النموذجية في الحاسوب

للفروع الأكاديمية و المهنية

الوحدة الرابعة – أمن المعلومات و التشفير

١	٢	٣
الفصل الأول **أمن المعلومات** أولاً مقدمة في أمن المعلومات – ص٣ ثانياً الهندسة الاجتماعية – ص١٤	الفصل الثاني **أمن الإنترنت** أولاً الاعتداءات الإلكترونية على الويب – ص٢٤ ثانياً تقنية تحويل العناوين الرقمية – ص٢٧	الفصل الثالث **التشفير** أولاً مفهوم علم التشفير و عناصره – ص٣٩ ثانياً خوارزميات التشفير – ص٤٣

أبنائي الطلبة .... نُقدم لكم هذه المادة لكي نكون معًا خطوة بخطوة نحو التميز – بإذن الله –

- اهتمت الشعوب قديماً بالحفاظ على سرية المعلومات ؟؟؟؟
  - للحفاظ على أسرارها وهيبتها ومكانتها
- اعتمدت سرية المعلومات على موثوقية حاملها و قدرته على توفير الظروف المناسبة لمنع اكتشافها
- بتطور العلم واستخدام شبكات الحاسوب أصبح من الضروري إيجاد طرائق جديدة لحماية المعلومات ، منها :
  - طرائق مادية
  - تطورت لحماية قنوات الاتصال والمعلومات
  - استخدام أساليب كثيرة لحماية المعلومات والأجهزة الخاصة فيها
  - تدريب الكادر البشري وتوعيته

الفصل الأول
أمن المعلومات

سؤال : علل .. يُعدُّ أمن المعلومات من أهم الركائز التي تعتمد عليها الدول والمؤسسات والأفراد ؟
للحفاظ على موقفها العالمي سياسياً و مالياً

سؤال : ما هو سبب سهولة تناقل المعلومات والحصول عليها ؟
بسبب التطور الهائل الذي حصل في مجالي الإنترنت و البرمجيات

سؤال : 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

أولاً مقدمة في أمن المعلومات

سؤال : أحد الآتية هو فرع من فروع أمن المعلومات ، هو :

أ) التجارة الإلكترونية ب) المعرفة الضمنية ج) أمن الشبكات وكيفية حمايتها د) الروبوتات

الجواب (ج) :
أمن الشبكات وكيفية حمايتها

- ما هو أمن المعلومات ؟
- كيف نقوم بالحدّ من مخاطر أمن المعلومات ؟؟
- ما هي ضوابط أمن المعلومات ؟؟؟

Gooo

1 مفهوم 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 **إبقائها متاحة** للأفراد المصرح لهم باستخدامها .

سؤال : ما هي وظيفة أمن المعلومات ؟

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 .

سؤال : **علل. أمن المعلومات يعمل على حماية المعلومات والمعدات المستخدمة لتخزينها ومعالجتها ونقلها من السرقة أو التطفل أو من الكوارث الطبيعية**

ليعمل على إبقائها متاحة للأفراد المصرح لهم باستخدامها

سؤال : أذكر الخصائص الأساسية لأمن المعلومات ؟

١) السرية ٢) السلامة ٣) توافر المعلومات

إليكم توضيح لهذه الخصائص :

السرّية **سرية المعلومات** **Confidentiality**

عدم القدرة على الحصول على المعلومات **إلا** من قِبَل الأشخاص المخول بهم بذلك

أي ..

أنَّ الشخص المخول هو الوحيد القادر على الوصول إلى المعلومات والاطلاع عليها

سرية المعلومات

- **مفهوم الأمن**
- **مفهوم الخصوصية**

- وهو مصطلح مرادف لمفهومي الأمن (**Security**) والخصوصية (**Privacy**)
- **مثال** على سرية المعلومات :
  - المعلومات الشخصية
  - الموقف المالي لشركة ما قبل إعلانه
  - المعلومات العسكرية

سؤال : أذكر أمثلة على بيانات يعتمد أمنها على مقدار الحفاظ على سريتها ؟

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

السلامة Integrity

أي حماية الرسائل أو المعلومات التي تمَّ تداولها ، والتأكد بأنها لم تتعرض لأي تعديل **سواء** :
إضافة .. **أم** .. استبدال .. **أم** .. حذف جزء منها

أمثلة على سلامة المعلومات :

- نتائج طلبة الثانوية العامة (الحفاظ على سلامة هذه النتائج من أي تعديلات)
- قوائم القبول الموحد للجامعات الأردنية والتخصصات التي قُبِلَ بها الطلبة
  (العمل على حماية القوائم من أي **تعديل** أو **حذف** أو **تبديل** أو **تغيير**)

سؤال : أذكر أمثلة على أهمية سلامة المعلومات فيها ؟

١) نتائج طلبة الثانوية العامة
٢) قوائم القبول الموحد للجامعات الأردنية والتخصصات التي قُبِلَ بها الطلبة

التوافر توافر المعلومات Availabiltiy

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

- يُعدُّ الحفاظ على سلامة المعلومات وسريتها **أمرين مهمين** :
  - وتكون المعلومات **بلا فائدة** ...
    إذا لم تكن متاحة للأشخاص المصرح لهم بالتعامل معها
  - أو أنَّ الوصول إليها يحتاج إلى **وقتٍ كبير**

سؤال : أذكر أمثلة على وسائل عدم توافر المعلومات (ما يقوم به المخترقون) ؟

١) حذفها ٢) الاعتداء على الأجهزة التي تُخَزَّن فيها هذه المعلومات

الحذف والاعتداء على الأجهزة التي تخزن فيها المعلومات ، هي أمثلة على :
أ) عدم توافر المعلومات
ب) السلامة ج) سرية المعلومات
د) الاختراق
الإجابة

أحد الآتية لا تعتبر من الخصائص الأساسية لأمن المعلومات ، هي :
أ) السرية ب) التخزين
ج) التوافر د) السلامة
الإجابة

2 المخاطر التي تُهدّد أمن المعلومات

ما هي أنواع المخاطر التي تُهدد أمن المعلومات ؟

١) التهديدات ٢) الثغرات

1 التهديدات Threats

- يحدث التهديد لأسباب **طبيعية** ، مثل :
  - حدوث حريق
  - انقطاع التيار الكهربائي

  مما يُؤدي إلى فقدان المعلومات

- يحدث التهديد لأسباب **بشرية**
  - ممكن تكون غير متعمدة
    - وتحدث نتيجة **لإهمال أو خطأ**

    مثل كتابة عنوان بريد إلكتروني بشكل غير صحيح
  - وقد تكون متعمدة ... وهي قسمين :
    - (١) **غير موجهة لجهاز معين** ... ((**مثل نشر فيروس** بين الحواسيب))
    - (٢) **موجهة لجهاز معين** .. ويُسمَّى الهجوم الإلكتروني **Attack** أو الاعتداء الإلكتروني

مثل [سرقة جهاز الحاسوب أو إحدى المعدات التي تحفظ المعلومات
أو التعديل على ملف أو حذف
أو الكشف عن بيانات سرية
أو منع الوصول إلى المعلومات **]**

سؤال : أذكر أنواع (الأسباب) التهديدات التي تهدد أمن المعلومات .

١) طبيعية ٢) بشرية

سؤال : ما هي أنواع (الأسباب) التهديدات البشرية التي تهدد أمن المعلومات ؟

١) غير متعمدة ٢) متعمدة

سؤال : أذكر أقسام التهديدات البشرية المتعمدة و التي تهدد أمن المعلومات ؟

١) غير موجهة لجهاز معين ٢) موجهة لجهاز معين

سؤال : ما هو مفهوم الهجوم الإلكتروني أو الاعتداء الإلكتروني ؟

هو قسم من التهديدات البشرية على المعلومات وتكون متعمدة ، وهي موجهة لجهاز معين .

مثل :
سرقة جهاز الحاسوب
أو إحدى المعدات التي تحفظ المعلومات
أو التعديل على ملف أو حذف
أو الكشف عن بيانات سرية
أو منع الوصول إلى المعلومات

سؤال : أذكر أمثلة على الهجوم الإلكتروني أو الاعتداء الإلكتروني ؟

- سرقة جهاز الحاسوب أو إحدى المعدات التي تحفظ المعلومات
- التعديل على ملف أو حذف
- الكشف عن بيانات سرية
- منع الوصول إلى المعلومات

الهجوم الإلكتروني [الاعتداء الإلكتروني]
تهديد موجه ومتعمّد لجهاز معين و بقصد الإضرار به

