الفصل الأول : أمن المعلومات

- **يعد أمن المعلومات من أهم الركائز التي تعتمد عليها الدول والمؤسسات والأفراد في الحفاظ على موقفها العالمي سياسياً ومالياً.**
- **بسبب وجود المخترقين والمتطفلين بشكل كبير** فقد وجب الاهتمام بكل ما يخص المعلومة من أجهزة تخزين ومعالجة والاهتمام بالكادر البشري الذي يتعامل معها ، **بالإضافة إلى** الحفاظ على المعلومات نفسها.

أولاً | مقدمة في أمن المعلومات

- **مفهوم أمن المعلومات :**

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 إبقائها متاحة للأفراد المصرح لهم باستخدامها.

- **يهدف أمن المعلومات للحفاظ على ثلاثة خصائص أساسية هي :**

أ – السرية :

– تعني أن الشخص المخول هو الوحيد القادر على الوصول إلى المعلومات والاطلاع عليها.

– هو مصطلح مرادف لمفهومي **الأمن والخصوصية.**

– من الأمثلة على المعلومات التي يعتمد أمنها على مقدار الحفاظ على سريتها :

(١) المعلومات الشخصية. (٢) الموقف المالي لشركة قبل إعلانه. (٣) المعلومات العسكرية.

ب – السلامة :

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

– عند نشر نتائج طلبة الثانوية العامة يجب الحفاظ على هذه النتائج من أي تعديلات.

– عند صدور قوائم القبول الموحد للجامعات الأردنية والتخصصات التي قُبل الطلبة فيها فلا بد من حماية هذه القوائم من أي تعديل أو حذف أو تغيير أو تبديل.

ج – توافر المعلومات : تكون المعلومات رغم الحفاظ على سلامتها وسريتها بلا فائدة في حالتين :

(١) إذا لم تكن متاحة للأشخاص المصرح لهم بالتعامل معها. (٢) أن الوصول إليها يحتاج إلى وقت كبير.

– من الوسائل التي يقوم بها المخترقون جعل هذه المعلومات غير متاحة **إما بحذفها أو الاعتداء على الأجهزة التي تُخزن فيها** هذه المعلومات.

- **المخاطر التي تهدد أمن المعلومات :**

تقسم المخاطر التي تهدد أمن المعلومات إلى نوعين رئيسين ، هما <u>التهديدات</u> و <u>الثغرات</u>.

(أ) <u>التهديدات</u>			
أسباب بشرية			**أسباب طبيعية**
<u>متعمدة</u>		<u>غير متعمدة</u>	حدوث حريق.
موجهة لجهاز معين في مكان معين	غير موجهة لجهاز معين	نتيجة لإهمال أو خطأ.	انقطاع التيار الكهربائي.
الهجوم(الاعتداء) الالكتروني. • من الأمثلة عليها : (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.	نشر برامج خبيثة في المواقع الإلكترونية **(نشر الفيروسات)**	كتابة ٢٤ بدل من ٤٢ **أو** كتابة عنوان بريد الكتروني بشكل غير صحيح.	

- يعد **الهجوم الالكتروني/ الاعتداء الإلكتروني** من أخطر أنواع التهديدات.
- يعتمد نجاح أي هجوم/اعتداء الكتروني على <u>ثلاثة عوامل رئيسية</u> يجب أخذها بالحسبان لتقييم التهديد وهي :

(١) الدافع. **(٢) الطريقة.** **(٣) فرصة النجاح.**

– تتنوع **دوافع الأفراد** لتنفيذ هجوم إلكتروني فقد تكون :

(١) رغبة في الحصول على المال. (٢) محاولة لإثبات القدرات التقنية. (٣) قصد الإضرار بالآخرين

– تتضمن **الطريقة :**

(١) المهارات التي يتميز بها المعتدي الالكتروني. (٣) معرفته بتصميم وآلية عمل النظام.

(٢) قدرته على توفير المعدات والبرمجيات الحاسوبية التي يحتاج إليها. (٤) معرفة نقاط القوة والضعف لهذا النظام.

– تتمثل **فرصة نجاح الهجوم الالكتروني :**

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

- **أنواع الاعتداءات الإلكترونية** التي قد تتعرض لها المعلومات :

(١) التنصت على المعلومات :

الهدف منه الحصول على المعلومات السرية حيث يتم **الإخلال بسريتها**.

(٢) التعديل على المحتوى :

يتم اعتراض المعلومات وتغيير محتواها وإعادة إرسالها للمستقبل من دون علمه بتغيير محتواها.

بهذا النوع يكون **الإخلال بسلامة المعلومات**.

(٣) الإيقاف :

يتم قطع قناة الاتصال ومن ثم منع المعلومات من الوصول إلى المستقبل.

في هذه الحالة تصبح **المعلومات غير متوافرة**.

(٤) الهجوم المزوّر أو المفبرك :

يتمثل بإرسال المعتدي الإلكتروني رسالة إلى أحد الأشخاص على الشبكة يخبره فيها بأنه صديقه ويحتاج إلى معلومات أو كلمات سرية خاصة.

تتأثر بهذه الطريقة **سرية وسلامة المعلومات**.

(ب) الثغرات

- **مفهوم الثغرات :**

يقصد بها نقطة الضعف في النظام التي قد تتسبب في فقدان المعلومات أو هدم النظام أو تجعله عرضة للاعتداء الالكتروني سواء أكانت : **(١) في الإجراءات المتبعة** مثل عدم تحديد صلاحيات الوصول إلى المعلومات.

(٢) مشكلة في تصميم النظام. **(٣) عدم كفاية الحماية المادية للأجهزة والمعلومات.**

- **الحد من مخاطر أمن المعلومات :**

– يرى المختصون في مجال أمن المعلومات بأن الحفاظ على المعلومات وأمنها ينبع من التوازن بين **تكلفة الحماية وفعالية الرقابة** من جهة **مع احتمالية الخطر** من جهة أخرى

– وضعت مجموعة من الضوابط في نظام المعلومات **لتقليل المخاطر التي قد تتعرض لها المعلومات والحد منها.**

– من أهم الضوابط التي تستخدم في نظام المعلومات :

(١) الضوابط المادية :

يقصد بها مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها ؛ **باستخدام الجدران والأسوار والأقفال، وجود حراس الأمن وغيرها من أجهزة إطفاء الحريق** .

(٢) الضوابط الإدارية :

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

(٣) الضوابط التقنية :

هي الحماية التي تعتمد على التقنيات المستخدمة سواء أكانت **معدات** أم **برمجيات**.

