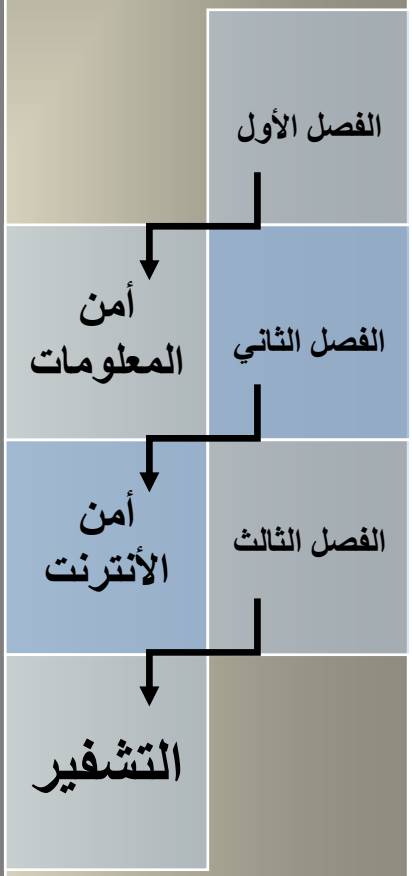
2017
2018

علوم الحاسوب

الوحدة الرابعة

أمن المعلومات والتشفير



المنهاج الجديد لمادة علوم الحاسوب

الثانوية العامة (التوجيهي)

إعداد : الأستاذ عبدالله الفقيه
إربد – 0777355388
aam.faqeeh@gmail.com

قائمة المحتويات
الوحدة الرابعة
أمن المعلومات والتشفير

الفصل الأول

أمن المعلومات

أولاً : مقدمة في أمن المعلومات

مفهوم أمن المعلومات : هو علم يعمل على حماية المعلومات والمعدات المستخدمة لتخزينها ومعالجتها ونقلها، من السرقة أو التطفل أو من الكوارث الطبيعية أو غيرها من المخاطر.

يعمل علم أمن المعلومات على إبقاء المعلومات متاحة للأفراد المصرح لهم باستخدامها.

خصائص أمن المعلومات الأساسية :-

1- سرية المعلومات.
وتعني أن الشخص المخول هو الوحيد القادر على الوصول إلى المعلومات والاطلاع عليها.
ومصطلح السرية مرادف لمفهومي الأمن والخصوصية.
وتعد المعلومات الشخصية، والموقف المالي لشركة ما قبل إعلانه، والمعلومات العسكرية؛ بيانات يعتمد أمنها على مقدار الحفاظ على سريتها.

2- سلامة المعلومات.
وتعني حماية الرسائل أو المعلومات التي تم تداولها، والتأكد بأنها لم تتعرض لأي عملية تعديل سواء بالإضافة أو الاستبدال أو حذف جزء منها.
على سبيل المثال عند نشر نتائج طلبة الثانوية العامة، لا بد من الحفاظ على سلامة هذه النتائج من أي تعديلات، وكذلك أيضاً عند صدور قوائم القبول الموحد للجامعات الأردنية والتخصصات التي قبل الطلبة فيها، فيجب من العمل على حماية هذه القوائم من أي تعديل أو حذف أو تبديل أو تغيير.

3- توافر المعلومات.
لا بد من أن تكون المعلومات متاحة ومتوافرة للأشخاص المصرح لهم بالتعامل معها وإلا كانت تلك البيات بدون فائدة، مهما كانت سرية ومحفوظة، وسيكون الوصول إليها يستهلك وقت كبير.
ومن الوسائل التي يقوم بها المخترقون (الهاكرز) بأن يجعلوا تلك البيانات غير متاحة، ويكون ذلك إما بحذفها أو الاعتداء على الأجهزة التي تخزن فيها هذه المعلومات.

المخاطر التي تهدد أمن المعلومات :-

1- التهديدات.

أ- أسباب طبيعية؛
- حدوث حريق.
- انقطاع التيار الكهربائي، وغيرها.

ب- أسباب بشرية؛
- غير متعمدة.
  1- نتيجة إهمال.
  2- نتيجة خطأ.
- متعمدة.
  1- موجهة لجهاز معين ويسمى هذا النوع (هجوم أو الاعتداء الإلكتروني).
  مثل سرقة جهاز الحاسوب، أو إحدى المعدات التي تحفظ المعلومات، أو التعديل على ملف أو حذفه، أو الكشف عن بيانات سرية أو منع الوصول إلى المعلومات.
  2- غير موجهة لجهاز معين، مثل نشر برامج خبيثة في المواقع الإلكترونية.

يعتمد نجاح الهجوم (الاعتداء) الإلكتروني، على عوامل رئيسية :-

1- الدافع. 2- الطريقة. 3- فرصة النجاح.

دوافع الأفراد لتنفيذ هجوم إلكتروني :-
أ- الحصول على مال.
ب- لإثبات القدرات التقنية.
ج- الإضرار الآخرين.

طرق تنفيذ الهجوم الإلكتروني تعتمد على :-
أ- المهارات التي يتميز بها المعتدي الإلكتروني.
ب- قدرته على توفير المعدات والبرمجيات التي يحتاج إليها.
ج- معرفته بتصميم النظام وآلية عمله.
د- معرفة نقاط القوة والضعف لهذا النظام.

فرصة نجاح الهجوم الإلكتروني تعتمد على :-
أ- تحديد الوقت المناسب للتنفيذ.
ب- كيفية الوصول إلى الأجهزة.