المعلم - بسَّام القواسمة
٠٧٨٨٠٨٥٩٣٨

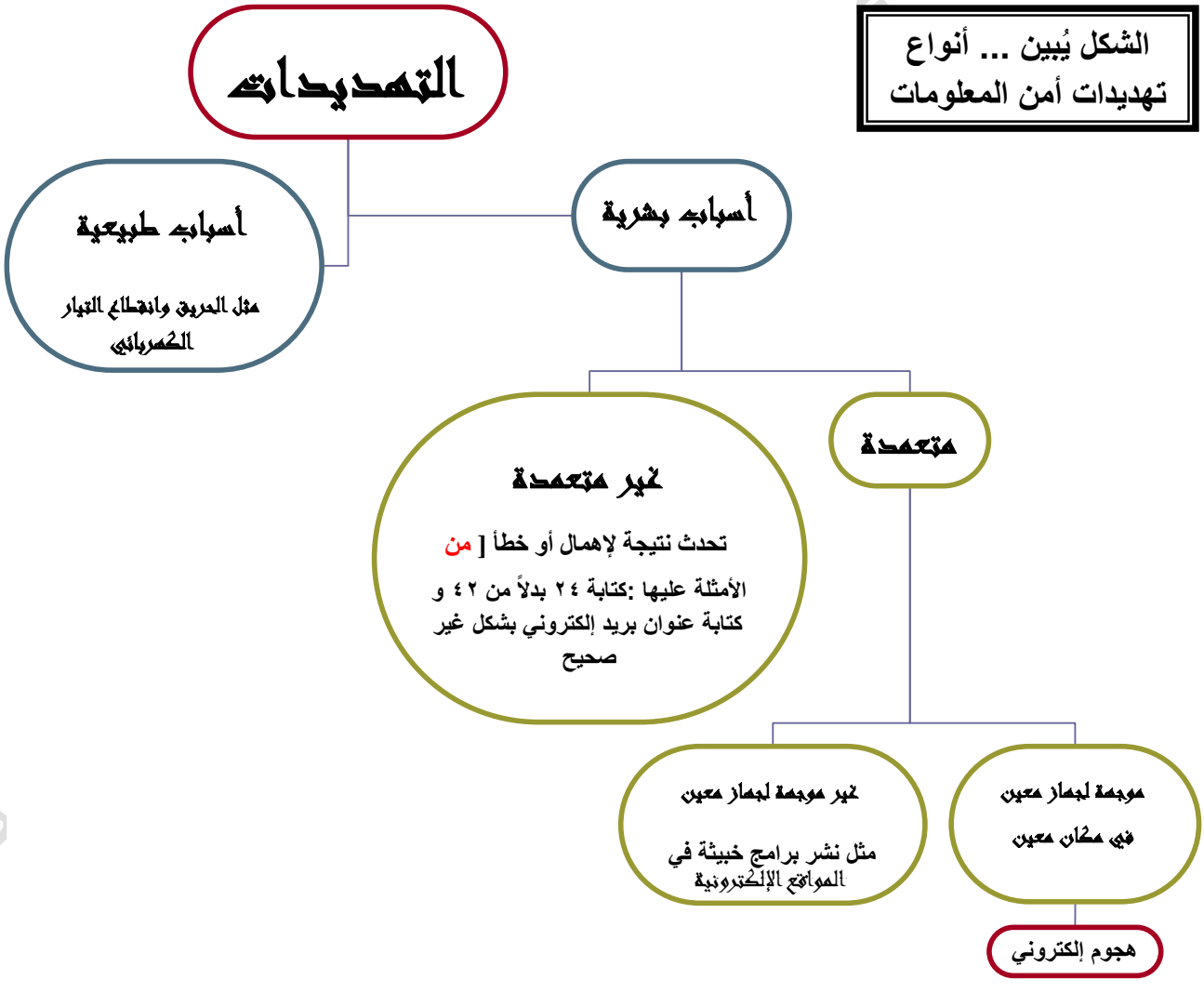
انقطاع التيار الكهربائي و الحريق توضح نوع من التهديدات ، هي :
أ) بشرية متعمدة
ب) طبيعية غير متعمدة
ج) طبيعية د) اهمال بشري
الإجابة

نشر برامج خبيثة ، هو نوع من أنواع التهديدات المتعلقة بالمعلومات ، تصنف أنها :
أ) متعمدة وغير موجهة لجهاز معين
ب) بشرية ج) طبيعية
د) متعمدة و موجهة لجهاز معين
الإجابة

تصنف التهديدات المتعلقة بالمعلومات إلى نوعين،هما :
أ) بشرية متعمدة
ب) حريق
ج) انقطاع التيار الكهربائي
د) بشرية و طبيعية
الإجابة

تهديد بشري متعمد وموجه لجهاز معين في مكان معين ، يسمّى :
أ) اختراق ب) نشر الفيروسات
ج) هجوم إلكتروني
د) نقطة ضعف في النظام
الإجابة

الشكل يُبين ... أنواع تهديدات أمن المعلومات



سؤال : أذكر أخطر أنواع التهديدات ؟

الاعتداء الإلكتروني

سؤال : أذكر العوامل الرئيسة لنجاح الهجوم أو الاعتداء الإلكتروني ؟

١) الدافع ٢) الطريقة ٣) فرصة النجاح

سؤال : علل..يجب الأخذ في الحسبان الدافع و الطريقة و فرصة النجاح عند الهجوم أو الاعتداء الإلكتروني؟

لتقييم التهديد الذي يتعرض له النظام

(١) سؤال : أذكر أمثلة على دوافع الأفرادعند تنفيذ الهجوم أو الاعتداء الإلكتروني ؟

١) رغبة في الحصول على المال
٢) محاولة لإثبات القدرات التقنية
٣) بقصد الإضرار بالآخرين

(٢) سؤال : ما الذي تتضمنه الطريقة في الهجوم الإلكتروني ؟

- المهارات التي يتميز بها المعتدي الإلكتروني
- قدرته على توفير المعدات والبرمجيات الحاسوبية التي يحتاج إليها
- معرفته بتصميم النظام وآلية عمله
- معرفة نقاط القوة والضعف لهذا النظام

(٣) سؤال : وضح كيف تتمثل فرصة نجاح الهجوم الإلكتروني ؟

- تحديد الوقت المناسب للتنفيذ
- كيفية الوصول إلى الأجهزة

واحدة من التالية تتمثل فيها فرصة نجاح الهجوم الإلكتروني ، هي :
أ) تحديد نوع الفيروس
ب) تحديد الوقت المناسب للتنفيذ
ج) متعمدة د) نشر فيروس
الإجابة

واحدة من التالية ليست من دوافع الأفراد لتنفيذ اعتداء إلكتروني ، هي :
أ) اثبات القدرات التقنية ب) الرغبة في المال
ج) أمور سياسية
د) الإضرار بالآخرين
الإجابة

قدرة المعتدي على توفير المعدات والبرمجيات الحاسوبية التي يحتاج إليها من الأمور التي تتضمنها الطريقة في الهجوم الإلكتروني .
أ) نعم
ب) لا
الإجابة

متى يجب الاهتمام بالدافع و الطريقة و فرصة النجاح؟
أ) لتقييم التهديد
ب) متعمدة
ج) موجهة لجهاز
د) عند الهجوم الإلكتروني
الإجابة

أنواع الاعتداءات الإلكترونية التي تتعرض إليها المعلومات

سؤال : **أذكر أنواع الاعتداءات الإلكترونية التي تتعرض إليها المعلومات ؟**

١) التنصت على المعلومات
٢) التعديل على المحتوى
٣) الإيقاف
٤) الهجوم المزور أو المفبرك

توضيح الاعتداءات الإلكترونية التي تتعرض لها المعلومات :

1 التنصت على المعلومات

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

2 التعديل على المحتوى

- **يتم اعتراض المعلومات ... وتغيير محتواها وإعادة إرسالها للمُستَقْبِل ... من دون أن يعلم بتغيير محتواها ...**
- **وهنا يكون الإخلال بسلامة المعلومات**

3 الإيقاف

- **يتم قطع قناة الاتصال ... ثم منع المعلومات من الوصول إلى المُستَقْبِل ...**
- **وهنا تُصبح المعلومات غير متوافرة**

4 الهجوم المزور أو المفبرك

- **يتمثل بإرسال المعتدي الإلكتروني رسالة إلى أحد الأشخاص على الشبكة ... يُخبره فيها بأنَّهُ صديقه ويحتاج إلى معلومات أو كلمات سرية خاصة ...**
- **تتأثر بهذه الطريقة سرية المعلومات**
- **وقد تتأثر أيضاً سلامتها**

2 الثغرات Vulnerability

- **هي نقطة ضعف في النظام ، سواء أكانت في الإجراءات المتبعة ، مثل :**
  - عدم تحديد صلاحيات الوصول إلى المعلومات
  - مشكلة في تصميم النظام
- **وعدم كفاية الحماية المادية للأجهزة والمعلومات .**

تُعدُّ من نقاط الضعف التي قد تتسبب في :

- فقدان المعلومات أو هدم النظام
- أو تجعله عرضةً للاعتداء الإلكتروني

3 الحدِّ من مخاطر أمن المعلومات

سؤال : ما السبب في وضع ضوابط للتقليل من مخاطر التي تتعرض لها المعلومات والحد منها ؟

لأنَّ المختصون في مجال أمن المعلومات يرون أنَّ الحفاظ على المعلومات وأمنها ...
ينبع من التوازن بين :

١) تكلفة الحماية وفعالية الرقابة من جهة
٢) احتمالية الخطر من جهة أخرى

ضوابط تقليل المخاطر على المعلومات والحدِّ منها

سؤال : أذكر الضوابط لتقليل المخاطر التي تتعرض لها المعلومات و للحد منها ؟

١) ضوابط مادية
٢) ضوابط إدارية
٣) ضوابط تقنية

توضيح ضوابط تقليل المخاطر على المعلومات :

1 الضوابط المادية

يُقصد بها :
مراقبة بيئة العمل و حمايتها من الكوارث الطبيعية وغيرها
مثل :
١ـ استخدام الجدران والأسوار
٢ـ استخدام الأقفال
٣ـ وجود حراس الأمن وغيرها
٤ـ أجهزة إطفاء الحريق

2 ضوابط إدارية

يُقصد بها :
تستخدم مجموعة من الأوامر والإجراءات المتفق عليها
مثل :
١ـ القوانين واللوائح والسياسات
٢ـ الإجراءات التوجيهية
٣ـ حقوق النشر
٤ـ براءات الاختراع و العقود والاتفاقيات

3 ضوابط تِقَنيّة

يُقصد بها :
هي الحماية التي تعتمد على التقنيات المستخدمة سواء كانت مكونات (hardware) أو برمجيات (Software) .
وتتضمن :
١ـ كلمات المرور
٢ـ منح صلاحيات الوصول
٣ـ بروتوكولات الشبكات و الجدر النارية
٤ـ التشفير
٥ـ تنظيم تدفق المعلومات في الشبكة

سؤال : ما هو ناتج عمل ضوابط تقليل المخاطر التي تتعرض لها المعلومات بشكل متكامل ؟

١- للوصول إلى أفضل النتائج

٢- للحد من الأخطار التي تتعرض لها المعلومات

يرى المختصون في أمن المعلومات أن التوازن بين تكلفة الحماية وفعالية الرقابة و احتمالية الخطر يتم من خلالهما الحفاظ على المعلومات وأمنها :

أ) نعم
ب) لا

الإجابة

واحدة من الآتية لا تُعتبر من ضوابط تقليل المخاطر على المعلومات :

أ) ضوابط لوجستية
ب) ضوابط مادية
ج) ضوابط إدارية
د) ضوابط تقنية

الإجابة

وجود حراس أمن وأجهزة إطفاء للحريق ، هي من الضوابط :