تتضمن **كلمات المرور، منح صلاحيات الوصول، وبرتوكولات الشبكات والجدر النارية، والتشفير، وتنظيم تدفق المعلومات في الشبكة.**

ثانياً | الهندسة الاجتماعية

- يعد العنصر البشري من أهم مكونات الأنظمة، والاهتمام به من أهم المجالات للحفاظ على أمن المعلومات.
- **إن اختيار الكادر البشري المسئول عن حماية الأنظمة يعتمد على عدة أمور، منها:**

(١) كفايته العلمية. (٢) اختبارات شفوية وورقية ومقابلات.

(٣) إخضاعهم إلى ضغوطات نفسية حسب موقعهم **للتأكد من قدرتهم على حماية النظام**.

(١) مفهوم الهندسة الاجتماعية:

- هي الوسائل والأساليب التي يستخدمها المعتدي الإلكتروني لجعل مستخدم الحاسوب في النظام يعطي معلومات سرية أو يقوم بعمل ما يسهّل عليه الوصول إلى أجهزة الحاسوب أو المعلومات المخزنة فيها.
- **تعد الهندسة الاجتماعية من أنجح وأسهل الوسائل المستخدمة للحصول على المعلومات غير مصرح بالإطلاع عليها وذلك لسببين؛ هما:**

(١) قلة اهتمام المتخصصين في مجال أمن المعلومات.

(٢) عدم وعي مستخدم الحاسوب بالمخاطر المترتبة عليها.

(٢) مجالات الهندسة الاجتماعية:

- تتركز الهندسة الاجتماعية في مجالين، هما: **(١) البيئة المحيطة. (٢) الجانب النفسي.**

(١) <u>البيئة المحيطة</u>: تشمل ما يأتي:

١. مكان 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 بسهولة ليحصل على المعلومات التي يريدها.

٢. الهاتف:

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

٣. النفايات الورقية

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 تحتويه من معلومات يمكن استغلالها في تتبع الموظفين أو الحصول على المعلومات المرغوبة.

٤. الإنترنت : من أكثر الوسائل شيوعاً ؛ **وذلك بسبب استخدام الموظفين أو مستخدمي الحاسوب عادة كلمة المرور نفسها للتطبيقات جميعها.**

حيث ينشئ المعتدي الإلكتروني موقعاً 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 عادةً ، **وبهذه الطريقة** يتمكن المعتدي الإلكتروني من الحصول عليها.

(٢) الجانب النفسي : يسعى المعتدي الإلكتروني هنا لكسب ثقة مستخدم الحاسوب ومن ثم الحصول على المعلومات التي يرغب بها.

- **من أشهر الأساليب التي يستخدمها المعتدي الإلكتروني للتأثير في الجانب النفسي للشخص المستهدف :**

١. الإقناع :

– يستطيع المعتدي إقناع الموظف أو 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 من دون تحليلها أو التفكير فيها ؛ ويحاول التأثير بهذه الطريقة عن طريق **إظهار نفسه بمظهر صاحب السلطة** أو **إغراء المستخدم بامتلاك خدمة نادرة**، حيث يقدم له عرضاً معيناً من خلال موقعه الإلكتروني لمدة محدودة يمكنه ذلك من الحصول على كلمة المرور.

– قد يلجأ المعتدي الإلكتروني إلى إبراز أوجه التشابه مع الشخص المستهدف **لإقناعه بأنه يحمل الصفات والاهتمامات نفسها** فيصبح الشخص أكثر ارتياحاً وأقل حذراً للتعامل معه فيقدم له ما يريد من معلومات.

٢. انتحال الشخصية والمداهنة :

– حيث يتقمص شخص شخصية آخر ، وهذا الشخص قد يكون شخصاً حقيقياً أو وهمياً.

– فقد ينتحل شخصية فني صيانة معدات الحاسوب أو عامل نظافة أو حتى المدير أو السكرتير.

– وبما أن الشخصية المنتحلة غالباً تكون ذات سلطة يبدي أغلب الموظفين خدماتهم ولن يترددوا بتقديم أي معلومات لهذا الشخص المسئول.

٣. مسايرة الركب :

– يرى الموظف بأنه إذا قام زملاؤه جميعهم بأمر ما فمن غير اللائق أن يأخذ موقفاً مغايراً.

– فعندما يقدّم شخص نفسه على ان إداري من فريق الدعم الفني ويرغب بعمل تحديثات على الأجهزة فإذا سمح له أحد الموظفين بعمل تحديث على جهازه فإن البقية يقومون بمسايرة زميلهم غالباً والسماح لهذا المعتدي باستخدام أجهزتهم لتحديثها ، ومن ثم يتمكن من الاطلاع على المعلومات التي يريدها والمخزنة على الأجهزة.

إجابات أسئلة الفصل الأول صفحة ١٣٨

السؤال الأول: وضح المقصود بكل من:

أ. أمن المعلومات:

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 إبقائها متاحة للأفراد المصرح لهم باستخدامها.

ب. الثغرات: يقصد بها نقطة الضعف في النظام التي قد تتسبب في فقدان المعلومات أو هدم النظام أو تجعله عرضة للاعتداء الالكتروني سواء أكانت في الإجراءات المتبعة مثل عدم تحديد صلاحيات الوصول إلى المعلومات، **أو** مشكلة في تصميم النظام **أو** عدم كفاية الحماية المادية للأجهزة والمعلومات

السؤال الثاني: يهدف أمن المعلومات للحفاظ على ثلاثة خصائص أساسية وهي(**السرية، السلامة، توافر المعلومات**)؛

حدّد أي من هذه للخصائص يتبع كل مما يأتي:

أ.	التأكد من عدم حدوث أي تعديل على المعلومات.	**سلامة المعلومات**
ب.	الشخص المخول هو الوحيد القادر على الوصول والإطلاع عليها.	**سرية المعلومات**
ج.	الوصول إلى المعلومات يحتاج إلى وقت كبير.	**توافر المعلومات**
د.	مصطلح مرادف لمفهومي **الأمن و الخصوصية.**	**سرية المعلومات**
هـ.	المعلومات العسكرية تخص.	**سرية المعلومات**

السؤال الثالث: هناك ثلاثة عوامل رئيسة تؤخذ بعين الاعتبار لتقييم التهديد، حدد العامل الذي تندرج تحته كل مما يأتي

أ.	الرغبة في إثبات الذات.	**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**
	القدرة على توفير المعدات والبرمجيات الحاسوبية.	**الطريقة**

السؤال الرابع: أربعة من أنواع الاعتداءات الإلكترونية التي تتعرض لها المعلومات:

(١) التنصت على المعلومات.	(٢) التعديل على المحتوى.
(٣) الهجوم المزوّر أو المفبرك.	(٤) الإيقاف.

السؤال الخامس: علل كل مما يأتي:

أ. استخدام بعض الضوابط في النظام.

لتقليل المخاطر التي تتعرض لها المعلومات والحد منها.

ب. تعد الهندسة الاجتماعية من أنجح الوسائل وأسهلها للحصول على المعلومات.

(١) بسبب قلة اهتمام المختصين في مجال أمن المعومات.

