعمل تحديثات على الأجهزة فإذا سمح له أحد الموظفين بعمل تحديث على جهازه
- فإن باقي الموظفين يقومون بمسايرة زميلهم غالبا والسماح لهذا المعتدي باستخدام أجهزتهم لتحديثها ومن ثم يتمكن من الإطلاع على المعلومات التي يريدها والمخزنة على الأجهزة.

اجابات اسئلة الوحدة الرابعة

أمن المعلومات و التشفير

أسئلة الفصل الأول – أمن المعلومات:

1- وضح المقصود بكل من:

- أمن المعلومات: هو العلم الذي يعمل على حماية المعلومات والمعدات المستخدمة لتخزينها ومعالجتها ونقلها من السرقة أو التطفل أو من الكوارث الطبيعية أو جميعها. ويعمل على إبقائها متاحة للأفراد المصرح لهم استخدامها.
- الثغرات: ويُقصد بها نقطة الضعف في النظام سواء أكانت في الإجراءات المُتبعة مثل عدم تحديد صلاحيات الوصول الى المعلومات، أو مشكلة في تصميم النظام، أو في مرحلة التنفيذ، كما أن عدم كفاية الحماية المادية للأجهزة والمعلومات تُعتبر من نقاط الضعف التي قد تتسبب في فقدان المعلومات أو هدم النظام أو تجعله عرضة للإعتداء الإلكتروني.

2-يهدف أمن المعلومات للحفاظ على ثلاثة خصائص أساسية هي (السرية، السلامة المعلومات، توافر المعلومات) حدد إلى أي من هذه الخصائص يتبع كل مما يأتي:

أ- التأكد من عدم حدوث أي تعديل على المعلومات **سلامة المعلومات**.

ب- الشخص المخوّل هو الوحيد القادر على الوصول إلى المعلومات والاطلاع عليها

السرية.

ج- الوصول إلى المعلومات يحتاج إلى وقت كبير توافر المعلومات.

د- مصطلح مرادف لمفهومي الأمن والخصوصية السرية.

هـ- المعلومات العسكرية تخص سرية المعلومات.

3-هناك ثلاثة عوامل رئيسة تؤخذ بعين الاعتبار لتقييم التهديد، بناءً على دراستك للوحدة حدد العامل الذي يندرج تحته كل مما يأتي؟

أ- الرغبة في إثبات القدرات الدافع.

ب- معرفة نقاط القوة والضعف للنظام الطريقة.

ج- تحديد الوقت المناسب لتنفيذ الهجوم الإلكتروني فرصة نجاح الهجوم.

د- الإضرار بالآخرين الدافع.

هـ- الرغبة في الحصول على المال الدافع.

و- القدرة على توفير المعدات والبرمجيات الحاسوبية الطريقة.

4-عدّد أربعة من أنواع الاعتداءات الإلكترونية التي تتعرض لها المعلومات؟

أ- التنصت على المعلومات.

ب- التعديل على المحتوى.

ج- الإيقاف.

د- الهجوم المزوّر أو المفبرك

5-علل ما يأتي:

أ- استخدام بعض الضوابط في النظام.

لتقليل المخاطر التي تتعرض لها المعلومات والحد منها.

ب- تُعد الهندسة الاجتماعية من أنجح الوسائل وأسهلها للحصول على المعلومات.

وذلك بسبب قلة اهتمام المتخصصين في مجال أمن المعلومات وعدم وعي

مستخدمي الحاسوب بالمخاطر المترتبة عليها.

6-قارن بين نوعي الضوابط المادية والضوابط الإدارية من حيث:

وجه المقارنة	الضوابط المادية	الضوابط الإدارية
المقصود بها	يُقصد بها مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها.	تستخدم مجموعة من الأوامر والإجراءات المتفق عليها.
أمثلة عليها	استخدام الجدران والأسوار، واستخدام الأقفال، ووجود حراس الأمن وغيرها من أجهزة إطفاء الحريق.	القوانين واللوائح والسياسات، الاجراءات التوجيهية وحقوق النشر وبراءات الاختراع والعقود والاتفاقيات.

7-وضح آلية عمل الهندسة الاجتماعية في كل مجال من المجالات الآتية:

المجال	آلية العمل
مكان العمل	يقوم بعض الموظفين بكتابة كلمات المرور على أوراق ملصقة بشاشة الحاسوب. وعند دخول الشخص غير المخوّل له الاستخدام كزبون أو حتى عامل نظافة أو صيانة يستطيع معرفة كلمات المرور ومن ثم يتمكن من الدخول إلى النظام بسهولة ليحصل على المعلومات التي يُريدها.
الهاتف	يتصل الشخص غير المخوّل بمركز الدعم الفني هاتفيًا ويطلب منه بعض المعلومات الفنية ويستدرجه للحصول على كلمات المرور وغيرها من المعلومات ليستخدمها فيما بعد.

انتحال الشخصية	حيث يقوم شخص بتقمص شخصية آخر وهذا الشخص قد يكون شخصًا حقيقيًا أو وهميًا. فقد ينتحل شخصية فني صيانة معدات الحاسوب أو عامل نظافة أو حتى المدير أو السكرتير. وبما أن الشخصية المنتحلة غالبًا تكون ذات سلطة يقوم أغلب الموظفين بإبداء خدماتهم ولن يترددوا بتقديم أي معلومات لهذا الشخص المسؤول.
الاقناع	يستطيع المعتدي إقناع الموظف او مستخدم الحاسوب بطريقة مباشرة بحيث يقدم الحجج المنطقية والبراهين. وقد يستخدم طريقة غير مباشرة بحيث يعمد إلى تقديم إيحاءات نفسية تحث المستخدم على قبول المبررات دون تحليلها أو التفكير فيها ويحاول التأثير بهذه الطريقة من خلال إظهار نفسه بمظهر صاحب السلطة، أو إغراء المستخدم بامتلاك خدمة نادرة حيث يقدم له عرض معين من خلال موقعه الالكتروني لفترة محددة يمكنه ذلك من الحصول على كلمة المرور. وقد يلجأ المعتدي الإلكتروني لإبراز أوجه التشابه مع الشخص المستهدف لإقناعه بأنه يحمل نفس الصفات والاهتمامات فيصبح الشخص اكثر ارتياحًا وأقل حذرًا للتعامل معه فيقدم له ما يريد من معلومات.

الفصل الثاني : أمن الإنترنت

١) علل : انتشار البرامج والتطبيقات بشكل كبير منها ما هو مجاني ومنها ما هو غير معروف المصدر ومنها ما هو مفتوح أي أنه يمكن استخدامه على الأجهزة المختلفة
وذلك بسبب اعتماد الأفراد والمؤسسات والحكومات على تكنولوجيا المعلومات والاتصالات بشكل واسع وفي شتى المجالات .

٢) علل :لا بد من إيجاد وسائل تعمل على حماية (الويب) والحد من الاعتداءات والأخطار التي تهددها
وذلك بسبب انتشار البرامج المقرصنة والمعلومات الخاصة بكيفية اقتحام المواقع .

٣) انتشرت البرامج و التطبيقات بشكل كبير على الإنترنت . أذكر انواع البرامج المنتشرة عبر الانترنت .
- البرامج المجانية .
- البرامج غير معروفة المصدر .
- البرامج المفتوحة : أي أنه يمكن استخدامه على الأجهزة المختلفة .

أولاً : الإعتداءات الإلكترونية على الويب

١) تتعرض تتعرض المواقع الإلكترونية لكثير من الاعتداءات الإلكترونية التي لا يحس بها المستخدم.
لانها غير مرئية.