أنواع الاعتداءات التي قد تتعرض لها المعلومات :-

أ- التنصت على المعلومات؛
والهدف منها الحصول على المعلومات السرية، حيث يتم الإخلال بسريتها.

ب- التعديل على المحتوى؛
يتم اعتراض المعلومات وتغيير محتواها وإعادة إرسالها للمستقبل، من دون أن يعلم بتغيير محتواها، وفي هذا النوع يكون الإخلال بسلامة المعلومات.

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

د- الهجوم المزور أو المفبرك؛
يتمثل هذا النوع بإرسال المعتدي الإلكتروني رسالة إلى أحد الأشخاص على الشبكة، يخبره فيها بأنه صديقه ويحتاج إلى معلومات أو كلمات سرية خاصة. تتأثر بهذه لطريقة سرية المعلومات وقد تتأثر أيضاً سلامتها.

2- الثغرات.
ويقصد بها نقطة ضعف 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.

الحد من مخاطر أمن المعلومات
الحفاظ على المعلومات وأمنها (حسب رأي المختصون بهذا المجال)، ينبع من التوازن بين تكلفة الحماية وفعالية الرقابة من جهة، مع احتمالية الخطر من جهة أخرى.
لذلك تم وضع مجموعة من الضوابط لتقليل المخاطر التي تتعرض لها المعلومات والحد منها.

ضوابط تقليل المخاطر التي قد تتعرض لها المعلومات :-
1- الضوابط المادية؛
يقصد بها مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها، وذلك باستخدام الجدران والأسوار والأقفال، ووجود حراس الأمن وغيرها من أجهزة إطفاء الحريق.

2- الضوابط الإدارية؛
وتستخدم مجموعة من الأوامر والإجراءات المتفق عليها.
مثل: القوانين واللوائح والسياسات ، والإجراءات التوجيهية وحقوق النشر وبراءات الاختراع والعقود والاتفاقيات.

3- الضوابط التقنية؛
وهي الحماية التي تعتمد على التقنيات المستخدمة، سواء أكانت معدات مادية أم برمجيات.
مثل: كلمات المرور، ومنح صلاحيات الوصول، وبروتوكولات الشبكات والجدر النارية، والتشفير، وتنظيم تدفق المعلومات في الشبكة.

وللوصول إلى أفضل النتائج، تعمل الضوابط السابقة بشكل متكامل، للحد من الأخطار التي تتعرض لها المعلومات.

ثانياً : الهندسة الاجتماعية

العنصر البشري من أهم مكونات الأنظمة.

الاهتمام بالعنصر البشري من أهم المجالات للحفاظ على أمن المعلومات.

آلية اختيار الكادر البشري المسؤول عن حماية الأنظمة يعتمد على :-

- **الكفاية العلمية للكادر.**
- **الاختبارات الشفوية والورقية.**
- **المقابلات.**
- **اخضاع الكادر إلى ضغوط نفسية حسب مواقعهم.**

الخطوة السابقة يتم تنفيذها بهدف التأكد من قدرات الكادر على حماية النظام.

الهندسة الاجتماعية من أخطر ما يهدد نظم المعلومات.

مفهوم الهندسة الاجتماعية : هي وسائل وأساليب يستخدمها المعتدي الإلكتروني لجعل مستخدم الحاسوب في النظام يعطي معلومات سرية، أو يقوم بعمل ما يسهل عليه الوصول إلى أجهزة الحاسوب أو المعلومات المخزنة فيها.

تعتبر الهندسة الاجتماعية من أنجح الوسائل وأسهلها، التي تستخدم للحصول على معلومات غير مصرح بالاطلاع عليها؛ وذلك **بسبب** قلة اهتمام المتخصصين في مجال أمن المعلومات، وعدم وعي مستخدمي الحاسوب بالمخاطر المترتبة عليها.

مجالات الهندسة الاجتماعية :-

1- **البيئة المحيطة.**

أ- مكان العمل.

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

ب- الهاتف.

حيث يقوم الشخص غير المخول بمركز الدعم الفني هاتفياً، ويطلب منه بعض المعلومات الفنية ويستدرجه للحصول على كلمات المرور وغيرها من المعلومات ليستخدمها في ما بعد.

ج- النفايات الورقية.

حيث يدخل شخص من 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، ويمكن استغلالها في تتبع أعمال الموظفين أو الحصول على المعلومات المرغوبة.

د- الإنترنت.

وهي من أكثر الوسائل شيوعاً، وذلك بسبب استخدام بعض الموظفين أو مستخدمي الحاسوب عادة كلمة المرور نفسها لجميع التطبيقات، حيث ينشئ المعتدي الإلكتروني موقعاً على الشبكة، يقدم خدمات معينة، ويشترط التسجيل فيه للحصول على هذه الخدمات، ويتطلب التسجيل في الموقع اسم مستخدم وكلمة مرور، وهي كلمة المرور نفسها التي يستخدمها الشخص عادة وبهذه الطريقة يتمكن المعتدي الإلكتروني من الحصول عليها.

2- الجانب النفسي.

يسعى المعتدي الإلكتروني لكسب ثقة مستخدم الحاسوب.

ومن أشهر الأساليب التي يستخدمها المعتدي الإلكتروني للحصول على المعلومات التي يرغب بها :-

أ- **الإقناع.**

وذلك من خلال قدرة المعتدي الإلكتروني إقناع الموظف أو مستخدم الحاسوب بطريقة **مباشرة**، بحيث يقوم بتقديم الحجج المنطقية والبراهين.