(٢) عدم وعي مستخدم الحاسوب بالمخاطر المترتبة عليها.

السؤال السادس: قارن بين نوعي **الضوابط المادية والضوابط الإدارية** من حيث:

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

السؤال السابع: توضيح آلية عمل الهندسة الاجتماعية في كل مجال من المجالات الآتية:

١. مكان 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 بسهولة ليحصل على المعلومات التي يريدها.

٢. الهاتف:

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

٣. انتحال الشخصية:

- حيث يتقمص شخص شخصية آخر، وهذا الشخص قد يكون شخصاً حقيقياً أو وهمياً.
- فقد ينتحل شخصية فني صيانة معدات الحاسوب أو عامل نظافة أو حتى المدير أو السكرتير.
- وبما أن الشخصية المنتحلة غالباً تكون ذات سلطة يبدي أغلب الموظفين خدماتهم ولن يترددوا بتقديم أي معلومات لهذا الشخص المسئول.

٤. الإقناع:

–يستطيع المعتدي إقناع الموظف أو 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 من دون تحليلها أو التفكير فيها ؛ ويحاول التأثير بهذه الطريقة عن طريق **إظهار نفسه بمظهر صاحب السلطة** أو **إغراء المستخدم بامتلاك خدمة نادرة**، حيث يقدم له عرضاً معيناً من خلال موقعه الإلكتروني لمدة محدودة يمكنه ذلك من الحصول على كلمة المرور.

– قد يلجأ المعتدي الإلكتروني إلى إبراز أوجه التشابه مع الشخص المستهدف **لإقناعه بأنه يحمل الصفات والاهتمامات نفسها** فيصبح الشخص أكثر ارتياحاً وأقل حذراً للتعامل معه فيقدم له ما يريد من معلومات.

الفصل الثاني: أمن الإنترنت

- **تم إيجاد وسائل تقنية تعمل على حماية الويب:**

(١) بسبب انتشار البرامج والتطبيقات المجانية وغير معروفة المصدر ومفتوحة المصدر"يمكن استخدامها في الأجهزة المختلفة".

(٢) الحد من الاعتداءات والأخطار التي تهدده بسبب انتشار البرامج المقرصنة والمعلومات الخاصة بكيفية اقتحام المواقع.

أولاً | الاعتداءات الإلكترونية على الويب

- **تتعرض المواقع الإلكترونية لكثير من الاعتداءات التي لا يحس بها المستخدم كونها غير مرئية.**
- **من أشهر الأمثلة على الاعتداءات الإلكترونية على الويب:**

١ – الاعتداء على متصفح الإنترنت (Browser Attack).	**٢ – الاعتداء على البريد الالكتروني** (E-mail Attack).

١ – الاعتداءات الإلكترونية على متصفحات الانترنت:

- **متصفح الانترنت:** برنامج ينقل المستخدم إلى صفحة **الويب** التي يريدها بمجرد كتابة العنوان والضغط على زر الذهاب ويمكنه من مشاهدة المعلومات على الموقع.
- يتعرض متصفح الإنترنت إلى الكثير من الأخطار **لأنها قابلة للتغيير من دون ملاحظة ذلك من قبل المستخدم.**
- **يتم الاعتداء الالكتروني على متصفحات الانترنت بطريقتين:**

١ – الاعتداء عن طريق (كود) بسيط يُمكن إضافته إلى المتصفح وباستطاعته القراءة والنسخ ، وإعادة إرسال أي شي يتم إدخاله من قبل المستخدم. **ويتمثل التهديد بالقدرة على الوصول إلى الحسابات المالية والبيانات الحساسة الأخرى.**

٢ – توجيه المستخدم إلى صفحة أخرى غير الصفحة التي يريدها.

٢ – الاعتداءات الإلكترونية على البريد الالكتروني:

- تحدث اعتداءات على الويب من خلال البريد الإلكتروني، **لأن بعض الرسائل الإلكترونية التي تحمل عروضاً وهمية وروابط تحمل عناوين جذابة وتكون مزيفة ولا يمكن اكتشافها من خلال الأشخاص قليلي الخبرة والتي تحمل روابط لنقل المستخدم لصفحات أخرى.**
- **يحاول المعتدي الإلكتروني التعامل مع الأشخاص قليلي الخبرة**، حيث يقدّم 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 (NAT)

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

- تُسهم في حماية الجهاز في الشبكة الداخلية من أي هجوم قد يُشن عليه بناءً على معرفة العناوين الرقمية.
- هي إحدى الطرائق المستخدمة لحماية المعلومات من الاعتداءات الإلكترونية.

١ – العناوين الرقمية الإلكترونية IP Address :

- يرتبط ملايين الأشخاص عبر شبكة الانترنت بملايين الأجهزة، **ولكل جهاز حاسوب أو هاتف خلوي عنوان رقمي خاص به يميزه عن غيره يسمى (IP Address).**
- **تقسم العناوين الرقمية الإلكترونية إلى نوعين:**

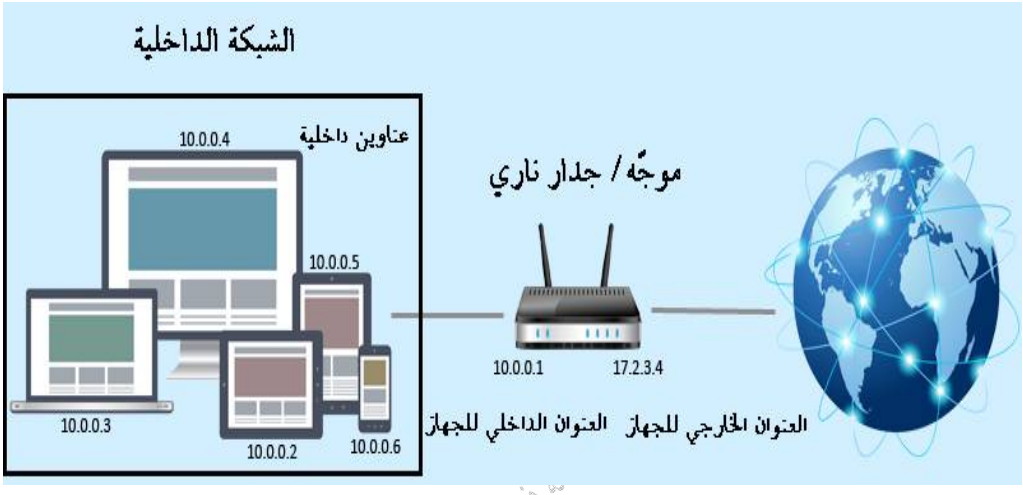
١ – العناوين الرقمية (IPv4).	تتكون من أربعة مقاطع يفصل بينها نقاط. "٣٢ خانة ثنائية". كل مقطع من هذه المقاطع يأخذ رقماً من (0) إلى (255) كالآتي: **215.002.004.216**
١ – العناوين الرقمية (IPv6).	تتكون من ثمانية مقاطع بدلاً من أربعة. " ١٢٨ خانة ثنائية" العناوين الالكترونية (IPv6) أكثر من العناوين الالكترونية (IPv4).