أ) الإدارية
ب) التقنية
ج) الاقتصادية
د) المادية

الإجابة

استخدام مجموعة من الأوامر والاجراءات المتفق عليها في الضوابط الإدارية ، أحد الآتية مثالا عليها :

أ) حقوق النشر
ب) حقوق التعليم
ج) حقوق البرمجة
د) حقوق طباعة الإعلانات

الإجابة

أحد الآتية ليست من أنواع الاعتداءات الإكترونية على المعلومات :

أ) التنصت على المعلومات
ب) التعديل على المعدات
ج) الإيقاف
د) الهجوم المفبرك

الإجابة

الحصول على المعلومة يُؤدي إلى الإخلال بسريتها،ويتم من خلال نوع من أنواع الاعتداءات الإلكترونية ، هو :

أ) التعديل على المحتوى
ب) الهجوم المزور
ج) التنصت على المعلومات
د) الإيقاف

الإجابة

نوع من الإعتداءات الإلكترونية على المعلومات يؤثر في سرية المعلومة وسلامتها ، هو :

أ) الإيقاف
ب) التعديل على المحتوى
ج) التنصت
د) الهجوم المزور

الإجابة

مشكلة في تصميم النظام وعدم تحديد صلاحيات الوصول للمعلومات ، تُعتبر :

أ) نقطة ضعف في النظام
ب) فقدان المعلومات
ج) عدم كفاية الحماية المادية
د) يكون عرضة للإعتداء

الإجابة

عدم كفاية الحماية المادية للأجهزة والمعلومات ، قد يتسبب في :

أ) فقدان المعلومات
ب) هدم النظام
ج) جعله عرضة للهجوم الإلكتروني
د) جميع ما ذكر

الإجابة

بروتوكولات الشبكات و تنظيم تدفق المعلومات في الشبكة ، جميعها أمثلة على نوع من أنواع ضوابط تقليل المخاطر على المعلومات ، هي :

أ) ضوابط إدارية ب) ضوابط فنية
ج) ضوابط تقنية
د) ضوابط مادية

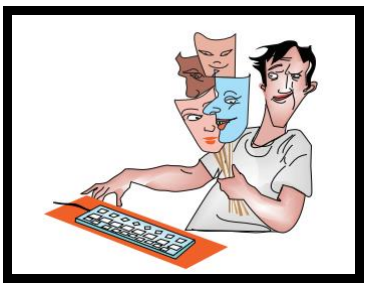
الإجابة

ثانيًا

الهندسة الاجتماعية

- ما هو المقصود في الهندسة الاجتماعية ؟
- ما هي مجالات الهندسة الاجتماعية ؟؟
- ما المقصود بالجانب النفسي في الهندسة الاجتماعية ؟؟؟

Gooo



سؤال : ما سبب الاهتمام في العنصر البشري في مجال أمن المعلومات ؟

١) هو من أهم مكونات الأنظمة
٢) من أهم المجالات للحفاظ على أمن المعلومات

سؤال : وضح كيفية اختيار الكادر البشري المسؤول عن حماية الأنظمة ؟

على ماذا يعتمد الاختيار ؟

١) كفايته العلمية
٢) اختبارات شفوية وورقية
٣) إخضاعهم إلى ضغوط نفسية (كلٌّ حسب موقعهم)

سؤال : علل .. يتعرض الكادر البشري المسؤول عن حماية الأنظمة إلى ضغوط واختبارات ؟

للتأكد من قدرتهم على حماية النظام

سؤال : أذكر أخطر ما يُهدد نُظم المعلومات ؟

الهندسة الاجتماعية

1 مفهوم الهندسة الاجتماعية

- هي **الوسائل والأساليب** التي يستخدمها المعتدي الإلكتروني
- لجعل مستخدم الحاسوب في النظام **يُعطي معلومات** سرية أو يقوم بعمل ما
- **يُسَهِّل** عليه الوصول إلى أجهزة الحاسوب أو المعلومات المُخَزَّنة فيها .

سؤال : علل .. تُعدُّ الهندسة الاجتماعية من أنجح الوسائل وأسهلها المستخدمة في الحصول على معلومات غير مصرح بالاطلاع عليها ؟

بسبب :

١) قلة اهتمام المتخصصين في مجال أمن المعلومات

٢) عدم وعي مستخدمي الحاسوب بالمخاطر المترتبة عليها

2 مجالات الهندسة الاجتماعية

تتركز الهندسة الاجتماعية في مجالين هما ....

(1) البيئة المحيطة

(2) الجانب النفسي

البيئة المحيطة تشمل

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

الجانب النفسي تشمل

١- الإقناع
٢- انتحال الشخصية والمداهنة
٣- مسايرة الركب

توضيح كل ما تشمله البيئة المحيطة :

1 مكان العمل

يكتب ..
بعض الموظفين كلمات المرور على أوراق ملصقة بشاشة الحاسوب
وعند دخول الشخص غير المخول له الاستخدام
(كزبون أو حتى عامل نظافة أو عامل صيانة)
النتيجة ..
يستطيع معرفة كلمة المرور =>
وبعدها يتمكن من الدخول إلى النظام بسهولة
(ليحصل على المعلومات التي يُريدها)

2 الهاتف

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

3 النفايات الورقية

يدخل الأشخاص غير المخولين إلى مكان العمل
ويجمعون النفايات التي قد تحتوي على :
١ـ كلمات المرور
٢ـ معلومات تخص الموظفين
٣ـ أرقام هواتفهم وبياناتهم الشخصية
٤ـ قد تحتوي على تقويم العام السابق وكل ما يحتويه من معلومات
النتيجة :
١ـ يُمكن استغلالها في تتبع أعمال الموظفين
٢ـ الحصول على المعلومات المرغوبة

4 الإنترنت

من أكثر الوسائل شيوعاً ...
بسبب استخدام الموظفين أو مستخدمي الحاسوب عادةً كلمة المرور نفسها للتطبيقات جميعها .
حيثُ يُنشئ المعتدي الإلكتروني موقعاً على الشبكة
يُقدم خدمات معينة
ويشترط التسجيل فيه للحصول على هذه الخدمات
يتطلب التسجيل في الموقع (اسم مستخدم و كلمة المرور) .
وهي كلمة المرور نفسها التي يستخدمها الشخص عادةً =>
النتيجة :
وبهذه الطريقة يتمكن المعتدى الإلكترونى من الحصول عليها

من أهم مكونات الأنظمة ومن أهم المجالات للحفاظ على أمن المعلومات ، هو:
أ) الهاتف
ب) النفايات الورقية
ج) العنصر البشري
د) الإنترنت
الإجابة

يعتمد اختيار الكادر البشري المسؤول عن حماية الأنظمة على أمور عدة ، منها :
أ) كفايته العلمية
ب) اختبارات شفوية وورقية
ج) إخضاعهم إلى ضغوط نفسية
د) جميع ما ذكر
الإجابة

يتعرض الكادر البشري المسؤول عن حماية الأنظمة إلى ضغوط واختبارات ، بسبب :
أ) للتأكد من قدرتهم التقنية
ب) للتأكد من قدرتهم المعلوماتية
ج) للتأكد من قدرتهم المعرفية
د) للتأكد من قدرتهم على حماية النظام
الإجابة

أخطار نظم المعلومات عديدة ، من أخطرها :
أ) الهندسة الاجتماعية
ب) البيئة المحيطة
ج) الجانب النفسي
د) النفايات الورقية
الإجابة

أحد التالية ، هي الوسائل والأساليب التي يستخدمها المعتدي الإلكتروني :
أ) الهندسة الاجتماعية
ب) التعديل على المعدات
ج) الإيقاف
د) الهجوم المفبرك
الإجابة

بعد تجميع النفايات الورقية من مكاتب الموظفين ، يمكن للشخص غير المخول الحصول على :
أ) كلمات المرور ب) معلومات تخص الموظفين
ج) أرقام هواتفهم وبياناتهم الشخصية
د) جميع ما ذكر
الإجابة

من أكثر الوسائل شيوعاً بسبب استخدام الموظفين أو مستخدمي الحاسوب عادةً كلمة المرور نفسها للتطبيقات جميعها ، هذه من الأمور المتعلقة بالبيئة المحيطة،هي :
أ) الإقناع ب) الإنترنت
ج) انتحال الشخصية
د) مسايرة الركب
الإجابة

الإقناع ومسايرة الركب وانتحال الشخصية والمداهنة جميعها من ضمن :
أ) الجانب النفسي
ب) الإنترنت
ج) مكان العمل
د) البيئة المحيطة
الإجابة

الجانب النفسي :

- يسعى المعتدي الإلكتروني هنا لكسب ثقة مستخدم الحاسوب
  - ومن ثم ... الحصول على المعلومات التي يرغب بها
    - يستخدم لذلك أساليب ... من أشهرها :

توضيح كل ما يشمله الجانب النفسي :

1 الإقناع

يستطيع المعتدي إقناع الموظف أو مستخدم الحاسوب بطريقتين ، هما :

١) مباشرة :
بحيث يُقدِّم الحجج المنطقية والبراهين .

٢) غير مباشرة :
وتتم كما يلي :

أ) 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

ب) أو إغراء المستخدم بامتلاك خدمة نادرة (حيث يُقدم له عرضاً مُعيناً من خلال موقعه الإلكتروني لمدة محدودة)
نتيجة ذلك :
يُمكّنه ذلك من الحصول على كلمة المرور .

ج) وقد يلجأ المعتدي الإلكتروني إلى إبراز أوجه التشابه مع الشخص المستهدف ، السبب :
لإقناعه بأنه يحمل الصفات والاهتمامات نفسها
نتيجة ذلك :
أ) يُصبح الشخص أكثر ارتياحاً و أقل حذراً للتعامل معه
ب) فيقدم له ما يريد من معلومات.