وقد يستخدم طريقة **غير مباشرة** وذلك من خلال تقديم إيحاءات نفسية، تحث المستخدم على قبول المبررات من دون تحليلها أو التفكير في مصداقيتها، ويحاول التأثير بهذه الطريقة عن طريق إظهار نفسه بمظهر صاحب السلطة.

وقد يحاول بطريقة إغراء المستخدم بامتلاك خدمة نادرة، وذلك من خلال تقديم عرضاً معيناً بموقعه الإلكتروني مثلاً ولفترة محددة، مما يمكنه من الحصول على كلمة المرور.

وقد يلجأ المعتدي الإلكتروني إلى إبراز أوجه تشابه مع الشخص المستهدف، لإقناعه بأنه يحمل الصفات والاهتمامات نفسها، فيصبح بذلك هو الشخص الأكثر ارتياحاً لدى المستهدف يكون أقل حذراً في التعامل معه، فيقدم له ما يريد من المعلومات.

ب- **انتحال الشخصية والمداهنة.**

حيث يقوم المعتدي الإلكتروني بتقمص شخصية آخر، وهذا الشخص قد يكون شخصاً حقيقياً أو وهمياً.

مثل انتحال شخصية فني صيانة حاسوب، أو عامل نظافة أو حتى المدير أو السكرتير.

وبما أن الشخصية المنتحلة غالباً ما تكون ذات سلطة، فيبدي أغلب الموظفين خدماتهم، ولن يترددوا بتقديم أي معلومات لهذا الشخص على أنه المسؤول.

ج- **مسايرة الركب.**

حيث يرى الموظف بأنه إذا قام زملاؤه جميعهم بأمر ما، فمن غير اللائق أن يأخذ هو موقفاً مغايراً، فعندما يقدم شخص نفسه على أنه إداري من فريق الدعم الفني، ويرغب بعمل تحديثات على الأجهزة، فّذا سمح له أحد الموظفين بعمل تحديث على جهازه؛ فإن باقي الموظفين يقومون بمسايرة زميلهم غالباً، والسماح لهذا المعتدي الإلكتروني باستخدام أجهزتهم لتحديثها، ومن ثم يتمكن من الاطلاع على المعلومات التي يريدها والمخزنة على الأجهزة.

إجابات أسئلة الفصل الأول من الوحدة الرابعة (صفحة 138 + 139)

السؤال الأول

- هو علم يعمل على حماية المعلومات والمعدات المستخدمة لتخزينها ومعالجتها ونقلها، من السرقة أو التطفل أو من الكوارث الطبيعية أو غيرها من المخاطر.

- نقطة ضعف في النظام سواء أكانت في الإجراءات المتبعة، مثل عدم تحديد صلاحيات الوصول إلى المعلومات، أم مشكلة في تصميم النظام.

السؤال الثاني

أ- سلامة المعلومات. ب- سرية المعلومات.

ج- توافر المعلومات. د- سرية المعلومات.

هـ- سرية المعلومات.

السؤال الثالث

أ- الدافع. ب- الطريقة. ج- فرصة النجاح.

د- الدافع. هـ- الدافع. و- الطريقة.

السؤال الرابع

أ- التنصت على المعلومات. ب- التعديل على المحتوى.
ج- الإيقاف. د- الهجوم المزور أو المفبرك.

السؤال الخامس

أ- للحفاظ على المعلومات، وأمنها، والتقليل والحد من المخاطر التي قد تتعرض لها المعلومات.
ب- بسبب قلة اهتمام المتخصصين في مجال أمن المعلومات، وعدم وعي مستخدمي الحاسوب بالمخاطر المترتبة عليها.

السؤال السادس

وجه المقارنة	الضوابط المادية	الضوابط الإدارية
	مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية	مجموعة من الأوامر والإجراءات المتفق عليها
	الجدران ، الأسوار ، الأقفال ، حراس أمن ، أجهزة إطفاء حريق	القوانين واللوائح والسياسات ، الإجراءات التوجيهية ، حقوق النشر ، براءات الاختراع ، العقود والاتفاقيات

السؤال السابع

المجال	آلية العمل
	يكتب بعض الموظفين كلمات المرور على أوراق ملصقة بشاشة الحاسوب. **وعند دخول الشخص غير المخول له الاستخدام، كزبون أو عامل نظافة أو عامل صيانة، يستطيع معرفة كلمات المرور.** **ومن ثم يتمكن من الدخول إلى النظام ليحصل على المعلومات التي يريدها.**
	يقوم الشخص غير المخول بمركز الدعم الفني هاتفياً، ويطلب منه بعض المعلومات الفنية ويستدرجه للحصول على كلمات المرور وغيرها من المعلومات ليستخدمها في ما بعد.
	يقوم المعتدي الإلكتروني بتقمص شخصية آخر، وهذا الشخص قد يكون شخصاً حقيقياً أو وهمياً.
	من خلال قدرة المعتدي الإلكتروني إقناع الموظف أو مستخدم الحاسوب بطريقة مباشرة، بحيث يقوم بتقديم الحجج المنطقية والبراهين. **وقد يستخدم طريقة غير مباشرة وذلك من خلال تقديم إيحاءات نفسية، تحث المستخدم على قبول المبررات من دون تحليلها أو التفكير في مصداقيتها، ويحاول التأثير بهذه الطريقة عن طريق إظهار نفسه بمظهر صاحب السلطة.** **وقد يحاول بطريقة إغراء المستخدم بامتلاك خدمة نادرة، وذلك من خلال تقديم عرضاً معيناً بموقعه الإلكتروني مثلاً ولفترة محددة، مما يمكنه من الحصول على كلمة المرور.** **وقد يلجأ المعتدي الإلكتروني إلى إبراز أوجه تشابه مع الشخص المستهدف، لإقناعه بأنه يحمل الصفات والاهتمامات نفسها، فيصبح بذلك هو الشخص الأكثر ارتياحاً لدى المستهدف يكون أقل حذراً في التعامل معه، فيقدم له ما يريد من المعلومات.**