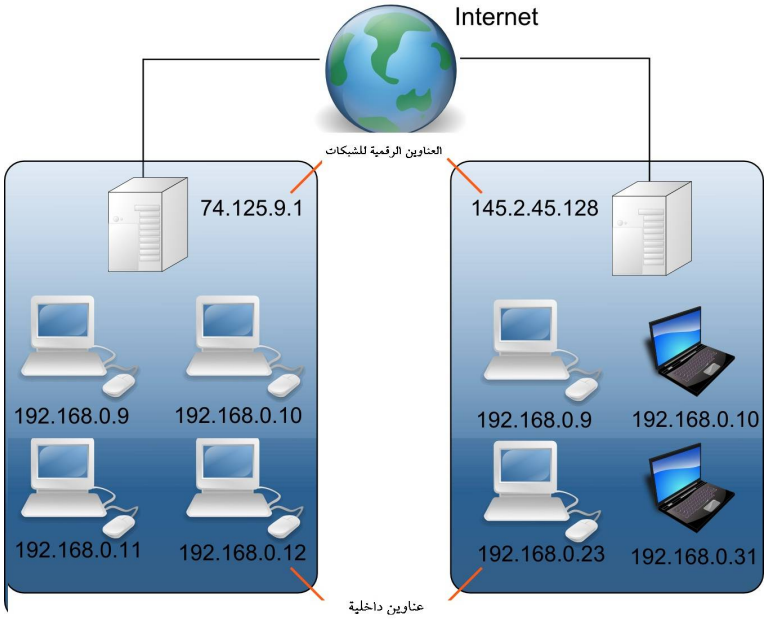
على الرغم من استخدام (IPv6) إلا إنه لا يكفي لإتاحة عدد هائل من العناوين الرقمية ولحل هذه المعضلة وجد ما يسمى **تقنية تحويل العناوين الرقمية (NAT).**

٢ – مفهوم تقنية تحويل العناوين الرقمية (NAT):

- تتمتع **أيانا(IANA)**بالسلطة المسئولة عن منح أرقام الانترنت المخصصة لإعطاء العناوين الرقمية للأجهزة على الانترنت
- **بسبب قلة أعداد هذه العناوين مقارنة بعدد المستخدمين ؛** فإنها تعطي الشبكة الداخلية عنواناً واحداً (مجموعة عناوين) ويكون معرِّفاً لها عند التعامل في شبكة الإنترنت.
- كل شبكة داخلية تمنح عنواناً خاصاً بها على الانترنت مختلفاً عن العناوين الأخرى.
- 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.**
- **العنوان الرقمي للشبكة الداخلية لن يتكرر.**

- عند رغبة أحد الأجهزة بالتواصل مع جهاز خارج الشبكة الداخلية **يعدّل** العنوان الرقمي الخاص به **باستخدام تقنية تحويل العناوين الرقمية (NAT)** وذلك يتم باستخدام جهاز وسيط ، يكون غالباً **موجّهاً** (router) أو **جداراً نارياً**، الذي يحوّل 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 بالمرسل.
- عندما يقوم الجهاز الهدف بالرد على رسالة الجهاز المرسل تصل إلى الجهاز الوسيط الذي يحوّل **العنوان الرقمي الخارجي** إلى عنوان داخلي من خلال سجل المتابعة لديه ويعيده بذلك إلى الجهاز المرسل.





IANA

٣ – آلية عمل تقنية تحويل العناوين الرقمية (NAT) :

○ **تعمل تقنية تحويل العناوين الرقمية بعدة طرائق، منها :**

أ – النمط الثابت للتحويل :	يتم عن طريق هذا النمط تخصيص عنوان رقمي خارجي لكل جهاز داخلي، وهذا العنوان الرقمي ثابت لا يتغير.
ب – النمط المتغير للتحويل :	يتم إعطاء عنوان رقمي مؤقت للتواصل مع الأجهزة خارج الشبكة وحين انتهاء الاتصال يصبح هذا الرقم متاحاً لأي جهاز أخر داخل الشبكة. 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 من عملية التراسل ويعد هذا العنوان **عنواناً رقمياً خاصاً بالجهاز.** عند انتهاء عملية التراسل يفقد الجهاز الداخلي هذا العنوان **ويصبح** العنوان متاحاً للتراسل مرة أخرى. **عند 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.**

إجابات أسئلة الفصل صفحة ١٤٥

السؤال الأول: أسباب إيجاد وسائل تقنية لحماية الإنترنت:

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

السؤال الثاني: أشهر الاعتداءات على الويب:

(١) الاعتداءات الالكترونية على متصفحات الانترنت. (٢) الاعتداءات الالكترونية على البريد الالكتروني.

السؤال الثالث: حدد نوع الاعتداء في كل مما يأتي:

أ.	توجيه المستخدم إلى صفحة أخرى غير الصفحة التي يريدها.	**اعتداء على متصفح الانترنت**
ب.	كود بسيط يمكن إضافته إلى المتصفح وباستطاعته القراءة والنسخ وإعادة الإرسال لأي شيء يتم إدخاله من قبل المستخدم.	**اعتداء على متصفح الانترنت**
ج.	يتضمن عروضاً وهمية ومضللة ويحتوي رابط يتم الضغط عليه للحصول على معلومات إضافية.	**اعتداء على البريد الالكتروني**

السؤال الرابع: وضح ما يأتي:

أ. تحدث اعتداءات على (الويب) من خلال البريد الالكتروني.

لأن بعض الرسائل الالكترونية التي تحمل عروضاً وهمية وروابط تحمل عناوين جذابة وتكون مزيفة ولا يمكن اكتشافها من خلال الأشخاص قليلي الخبرة والتي تحمل روابط لنقل المستخدم لصفحات أخرى.

ب. تحافظ تقنية تحويل العناوين الرقمية على أمن المعلومات في الويب.

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

السؤال الخامس: الفرق بين العناوين الرقمية IPv4 و IPv6 :

IPv4: تتكون من أربع مقاطع (٣٢ بت).

IPv6: تتكون من ثمانية مقاطع (١٢٨ بت).

السؤال السادس: المانح لأرقام الانترنت المخصصة لإعطاء العناوين الرقمية:

السلطة المسئولة عن منح أرقام الانترنت المخصصة لإعطاء العناوين الرقمية للأجهزة على الانترنت هي **IANA**.

السؤال السابع: وظيفة الجهاز الوسيط سواء أكان موجه أو جدار ناري:

يقوم بتحويل العنوان الرقمي الداخلي إلى عنوان رقمي خارجي للجهاز.