٢) تتعرض المواقع الإلكترونية لكثير من الاعتداءات الإلكترونية التي لا يحس بها المستخدم كونها غير مرئية .اذكر أنواع / أمثلة على هذه الاعتداءات .
١. الاعتداء على متصفح الإنترنت (Browsers attack)
٢. الاعتداء على البريد الإلكتروني (E- mail attack)

١- الاعتداءات الإلكترونية على متصفحات الإنترنت :

١) وضح المقصود بمفهوم متصفح الإنترنت ؟
برنامج ينقل المستخدم إلى صفحة (الويب) التي يريدها بمجرد العنوان والضغط على زر الذهاب ويمكنه من مشاهدة المعلومات على الموقع .

٢) علل : يتعرض متصفح الإنترنت إلى الكثير من الأخطار .
لأنها قابلة للتغيير من دون ملاحظة ذلك من قبل المستخدم .

٣) يتعرض متصفح الإنترنت إلى الكثير من الأخطار لأنها قابلة للتغيير من دون ملاحظة ذلك من قبل المستخدم ويمكن أن يتم هذا الاعتداء بطريقتين ، اذكرهما ؟

أ- الاعتداء عن طريق (كود) بسيط يمكن إضافته إلى المتصفح وباستطاعته القراءة والنسخ وإعادة إرسال أي شيء يتم إدخاله من قبل المستخدم ويتمثل التهديد بالقدرة على الوصول إلى الحسابات المالية والبيانات الحساسة الأخرى .

ب- توجيه المستخدم إلى صفحة أخرى غير الصفحة التي يريدها

٢- الاعتداءات الإلكترونية على البريد الالكتروني

١) كيف تتم الاعتداءات الإلكترونية على البريد الالكتروني .

من خلال وصول الرسائل الإلكترونية المزيفة إلى البريد الإلكتروني .

٢) كيف يحاول المعتدي الإلكتروني التعامل مع الأشخاص القليلي الخبرة من خلال البريد الالكتروني . / أعط مثالاً على الاعتداءات الإلكترونية على البريد الالكتروني .

- حيث يقدم عروض شراء لمنتجات بعض المصممين بأسعار زهيدة أو رسائل تحمل عنوان كيف تصبح ثريا .
- وهذه الرسائل تحتوي روابط للمزيد من المعلومات يرجى الضغط عليه وغيرها من الرسائل المزيفة والمضللة التي تحتاج إلى وعي من المستخدم .

أولاً : تقنية تحويل العناوين الرقمية

١) وضح المقصود بمفهوم تقنية تحويل العناوين الرقمية .

هي التقنية التي تعمل على إخفاء العنوان الرقمي للجهاز في الشبكة الداخلية ليتوافق مع العنوان الرقمي المعطى للشبكة .

٢) علل: تسهم تقنية تحويل العناوين الرقمية في حماية جهاز الحاسوب من أي هجوم قد يشن عليه بناء على معرفة العناوين الرقمية.

لأن الجهاز الداخلي غير معروف بالنسبة إلى الجهات الخارجية

ملاحظة : تقنية تحويل العناوين الرقمية هي إحدى الطرائق المستخدمة لحماية المعلومات من الاعتداءات الإلكترونية .

٣) وضح كيف تتم حماية المعلومات من الاعتداءات الإلكترونية .

١- **العناوين الرقمية الإلكترونية IP Address** .

١) **كيف يرتبط الأشخاص عبر شبكة الإنترنت .**

من خلال ملايين الأجهزة ولكل جهاز حاسوب أو هاتف خلوي عنوان رقمي خاص به يميزه عن غيره يسمى : ((Internet Protocol address (IP Address)).

٢) مم يتكون العنوان الرقمي الإلكتروني (IP address) .

يتكون من (٣٢) خانة ثنائية تتوزع على أربعة مقاطع يفصل بينها نقاط وهذا ما يسمى بـ ip4 وكل مقطع من هذه المقاطع يتضمن رقم من (0) إلى (255) كالآتي :

215.002.004.216

٣) وضح المقصود ب (IP4) / (IP Address) .
هو عنوان رقمي لأجهزة الحاسوب أو الهواتف الخلوية يتكون من ٣٢ خانة تتوزع على أربعة مقاطع يفصل بينها فواصل و كل مقطع من هذه المقاطع يتضمن رقم من (0) إلى (255) .

٤) ما هي نتائج التطور الهائل في أعداد مستخدمي الإنترنت على العناوين الرقمية الإلكترونية .
ظهرت الحاجة إلى عناوين إلكترونية أكثر وطورت هذه العناوين لما يسمى ipv6 الذي يتكون من ثمانية مقاطع بدلا من أربعة .

٥) علل : ظهور العناوين الإلكترونية IPV6 بدلاً من IP4 .
بسبب التطور الهائل في أعداد مستخدمي الإنترنت (زيادة أعداد مستخدمي الإنترنت)

٦) علل : ظهور تقنية تحويل العناوين الرقمية أو ما اصطلح على تسميته **(network address translation (nat))**
لأن ipv6 لا يكفي لإتاحة عدد هائل من العناوين الرقمية ولحل هذه المعضلة .

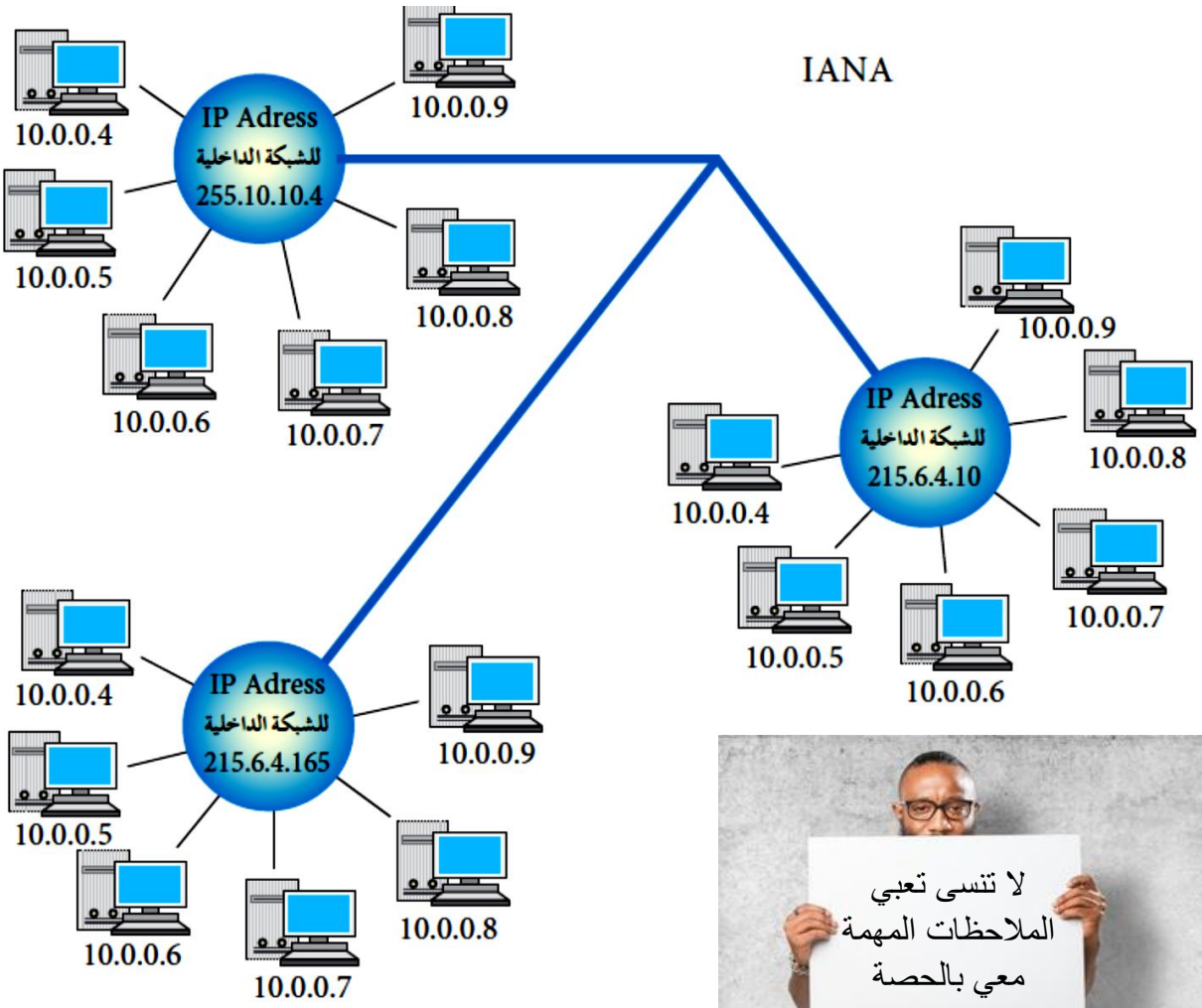
٧) كيف تم حل مشكلة IPV6 .
وجد ما يسمى تقنية تحويل العناوين الرقمية أو ما اصطلح على تسميته **(network address translation (nat))**