الفصل الثاني

أمن الإنترنت

انتشار البرامج والتطبيقات بشكل كبير وواسع وفي شتى المجالات يعود إلى اعتماد الأفراد والمؤسسات والحكومات على تكنولوجيا المعلومات والاتصالات.

هذه البرامج والتطبيقات منها ما هو مجاني، ومنها ما هو غير معروف المصدر، ومنها ما هو مفتوح (أي أنه يمكن استخدامه على الأجهزة المختلفة)، كما انتشرت البرامج المقرصنة والمعلومات الخاصة بكيفية اقتحام المواقع، فكان لا بد من إيجاد وسائل تعمل على حماية الإنترنت (الويب) والحد من الاعتداءات والأخطار التي تهددها.

أولاً : الاعتداءات الإلكترونية على الويب

تتصف الاعتداءات الإلكترونية التي تتعرض لها المواقع الإلكترونية بأنها غير مرئية لذلك لا يحس بها المستخدم.

من الأمثلة على هذه الاعتداءات الإلكترونية :-

1- الاعتداءات على متصفحات الإنترنت Browsers Attack.

متصفح الإنترنت : هو برنامج ينقل المستخدم إلى صفحة (الويب) التي يريدها بمجرد كتابة العنوان والضغط على زر الذهاب، ويمكنه من مشاهدة المعلومات على الموقع.

يتعرض متصفح الإنترنت للكثير من الأخطار لأنها قابلة للتغيير من دون ملاحظة ذلك من قبل المستخدم، ويمكن أن يتم هذا الاعتداء بطريقتين :-

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.

2- الاعتداءات الإلكترونية على البريد الإلكتروني E-mail Attack.

تصل الكثير من الرسائل الإلكترونية إلى البريد الإلكتروني، بعض هذه الرسائل الإلكترونية مزيفة، بعضها يسهل اكتشافه، وبعضها الآخر استخدم بطريقة احترافية.

يحاول المعتدي الإلكتروني التعامل مع الأشخاص قليلي الخبرة، حيث عروض شراء لمنتجات بعض المصممين بأسعار زهيدة أو رسائل تحمل عنوان كيف تصبح ثرياً، وهذه الرسائل تحتوي روابط يتم الضغط عليها للحصول على مزيد من المعلومات. وغيرها من الرسائل المزيفة والمضللة التي تحتاج إلى وعي من المستخدم.

ثانياً : تقنية تحويل العناوين الرقمية IP Addresses

وهي التقنية التي تعمل على عدم إظهار العنوان الرقمي للجهاز في الشبكة الداخلية، ليتوافق مع العنوان الرقمي المعطى للشبكة. وهذا يعني أن الجهاز الداخلي غير معروف بالنسبة إلى الجهات الخارجية وهذا يسهم في حمايته من أي هجوم قد يتم عليه بناء على معرفة العناوين الرقمية، وهذه هي إحدى الطرق المستخدمة لحماية المعلومات من الاعتداءات الإلكترونية.

- **العناوين الرقمية الإلكترونية IP Addresses**

يرتبط ملايين الأشخاص عبر شبكة الإنترنت بملايين الأجهزة، ولكل جهاز حاسوب أو هاتف لوي عنوان رقمي خاص به يميزه عن غيره يسمى :- Internet Protocol Address (IP Address).

ويتكون هذا العنوان الرقمي من 32 خانة ثنائية تتوزع على أربعة مقاطع يفصل بينها نقاط، ويسمى (IP4) وكل مقطع من هذه المقاطع يتضمن رقماً من 0 إلى 255 ، كالآتي :-
962.777.355.388

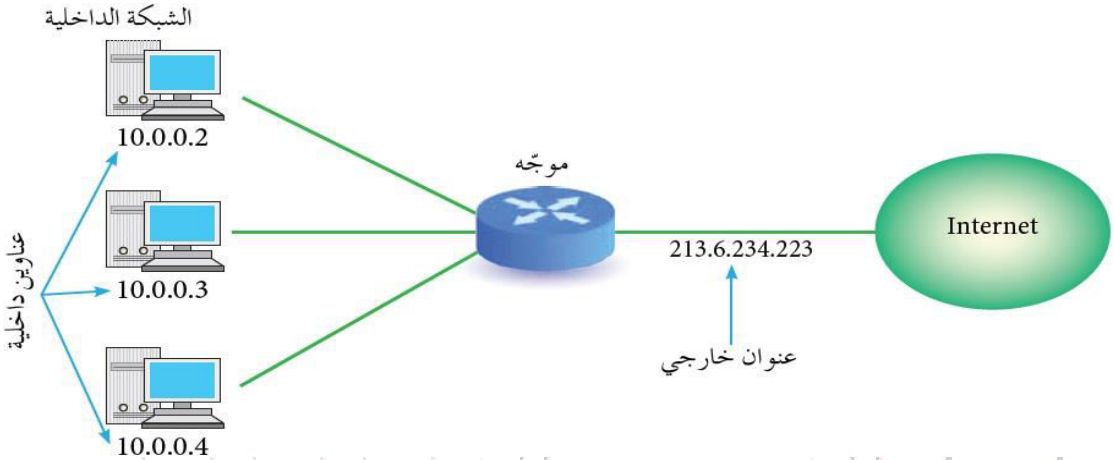
ونظراً للتطور الهائل في أعداد مستخدمي الإنترنت؛ ظهرت الحاجة إلى عناوين إلكترونية أكثر، وطورت هذه العناوين لما يسمى IPv6، الذي يتكون من ثمانية مقاطع بدلاً من أربعة.
وعلى الرغم من استخدام IPv6 إلا أنه لا يكفي لإتاحة عدد هائل من العناوين الرقمية، ولحل هذه المعضلة، وجد ما يسمى تقنية تحويل العناوين الرقمية أو **Network Address Translation(NAT)**.