السؤال الثامن: مقارنة بين طريقتي العمل النمط الثابت لتحويل العناوين الرقمية والنمط المتغير لتحويل العناوين الرقمية:

أ – النمط الثابت للتحويل:	يتم عن طريق هذا النمط تخصيص عنوان رقمي خارجي لكل جهاز داخلي، وهذا العنوان الرقمي ثابت لا يتغير.
ب – النمط المتغير للتحويل:	يتم إعطاء عنوان رقمي مؤقت للتواصل مع الأجهزة خارج الشبكة وحين انتهاء الاتصال يصبح هذا الرقم متاحاً لأي جهاز أخر داخل الشبكة.

الفصل الثالث: التشفير

ظهرت الحاجة للحفاظ على سرية المعلومات منذ قدم البشرية، في المجالين العسكري والدبلوماسي خاصة، وتم آنذاك إيجاد الوسائل التي يمكن نقل الرسالة عن طريقها والمحافظة على سريتها في الوقت نفسه.

أولاً | مفهوم علم التشفير وعناصره

١ – مفهوم التشفير والهدف منه:

- **التشفير:**

تغيير محتوى الرسالة الأصلية سواء أكان التغيير **بمزجها بمعلومات أخرى** أم **استبدال الأحرف الأصلية والمقاطع بغيرها**، أم **تغيير لمواقع الحرف بطريقة لن يفهمها إلا مُرسل الرسالة ومستقبلها فقط باستخدام خوارزمية معينة أو مفتاح خاص.**

- **الهدف من التشفير:**

الحفاظ على سرية المعلومات في أثناء تبادلها بين مرسل المعلومة ومستقبلها وعدم الاستفادة منها أو فهم محتواها؛ حتى لو تم الحصول عليها من قبل أشخاص معترضين.

- **يعد التشفير من أفضل الوسائل المستخدمة للحفاظ على أمن المعلومات:**

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

٢ – عناصر عملية التشفير:

- **تضمن عملية التشفير أربعة عناصر أساسية هي:**

(١) خوارزمية التشفير:	مجموعة من الخطوات المستخدمة لتحويل الرسالة الأصلية إلى رسالة مشفرة.
(٢) مفتاح التشفير:	سلسلة من الرموز المستخدمة في التشفير وتعتمد قوة التشفير على قوة هذا المفتاح.
(٣) النص الأصلي:	محتوى الرسالة الأصلية قبل التشفير وبعد عملية فك التشفير.
(٤) نص الشيفرة:	الرسالة بعد عملية التشفير.

ثانياً | خوارزميات التشفير

●**تصنف خوارزميات التشفير بناءً على عدة معايير منها :**

(١) العملية المستخدمة في التشفير.	(٢) المفتاح المستخدم.	(٣) كمية المعلومات المرسلة ،

١ – التشفير المعتمد على عملية التشفير:

○ **يقسم إلى نوعين :**

(١) طريقة التشفير بالتعويض :	طريقة لتشفير النصوص يتم من خلالها استبدال حرف مكان حرف أو مقطع مكان مقطع ومثال عليها شيفرة الإزاحة.
(٢) طريقة التشفير بالتبديل :	طريقة تشفير يتم فيها تبديل أماكن الأحرف وذلك عن طريق إعادة ترتيب أحرف الكلمة بشرط استخدام الأحرف نفسها من دون إجراء أي تغيير عليها. وعند عملية التبديل يختفي معنى النص الحقيقي و**هذا يشكل عملية التشفير**، شريطة أن تكون قادراً على استرجاع النص الأصلي منها **وهذا ما يسمى عملية فك التشفير.**

●**خوارزمية الخط المتعرج Zig Zag Cipher**

تتميز بأنها سهلة وسريعة ويمكن تنفيذها يدوياً باستخدام الورقة والقلم كما انه يمكن فك تشفيرها بسهولة.

أ) خطوات التشفير: للقيام بتشفير النص حسب خوارزمية الخط المتعرج نتبع الخطوات الآتية :

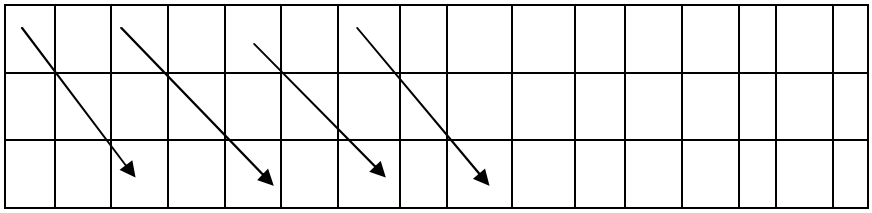
(١) حدد عدد الأسطر المستخدمة لتشفير النص. حيث أن عدد الأسطر يعد مفتاح التشفير ولا يلزمنا معرفة عدد الأعمدة ؛ ابدأ بأي عدد من الأعمدة ويمكن الزيادة عند الحاجة.

(٢) أملأ الفراغ في النص الأصلي بمثلث مقلوب ▼ .

استخدام المثلث المقلوب بديلاً للفراغ لغايات تسهيل الحل فقط.

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

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



●**مثال١ : شفّر النص الآتي علماً بأن مفتاح التشفير سطرين.**

I love my country

١. مفتاح التشفير سطران.

٢. أملأ الفراغ بالنص الأصلي بمثلث مقلوب ▼ .

I▼love▼my▼country

٣. وزع أحرف النص بشكل قطري.

I		**l**		**v**		▼		**y**		**c**		**u**		**t**		**y**
	▼		**o**		**e**		**m**		▼		**o**		**n**		**r**		▼

٤. يجب وضع ▼ في الفراغ الأخير لكي تصبح الأطوال متساوية.

٥. اكتب النص المشفر سطراً سطراً.

النص الأصلي:	I love my country
النص المشفر:	Ilv▼ycuty▼oem▼onr▼ Ilv ycuty oem onr

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

●**يمكن تشفير أحرف اللغة العربية باستخدام هذه الخوارزمية ولكنها غير متضمنة وغير مطلوبة.**

●**تشفير نص يحتوي على علامات ترقيم غير متضمن وغير مطلوب في الكتاب.**

●**مثال٢ : جد النص المشفّر للنص ألأصلي الآتي علماً بأن مفتاح التشفير هو خمسة سطور.**

Stay positive this year makes you happy all life

١) مفتاح التشفير خمسة سطور.

٢) أملأ الفراغ بالنص الأصلي بمثلث مقلوب ▼ .

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

٣) وزع أحرف النص بشكل قطري.

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		▼

٤) يتم وضع مثلث مقلوب ▼ في المربع الأخير وذلك كي تصبح الأطوال متساوية.