٢- مفهوم تقنية تحويل العناوين الرقمية nat

١) من هي السلطة المسؤولة عن منح أرقام الإنترنت المخصصة لإعطاء العناوين الرقمية للأجهزة على الإنترنت.
أيانا ((internet assigned number authority (iana)

٢) علل : تتمتع أيانا ((internet assigned number authority (iana) بالسلطة المسؤولة عن منح أرقام الإنترنت المخصصة .
لإعطاء العناوين الرقمية للأجهزة على الإنترنت.

٣) علل : تقوم أيانا بإعطاء الشبكة الداخلية عنوانا واحدا (أو مجموعة عناوين) ويكون معرفا لها عند التعامل في شبكة الإنترنت .
وبسبب قلة أعداد هذه العناوين مقارنة بعدد المستخدمين.



: العناوين الرقمية للشبكات والأجهزة.

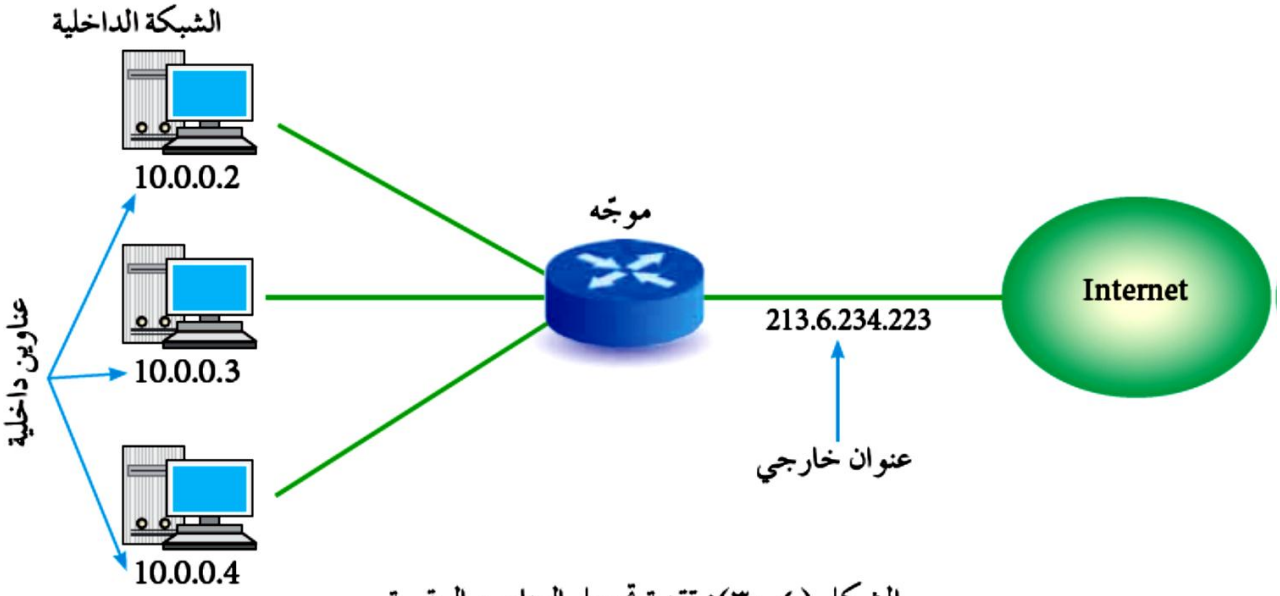
توضيح :

- نلاحظ من الشكل السابق وجود ثلاث شبكات داخلية وكل شبكة منحت عنوانا خاصا بها على الإنترنت مختلفا عن العناوين الأخرى مثلا العنوان 255.10.10.4 هو لشبكة على الإنترنت وهذا العنوان لا يمكن ان يمنح لشبكة أخرى وكذلك الأمر بالنسبة إلى العنوانين 215.6.4.10 و 215.6.4.165 .

- تعطي الشبكة الداخلية كل جهاز داخل الشبكة عنوانا رقميا لغرض الاستخدام الداخلي فقط ولا يعترف بهذا العنوان خارج الشبكة وهذا يعني أن العنوان الرقمي للجهاز داخل الشبكة يمكن أن يتكرر في أكثر من شبكة داخلية مثل العنوان (10.0.0.8) لكن العنوان الرقمي للشبكة الداخلية لن يتكرر.

- وعند رغبة أحد الأجهزة بالتواصل مع جهاز خارج الشبكة الداخلية يعدل العنوان الرقمي الخاص به باستخدام تقنية تحويل العناوين الرقمية (nat) وذلك يتم باستخدام جهاز وسيط يكون غالبا موجه أو جدارا ناريا يحول العنوان الرقمي الداخلي إلى **عنوان رقمي خارجي** ويسجل ذلك في سجل خاص للمتابعة

- يتم التواصل مع الجهاز الهدف في الشبكة الأخرى عن طريق هذا الرقم الخارجي على أنه العنوان الخاص بالجهاز المرسل وعندما يقوم الجهاز الهدف بالرد على رسالة الجهاز المرسل تصل إلى الجهاز الذي يحول **العنوان الرقمي الخارجي** إلى عنوان داخلي من خلال سجل المتابعة لديه ويعيده بذلك إلى الجهاز المرسل



الشكل (٤ – ٣): تقنية تحويل العناوين الرقمية.

٤) **علل : تعطي الشبكة الداخلية كل جهاز داخل الشبكة عنوانا رقميا .**
لغرض الاستخدام الداخلي فقط ولا يعترف بهذا العنوان خارج الشبكة

٥) **علل :العنوان الرقمي للجهاز داخل الشبكة يمكن أن يتكرر في أكثر من شبكة داخلية**
لانه مخصص الاستخدام الداخلي فقط ولا يعترف بهذا العنوان خارج الشبكة

٦) **علل : لا يمكن أن يتكرر العنوان الداخلي لاكثر من جهاز لنفس الشبكة .**
لان العنوان مخصص للتمييز بين الاجهزة في الاستخدام الداخلي فإذا تكرر لن نستطيع التمييز بين الأجهزة .

٧) **متى يتم التعديل على العنوان الرقمي الخاص بالجهاز .**
عند رغبة أحد الأجهزة بالتواصل مع جهاز خارج الشبكة الداخلية .

٨) **كيف يتم التعديل على العنوان الرقمي الخاص بالجهاز .**
باستخدام تقنية تحويل العناوين الرقمية (nat) وذلك يتم باستخدام جهاز وسيط يكون غالبا موجه أو جدارا ناريا يحول العنوان الرقمي الداخلي إلى **عنوان رقمي خارجي** ويسجل ذلك في سجل خاص للمتابعة .

٩) وضح المقصود بتقنية تحويل العناوين الرقمية (nat) .
هي تقنية تستخدم للتعديل على العنوان الرقمي الخاص بالجهاز عند رغبته بالتواصل مع جهاز خارج الشبكة الداخلية . وذلك يتم باستخدام جهاز وسيط يكون غالبا موجه أو جدارا ناريا يحول العنوان الرقمي الداخلي إلى **عنوان رقمي خارجي** ويسجل ذلك في سجل خاص للمتابعة .