2 انتحال الشخصية والمداهنة

حيث يتقمص شخص شخصية آخر :
هذا الشخص قد يكون شخصاً حقيقياً أو وهمياً
منها :
١- فقد ينتحل شخصية فني صيانة معدات الحاسوب
٢- عامل نظافة
٣- حتى المدير
٤- السكرتير
ولأنَّ .. الشخصية المنتحلة غالباً تكون ذات سلطة :
١- يُبدي أغلب الموظفين خدماتهم
٢- ولن يترددوا بتقديم أي معلومات لهذا الشخص المسؤول

3 مسايرة الركب

حيث يرى الموظف بأنه إذا قام زملاؤه جميعهم بأمر ما
- فمن غير اللائق أن يأخذ هو موقفاً مغايراً
توضيح :
فعندما يُقدم شخص نفسه على أنَّهُ إداري من فريق الدعم الفني ، ويرغب بعمل تحديثات على الأجهزة ..
- فإذا سمح له أحد الموظفين بعمل تحديث على جهازه
- فإنَّ باقي الموظفين يقومون بمسايرة زميلهم غالباً
- والسماح لهذا المعتدي باستخدام أجهزتهم لتحديثها
النتيجة :
ومن ثم =>
يتمكن من الإطلاع على المعلومات التي يُريدها والمخزنة على الأجهزة

والله الـ 200 في متناول اليّد
المادة فِعلاً من الآخر

الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله
الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله

إجابات أسئلة الفصل الأول

أسئلة الفصل

١ – وضّح المقصود بكلٍّ من: أمن المعلومات، الثغرات.

إجابة (١)

أمن المعلومات	وهو 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
الثغرات	وهي نقطة الضعف في النظام سواء أكانت في الإجراءات المتبعة مثل عدم تحديد صلاحيات الوصول إلى المعلومات أو مشكلة في تصميم النظام وعدم كفاية الحماية المادية للأجهزة والمعلومات تُعدُّ من نقاط الضعف التي قد تتسبب في فقدان المعلومات أو هدم النظام أو تجعله عرضةً للاعتداء الإلكتروني

٢ – يهدف أمن المعلومات للحفاظ على ثلاث خصائص أساسية هي: (سرّية المعلومات، وسلامة المعلومات، وتوافر المعلومات) حدّد إلى أي هذه الخصائص يتبع كلّ مما يأتي:

أ – التأكد من عدم حدوث أي تعديل على المعلومات .....

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

جـ– الوصول إلى المعلومات يحتاج إلى وقت كبير .....

د – مصطلح مرادف لمفهومي الأمن والخصوصية .....

هـ – المعلومات العسكرية .....

إجابة (٢)

(أ)	(ب)	(ج)	(د)	(هـ)
سلامة المعلومات	سرية المعلومات	توافر المعلومات	سرية المعلومات	سرية المعلومات

٣ – توجد ثلاثة عوامل رئيسة تؤخذ في الحسبان لتقييم التهديد. بناءً على دراستك الوحدة، حدّد العامل الذي يندرج تحته كلّ مما يأتي:

أ – الرغبة في إثبات القدرات .....

ب– معرفة نقاط القوة والضعف للنظام .....

جـ– تحديد الوقت المناسب لتنفيذ الهجوم الإلكتروني .....

د – الإضرار بالآخرين .....

هـ – الرغبة في الحصول على المال .....

و – القدرة على توفير المعدات والبرمجيات الحاسوبية .....

إجابة (٣)

(أ)	(ب)	(ج)	(د)	(هـ)	(و)
الدافع	الطريقة	فرصة النجاح	الدافع	الدافع	الطريقة

٤ – عدّد أربعة من أنواع الاعتداءات الإلكترونية، التي تتعرّض لها المعلومات.

إجابة (٤)

١) التنصت على المعلومات
٢) التعديل على المحتوى
٣) الإيقاف
٤) الهجوم المزور أو المفبرك

٥ – علّل ما يأتي:

أ – استخدام بعض الضوابط في نظام المعلومات.

ب– تُعدّ الهندسة الاجتماعية من أنجح الوسائل وأسهلها للحصول على المعلومات.

إجابة (٥)

(أ)	لأنَّ المختصون في مجال أمن المعلومات ... يرون أنَّ الحفاظ على المعلومات وأمنها ... ينبع من التوازن بين تكلفة الحماية وفعالية الرقابة من جهة .. و .. احتمالية الخطر من جهة أخرى .
(ب)	١) بسبب قلة اهتمام المتخصصين في مجال أمن المعلومات ٢) عدم وعي مستخدمي الحاسوب بالمخاطر المترتبة عليها

٦- قارن بين الضوابط المادية والضوابط الإدارية، من حيث:

وجه المقارنة	الضوابط المادية	الضوابط الإدارية
المقصود بها		
أمثلة عليها		

إجابة (٦)

وجه المقارنة	الضوابط المادية	الضوابط الإدارية
المقصود بها	يُقصد بها ... مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها ...	تُستخدم مجموعة من الأوامر والإجراءات المتفق عليها ...
أمثلة عليها	مثل (استخدام الجدران والأسوار و استخدام الأقفال ... ووجود حراس الأمن وغيرها ... وأجهزة إطفاء الحريق	مثل (القوانين واللوائح والسياسات والإجراءات التوجيهية و حقوق النشر و براءات الاختراع و العقود والاتفاقيات)

٧ – وضّح آلية عمل الهندسة الاجتماعية، في كلّ مجال من المجالات الآتية:

المجال	آلية العمل
مكان العمل	
الهاتف	
انتحال الشخصية	
الإقناع	

إجابة (٧)

المجال	آلية العمل
مكان العمل	يكتب بعض الموظفين كلمات المرور على أوراق ملصقة بشاشة الحاسوب ... وعند دخول الشخص غير المخول له الاستخدام (كزبون أو حتى عامل نظافة أو عامل صيانة ... يستطيع معرفة كلمة المرور => وبعدها يتمكن من الدخول إلى النظام بسهولة (ليحصل على المعلومات التي يُريدها)
الهاتف	يتصل الشخص غير المخول بمركز الدعم الفني هاتفياً ... يطلب إليه بعض المعلومات الفنية ... ويستدرجه للحصول على كلمات المرور وغيرها من المعلومات => ليستخدمها في ما بعد
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) . ولأنَّ ((الشخصية المنتحلة غالباً تكون ذات سلطة ... يُبدي أغلب الموظفين خدماتهم ... ولن يترددوا بتقديم أي معلومات لهذا الشخص المسؤول))
الإقناع	يستطيع المعتدي إقناع الموظف أو مستخدم الحاسوب بطريقة مباشرة ... بحيث يُقدِّم 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...

الفصل الثاني أمن الإنترنت

سؤال : علل .. انتشرت البرامج والتطبيقات المجانية و غير معروفة المصدر و المفتوحة وبرامج القرصنة ؟

بسبب اعتماد :
الأفراد والمؤسسات والحكومات على تكنولوجيا المعلومات والاتصالات بشكل واسع و في شتى المجالات

سؤال : ما هو سبب وجود وسائل تعمل على حماية الويب والحد من الاعتداءات و الأخطار التي تهددها؟

بسبب :
١) إنتشار البرامج والتطبيقات بشكل كبير ، **وهي** :
أ- المجاني ب- غير معروف المصدر ج- المفتوح
٢) إنتشار البرامج المقرصنة والمعلومات الخاصة بكيفية اقتحام المواقع

سؤال : أذكر أنواع البرامج والتطبيقات التي انتشرت بشكل كبير بسبب اعتماد الأفراد والمؤسسات والحكومات على تكنولوجيا المعلومات والاتصالات بشكل واسع و في شتى المجالات ؟
١) البرامج المجانية
٢) برامج غير معروفة المصدر
٣) برامج مفتوحة (أي استخدامها على الأجهزة المختلفة)

أولاً الاعتداءات الإلكترونية على الويب

سؤال : علل ..لا يشعر المستخدم بكثير من الاعتداءات الإلكترونية التي تتعرض المواقع الإلكترونية لها ؟

بسبب أنها غير مرئية

سؤال : أذكر أمثلة على الاعتداءات الإلكترونية ؟
١) الاعتداء على متصفح الإنترنت (**Browsers Attack**)
٢) الاعتداء على البريد الإلكتروني (**E-mail Attack**)

1 الاعتداءات الإلكترونية على متصفحات الإنترنت

متصفح الإنترنت :

- برنامج ينقل المستخدم إلى صفحة (**الويب**) التي يريدها
- بمجرد **كتابة العنوان** و الضغط على زر **الذهاب**
- **ويُمَكِّنُهُ** من مشاهدة المعلومات على الموقع .

سؤال : **علل .. يتعرض متصفح الإنترنت إلى الكثير من الأخطار ؟**

بسبب أنها قابلة للتغيير من دون ملاحظة ذلك من قبل المستخدم

سؤال : **عدّد طُرق الاعتداء على متصفحات الإنترنت ؟**

أ) الاعتداء عن طريق كود بسيط
ب) توجيه المستخدم إلى صفحة أخرى غير الصفحة التي يُريدها

سؤال : **وضّح كيف يستفيد المعتدي بعد إضافة كود بسيط على متصفح الإنترنت ؟**

يتم الاعتداء عن طريق **كود بسيط** ، يُمكن إضافته إلى المتصفح ، حيث يتمكن مما يلي

* **باستطاعته** :
القراءة والنسخ وإعادة إرسال أي شيء يتم إدخاله من قبل المستخدم
* و **يتمثل التهديد** :
بالقدرة على الوصول إلى الحسابات المالية والبيانات الحساسة الأخرى