٥) يكتب النص المشفر سطراً سطراً ونرتبه 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 الأصلي :	Stay positive this year makes you happy all life
النص المشفر :	Spiheayaaitoviakoplfasesreupleyi▼ ▼▼s▼ y▼ ▼▼ttym▼ h▼ l▼
	Spiheayaaitoviakoplfasesreupleyi s y ttym h l

●**مثال٣ : شفّر النص الآتي علماً بأن مفتاح التشفير هو أربعة سطور.**

Stop thinking about your past mistakes

١) أملأ الفراغ بالنص الأصلي بمثلث مقلوب ▼ .

Stop▼thinking▼about▼your▼past▼mistakes

٢) وزع أحرف النص بشكل قطري في جدول يتكون من أربعة سطور.

S		▼		n		g		o		y		▼		t		s		e			
	t		t		k		▼		u		o		p		▼		t		s		
		o		h		i		a		t		u		a		m		a		▼	
			p		i		n		b		▼		r		s		i		k		▼

السطر الأول	S▼ n g o y ▼t s e
السطر الثاني	t t k ▼u o p▼ t s
السطر الثالث	o h i a t u a m a▼
السطر الرابع	p i n b▼ r s i k ▼

النص المشفر :	S▼ngoy▼tsettk▼ uop▼tsohiatuama▼ pinb▼ rsik
	S ngoy tsettk uop tsohiatuama pinb rsik

●**مثال: شفّر النص الآتي علماً بأن مفتاح التشفير هو ثلاثة سطور.**

Never give up on your goals

١) أملأ الفراغ بالنص الأصلي بمثلث مقلوب ▼ .

Never▼give▼up▼on▼your▼goals

٢) وزع أحرف النص بشكل قطري في جدول يتكون من ثلاثة سطور.

N		e		g		e		p		n		o		▼		a		
	e		r		i		▼		▼		▼		u		g		l	
		v		▼		v		u		o		y		r		o		s

السطر الأول	N e g e p n o▼ a
السطر الثاني	e r i ▼▼▼ u g l
السطر الثالث	v▼ v u o y r o s

النص المشفر:	Ngepno▼aeri▼▼▼uglv▼vuoyros
	Ngepno aeri uglv vuoyros

ب) عملية فك التشفير: للقيام بفك تشفير رسالة نتبع الخطوات الآتية:

١. أملأ الفراغات بمثلثات مقلوبة.

٢. قسّم النص المشفر إلى أجزاء اعتماداً على عدد الأسطر (مفتاح التشفير).

عدد الأجزاء = عدد الأسطر.

لتحديد عدد الأحرف في كل جزء نقوم بما يأتي:

عدد الأحرف في كل جزء = (عدد الأحرف + عدد الفراغات) ÷ عدد الأسطر

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

● **مثال١: جد النص الأصلي للنص المشفر الآتي؛ علماً بأن مفتاح التشفير سطران:**

Ilv ycuty oem onr

Ilv▼ycuty▼oem▼onr

قسّم النص المشفر إلى جزأين؛ لأن مفتاح التشفير سطران.

ملاحظة هامة: إذا كان الناتج عدداً كسرياً **نقرّبه إلى أقرب عدد صحيح أكبر منه.**

عدد الأحرف في كل جزء = ١٧ ÷ ٢ = ٨,٥ « ٩.

الجزء الأول يتكون من تسعة رموز.

الجزء الأول	I l v ▾ y c u t y
الجزء الثاني	▾oem ▾ o n r

نأخذ الحرف الأول من كل 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

I love my country

● **مثال٢** : جد النص الأصلي للنص المشفر الآتي ؛ باستخدام خوارزمية الخط المتعرج، علماً بأن مفتاح التشفير هو خمسة سطور.

Spiheayaaitoviakoplfasesreupleyi▼ ▼▼s▼ y▼ ▼▼ttym▼ h▼ l▼

قسّم النص المشفر إلى خمسة أجزاء ؛ لأن مفتاح التشفير خمسة سطور.

عدد الأحرف في كل جزء = ٥٠ ÷ ٥ = ١٠ أحرف في كل جزء.

الجزء الأول	Spiheayaai
الجزء الثاني	toviakoplf
الجزء الثالث	asesreuple
الجزء الرابع	yi▾ ▾▾s▾ y▾ ▾
الجزء الخامس	▾ttym▾ h▾ l▾

نأخذ الحرف الأول من كل جزء بشكل عمودي (حرف **S** من الجزء الأول و الحرف **t** من الجزء الثاني و **a** 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

Stay positive this year makes you happy all life

● **مثال٣ : فك تشفير النص الآتي باستخدام خوارزمية الخط المتعرج :**

Bieno▼itsee▼▼uali▼lviyrbie▼

● **علماً بأن مفتاح التشفير ثلاثة أسطر.**

قسّم النص المشفر إلى ثلاثة أجزاء ؛ لأن مفتاح التشفير ثلاثة سطور.

عدد الأحرف في كل جزء = ٢٧ ÷ ٣ = ٩ أحرف في كل جزء.

الجزء الأول	B i e n o ▼ i t s
الجزء الثاني	e e ▼ ▼ u a l i ▼
الجزء الثالث	l v i y r b i e ▼

نأخذ الحرف الأول من كل جزء بشكل عمودي (حرف B من الجزء الأول والحرف e من الجزء الثاني والحرف l من الجزء الثالث) ونضمها إلى بعضها البعض ، ثم الحرف الثاني من كل جزء ثم الثالث وهكذا

Believe▾in▾your▾abilities▾▾

Believe in your abilities

●**مثال٤ : جد النص الأصلي للنص المشفر الآتي ؛ باستخدام خوارزمية الخط المتعرج ، علماً بأن مفتاح التشفير هو سبعة سطور.**

Eoterkodnhmon▾u▾eemelci▾n▾siasmtdsgt▾o▾a▾hi▾vfrtt

● **علماً بأن مفتاح التشفير سبعة أسطر.**

قسّم النص المشفر إلى سبعة أجزاء ؛ لأن مفتاح التشفير سبعة سطور.

عدد الأحرف في كل جزء = ٤٩ ÷ ٧ = ٧ أحرف في كل جزء.