- **مفهوم تقنية تحويل العناوين الرقمية NAT**

تتمتع أيانا ((Internet Assigned Numbers Authority (IANA) بالسلطة المسؤولة عن منح أرقام الإنترنت المخصصة لإعطاء العناوين الرقمية للأجهزة على الإنترنت.

وبسبب قلة أعداد هذه العناوين مقارنة بعدد المستخدمين، فإنها تعطي الشبكة الداخلية عنواناً واحداً أو مجموعة عناوين، ويكون معرفاً لها عند التعامل في شبكة الإنترنت.
تعطي الشبكة الداخلية كل جهاز داخل الشبكة عنواناً رقمياً **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**، بينما العنوان الرقمي للشبكة الداخلية لن يتكرر أبداً.
وعند رغبة أحد الأجهزة بالتواصل مع جهاز خارج الشبكة الداخلية، يتم تعديل العنوان الرقمي الخاص به، وذلك باستخدام تقنية تحويل العناوين الرقمية (IANA).
ويتم ذلك باستخدام جهاز وسيط، في الغالب يكون جهاز موجهاً (Router) أو جداراً نارياً (Firewall) 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 الوسيط الذي يحول العنوان الرقمي الخارجي إلى عنوان داخلي من خلال سجل المتابعة لديه، وبذلك إلى الجهاز المرسل، كما هو موضح في الشكل الآتي :-



- **آلية عمل تقنية تحويل العناوين الرقمية :-**

تعمل تقنية تحويل العناوين الرقمية بعدة طرق، منها :-

1- **النمط الثابت للتحويل :**

ويتم عن طريق هذا النمط تخصيص عنوان رقمي خارجي لكل جهاز داخلي، وهذا العنوان الرقمي ثابت لا يتغير.

2- **النمط المتغير للحويل :**

بهذه الطريقة 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 خارجياً؛ فإنه يتواصل مع الجهاز الوسيط الذي يعطيه عنواناً خارجياً مؤقتاً يستخدمه ل لحين الانتهاء عملية التراسل، ويفقد الجهاز الداخلي هذا العنوان، ويصبح العنوان متاحاً للتراسل مرة أخرى، وعند رغبة الجهاز نفسه بالتراسل مرة أخرى، قد يعطى عنواناً م مختلفاً عن المرة السابقة، وهذا ما يفسر اختلاف IP Address للجهاز نفسه عند تراسله أكثر من مرة.

إجابات أسئلة الفصل من الوحدة الرابعة (صفحة 145)

السؤال الأول

1- انتشار برامج القرصنة، والمعلومات الخاصة التي تشرح كيفية اقتحام المواقع.
2- للحد من الاعتداءات والأخطار التي تهدد الإنترنت.

السؤال الثاني

1- الاعتداءات الإلكترونية على متصفحات الإنترنت.
2- الاعتداءات الإلكترونية على البريد الإلكتروني.

السؤال الثالث

أ- اعتداءات إلكترونية على متصفحات الإنترنت.
ب- اعتداءات إلكترونية على متصفحات الإنترنت.
ج- اعتداءات إلكترونية على البريد الإلكتروني.

السؤال الرابع

أ- تصل الكثير من الرسائل الإلكترونية إلى البريد الإلكتروني، بعض هذه الرسائل الإلكترونية مزيفة، بعضها يسهل اكتشافه، وبعضها الآخر استخدم بطريقة احترافية.
يحاول المعتدي الإلكتروني التعامل مع الأشخاص قليلي الخبرة، حيث عروض شراء لمنتجات بعض المصممين بأسعار زهيدة أو رسائل تحمل عنوان كيف تصبح ثرياً، وهذه الرسائل تحتوي روابط يتم الضغط عليها للحصول على مزيد من المعلومات. وغيرها من الرسائل المزيفة والمضللة التي تحتاج إلى وعي من المستخدم.

ب- وهي التقنية التي تعمل على عدم إظهار العنوان الرقمي للجهاز في الشبكة الداخلية، ليتوافق مع العنوان الرقمي المعطى للشبكة. وهذا يعني أن الجهاز الداخلي غير معروف بالنسبة إلى الجهات الخارجية وهذا يسهم في حمايته من أي هجوم قد يتم عليه بناء على معرفة العناوين الرقمية، وهذه هي إحدى الطرق المستخدمة لحماية المعلومات من الاعتداءات الإلكترونية.

السؤال الخامس

IP4 يتكون من أربعة مقاطع، بينما IPv6 من ثمانية مقاطع.