سؤال : **ما هو التهديد الناتج بعد إضافة كود بسيط على متصفح الإنترنت ؟**

يتمثل التهديد بالقدرة على الوصول إلى الحسابات المالية والبيانات الحساسة الأخرى

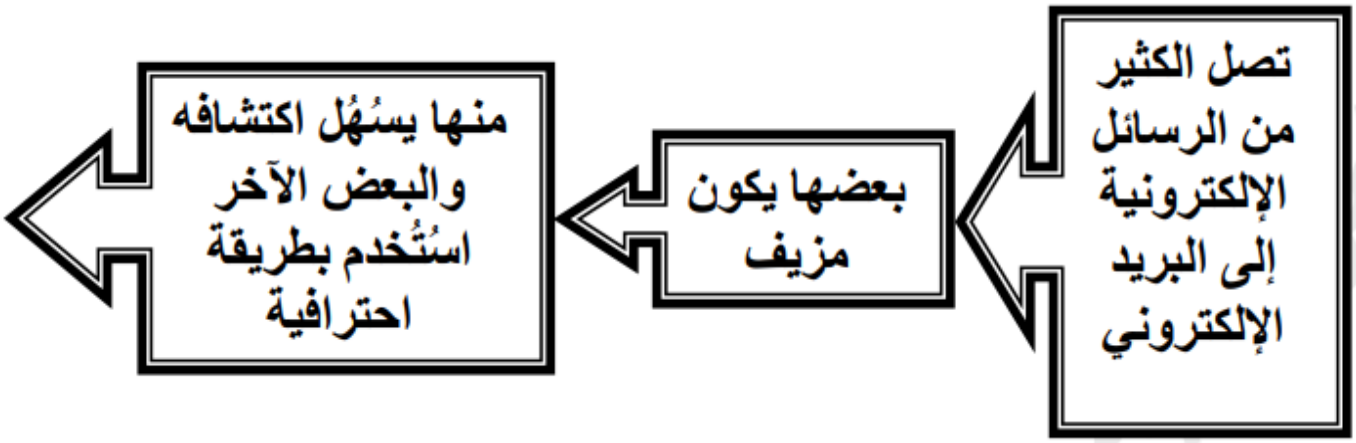
أحد التالية لا يُعتبر من البرامج والتطبيقات المنتشرة بشكل كبير ، هو :
أ) المفتوح
ب) غير معروف المصدر
ج) العنصر البشري
د) المجاني

الإجابة

إضافة كود بسيط على متصفح الإنترنت ، تُمكن المعتدي من :
أ) التعامل مع البرامج
ب) النجاح في اختبارات شفوية وورقية
ج) قراءة ونسخ وإعادة إرسال أي شيء
د) كتابة عنوان الموقع

الإجابة

2 الاعتداءات الإلكترونية على البريد الإلكتروني



☜ **سؤال : من هي الفئة المستهدفة من قِبَل مرسل الرسائل الإلكترونية المزيفة (المعتدي الإلكتروني)؟**

الأشخاص قليلي الخبرة

☜ **سؤال : كيف يتمكن مرسل الرسائل الإلكترونية المزيفة من الاعتداء ؟**

١) يُقدم عروض شراء لمنتجات بعض المصممين بأسعار زهيدة
٢) أو ... رسائل تحمل عنوان **كيف تُصبح ثرياً ؟**

=> تحتوي هذه الرسائل روابط ... للمزيد من المعلومات يُرجى **الضغط عليه** .

☜ **سؤال : ما فائدة الروابط داخل الرسائل الإلكترونية المزيفة بالنسبة لمرسل الرسائل (المعتدي) ؟**

☜ **سؤال : ما الضرر الناتج عن الروابط داخل الرسائل الإلكترونية المزيفة بالنسبة لمستقبل الرسائل (قليلي الخبرة) ؟**

للحصول على مزيد من المعلومات

☜ **سؤال : الرسائل الإلكترونية المزيفة والمضللة في البريد الإلكتروني كثيرة ، بيّن كيف لا نتأثر بها (أي نُقلل ضررها) ؟**

تحتاج لوعي المستخدم

☜☞ الحمد لله ☜☞ الحمد لله ☜☞ الحمد لله ☜☞ الحمد لله ☜☞ الحمد لله ☜☞ الحمد لله ☜☞ الحمد لله ☜☞
☜☞ الحمد لله ☜☞ الحمد لله ☜☞ الحمد لله ☜☞ الحمد لله ☜☞ الحمد لله ☜☞ الحمد لله ☜☞ الحمد لله ☜☞

ثانيًا تقنية تحويل العناوين الرقمية

تقنية تحويل العناوين الرقمية :

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

سؤال : ما هو ناتج إخفاء العنوان الرقمي للجهاز في الشبكة الداخلية (الفائدة) ؟

يُصبح الجهاز الداخلي **غير معروف** بالنسبة إلى الجهات الخارجية

النتيجة :

حيث يُسهم في **حمايته** من أي هجوم قد يُشن عليه بناءً على معرفة العناوين الرقمية

سؤال :اذكر الطريقة التي تُعتبر إحدى الطرق المستخدمة لحماية المعلومات من الاعتداءات الإلكترونية ؟

تقنية تحويل العناوين الرقمية

سؤال : ما هي خطوات تقنية تحويل العناوين الرقمية لحماية المعلومات من الاعتداءات الإلكترونية ؟

١) العناوين الرقمية الإلكترونية **IP Adress**
٢) مفهوم تقنية تحويل العناوين الرقمية **NAT**

توضيح الطرائق المستخدمة لحماية المعلومات من الاعتداءات الإلكترونية :

1 العناوين الرقمية الإلكترونية IP Address

يرتبط ملايين الأشخاص عبر شبكة الإنترنت بملايين الأجهزة .
ولكل جهاز حاسوب أو (هاتف خلوي) عنوان رقمي خاص به (يُميزه عن غيره)
يُسمى IP Address

IP Address :

- يتكون من أربعة مقاطع يفصل بينها نقاط
- ويُسمى (IPv4)
- كل مقطع يتضمن رقم (من 0 إلى 255).

	IP Address	
Internet	Protocol	Address

سؤال : يتكون من أربعة مقاطع يفصل بينها نقاط ، ويُسمّى IPv4 ، كل مقطع يتضمن رقم (من 0 إلى 255) ، هو :

أ) IP Address
ب) العنوان الرقمي الإلكتروني
ج) عنوان رقمي خاص بكل جهاز حاسوب وهاتف خلوي
د) جميع ما ذُكر

الجواب :
دائرة (د) – جميع ما ذكر

سؤال : اكتب مثالاً على العنوان الرقمي الخاص بجهاز حاسوب ؟

مثال عليه ... 215.002.004.216

سؤال : ما هي مراحل تطور العناوين الإلكترونية ؟

١) IPv4 ٢) IPv6 ٣) NAT

سؤال : أذكر سبب تطور العناوين الإلكترونية للأجهزة إلى IPv6 ؟

- كانت العناوين ضمن IPv4
- بظهور التطور الهائل في أعداد المستخدمين للإنترنت ...
(أصبحت الحاجة ضرورية إلى عناوين إلكترونية أكثر)
- فطُوِّرت هذه العناوين إلى IPv6

سؤال : كم عدد المقاطع التي يتكون منها IPv6 ؟

ثمانية مقاطع

NAT
Network Address Translation

سؤال : قارن بين العناوين الإلكترونية IPv4 ، والعناوين الإلكترونية IPv6 من حيث :
(عدد المقاطع ، عدد المستخدمين) ؟

وجه المقارنة	IPv4	IPv6
عدد المقاطع	٤ مقاطع	٨ مقاطع
عدد المستخدمين	ملايين من الأشخاص	عدد هائل من المستخدمين

سؤال : لحل مُشكلة IPv6 الناتج عن زيادة عدد المستخدمين ، تمّ إيجاد تقنية جديدة ، اذكرها ؟
تقنية تحويل العناوين الرقمية NAT

سؤال : ما سبب ظهور تقنية تحويل العناوين الرقمية NAT ؟
لأنَّ IPv6 لا تكفي لإتاحة عدد هائل من العناوين الرقمية

2 مفهوم تقنية تحويل العناوين الرقمية NAT

تتمتع أيانا (IANA) بالسلطة المسؤولة عن منح أرقام الإنترنت المخصصة لإعطاء العناوين الرقمية للأجهزة على الإنترنت .
- وبسبب قلة أعداد هذه العناوين مقارنة بعدد المستخدمين
- فإنها تُعطي الشبكة الداخلية عنواناً واحداً (أو مجموعة عناوين)
- يكون مُعَرِّفاً لها عند التعامل في شبكة الإنترنت .

سؤال : أذكر مثالاً على كيفية توزيع عناوين الشبكات من قبل IANA ؟

- كل شبكة داخلية تُمنح عنواناً خاصاً بها على الإنترنت
  (**مختلفاً عن العناوين الأخرى**)
  - مثل (255.10.10.4) عنوان لشبكة داخلية
    (لا يتكرر و لا يُمنح لشبكة أخرى)

- تُعطي الشبكة الداخلية كل جهاز داخل الشبكة ... **عنواناً رقمياً** –
  لغرض الاستخدام الداخلي **فقط** .. (**لا يتم التعرف عليه خارج الشبكة**)
  - أي يُمكن تكراره في شبكات داخلية أخرى (في **نفس** الشبكة **لا يتكرر**)
  - مثل (10.0.0.8)

سؤال : الشبكة الداخلية ، تُعطي كل جهاز فيها عنواناً رقمياً لغرض :

أ) الاستخدام الداخلي والخارجي معاً
ب) الاستخدام الداخلي فقط
ج) الاستخدام الخارجي فقط
د) الاستخدام في جميع الشبكات

الجواب :
دائرة (ب) – الاستخدام الداخلي فقط

سؤال : تقوم أيانا بإعطاء الشبكة الداخلية عنواناً واحداً فقط ، بسبب قلة أعداد العناوين ، مُقارنة بعدد المستخدمين للإنترنت .