الجزء الأول	E o t e r k o
الجزء الثاني	d n h m o n ▼
الجزء الثالث	u ▼ e e m e l
الجزء الرابع	c i ▼ n ▼ s i
الجزء الخامس	a s m t d s g
الجزء السادس	t ▼ o ▼ a ▼ h
الجزء السابع	i ▼ v f r t t

Education is the movement from darkness to light

٢ – التشفير المعتمد على المفتاح :

- يعتمد هذا النوع من التشفير على عدد المفاتيح المستخدمة في عملية التشفير ؛ **وعليه** فإن أمن الرسالة أو المعلومة يعتمد على سرية المفتاح وليس على تفاصيل الخوارزمية.
- يقسم هذا النوع من التشفير إلى نوعين :

(١) خوارزميات المفتاح الخاص : **(الخوارزميات التناظرية)**	يطلق عليها أيضاً اسم الخوارزميات التناظرية ؛ **حيث أن المفتاح نفسه يستخدم لعملتي التشفير وفك التشفير** ويتم الاتفاق على اختياره قبل بدء عملية التراسل بين المرسل والمستقبل ؛ **لذا تسمى أيضاً خوارزميات المفتاح الخاص ،** 
(٢) خوارزميات المفتاح العام : **(الخوارزميات اللاتناظرية)**	تستخدم هذه الخوارزميات مفتاحين ، أحدهما **يستخدم لتشفير الرسالة ويكون معروفاً (للمرسل والمستقبل)** ويسمى **المفتاح العام** ، والآخر **يكون معروفاً لدى المستقبل فقط ويستخدم لفك التشفير** ويسمى **المفتاح الخاص.** يتم إنتاج المفتاحين من خلال عمليات رياضية ولا يمكن معرفة المفتاح الخاص. يسمى هذا النوع أيضاً **الخوارزميات اللاتناظرية.**  **المفتاح العام** يستخدم للتشفير ومرئي للجميع. **المفتاح الخاص** يستخدم لفك التشفير و لا يعرفه سوى المستقبل.

٣ – التشفير المعتمد على كمية المعلومات المرسلة :

○ **يقسم التشفير المعتمد على كمية المعلومات المرسلة إلى قسمين :**

(أ) شيفرات التدفق :	يعمل **هذا النوع من الخوارزميات على تقسيم الرسالة إلى مجموعة أجزاء ، ويُشفر كل جزء منها على حدة ، ومن ثم يرسله.**
(ب) شيفرات الكتل : **(الخوارزميات اللاتناظرية)**	تقسم الرسالة أيضاً إلى أجزاء ولكن **بحجم أكبر من حجم الأجزاء** في شيفرات التدفق ، **ويُشفّر أو يفكّ تشفير كل كتلة على حدة.** يختلف عن شيفرات التدفق **بأن حجم المعلومات أكبر لذا فإنها أبطأ.**

إجابات أسئلة الفصل الثالث صفحة ١٥٨

السؤال الأول: وضح المقصود بكل من:

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

السؤال الثاني: يعتبر التشفير من أفضل الوسائل المستخدمة للحفاظ على أمن المعلومات:

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

السؤال الثالث: الهدف من علم التشفير و عناصره :

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

عناصر علم التشفير:

١ – خوارزمية التشفير. ٢ –مفتاح التشفير. ٣ –النص الأصلي. ٤ – النص المشفر.

السؤال الرابع: حدد إلى أي من عناصر التشفير يتبع كل مما يأتي:

أ. مجموعة من الخطوات المستخدمة لتحويل الرسالة الأصلية إلى رسالة مشفرة.	**(خوارزمية التشفير)**
ب. الرسالة بعد عملية التشفير.	**(النص المشفر)**
ج. سلسلة من الرموز التي تستخدم من خلال خوارزمية التشفير.	**(مفتاح التشفير)**
د. الرسالة قبل عملية التشفير.	**(النص الأصلية)**

السؤال الخامس: المعايير التي يتم تصنيف خوارزميات التشفير بناءً عليها:

أ. العملية المستخدمة في التشفير. ب. المفتاح المستخدم. ج. كمية البيانات المرسلة.

السؤال السادس: الفرق بين طريقتي التشفير باستخدام عملية التبديل وعملية التعويض:

أ. التشفير بالتعويض: استبدال حرف مكان حرف أو مقطع مكان مقطع ومثال عليها شيفرة الإزاحة.

ب. التشفير بالتبديل: تبديل أماكن الأحرف من خلال إعادة ترتيب أحرف الكلمة بشرط استخدام نفس الأحرف دون إجراء أي تبديل أو تغيير عليها.

السؤال السابع: سبب تسمية خوارزميات المفتاح الخاص بهذا الاسم:

لأن نفس المفتاح يستخدم لعمليتي التشفير وفك التشفير.

السؤال الثامن: إيجاد النص المشفر لكل نص باستخدام خوارزمية الخط المتعرج:

أ –

Let us keep our home safe and united

علماً بأن مفتاح التشفير: ثلاثة أسطر.

Let▼us▼keep▼our▼home▼safe▼and▼united

١) وزع أحرف النص بشكل قطري في جدول يتكون من ثلاثة سطور.

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

السطر الأول	L ▼ ▼ e o ▼ m s e n u t
السطر الثاني	e u k p u h e a ▼ d n e
السطر الثالث	t s e ▼ r o ▼ f a ▼ i d

النص المشفر:	L▼▼eo▼msenuteukpuhea▼dnetse▼ro▼fa▼id
	L eo msenuteukpuhea dnetse ro fa id

ب

Investing in people is more important than investing in things

علماً بأن مفتاح التشفير: ثمانية أسطر.

Investing▼in▼people▼is▼more▼important▼than▼investing▼in▼things

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▼▼
Igporattn lrtnihvieea nien nigns iitn gtpsm visie pten nomohs

السؤال التاسع : فك تشفير النص الآتي مستخدماً خوارزمية الخط المتعرج علماً بأن مفتاح التشفير عشرة أسطر.

Tnr▼▼o▼eie▼t▼ndbhwvureeeci▼▼sagfmtthuu▼ittsioeutnn

قسّم النص المشفر إلى عشرة أجزاء ؛ لأن مفتاح التشفير عشرة سطور.

عدد الأحرف في كل جزء = ٥٠ ÷ ١٠ = ٥ أحرف في كل جزء.