السؤال السادس

أيانا IANA.

السؤال السابع

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 الوسيط الذي يحول العنوان الرقمي الخارجي إلى عنوان داخلي من خلال سجل المتابعة لديه، وبذلك إلى الجهاز المرسل.

السؤال الثامن

النمط الثابت للتحويل :

ويتم عن طريق هذا النمط تخصيص عنوان رقمي خارجي لكل جهاز داخلي، وهذا العنوان الرقمي ثابت لا يتغير.

النمط المتغير للحويل :

بهذه الطريقة 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 خارجياً؛ فإنه يتواصل مع الجهاز الوسيط الذي يعطيه عنواناً خارجياً مؤقتاً يستخدمه لحين الانتهاء عملية التراسل، ويفقد الجهاز الداخلي هذا العنوان، ويصبح العنوان متاحاً للتراسل مرة أخرى. وعند رغبة الجهاز نفسه بالتراسل مرة أخرى، قد يعطى عنواناً مختلفاً عن المرة السابقة، وهذا ما يفسر اختلاف IP Address للجهاز نفسه عند تراسله أكثر من مرة.

الفصل الثالث
التشفير

أولاً : مفهوم علم التشفير وعناصره

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

أهداف التشفير :-

1- الحفاظ على سرية المعلومات في أثناء تبادلها بين مرسل المعلومة ومستقبلها.
2- عدم الاستفادة من الرسالة أو فهم محتواها، حتى لو تم الحصول عليها من قبل أشخاص معترضين.

يعد التشفير من أفضل الطرق المستخدمة للحفاظ على أمن المعلومات، حيث يعمل على إخفائها عن الأشخاص غير المصرح لهم بالاطلاع عليها.

عناصر عملية التشفير :-

1- خوارزمية التشفير.

تعلمت سابقاً أن الخوارزمية هي مجموعة من الخطوات المتسلسلة منطقياً ورياضياً لحل مشكلة ما. **خوارزمية التشفير** : هي مجموعة من الخطوات المستخدمة لتحويل الرسالة الأصلية إلى رسالة مشفرة.

2- مفتاح التشفير.

وهو سلسلة من الرموز المستخدمة في خوارزمية التشفير.
وتعتمد قوة التشفير على قوة المفتاح المستخدم.

3- النص الأصلي.

يقصد بها محتوى الرسالة الأصلية قبل التشفير، وهو أيضاً النص الناتج بعد عملية فك التشفير.

4- نص الشيفرة.

وهو نص الرسالة بعد تنفيذ عملية التشفير.

ثانياً : خوارزميات التشفير

يتم تصنيف خوارزميات التشفير بناء على عدة معايير منها :-

- استخدام المفتاح.
- كمية المعلومات المرسلة.
- العملية المستخدمة في عملية التشفير.

بعض أنواع خوارزميات التشفير :-

- **(حسب معيار استخدام المفتاح)**

تعتمد هذه الأنواع على عدد المفاتيح المستخدمة في عملية التشفير، وعليه فإن أمن الرسالة أو المعلومة يعتمد على سرية المفتاح، وليس على تفاصيل الخوارزمية.

- خوارزميات المفتاح الخاص.

يطلق على هذا النوع اسم **الخوارزميات التناظرية**، وذلك لأن المفتاح نفسه يستخدم لعمليتي التشفير وفك التشفير، ويتم الاتفاق على اختياره قبل بدء عملية التراسل بين المرسل والمستقبل، لذا تسمى أيضاً **خوارزميات المفتاح السري**.

- خوارزميات المفتاح العام.

يستخدم هذا النوع من الخوارزميات مفتاحين، أحدهما يستخدم لتشفير الرسالة ويكون معروفاً للمرسل والمستقبل ويسمى المفتاح العام.

والآخر يستخدم لفك التشفير ويكون معروفاً للمستقبل فقط، ويسمى المفتاح الخاص.

ويتم انتاج المفتاحين من خلال عمليات رياضية، ولا يمكن معرفة المفتاح الخاص من خلال المفتاح العام، ويطلق على هذا النوع أيضاً اسم **الخوارزميات اللا تناظرية**.

- **(حسب معيار كمية المعلومات المرسلة)**

- خوارزميات التدفق (شيفرات التدفق).

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

- خوارزميات الكتل (شيفرات الكتل).

يقوم هذا النوع من الخوارزميات بتقسيم الرسالة إلى أجزاء (بحجم أكبر من خوارزميات التدفق مما يجعلها أبطأ)، ويشفر أو يفك تشفير كل كتلة على حدة.

- **(حسب معيار العملية المستخدمة في التشفير)**

- خوارزميات التعويض.

تعني هذه الطريقة استبدال حرف مكان حرف أو مقطع مكان مقطع، مثل طريقة شيفرة الإزاحة.

- خوارزميات التبديل.

بهذه الطريقة يتم تبديل أماكن الأحرف نفسها من دون إجراء أي تغيير عليها.

عند تنفيذ عملية التبديل يختفي معنى النص الحقيقي، وهذا يشكل عملية التشفير، شريطة أن تكون قادراً على استعادة النص الأصلي منها، وهذا ما يسمى عملية فك التشفير.

أحد أنواع خوارزميات التبديل هي خوارزمية الخط المتعرج ،،،

خوارزمية الخط المتعرج Zig Zag Cipher

تتميز هذه الخوارزمية بأنها سهلة وسريعة ويمكن تنفيذها يدوياً باستخدام الورقة والقلم، كما أنه يمكن فك تشفيرها بسهولة.