(عبارة خاطئة)

الصواب :

[عنواناً واحداً أو مجموعة من العناوين]

سؤال : الشبكات الداخلية ، تُعطي كل جهاز فيها عنواناً رقمياً خاصاً به ، ولا يُعترف بهذا العنوان خارج هذه الشبكات :

الجواب (عبارة صحيحة)

سؤال : إحدى العبارات التالية تُعتبر صحيحة ، هي :

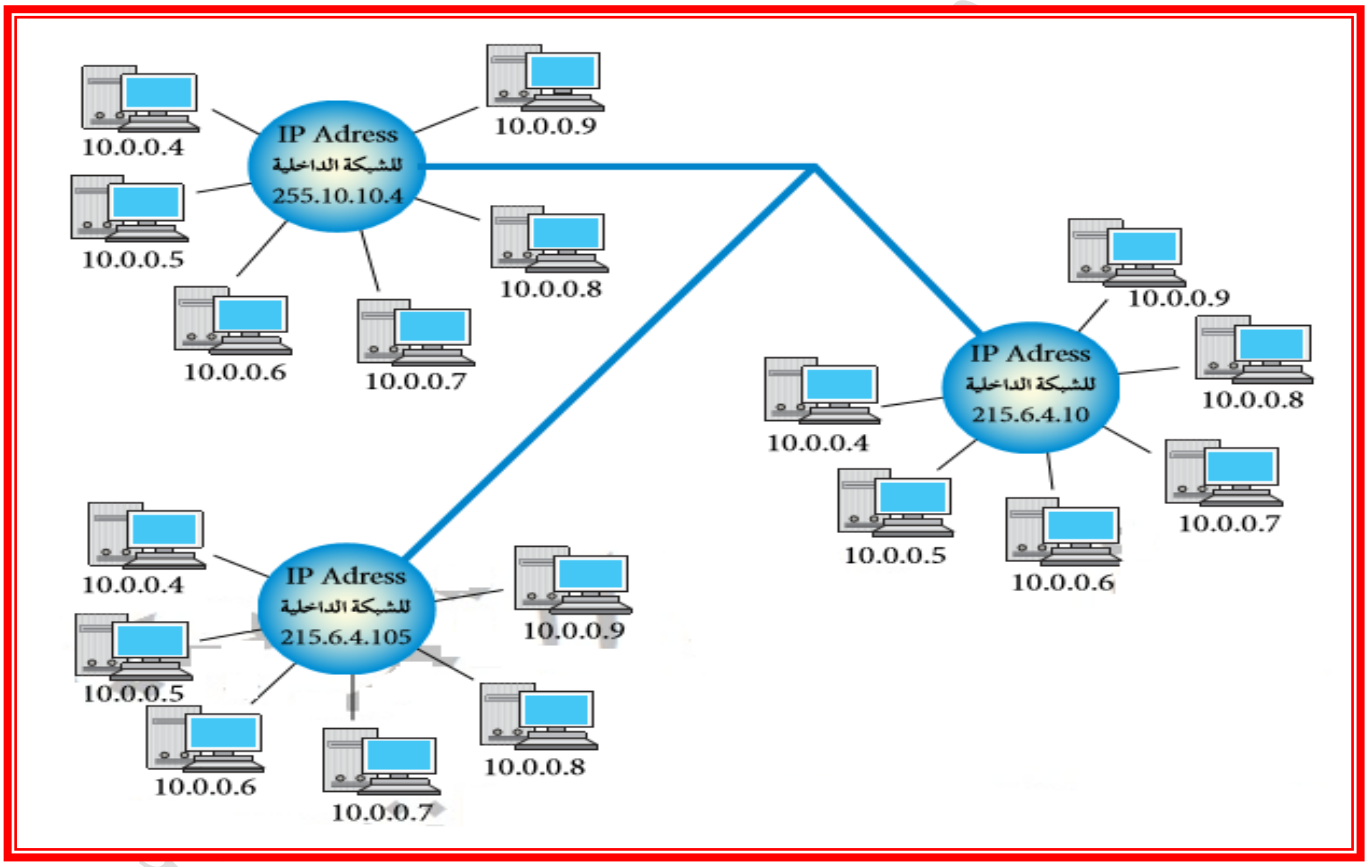
أ) لا يُعترف بعنوان الجهاز الداخلي خارج الشبكة
ب) يتم التعامل مع العناوين من 8 مقاطع فقط
ج) العنوان الخاص بالهواتف الخلوية يتكون من 3 مقاطع
د) NAT هي السلطة المسؤولة عن منح أرقام الإنترنت المخصصة لإعطاء العناوين للأجهزة

الجواب :
دائرة (أ) – لا يُعترف بعنوان الجهاز الداخلي خارج الشبكة

أيانا IANA :

- السلطة المسؤولة عن منح أرقام الإنترنت
- المخصصة لإعطاء العناوين الرقمية للأجهزة على الإنترنت

[الشكل التالي - يُوضح العناوين الرقمية للشبكات و الأجهزة]



آلية استخدام تقنية NAT

سؤال : وضح آلية استخدام تقنية NAT ؟

1) عند **رغبة** أحد الأجهزة بالتواصل مع جهاز خارج الشبكة الداخلية
   - **يُعدل** العنوان الرقمي الخاص به (باستخدام تقنية تحويل العناوين الرقمية **NAT**)
   - يتم من خلال استخدام **جهاز وسيط** (غالباً ما يكون موجِّه أو جدار ناري)
2) يقوم على تحويل الرقم الداخلي إلى[**عنوان رقمي خارجي**]
3) ويُسجَّل ذلك في سجل خاص **للمتابعة**

سؤال : تقوم أيانا بتعديل العنوان الرقمي الخاص بالجهاز عند رغبته بالتواصل مع جهاز آخر .

(عبارة خاطئة)

الصواب :

[تقوم NAT أو تقنية تحويل العناوين الرقمية]

سؤال : يتم تعديل العنوان الرقمي الخاص بالجهاز عند رغبته بالتواصل مع جهاز آخر من خلال استخدام جهاز وسيط .

الجواب (عبارة صحيحة)

سؤال : يتم استخدام جهاز وسيط لتعديل العنوان الرقمي الخاص بالجهاز مثل الموجه .

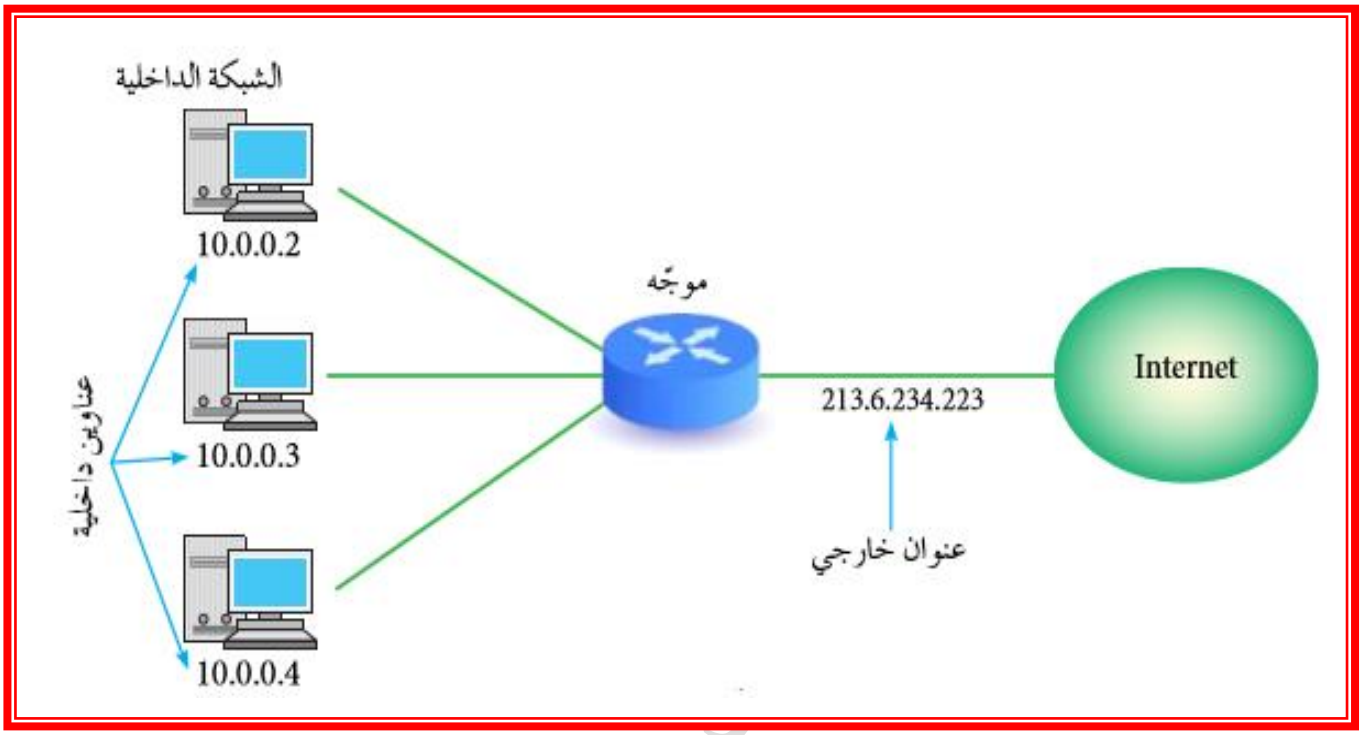
الجواب (عبارة صحيحة)

التواصل بين جهازين من شبكات مختلفة

سؤال : كيف يتم التواصل بين جهازين من شبكات مختلفة ؟

1) يتم التواصل مع الجهاز الهدف في شبكة أخرى
   - عن طريق هذا **الرقم الخارجي**
     - (على أنه العنوان الخاص بالجهاز **المرسل**)
2) عندما يقوم الجهاز الهدف **بالرد** على رسالة الجهاز المرسل
3) تصل إلى الجهاز الوسيط .
   - الذي يُحَوّل **العنوان الرقمي الخارجي** إلى عنوان داخلي
     - (من خلال سجل المتابعة لديه)
4) ويُعيده بذلك إلى الجهاز المرسل

[الشكل يوضح كيفية التواصل بين جهازين من شبكتين مختلفتين باستخدام تقنية تحويل العناوين الرقمية] - صفحة (١٤٤) من الكتاب



ما هو سبب التحول من IPv4 إلى IPv6 ، هو :
أ) التطور الهائل في أعداد المستخدمين للإنترنت
ب) العناوين غير معروفة المصدر
ج) العنصر البشري
د) بسبب تطور Nat
الإجابة

يتم التواصل مع الجهاز الهدف في شبكة أخرى ، من خلال :
أ) الرقم الداخلي
ب) IANA
ج) الرقم الخارجي
د) NAT
الإجابة

متى يتم تعديل العنوان الرقمي الخاص بالجهاز ، أثناء عملية الاتصال :
أ) عند رغبة أحد الأجهزة بالتواصل مع جهاز خارج الشبكة الداخلية
ب) عند الانتهاء من عملية الاتصال
ج) عند التواصل مع الوسيط
د) عند التعامل مع IANA
الإجابة