١٠) ما هي الأجهزة التي يقوم بتحويل العناوين الرقمية / ما هي الأجهزة التي يتم من خلالها الإتصال مع الاجهزة الخارجية .
موجه أو جدارا ناريا

١١) ما وظيفة الموجه أو الجدار الناري .
يحول العنوان الرقمي الداخلي إلى **عنوان رقمي خارجي** ويسجل ذلك في سجل خاص للمتابعة .

٣- آلية عمل تقنية تحويل العناوين الرقمية

١) اذكر الطرق التي تعمل بها تقنية تحويل العناوين الرقمية ؟
أ- **النمط الثابت للتحويل** : ويتم عن طريق هذا النمط تخصيص عنوان رقمي خارجي لكل جهاز داخلي وهذا العنوان الرقمي ثابت لا يتغير .

كل جهاز إلو رقمين (رقم للإستخدام الداخلي و رقم للإستخدام الخارجي) .

ب- النمط المتغير للتحويل :
١) وضح آلية عمل النمط المتغير للتحويل .
- يكون لدى الجهاز الوسيط عدد من العناوين الرقمية الخارجية ولكنها غير كافية لعدد الأجهزة في الشبكة .
- هذه العناوين تبقى متاحة لجميع الأجهزة على الشبكة .
- وعند رغبة أحد الأجهزة بالتراسل خارجيا فانه يتواصل مع الجهاز الوسيط الذي يعطيه عنوانا خارجيا مؤقتا يستخدمه لحين الانتهاء من عملية التراسل خارجيا مؤقتا يستخدمه ويعد هذا العنوان عنوانا رقميا خاصا بالجهاز
- عند انتهاء عملية التراسل يفقد الجهاز الداخلي هذا العنوان ويصبح العنوان متاحا للتراسل مرة أخرى
- وعند رغبة الجهاز نفسه بالتراسل مرة أخرى قد يعطى عنوانا مختلفا عن المرة السابقة وهذا ما يفسر اختلاف IP Address للجهاز نفسه عند تراسله أكثر من مرة .

٢) أين توجد العناوين الرقمية الخارجية في النمط المتغير للتحويل .
لدى الجهاز الوسيط

٣) علل (فسر) : اختلاف IP Address للجهاز نفسه عند تراسله أكثر من مرة في النمط المتغير للتحويل .

لأن العناوين تكون مخزنة لدى الجهاز الوسيط و عند القيام بعملية التراسل خارجياً يأخذ المرسل العنوان المتاح و يرسل فيه و عند رغبته بالارسال مرة أخرى من الممكن أن يكون العنوان الذي أخذه في المرة السابقة غير متوفر و بالتالي يأخذ عنواناً آخر .

أسئلة الفصل الثاني- أمن الانترنت:

1- تم إيجاد وسائل تقنية لحماية الويب، علل ذلك.

للحد من الاعتداءات والأخطار التي تهدده بسبب انتشار البرامج المقرصنة والمعلومات الخاصة بكيفية اقتحام المواقع.

2- ما هي أشهر الاعتداءات على الويب؟

أ- الاعتداءات الالكترونية على متصفحات الانترنت.

ب-الاعتداءات الالكترونية على البريد الالكتروني.

3- حدد نوع الاعتداء في كل مما يأتي:

أ- توجيه المستخدم إلى صفحة أخرى غير الصفحة التي يريدها اعتداء على متصفح الانترنت.

ب-كود بسيط يُمكن إضافته إلى المتصفح وباستطاعته القراءة، والنسخ، واعادة الارسال لأي شيء يتم إدخاله من قبل المُستخدم. اعتداء على متصفح الانترنت

ج- يتضمن عروض وهمية ومضللة ويحتوي رابط يتم الضغط عليه للحصول على معلومات إضافية. اعتداءات على البريد الالكتروني.

4- وضح ما يأتي:

- **تحدث اعتداءات على الويب من خلال البريد الالكتروني.**

لأن بعض الرسائل الالكترونية التي تحمل عروضًا وهمية وروابط تحمل عناوين جذابة وتكون مُزيفة ولا يمكن اكتشافها من خلال الاشخاص قليلي الخبرة والتي تحمل روابط لنقل المستخدم لصفحات اخرى.

- **تُحافظ تقنية تحويل العناوين الرقمية على أمن المعلومات في الويب، وضح ذلك.**

من خلال إخفاء العنوان الرقمي الداخلي لجهاز الحاسوب فيمنع ذلك من الاعتداء عليه.

5- ما الفرق بين العناويين الرقمية IP4و IPv6 .

IP4 : تتكون من أربع مقاطع.

IPv6: تتكون من ثمانية مقاطع.

6- من المانح لأرقام الانترنت المخصصة لإعطاء العناوين الرقمية.

السلطة المسؤولة عن منح ارقام الانترنت المخصصة لإعطاء العناوين الرقمية للاجهزة على الانترنت هي أيانا.

7- ما وظيفة الجهاز الوسيط سواء أكان موّجه أو جدار ناري.

يقوم بتحويل العنوان الرقمي الداخلي إلى عنوان رقمي خارجي.

8- قارن بين طريقتي العمل لكل من:

النمط الثابت لتحويل العناوين الرقمية والنمط المتغير لتحويل العناوين الرقمية.

النمط الثابت لتحويل العناوين الرقمية: يقوم بتخصيص عنوان رقمي خارجي لكل جهاز داخلي وهذا العنوان الرقمي ثابت لا يتغير.

النمط المتغير لتحويل العناوين الرقمية: يتم اعطاء الجهاز عنوان رقمي مؤقت للتواصل مع الاجهزة خارج الشبكة وحين انتهاء الإتصال يُصبح هذا الرقم مُتاحًا لأي جهاز أخر.

الفـصـل الثـالـث : التـشفيـر

١) علل : تم إيجاد الوسائل التي يمكن نقل الرسالة عن طريقها والمحافظة على سريتها في الوقت نفسه . / علل : لا بد من إيجاد طرائق لحماية المعلومات .

بسبب ظهور الحاجة للحفاظ على سرية المعلومات منذ قدم البشرية في المجالين العسكري والدبلوماسي خاصة .

أولاً : مفهوم علم التشفير وعناصره

١- مفهوم التشفير والهدف منه

١) وضح المقصود بالتشفير .

التشفير هو تغيير محتوى الرسالة الأصلية سواء أكان التغيير بمزجها بمعلومات أخرى ،أم استبِدال الأحرف الأصلية والمقاطع بغيرها ،ام تغيير لمواقع الأحرف بطريقة لن يفهمها إلا مُرسل الرسالة ومُستقبِلها فقط، باستخدام خوارزمية معيّنة ومفتاح خاص

٢) كيف يتم تغيير محتوى الرسالة الأصلية / كيف يتم التشفير .

- بمزجها بمعلومات أخرى .
- استبِدال الأحرف الأصلية والمقاطع بغيرها .
- تغيير لمواقع الأحرف بطريقة لن يفهمها إلا مُرسل الرسالة ومُستقبِلها فقط، باستخدام خوارزمية معيّنة ومفتاح خاص

٣) ما هدف التشفير.

- الحفاظ على سرّية المعلومات في أثناء تبادلها بين مُرسل المعلومة ومُستقبِلها .
- عدم الاستفادة منها أو فهم محتواها؛ حتى لو تم الحصول عليها من قِبَل أشخاص معترضين.

٤) علل : يُعدّ التشفير من أفضل الطرق المُستخدمة للحفاظ على أمن المعلومات .