ـ خطوات التشفير :-

1- حدد عدد الأسطر التي ستستخدم لتشفير النص، حيث ان عدد الأسطر يعد مفتاح التشفير، ولا يلزمنا معرفة عدد الأعمدة (ابدأ بأي عدد من الأعمدة ويمكن الزيادة عن الحاجة).

ملاحظة : مفتاح التشفير يتم الاتفاق عليه مسبقاً بين المرسل والمستقبل فقط. ولكن سيتم تزويدنا به لغايات حل السؤال.

2- املأ الفراغ في النص الأصلي بمثلث مقلوب ▽.

ملاحظة : استخدام المثلث المقلوب بديلاً للفراغ فقط للتسهيل في الحل.

3- أنشئ جدولاً يعتمد على عدد الأسطر (مفتاح التشفير).

4- وزع أحرف النص المراد تشفيره بشكل قطري ↘، حسب اتجاه الأسهم.

5- ضع مثلثاً مقلوباً في الفراغ الأخير، وذلك كي تكون الأطوال متساوية.

6- أكتب النص المشفر سطراً، سطراً.

مثال :

شفر النص الآتي، علماً أن مفتاح التشفير سطران. I Love my country

الحل :

نتبع الخطوات السابقة، كالآتي :-

1- نحدد مفتاح التشفير هو سطران.

2- نملأ الفراغات بمثلث مقلوب، كالآتي :-

I▽Love▽my▽country

3- ننشئ جدولاً (نراعي عدد الأسطر وهو 2).

4- نوزع الأحرف، بشكل قطري حسب اتجاه السهم.

5- نضع مثلثاً مقلوباً في الفراغ الأخير.

I		L		v		▽		y		c		u		t		y	
	▽		o		e		m		▽		o		n		r		▽

6- نقوم بكتابة النص المشفر سطراً، سطراً، كالآتي :- ILv▽ycuty▽ oem▽ onr

النص الأصلي : I Love my country

النص المشفر : ILv ycuty oem onr

ملاحظة : يمكن تشفير أحرف اللغة العربية باستخدام هذه الخوارزميات وعلامات الترقيم، ولكنها غير متضمنة في الكتاب، وغير مطلوبة.

مثال :

شفر النص الآتي، علماً أن مفتاح التشفير هو ثلاثة أسطر. Abdulla Faqeeh

الحل :

A		u		a		F		e		
	b		l		h		a		e	
		d		l		▽		q		h

حروف السطر الأول : AuaFe
حروف السطر الثاني : blhae
حروف السطر الثالث : dl▽qh

الآن نقوم بتجميع الأسطر، كالآتي :- AuaFeblhaedl▽qh

النص الأصلي : Abdulla Faqeeh
النص المشفر : AuaFeblhaedl qh

مثال :
شفر النص الآتي، علماً أن مفتاح التشفير أربعة أسطر. I Like Irbid
الحل :

I		k		r			
	▽		e		b		
		L		▽		i	
			i		I		D

حروف السطر الأول : Ikr
حروف السطر الثاني : ▽eb
حروف السطر الثالث : L▽i
حروف السطر الرابع : iId

الآن نقوم بتجميع الأسطر، كالآتي :- Ikr▽eb L▽i iId

النص الأصلي : I Like Irbid
النص المشفر : Ikr ebL iiId

- خطوات فك التشفير :-
1- نملأ الفراغات بمثلث مقلوب.
2- نقسم النص المشفر إلى أجزاء، اعتمادا على عدد الأسطر (مفتاح التشفير)، أي أن عدد الأجزاء يساوي عدد الأسطر.
ولتحديد عدد الأحرف في كل جزء، نقوم بالعملية الحسابية الآتية :-
مجموع أحرف النص المشفر (بما فيها الفراغات) ÷ عدد الأجزاء
إذا كان ناتج المعادلة عدداً غير صحيح، فيجب **تقريبه** إلى أقرب عدد صحيح.
فمثلاً إذا كان الناتج 4.6 فيتم تقريبه إلى العدد 5، وهذا يعني أن كل جزء سيتكون من 5 حروف (بما فيها الفراغات)، **باستثناء الجزء الأخير فقد يكون 5 حروف أو أقل**.
3- نكتب الحرف الأول من كل جزء، ثم الحرف الثاني من كل جزء، ثم الحرف الثالث من كل جزء، وهكذا ،،،

مثال :
جد النص الأصلي للنص المشفر الآتي، علماً أن مفتاح التشفير سطران.
ILv ycuty oem onr

الحل :

1- نملأ الفراغات بمثلثات مقلوبة، كالآتي :-

ILv▽ycuty▽oem▽onr

2- نحدد عدد الأحرف في كل جزء، وذلك بواسطة المعادلة السابقة، كالآتي :-

17 ÷ 2 = 8.5 بما أن الناتج عدد غير صحيح، لذلك نقوم **بتقريبه** إلى أقرب عدد صحيح وهو العدد 9، وذلك يعني أن الجزء الأول يتكون من تسعة رموز (حروف وفراغات).

الجزء الأول : ILv▽ycuty (9 حروف بما فيها الفراغات)

الجزء الثاني : ▽oem▽onr

3- نأخذ الحرف الأول من كل جزء بشكل عمودي، ثم الحرف الثاني من كل جزء وهكذا

فيكون الناتج كالآتي :- **I Love my country**

مثال :

جد النص الأصلي للنص المشفر الآتي، علماً بأن مفتاح التشفير ثلاثة أسطر.