أحد مراحل تطور العناوين الإلكترونية يتكون من 8 مقاطع :
أ) IANA
ب) IPv4
ج) NAT
د) IPv6
الإجابة

3 آلية عمل تقنية تحويل العناوين الرقمية NAT

تعمل بعدة طرق (آليات) ، منها :

1 النمط الثابت للتحويل

- **يتم من خلاله تخصيص عنوان رقمي خارجي لكل جهاز داخلي**
- **وهو ثابت لا يتغير**

2 النمط المتغير للتحويل

- **يكون لدى الجهاز الوسيط عدد من العناوين الرقمية الخارجية لكنها غير كافية لعدد الأجهزة في الشبكة**
- **حيث تبقى متاحة لجميع الأجهزة على الشبكة**

- ✓ عند **رغبة** أحد الأجهزة الداخلية بالتراسل خارجياً
- ✓ **يتواصل** مع الجهاز الوسيط الذي **يُعطيه** عنواناً خارجياً مؤقتاً **يستخدمه** لحين الانتهاء من عملية التراسل
  [ويُعدُّ هذا العنوان –عنواناً رقمياً خاصاً بالجهاز]
- ✓ **يفقد** الجهاز الداخلي هذا العنوان ، عند الانتهاء من عملية التراسل
- ✓ **يُصبح** العنوان مُتاحاً للتراسل مرة أخرى

سؤال : ماذا يحدث للعنوان الخارجي للجهاز عند انتهاء عملية التراسل ؟

يفقد الجهاز الداخلي هذا العنوان
(حيث يُصبح العنوان متاحاً للتراسل مرة أخرى)

سؤال : عند رغبة نفس الجهاز بالتراسل مرة أخرى هل يُعطى نفس العنوان الخارجي للجهاز السابق ؟
قد يُعطى عنواناً مختلفاً عن المرة السابقة

سؤال : علل ..
اختلاف IP Address للجهاز نفسه عند تراسله أكثر من مرة من خلال النمط المتغير للتحويل ؟
لأن الجهاز الوسيط يقوم بإعطاء الجهاز الذي يرغب بالتراسل مرة أخرى عنواناً مختلفاً عن المرة السابقة وحسب المتاح لديه

النمط الثابت لتحويل العناوين الرقمية :
- طريقة يتم من خلالها تخصيص عنوان رقمي خارجي لكل جهاز داخلي
- وهذا العنوان الرقمي ثابت لا يتغيّر
- يستخدمه الجهاز في كل مرّة يرغب فيها بالاتصال مع الأجهزة خارج الشبكة

النمط المتغيّر لتحويل العناوين الرقمية :
- نمط يتم من خلاله تخصيص عنوان رقمي للجهاز
- عند رغبته في التواصل مع جهاز خارج الشبكة يستخدمه
- وعند انتهاء عملية الاتصال .. يُصبح هذا العنوان الرقمي مُتاحاً للأجهزة الأخرى

عنوان رقمي ثابت خارجي لا يتغير يُخصص لكل جهاز في حال الاتصال خارج الشبكة ، هو :
أ) النمط الثابت لتحويل العناوين الرقمية الخاص بالهواتف فقط
ب) أيانا
ج) النمط الثابت لتحويل العناوين الرقمية
د) nat
الإجابة

عناوين رقمية خاردية لدى الوسيط غير كافية ولكنها متاحة لجميع الأجهزة على الشبكة هذه طريقة :
أ) النمط المتغير لتحويل العناوين الرقمية
ب) الاختبارات الشفوية والرقمية
ج) النمط المتغير
د) كتابة عنوان الموقع
الإجابة

إجابات أسئلة الفصل الثاني

أسئلة الفصل

١- ما أسباب إيجاد وسائل تقنية لحماية الإنترنت؟

إجابة (١)

للحد من الاعتداءات والأخطار التي تهددها بسبب انتشار البرامج والتطبيقات بشكل كبير (المجاني ، غير معروف المصدر ، المفتوح) ... والبرامج المقرصنة والمعلومات الخاصة بكيفية اقتحام المواقع .

٢- ما أشهر الاعتداءات على (الويب)؟

إجابة (٢)

١) الاعتداء على متصفح الإنترنت ٢) الاعتداء على البريد الإلكتروني

٣- حدّد نوع الاعتداء في كلٍّ مما يأتي:

أ - توجيه المستخدم إلى صفحة أخرى غير الصفحة التي يريدها.

ب- كود بسيط يُمكن إضافته إلى المتصفّح وباستطاعته القراءة، والنسخ، واعادة الإرسال لأي شيء يتم إدخاله من قِبَل المُستخدم.

جـ- يتضمن عروضًا وهمية ومضلّلة، ويحتوي رابطًا يتم الضغط عليه للحصول على معلومات إضافية.

إجابة (٣)

(أ)	(ب)	(ج)
إعتداء على متصفحات الإنترنت	إعتداء على متصفحات الإنترنت	إعتداء على البريد الإلكتروني

٤ – وضّح ما يأتي:

أ – تحدث اعتداءات على (الويب) من خلال البريد الإلكتروني.

ب– تُحافظ تقنية تحويل العناوين الرقمية على أمن المعلومات في (الويب).

إجابة (٤)

(أ)	١) يُقدم عروض شراء لمنتجات بعض المصممين بأسعار زهيدة ٢) أو ... رسائل تحمل عنوان كيف تُصبح ثرياً <= تحتوي هذه الرسائل روابط ... للمزيد من المعلومات يُرجى الضغط عليه . <= تحتاج لوعي المستخدم
(ب)	- هي التقنية التي تعمل على إخفاء العنوان الرقمي للجهاز في الشبكة الداخلية ...ليتوافق مع العنوان الرقمي المُعطى للشبكة ... - يُصبح الجهاز الداخلي غير معروف بالنسبة إلى الجهات الخارجية ... * **حيث يُسهم في حمايته من أي هجوم قد يُشن عليه بناءً على معرفة العناوين الرقمية**

٥ – ما الفرق بين العناوين الرقمية IPv4 و IPv6؟

إجابة (٥)

العناوين الرقمية IP4	العناوين الرقمية IPv6
يتكون من (32 خانة) ثنائية ... تتوزع على أربعة مقاطع يفصل بينها نقاط ... ويُسمى (IPv4)... كل مقطع يتضمن رقم من (0 إلى 255) ... مثال عليه ... (215.002.004.216) **أو ... ((تتكون من أربعة مقاطع))**	كانت العناوين ضمن IPv4 ... بظهور التطور الهائل في أعداد المستخدمين للإنترنت ... (أصبحت الحاجة ضرورية إلى عناوين إلكترونية أكثر) ... فطُوّرت هذه العناوين إلى IPv6 **أو ... ((تتكون من ثمانية مقاطع))**

٦ – مَن السلطة المسؤولة عن منح أرقام الإنترنت المخصصة لإعطاء العناوين الرقمية؟

إجابة (٦)

تتمتع أيانا (IANA) بهذه السلطة

٧ – ما وظيفة الجهاز الوسيط؟

إجابة (٧)

1) عند رغبة أحد الأجهزة بالتواصل مع جهاز خارج الشبكة الداخلية ...
2) يُعدل العنوان الرقمي الخاص به .. باستخدام تقنية تحويل العناوين الرقمية NAT
3) من خلال استخدام جهاز وسيط (غالباً ما يكون موجِّه أو جدار ناري)
4) يقوم على تحويل الرقم الداخلي ... إلى ... [عنوان رقمي خارجي]
5) ويُسجَّل ذلك في سجل خاص للمتابعة

٨ – قارن بين طريقتي العمل لكلٍّ من:

النمط الثابت لتحويل العناوين الرقمية، والنمط المتغير لتحويل العناوين الرقمية.

إجابة (٨)

النمط الثابت لتحويل العناوين الرقمية	النمط المتغير لتحويل العناوين الرقمية
يتم عن طريق تخصيص عنوان رقمي خارجي لكل .....جهاز داخلي ((وهو ثابت لا يتغير))	عند رغبة أحد الأجهزة بالتراسل خارجياً ... يتواصل مع الجهاز الوسيط ... الذي يُعطيه عنواناً خارجياً مؤقتاً ... يستخدمه لحين الانتهاء من عملية التراسل ... ويُعدُّ هذا العنوان – عنواناً رقمياً خاصاً بالجهاز ... وحين الانتهاء من الاتصال يُصبح هذا الرقم متاحاً لأي جهاز آخر

الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله
الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله

الفصل الثالث: التشفير

ظهرت الحاجة للحفاظ على سرية المعلومات منذ قدم البشرية .

- خاصة في المجال العسكري والدبلوماسي
- وكان لها وسائل لنقل الرسالة عن طريقها والمحافظة على سريتها في آن واحد

وبتطور العلم والوسائل التتكنولوجية الحديثة كان لا بد من وجود طرائق لحمايتها

أولاً: مفهوم علم التشفير وعناصره

- ما هو التشفير ؟
- ما هي عناصر التشفير ؟؟
- ما هو الهدف من التشفير ؟؟؟

Gooo

سؤال: متى يُستخدم تشفير المعلومات ؟
عند إجراء عمليات التراسل

كثيراً

1 مفهوم التشفير و الهدف منه

- هو **تغيير** محتوى الرسالة الأصلية
  - سواء كان التغيير **بمزجها** بمعلومات أخرى
  - أم **استبدال** الأحرف الأصلية والمقاطع بغيرها
  - أم **تغيير** لمواقع الأحرف بطريقة لن يفهمها إلا مُرسل الرسالة و مستقبلها فقط
- باستخدام خوارزمية معينة **و** مفتاح خاص .