لان التشفير يهدف إلى الحفاظ على سرّية المعلومات في أثناء تبادلها بين مُرسل المعلومة ومُستقبِلها ،وعدم الاستفادة منها أو فهم محتواها؛ حتى لو تم الحصول عليها من قِبَل أشخاص معترضين

٢- عناصر عملية التشفير :

١) أذكر عناصر التشفير .

أ- خوارزمية التشفير:

الخوارزمية : مجموعة من الخطوات المتسلسلة منطقيًّا ورياضيًّا لحلّ مشكلة ما.

خوارزمية التشفير : مجموعة الخطوات المُستخدمة لتحويل الرسالة الأصلية إلى رسالة مُشفّرة، وسنتحدث عنها بالتفصيل لاحقًا.

ب- مفتاح التشفير(Key): وهو سلسلة الرموز المُستخدمة في خوارزمية التشفير، وتعتمد قوة التشفير على قوة هذا المفتاح.

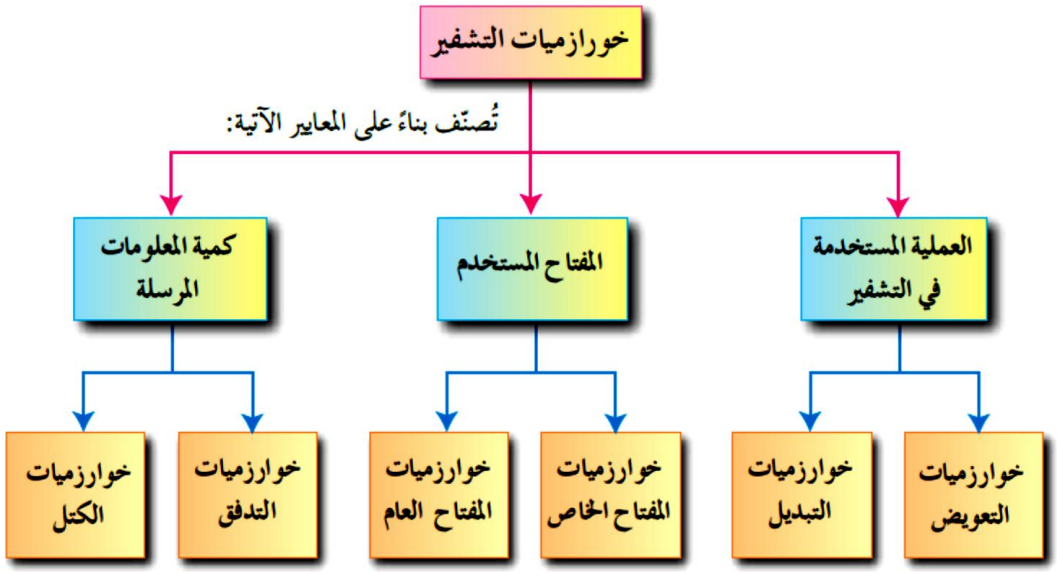
جـ- النص الأصلي(Plain Text): يُقصد بها محتوى الرسالة الأصلية قبل التشفير. وبعد عملية فكّ التشفير.

د - نص الشيفرة(Cipher Text): الرسالة بعد عملية التشفير.

ثانياً : خوارزميات التشفير

١) أذكر معايير تصنيف خوارزميات التشفير .

- استخدام المفتاح.
- كمية المعلومات المُرسلة.
- العملية المُستخدمة في عملية التشفير.



الشكل (٤– ٤): أنواع الخوارزميات.

١- التشفير المعتمد على نوع عملية التشفير :

١) يقسم التشفير المعتمد على نوع عملية التشفير إلى نوعين . أذكرهما .

- **تشفير التعويض:** طريقة لتشفير النصوص ، وتعني استبدال حرف مكان حرف أو مقطع مكان مقطع . ومثال عليها شيفرة الإزاحة .

- **تشفير التبديل :** طريقة تشفيرتقوم على تبديل أماكن الأحرف، وذلك عن طريق إعادة ترتيب أحرف الكلمة؛ بشرط استخدام الأحرف نفسها من دون إجراء أي تغيير عليها . **و** مثال عليها : خوارزمية الخط المتعرج .

٢) أذكر عمليات التشفير .

- **عملية التشفير :** اخفاء معنى النص الحقيقي . و تكون عند المرسل
- **عملية فك التشفير :** استرجاع النص الأصلي من النص المشفر . و تكون عند المستقبل .

خوارزمية الخط المتعرج (Zig Zag Cipher)

١) أذكر مميزات خوارزمية الخط المتعرج .

أ) خوارزمية سهلة وسريعة.

ب) يمكن تنفيذها يدويًّا باستخدام الورقة والقلم .

ج) يمكن فكّ تشفيرها بسهولة.

أ) **التشفير باستخدام خوارزمية الخط المتعرج .**

للقيام بتشفير النص حسب خوارزمية الخط المتعرج، اتبع الخطوات الآتية:

١ . حدّد عدد الأسطر التي ستُستخدم لتشفير النص. حيث إن عدد الأسطر يُعدّ مفتاح التشفير، ولا يلزمنا معرفة عدد الأعمدة (ابدأ بأي عدد من الأعمدة ويمكن الزيادة عند الحاجة)

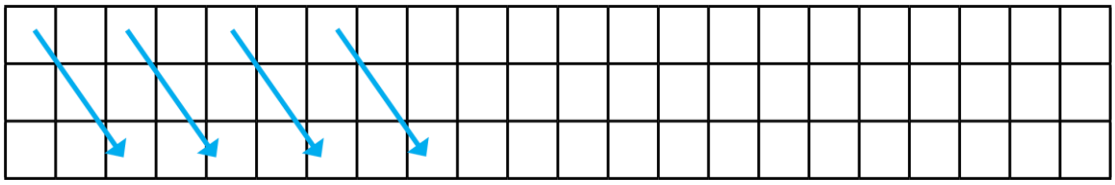
لاحظ : مفتاح التشفير يتم الاتفاق عليه مسبقًا من قِبَل مُرسل الرسالة ومُستقبِلها فقط. وسيتم تزويدك به في الامتحان لغايات حلّ السؤال.

٢ . املأ الفراغ في النص الأصلي بمثلث مقلوب ▽.

لاحظ : استخدام المثلث المقلوب بديلاً للفراغ لغايات تسهيل الحل فقط.

٣ . أنشىء جدولاً يعتمد على عدد الأسطر (مفتاح التشفير)

٤ . وزّع أحرف النص المراد تشفيره بشكل قطري، حسب اتجاه الأسهم.



٥. ضع مثلث مقلوبًا ∇ في الفراغ الأخير، وذلك كي تكون الأطوال متساوية .

٦. اكتب النص المُشفّر سطرًا سطرًا.

مثال (١) : شفّر النص الآتي، علمًا بأن مفتاح التشفير سطران.

I love my country

الحل : لإيجاد النص المُشفّر للنص السابق، اتبع الخطوات الآتية:

أ - حدّد مفتاح التشفير وهو سطران.

ب- املأ الفراغ بالنص الأصلي بمثلث مقلوب ∇ .

النص الأصلي: I ∇ love ∇ my ∇ country

جـ- أنشىء جدولاً، علمًا بان عدد الصفوف = 2.

د - وزّع أحرف النص بشكل قطري، حسب اتجاه الأسهم.

I		1		v		∇		y		c		u		t		y	
	∇		o		e		m		∇		o		n		r		

هـ - ضع مثلثًا مقلوبًا ∇ في الفراغ الأخير، وذلك كي تصبح الأطوال متساوية.

I		I		v		∇		y		c		u		t		y	
	∇		o		e		m		∇		o		n		r		∇

و - اكتب النص الـمُشفّر سطرًا سطرًا.

النص الأصلي : I love my country

النص الـمُشفر: Ilv ∇ ycuty ∇ oem ∇ onr

Ilv ycuty oem onr

نلاحظ بأن النص الـمُشفّر أخفى الرسالة، ولن يستطيع أي شخص متطفل أن يفهم محتواها.