AuaFeblhaedl qh

الحل :

AuaFeblhaedl ▽qh

عدد الحروف (بما فيها الفراغات) : 15

عدد الأحرف في كل جزء : 15 ÷ 3 = 5

الجز الأول : AuaFe

الجزء الثاني : blhae

الجزء الثالث : dl▽qh

الحرف الأول من كل جزء، والثاني من كل جزء، وهكذا ،،،

فيكون الناتج كالآتي :- **Abdullah Faqeeh**

إجابات أسئلة الفصل الثالث من الوحدة الرابعة (صفحة 158)

السؤال الأول

- هو تغيير محتوى الرسالة الأصلية سواء أكان التغيير بمزجها بمعلومات أخرى، أم استبدال الأحرف الأصلية والمقاطع بغيرها، أم تغيير لمواقع الأحرف بطريقة لن يفهمها إلا مرسل الرسالة ومستقبلها، باستخدام خوارزمية معينة ومفتاح خاص.
- استعادة النص الأصلي للنص المشفر.

السؤال الثاني

وذلك لأنه يعمل على إخفاء نص الرسالة عن الأشخاص غير المصرح لهم بالاطلاع عليها.

السؤال الثالث

أهداف التشفير :-

1- الحفاظ على سرية المعلومات في أثناء تبادلها بين مرسل المعلومة ومستقبلها.

2- عدم الاستفادة من الرسالة أو فهم محتواها، حتى لو تم الحصول عليها من قبل أشخاص معترضين.

عناصر عملية التشفير :-

1- خوارزمية التشفير.
2- مفتاح التشفير.
3- النص الأصلي.
4- نص الشيفرة.

السؤال الرابع

أ- خوارزمية التشفير.
ب- نص الشيفرة.
ج- مفتاح التشفير.
د- النص الأصلي.

السؤال الخامس

1- استخدام المفتاح.
2- كمية المعلومات المرسلة.
3- العملية المستخدمة في عملية التشفير.

السؤال السادس

- خوارزميات التعويض.

تعني هذه الطريقة استبدال حرف مكان حرف أو مقطع مكان مقطع، مثل طريقة شيفرة الإزاحة.

- خوارزميات التبديل.

بهذه الطريقة يتم تبديل أماكن الأحرف نفسها من دون إجراء أي تغيير عليها. عند تنفيذ عملية التبديل يختفي معنى النص الحقيقي، وهذا يشكل عملية التشفير، شريطة أن تكون قادراً على استعادة النص الأصلي منها، وهذا ما يسمى عملية فك التشفير.

السؤال السابع

وذلك لأن المفتاح نفسه يستخدم لعمليتي التشفير وفك التشفير.

السؤال الثامن

أ-

ب-

السؤال التاسع

إجابات أسئلة الوحدة الرابعة (صفحة 159+160)

السؤال الأول

(أسفل يمين "التهديدات") : بشرية
(أسفل يمين "متعمدة") : موجهة لجهاز معين في مكان معين.
(أسفل يسار "متعمد") : غير موجهة لجهاز معين.
(أسفل "غير متعمدة") : إهمال أو خطأ.
(أسفل "أسباب طبيعية) : الحريق ، أو انقطاع التيار الكهربائي.

السؤال الثاني

- هي وسائل وأساليب يستخدمها المعتدي الإلكتروني لجعل مستخدم الحاسوب في النظام يعطي معلومات سرية، أو يقوم بعمل ما يسهل عليه الوصول إلى أجهزة الحاسوب أو المعلومات المخزنة فيها.
- وتعني حماية الرسائل أو المعلومات التي تم تداولها، والتأكد بأنها لم تتعرض لأي عملية تعديل سواء بالإضافة أو الاستبدال أو حذف جزء منها.
- وهو سلسلة من الرموز المستخدمة في خوارزمية التشفير.

السؤال الثالث

أ- سلامة المعلومات.
ب- سرية المعلومات ، سلامة المعلومات.
ج- سرية المعلومات.
د- سرية المعلومات ، سلامة المعلومات.
هـ- توافر المعلومات.

السؤال الرابع

عند رغبة أحد الأجهزة بالتراسل خارجياً؛ فإنه يتواصل مع الجهاز الوسيط الذي يعطيه عنواناً خارجياً مؤقتاً يستخدمه لحين الانتهاء عملية التراسل، ويفقد الجهاز الداخلي هذا العنوان، ويصبح العنوان متاحاً للتراسل مرة أخرى، وعند رغبة الجهاز نفسه بالتراسل مرة أخرى، قد يعطى عنواناً مختلفاً عن المرة السابقة، وهذا ما يفسر اختلاف IP Address للجهاز نفسه عند تراسله أكثر من مرة.

السؤال الخامس

1- عدم تحديد صلاحيات الوصول إلى المعلومات.
2- مشكلة في تصميم النظام.
3- عدم كفاية الحماية المادية للأجهزة والمعلومات.

السؤال السادس

1- الإقناع.
2- انتحال الشخصية والمداهنة.
3- مسايرة الركب.

السؤال السابع

وذلك لأن الثغرات قد تتسبب في فقدان المعلومات أو هدم النظام، أو تجعله عرضة للاعتداء الإلكتروني.

السؤال الثامن

أ-

ب-

السؤال التاسع

السؤال العاشر

أ- - المفتاح الخاص.
- المفتاح العام.

ب- - التدفق.
- الكتل.

ج- - التعويض.
- التبديل.