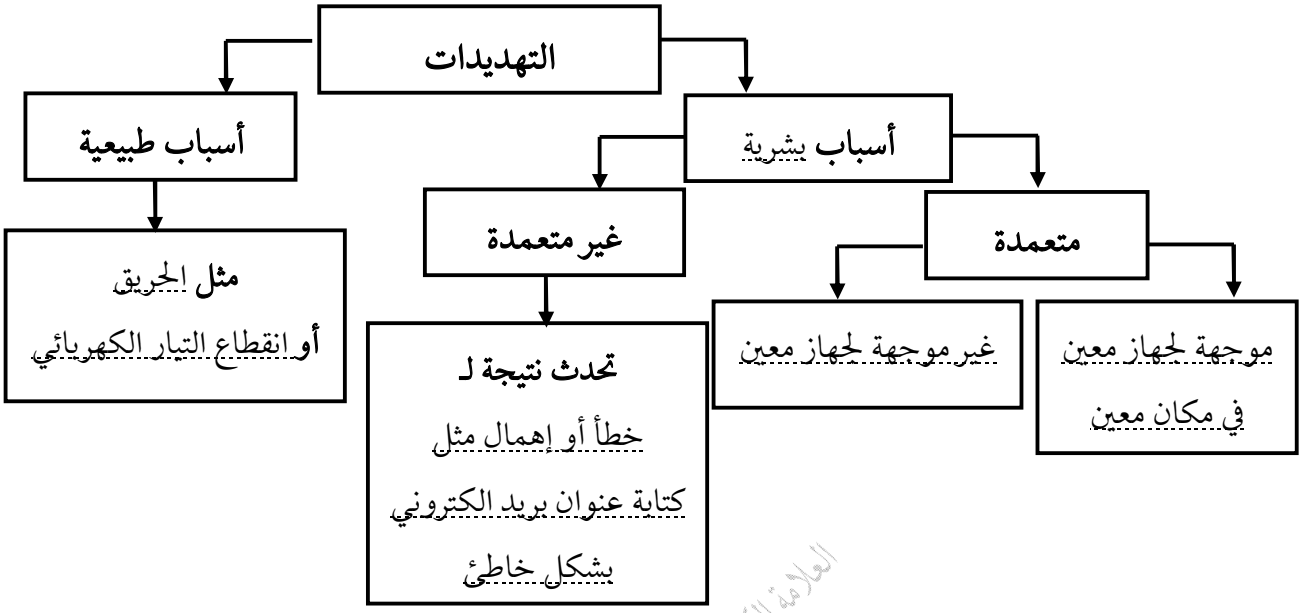
الجزء الأول	T n r ▼ ▼
الجزء الثاني	o ▼ e i e
الجزء الثالث	▼ t ▼ n d
الجزء الرابع	b h w v u
الجزء الخامس	r e e e c
الجزء السادس	i ▼ ▼ s a
الجزء السابع	g f m t t
الجزء الثامن	h u u ▼ i
الجزء التاسع	t t s i o
الجزء العاشر	e u t n n

نأخذ الحرف الأول من كل جزء لتشكيل النص الأصلي :

To▼brighten▼the▼future▼must▼invest▼in▼education

To brighten the future must invest in education

إجابات أسئلة الوحدة الرابعة صفحة ١٥٩

	الإجابة
١	• بناءً على دراستك أنواع التهديدات، أكمل الشكل الآتي: 
٢	• وضح المقصود بالمفاهيم الآتية: **الهندسة الاجتماعية**: هي الوسائل والأساليب التي يستخدمها المعتدي الإلكتروني لجعل مستخدم الحاسوب في النظام يعطي معلومات سرية أو يقوم بعمل ما يسهّل عليه الوصول إلى أجهزة الحاسوب أو المعلومات المخزنة فيها. **السلامة**: حماية الرسائل أو المعلومات التي تم تداولها والتأكد بأنها لم تتعرض لأي عملية تعديل سواء بالإضافة أم الاستبدال أم حذف جزء منها. **مفتاح التشفير**: سلسلة من الرموز المستخدمة في التشفير وتعتمد قوة التشفير على قوة هذا المفتاح.
٣	• عند تعرض المعلومات للهجمات الالكترونية يتأثر واحد أو أكثر من عناصر أمن المعلومات في ما يأتي بعض الاعتراضات للبيانات، حدد عناصر أمن المعلومات التي تتأثر بها: أ – اعتراض الرسالة والتغيير على محتواها. **سلامة المعلومات** ب – الهجوم المزور أو المفبرك. **سرية وسلامة المعلومات** ج – التنصت على المعلومات. **سرية المعلومات.** د – الإدعاء بأنه صديق ويحتاج إلى معلومات. **سلامة وسرية الرسالة.** هـ – قطع قناة الاتصال. **توافر المعلومات**

٤

- فسّر اختلاف **IP Address** للجهاز عند تراسله أكثر من مرة :

بسبب النمط المتغير لتحويل العناوين الرقمية NAT حيث يتم إعطاء الجهاز عنواناً رقمياً مختلفاً في كل مرة يتواصل فيها مع الأجهزة خارج الشبكة الداخلية.

٥

- من المخاطر التي تهدد الشبكات وجود الثغرات ، أذكر ثلاثة أمثلة عليها؟

١ – عدم تحديد صلاحيات الوصول إلى المعلومات.
٢ – مشكلة في تصميم النظام أو في مرحلة التنفيذ.
٣ – عدم كفاية الحماية المادية للأجهزة والمعلومات.

٦

- الوسائل التي يستخدمها المعتدي الالكتروني للتأثير على الجانب النفسي للشخص المستهدف :

١ – الإقناع.	٢ – انتحال الشخصية

٧

- تعد الثغرات من المخاطر التي تهدد أمن المعلومات ؛ وضح ذلك :

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

٨

- أوجد النص المشفر لكل نص مما يأتي مستخدماً خوارزمية الخط المتعرج Zig Zag :

أ. **Youth is the future and the spirit of our home**

مفتاح التشفير **أربعة سطور**

وزع أحرف النص بشكل قطري في جدول يتكون من أربعة سطور.

Y		**t**		▼		▼		**u**		**a**		**t**		**s**		**i**		**f**		**r**		**m**			
	o		▼		**T**		**f**		**r**		**n**		**h**		**p**		**t**		▼		▼		**e**		
		u		**i**		**h**		**u**		**e**		**d**		**e**		**i**		▼		**o**		**h**		▼	
			t		**S**		**e**		**t**		▼		▼		▼		**r**		**o**		**u**		**o**		▼

Yt▼▼uatsifrmo▼tfrnhpt▼▼euihuedei▼oh▼tset▼▼▼rouo▼	**النص المشفر** :
Yt uatsifrmo tfrnhpt euihuedei oh tset rouo	

٨

ب –

School is the place where great people and ideas are formed

مفتاح التشفير ستة أسطر.

School is the place where great people and ideas are formed

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	▼

النص المشفّر:

S▼eeetl▼▼oci▼▼▼▼eiarhspwgp▼drmo▼lhreaeeeotaeeona▼dlhcrapdsf▼

٩

- فك تشفير كل نص من النصوص الآتية علماً بان مفتاح التشفير هو ستة أسطر:

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

عدد أحرف النص + الفراغات(المثلثات) = ٤٨

عدد الأحرف في كل جزء = ٤٨ ÷ ٦ = ٨ أحرف في كل 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

نأخذ الحرف الأول من كل جزء لتشكيل النص الأصلي:

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

Home sweet home let us keep it sweet please

١٠

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

أ – المفتاح المستخدم :	**(١) باستخدام المفتاح الخاص.**	**(٢) باستخدام المفتاح العام.**
ب – كمية المعلومات المرسلة :	**(١) شيفرات التدفق.**	**(٢) شيفرات الكتل.**
ج – العملية المستخدمة للتشفير:	**(١) التشفير بالتعويض.**	**(٢) التشفير بالتبديل.**

" تمت بحمد الله وتوفيقه"

محبكم دوماً وليس يوماً

الأستاذ: سامر جديع ٢٠١٨