لاحظ :

١- يمكن تشفير أحرف اللغة العربية باستخدام هذه الخوارزميات، ولكنها غير مطلوبة في امتحان الثانوية العامة.

٢- لا يُطلب إلى الطلبة في امتحان الثانوية العامة تشفير نص يحتوي على علامات ترقيم.

مثال (٢) :

أوجد النص الـمُشفّر للنص الأصلي الآتي، علمًا بان مفتاح التشفير هو خمسة أسطر.

Stay positive this year makes you happy all life

الحل :

لتشفير النص السابق، اتبع الخطوات الآتية:

أ - حدّد مفتاح التشفير وهو خمسة أسطر، وتذكّر بأنه لا يلزمنا معرفة عدد الأعمدة .

ب- املأ الفراغ بالنص الأصلي بمثلث مقلوب ∇ .

Stay ∇ positive ∇ this ∇ year ∇ makes ∇ you ∇ happy ∇ all ∇ life

جـ- أنشىء جدولاً مكوّنًا من خمس أسطر ،أضف عددًا من الأعمدة عند الحاجة.

د - وزّع الأحرف بشكل قطري، حسب اتجاه الأسهم.

Stay ∇ positive ∇ this ∇ year ∇ makes ∇ you ∇ happy ∇ all ∇ life

s		p		i		h		e		a		y		a		a		i		
	t		o		v		i		a		k		o		p		l		f	
		a		s		e		s		r		e		u		p		l		e
			y		i		∇		∇		∇		s		∇		y		∇	
				∇		t		t		y		m		∇		h		∇		l

هـ - ضع مثلثًا مقلوبًا ∇ في الفراغ الأخير، وذلك كي تصبح الأطوال متساوية.

s		p		i		h		e		a		y		a		a		i		
	t		o		v		i		a		k		o		p		l		f	
		a		s		e		s		r		e		u		p		l		e
			y		i		∇		∇		∇		s		∇		y		∇	∇
				∇		t		t		y		m		∇		h		∇		l	∇

و - نكتب النص المُشفّر سطرًا سطرً، ونرتّبه على التوالي.

السطر الأول	S p i h e a y a a i
السطر الثاني	t o v i a k o p l f
السطر الثالث	a s e s r e u p l e
السطر الرابع	y i ∇ ∇ ∇ s ∇ y ∇ ∇
السطر الخامس	∇ t t y m ∇ h ∇ l ∇

النص المشفر :

Spiheayaaitoviakoplfasesreupleyi ∇ ∇ ∇ s ∇ y ∇ ∇ ∇ ttym ∇ h ∇ l ∇

Spiheayaaitoviakoplfasesreupleyi s y ttym h l

نشاط (٤ - ١): التشفير باستخدام خوارزمية الخط المتعرج.

بالتعاون مع أفراد مجموعتك ،شفّر النصوص الآتية باستخدام خوارزمية الخط المتعرج

- **Stop thinking about your past mistakes**

مفتاح التشفير أربعة أسطر.

- **Never give up on your goals**

مفتاح التشفير ثلاثة أسطر. .

ب- عملية فكّ التشفير: للقيام بفك تشفير رسالة، اتبع الخطوات الآتية:

١ . املأ الفراغات بمثلث مقلوب.

٢ . قسّم النص المُشفّر إلى أجزاء، اعتمادًا على عدد الأسطر (مفتاح التشفير) .أي أن عدد الأجزاء يساوي عدد الأسطر. ولتحديد عدد الأحرف في كل جزء؛ نقوم بما يأتي:

مجموع أحرف النص المشفّر ÷ عدد الأجزاء (عدد الأسطر)

٣ . اكتب الحرف الأول من كل جزء، ثم الحرف الثاني، ثم الحرف الثالث وهكذا.

مثال (٣) : أوجد النص الأصلي للنص المُشفّر الآتي، علمًا بأن مفتاح التشفير سطران.

Ilv ycuty oem onr

الحل:

لإيجاد النص الأصلي، اتبع الخطوات الآتية:

أ - املأ الفراغات بمثلث مقلوب.

Ilv ∇ ycuty ∇ oem ∇ onr

ب- قسّم النص الـمُشفّر إلى جزأين؛ لأن مفتاح التشفير سطران .إذا كان الناتـج عددًا كسريًّا ،نقرّبه إلى أقرب عدد صحيح أكبر منه

١٧ ÷ ٢ = ٨,٥

٨,٥ عدد صحيح نقرّبه إلى العدد ٩. ومن ثم، فإن الجزء الأول يتكون من تسعة رموز.

الجزء الأول	I L v ∇ y c u t y
الجزء الثاني	∇ o e m ∇ o n r

جـ- نأخذ الحرف الأول من كلّ جزء بشكل عمودي (حرف I من الجزء الأول والمثلث المقلوب من الجزء الثاني)، ثم الحرف الثاني من كل جزء(l من الجزء الأول و o من الجزء الثاني)، نضمّها للأحرف السابقة وهكذا.

I ∇ love ∇ my ∇ country

النص الأصلي: I love my country

مثال (٤) : أوجد النص الأصلي للنص الـمُشفّر الآتي؛ باستخدام خوارزمية الخط المتعرج، علمًا بأن مفتاح التشفير هو خمسة أسطر.

النص الـمُشفّر:

Spiheayaaitoviakoplfasesreupleyi ∇ ∇ ∇ s ∇ y ∇ ∇ ∇ ttym ∇ h ∇ l ∇

الحل : لإيجاد النص الأصلي، قم بما يأتي:

أ - قسّم النص الـمُشفّر إلى أجزاء، اعتمادًا على عدد الأسطر (مفتاح التشفير) .

مفتاح التشفير = عدد الأسطر = خمسة

لتحديد حدد الأحرف في كل جزء، قم بـما يأتي:

عدد الأحرف في كل جزء = مجموع أحرف النص الـمُشفّر ÷ عدد الأجزاء

٥٠ ÷ ٥= ١٠ أحرف في كل جزء.

السطر الأول	S p i h e a y a a i
السطر الثاني	t o v i a k o p l f
السطر الثالث	a s e s r e u p l e
السطر الرابع	y i ∇ ∇ ∇ s ∇ y ∇ ∇
السطر الخامس	∇ t t y m ∇ h ∇ l ∇

ب- يؤخذ الحرف الأول من كل جزء: الحرف S من الجزء الأول، والحرف t من الجزء الثاني، وa من الجزء الثالث، و y من الجزء الرابع، والمثلث المقلوب من الجزء الخامس، ونضمّها إلى بعضها بعضاً، ثم الحرف الثاني من كل جزء، ثم الثالث وهكذا...

Stay ∇ positive ∇ this ∇ year ∇ makes ∇ you ∇ happy ∇ all ∇ life

النص الأصلي:

Stay positive this year makes you happy all life

نشاط (٤ - ٢) : فكّ التشفير باستخدام خوارزمية الخط المتعرج.

بالتعاون مع أفراد مجموعتك، فكّ تشفير النصوص الآتية باستخدام خوارزمية الخط المتعرج.

- **Bieno ∇ its ee ∇ ∇ uali ∇ lviyrbie ∇.**

علمًا بأن مفتاح التشفير ثلاثة أسطر.

- **Eoterkodnhmon ∇ u ∇ eemelci ∇ n ∇ siasmtdsgt ∇ o ∇ a ∇ hltvfrtt.**

مفتاح التشفير سبعة أسطر.

٢- التشفير المعتمد على المفتاح

١) على ماذا يعتمد التشفير المعتمد على المفتاح .

على عدد المفاتيح المستخدمة في عملية التشفير .

٢) على ماذا يعتمد أمن الرسالة أو المعلومة في التشفير المعتمد على المفتاح .

يعتمد على سرّية المفتاح، وليس على تفاصيل الخوارزمية .

٣) يقسم التشفير المعتمد على المفتاح إلى قسمين . اذكرهما .

أ - خوارزميات المفتاح الخاص (Private-key Algorithms):

١) **علل : يُطلق على خوارزميات المفتاح الخاص اسم الخوارزميات التناظرية./ يُطلق على خوارزميات** المفتاح الخاص اسم خوارزميات المفتاح السري.

لان المفتاح نفسه يُستخدم لعمِليتي التشفير وفكّ التشفير ،ويتم الاتفاق على اختياره قبل بدء عملية التراسل بين المُرسل والمُستقبِل .

٢) **أذكر أسماء اخرى لخوارزميات المفتاح الخاص .**

- الخوارزميات التناظرية .
- خوارزميات المفتاح السري .

ب - خوارزميات المفتاح العام(Public- Key Algorithms):

١) وضح آلية التشفير بالمفتاح العام .

- تستخدم هذِه الخوارزميات مفتاحين (مفتاح عام و مفتاح خاص)
- أحدهما يُستخدم لتشفير الرسالة ويكون معروفًا (للمُرسل والـمُستقبل) ويُسمّى المفتاح العام.
- والآخر يكون معروفًا لدى المستقبل فقط، ويُستخدم لفكّ التشفير ويُسمّى المفتاح الخاص.
- يتم انتاج المفتاحين خلال عمليات رياضية.
- ولا يُمكن معرفة المفتاح الخاص من خلال معرفة المفتاح العام.

٢) أذكر أسماء اخرى لخوارزميات المفتاح العام .

- الخوارزميات اللاتناظرية .

٣ - التشفير المعتمد على كمية المعلومات المرسلة

١) يُقسم التشفير المعتمد على كمية المعلومات المرسلة إلى قسمين. أذكرهما .

أ - شيفرات التدفق Stream Ciphers:

١) وضح آلية التشفير باستخدام شيفرات التدفق .

- يعمل هذا النوع من الخوارزميات على تقسيم الرسالة إلى مجموعة أجزاء
- ويشفّر كل جزء منها على حدة .
- ومن ثم يرسله.

ب- شيفرات الكتل Block Ciphers:

١) وضح آلية التشفير باستخدام شيفرات الكتل .

- تُقسم الرسالة أيضا إلى أجزاء ولكن بحجم أكبر من حجم الأجزاء في شيفرات التدفّق.
- ويشفّر أو يفكّ تشفير كل كتلة على حدة.
- يختلف عن شيفرات التدفق، بأن حجم المعلومات أكبر؛ لذا، فإنها أبطأ.

٢) علل : شيفرات الكتل أبطأ من شيفرات التدفق .

لأن حجم المعلومات المنقولة عبر الرسالة أكبر

أسئلة الفصل الثالث- التشفير:

1-وضح المقصود بكل من:

- **التشفير:** تغيير محتوى الرسالة الأصلية سواء أكان التغيير بمزجها بمعلومات أخرى او استبدال الأحرف الأصلية والمقاطع بغيرها او تغيير لمواقع الأحرف بطريقة لن يفهمها إلا مرسل الرسالة ومستقبلها فقط، باستخدام خوارزمية معينة ومفتاح خاص.
- **فك التشفير:** عمليات إعادة الرسالة المشفرة إلى المحتوى الأصلي.

2-فسر ما يأتي:

يُعتبر التشفير من أفضل الوسائل المُستخدمة للحفاظ على أمن المعلومات.

لإنه يعمل على إخفاء محتوى الرسالة عن الأشخاص غير المصرح لهم مشاهدتها وفي حال تم إيجادها من قبل أشخاص آخرين فلن يتمكنوا من فهم محتواها.

3- ما لهدف من علم التشفير، وما هي عناصره؟

يهدف علم التشفير إلى الحفاظ على سرية المعلومات أثناء تبادلها بين مرسل المعلومة ومستقبلها وعدم الاستفادة منها أو فهم محتواها حتى لو تم الحصول عليها من قِبل أشخاص معترضين.

عناصر علم التشفير:

خوارزمية التشفير، مفتاح التشفير، النص الأصلي، النص المُشفر.

4-حدد إلى أي من عناصر التشفير يتبع كل مما يأتي:

أ- مجموعة من الخطوات المُستخدمة لتحويل الرسالة الأصلية إلى رسالة مُشفرة

خوارزمية التشفير.

ب- الرسالة بعد عملية التشفير . النص المُشفر.

ج- سلسلة من الرموز التي تُستخدم من خلال خورازمية التشفير مفتاح التشفير.

د- الرسالة قبل عملية التشفير. النص الأصلي.

5-عدد المعايير التي يتم تصنيف خوارزميات التشفير بناءً عليها.

العملية المستخدمة في التشفير، المُفتاح المُستخدم، وكمية البيانات المرسلة.

6- ما الفرق بين طريقتي التشفير باستخدام عملية التبديل وعملية التعويض.

طرق تشفير التعويض: استبدال حرف مكان حرف أو مقطع مكان مقطع ومثال عليها شيفرة الإزاحة.

طرق تشفير التبديل: يتم فيها تبديل أماكن الأحرف، وذلك من خلال إعادة ترتيب احرف الكلمة بشرط استخدام نفس الأحرف دون إجراء أي تبديل أو تغيير عليها.

7- لماذا سُميت خوارزميات المفتاح الخاص بهذا الاسم؟

لأن نفس المفتاح يُستخدم لعمليتي التشفير وفك التشفير.

8-أوجد النص المُشفر لكل نص مما يأتي باستخدام خورازمية الخط المتعرج Zig Zag:

أ- Let us keep our home safe and united

علمًا بأن **مفتاح التشفير**: ثلاثة أسطر.

L		▽		▽		e		o		▽		m		s		e		n		u		t	
	e		u		k		p		u		h		e		a		▽		d		n		e
		t		s		e		▽		r		o		▽		f		a		▽		i		d

L▽▽ eo▽msenuteukpuhea▽dnetse▽ ro▽ fa▽ id▽

ب- Investing in people is more important than investing in things

علمًا بأن **مفتاح التشفير**: ثمانية أسطر.

I		g		p		o		r		a		t		t					
	n		▽		l		r		t		n		i		h				
		v		i		e		e		a		▽		n		i			
			e		n		▽		▽		n		i		g		n		
				s		▽		i		i		t		n		▽		g	
					t		p		s		m		▽		v		i		s
						i		e		▽		p		t		e		n	▽
							n		o		m		o		h		s	▽	▽

Igporattn ▽lrtnihvieea ▽nien ▽▽ nigns ▽iitn ▽gtpsm ▽visie ▽pten ▽nomohs ▽▽

9- فك تشفير النص الآتي مستخدمًا خوارزمية الخط المتعرج Zig Zag علمًا بأن مفتاح التشفير عشرة أسطر.

أ- النص المُشفر:

Tnr∇∇o∇eie∇t∇ndbhwvureeeci∇∇sagfmtthuu∇ittsioeutnn

أ- تقسيم النص إلى عشرة أجزاء.

عدد أحرف النص 50 حرف ÷ 10 = 5 أحرف في كل جزء.

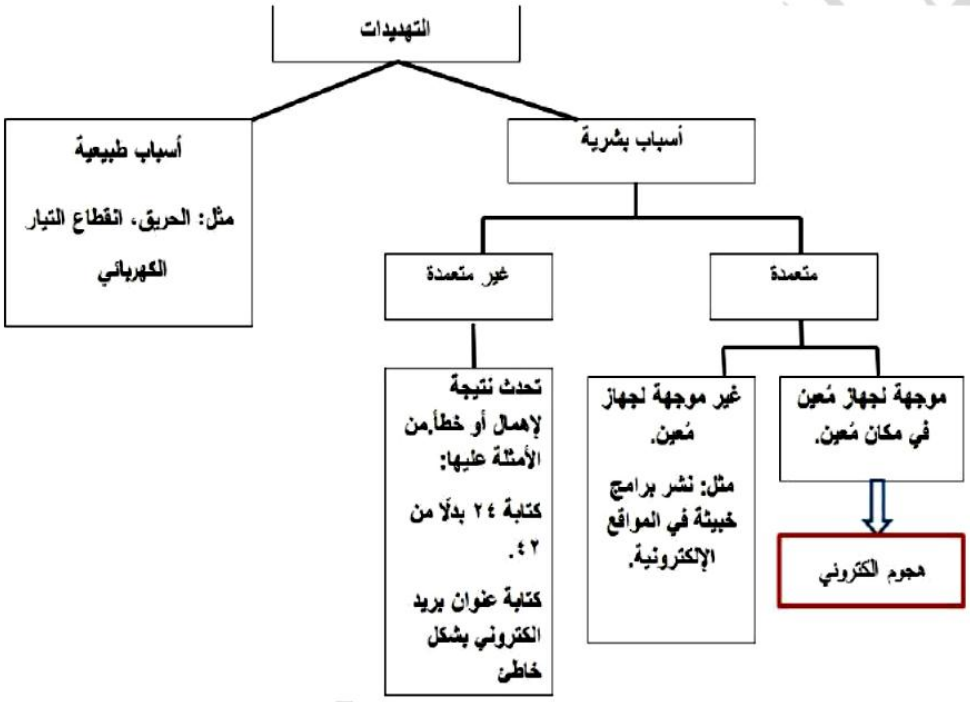
T n r ∇ ∇	الجزء الأول
o ∇ e i e	الجزء الثاني
∇ t ∇ n d	الجزء الثالث
b h w v u	الجزء الرابع
r e e e c	الجزء الخامس
i ∇ ∇ s a	الجزء السادس
g f m t t	الجزء السابع
h u u ∇ i	الجزء الثامن
t t s i o	الجزء التاسع
e u t n n	الجزء العاشر

ب- أخذ الحرف الأول من كل جزء لتشكيل النص الاصلي.

To∇brighten∇the∇future∇we∇must∇invest∇in∇education

أسئلة الوحدة

1- بناءً على دراستك لأنواع التهديدات أكمل الشكل الآتي:



2- وضح المقصود بالمفاهيم التالية؟

الهندسة الاجتماعية: **هي الوسائل والأساليب التي يستخدمها المعتدي الإلكتروني لجعل مستخدم الحاسوب في النظام يُعطي معلومات سرية أو يقوم بعمل ما أو التي يستخدمها ليتمكن من الوصول إلى أجهزة الحاسوب أو المعلومات المُخزنة فيها.**

السلامة: وتعني حماية الرسائل أو المعلومات التي تم تداولها والتأكد بأنها لم تتعرض لأي عملية تعديل سواءً: الإضافة، أو الاستبدال أو حذف جزء منها.

التشفير: هو تغيير محتوى الرسالة الأصلية سواء أكان التغيير بمزجها بمعلومات أخرى او استبدال الأحرف الأصلية والمقاطع بغيرها او تغيير لمواقع الأحرف بطريقة لن يفهمها إلا مرسل الرسالة ومستقبلها فقط، باستخدام خوارزمية معينة ومفتاح خاص.

3- عند تعرض المعلومات للهجمات الالكترونية يتأثر واحد أو أكثر من عناصر أمن المعلومات فيمايأتي بعض الاعتراضات للبيانات والمطلوب منك تحديد عناصر أمن المعلومات التي تتأثر بها.

أ- اعتراض الرسالة والتغيير على محتواها **سلامة المعلومات.**

ب- الهجوم المزور أو المفبرك **سرية المعلومات وسلامتها.**

ج- التنصت على المعلومات **سرية المعلومات.**

د- الإدعاء بأنه صديق ويحتاج إلى معلومات **سرية المعلومات وسلامتها.**

هـ- قطع قناة الاتصال **توافر المعلومات.**

4- فسر ، اختلاف IP address للجهاز عند تراسله أكثر من مرة.

بسبب النمط المتغير لتحويل العناوين الرقمية بحيث يتم إعطاء الجهاز عنوانًا رقميًا مختلفًا في كل مرة يتواصل فيها مع أجهزة خارج الشبكة الداخلية.

5- من المخاطر التي تُهدد الشبكات وجود الثغرات، اذكر ثلاث أمثلة عليها.

1-عدم تحديد صلاحيات الوصول الى المعلومات.

2-مشكلة في تصميم النظام او في مرحلة التنفيذ.

3-عدم كفاية الحماية المادية للأجهزة والمعلومات.

6- ما الوسائل التي يستخدمها المعتدي الالكتروني للتأثير على الجانب النفسي للشخص المستهدف؟

1- الاقناع 2- انتحال الشخصية

7- تعد الثغرات من المخاطر التي تهدد أمن المعلومات وضح ذلك

يُقصد بها نقطة الضعف في النظام سواء أكانت في الإجراءات المُتبعة مثل عدم تحديد صلاحيات الوصول الى المعلومات، أو مشكلة في تصميم النظام، كما أن عدم كفاية الحماية المادية للأجهزة والمعلومات تُعتبر من نقاط الضعف التي قد تتسبب في فقدان المعلومات أو هدم النظام أو تجعله عرضة للاعتداء الإلكتروني.

8- أوجد النص المُشفر لكل نص مما يأتي مستخدمًا خوارزمية الخط المتعرج Zig Zag:

أ- Youth is the future and the spirit of our home

علمًا بأن **مفتاح التشفير** أربعة أسطر.

Y		h		∇		∇		u		a		s		i		f		r		m	
	o		∇		t		f		r		n		p		t	∇		∇		e	
		u		i		h		u		e		d		i	∇		o		h		∇
			t		s		e		t		∇		∇		r		o		u		o

النص المشفر:

Yh∇∇ uasifrmo∇tfrnpt∇∇ euihuedi∇oh∇tset∇∇ rouo∇

ب- School is the place where great people and ideas are formed

علمًا بأن مفتاح التشفير ستة أسطر.

S		∇		e		e		e		t		l		∇		∇		o			
	c		i		∇		∇		∇		∇		e		i		a		r		
		h		s		p		w		g		p		∇		d		r		m	
			o		∇		l		h		r		e		a		e		e		e
				o		t		a		e		e		o		n		a		∇		d
					l		h		c		r		a		p		d		s		f	

S∇eeetl∇∇ oci ∇∇∇∇eiarhspwgp ∇drmo ∇lhreaeeeotaeeona ∇dlhcrapdsf ∇∇

9- فك تشفير كل نص من النصوص الآتية مستخدمًا خوارزمية الخط المتعرج Zig Zag علمًا بأن مفتاح التشفير ستة أسطر.

النص المُشفر:

Hwote ∇∇eoem∇esp∇meeupwl∇et∇s∇ee∇∇∇l∇iea∇shektts∇

عدد أحرف النص 48 حرف

48 ÷ 6 = 8 أحرف بكل سطر

H w o t e ∇ ∇ e	الجزء الأول
o e m ∇ e s p ∇	الجزء الثاني
m e e u p w l ∇	الجزء الثالث
e t ∇ s ∇ e e ∇	الجزء الرابع
∇ ∇ l ∇ i e a ∇	الجزء الخامس
s h e K t t s ∇	الجزء السادس

Home∇sweet∇home∇let∇us∇keep∇it∇sweet∇please

10- حدد أنواع خوارزميات التشفير إذا تم تقسيمها بناءً على المعايير الآتية:

أ- المفتاح المستخدم: **خوارزميات التشفير باستخدام المفتاح الخاص ، وخوارزميات التشفير باستخدام المفتاح العام.**

ب- كمية المعلومات المُرسلة: **شيفرات التدفق وشيفرات الكتل.**

ج- العملية المُستخدمة للتشفير: **التشفير بالتعويض أو التشفير بالتبديل.**