سؤال : أذكر الهدف من عملية التشفير للمعلومات ؟

١) الحفاظ على سرية المعلومات أثناء تبادلها بين مرسل المعلومة ومستقبلها
٢) عدم الاستفادة من المعلومات أو فهم محتواها حتى لو تم الحصول عليها من قبل أشخاص معترضين

سؤال : علل .. التشفير يُعد من أفضل الطرق المستخدمة للحفاظ على أمن المعلومات ؟

لأنه يعمل على إخفائها عن الأشخاص غير المصرح لهم بالاطلاع عليها

سرية المعلومات ظهرت منذ القدم في مجالات عديدة ، منها :
أ) لإخفاء الرسالة
ب) الاتصالات السلكية
ج) العسكري والدبلوماسي
د) التواصل عن بعد
الإجابة

السبب لوجود وسائل للحفاظ على سرية المعلومات منذ قدم البشرية ، هو :
أ) النمط المتغير لتحويل العناوين الرقمية
ب) المحافظة على السلامة
ج) إخفاء الرسالة
د) نقل والمحافظة على الرسالة
الإجابة

التشفير بالمزج والاستبدال والتغيير على المعلومات ، يتم من خلال :
أ) إخفاء الرسالة الأصلية
ب) محتوى الرسالة الأصلية
ج) سرية الرسالة الأصلية
د) كتابة الرسالة الأصلية
الإجابة

التشفير من أفضل الطرق المستخدمة للحفاظ على أمن المعلومات ، بسبب :
أ) لأنها مهمة
ب) إخفائها عن العملاء
ج) إخفائها عن الأشخاص غير المصرح لهم
د) لأنها معلومات مالية
الإجابة

2 عناصر عملية التشفير

سؤال : أذكر عناصر عملية التشفير ؟

أ) خوارزمية التشفير
ب) مفتاح التشفير
ج) النص الأصلي
د) نص الشيفرة

توضيح عناصر عملية التشفير :

أ خوارزمية التشفير

مجموعة الخطوات المستخدمة لتحويل الرسالة الأصلية إلى رسالة مشفرة

سؤال : ما هو مفهوم الخوارزمية ؟

مجموعة من الخطوات المتسلسلة **منطقياً و رياضياً**
لحل مشكلة ما

سؤال : قارن بين الخوارزمية وخوارزمية التشفير ؟

الخوارزمية	خوارزمية التشفير
مجموعة من الخطوات المتسلسلة منطقياً ورياضياً لحل مشكلة ما	مجموعة الخطوات المستخدة لتحويل الرسالة الأصلية إلى رسالة مشفرة

ب مفتاح التشفير

هو سلسلة الرموز (عدد الأسطر) المستخدمة في خوارزمية التشفير
وتعتمد قوة التشفير على قوة هذا المفتاح

ج النص الأصلي

يُقصد بها محتوى الرسالة الأصلية قبل التشفير
و بعد عملية فكّ التشفير

د نص الشيفرة

الرسالة بعد عملية التشفير

يعتبر محتوى الرسالة الأصلية قبل التشفير و بعد عملية فكّ التشفير ، هو :
أ) نص الشيفرة
ب) النص الأصلي
ج) مفتاح التشفير
د) خوارزمية التشفير
الإجابة

مجموعة من الخطوات المتسلسلة منطقياً ورياضياً لحل مشكلة ما ، هذا المفهوم ينطبق على :
أ) الرسالة الأصلية
ب) خوارزمية التشفير
ج) الرسالة المشفرة
د) الخوارزمية
الإجابة

واحدة من الآتية لا نعتبره من عناصر عملية التشفير ، هو :
أ) مفتاح التشفير
ب) النص الأصلي
ج) مرسل الرسالة
د) الرسالة المشفرة
الإجابة

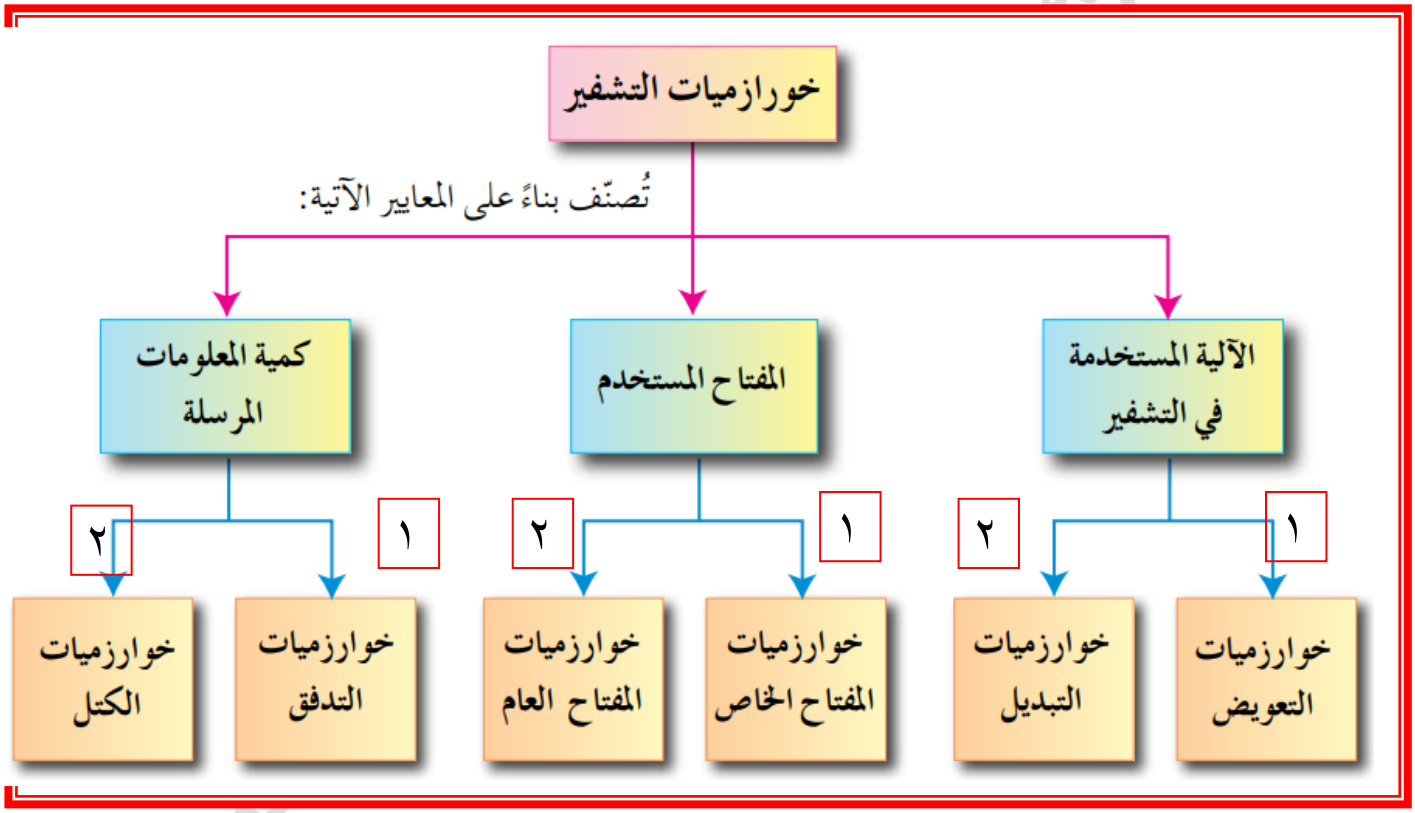
بعد عملية التشفير تنتج رسالة غير مفهومة إلا لمرسل الرسالة و مستقبلها ، وهي :
أ) الرسالة الأصلية
ب) نص الشيفرة
ج) مفتاح التشفير
د) النص الأصلي
الإجابة

ثانيًا خوارزمية التشفير

سؤال : أذكر معايير تصنيف خوارزميات التشفير ؟

١) استخدام المفتاح
٢) كمية المعلومات المرسلة
٣) العملية المستخدمة في عملية التشفير

[أنواع الخوارزميات] الشكل (٤-٤)



خوارزمية التدفق و الكتل من خوارزميات التشفير التي تُصنف بناء على معيار :
أ) مصدر التشفير
ب) المفتاح المستخدم
ج) العملية المستخدمة في التشفير
د) كمية البيانات المرسلة
الإجابة

واحدة من التالية تعتبر من الخوارزميات المصنفة على أساس العملية المستخدمة في التشفير ، هي :
أ) التعويض
ب) التدفق
ج) الكتل
د) المفتاح العام
الإجابة

توضيح لأنواع خوارزميات التشفير بناءً على المعايير المصنّفه من خلالها :

1 التشفير المعتمد على آلية التشفير

سؤال : أذكر طرائق التشفير المعتمد على نوع عملية التشفير ؟

١) تشفير التعويض ٢) تشفير التبديل

طريقة تشفير التعويض :

- طريقة لتشفير النصوص
- يتم خلالها استبدال حرف مكان حرف أو مقطع مكان مقطع

سؤال : ما هي خوارزمية التشفير التي تُعتبر مثالاً على طريقة التشفير بالتعويض ؟

مثال عليها : **شيفرة الإزاحة**

طريقة تشفير التبديل :

- طريقة تشفير تقوم على تبديل **أماكن** الأحرف
  - وذلك عن طريق **إعادة ترتيب** أحرف الكلمة
- **بشرط** استخدام الأحرف نفسها من دون إجراء أي تغيير عليها

* * *

- **في طريقة تشفير التبديل لا يتم إجراء أي تغيير الحروف**
- **في طريقة تشفير التبديل يختفي معنى النص الحقيقي ، وهذا يُشكل عملية التشفير**

سؤال : ما هي النتيجة من جراء تنفيذ التشفير من خلال عملية التبديل على نص الرسالة الأصلية ؟

يختفي معنى النص الحقيقي

سؤال : **تنفيذ التشفير من خلال عملية التبديل على نص الرسالة الأصلية وإختفاء معنى النص الحقيقي ، ماذا تُشكل هذه العملية ؟**

هذا يُشكل عملية التشفير

بشرط :

أن تكون قادراً على استرجاع النص الأصلي منها [وتسمى عملية فك التشفير]

- **ومثال عليها :**
  - **خوارزمية الخط المتعرج Zig Zag**

شكله الموضوع
في آخره
معقول !!!!
يعني الـ 200
مزبوط سهله
والله سهله

خوارزمية الخط المتعرج (Zig Zag Cipher)

سؤال : بما تتميز خوارزمية الخط المتعرج؟

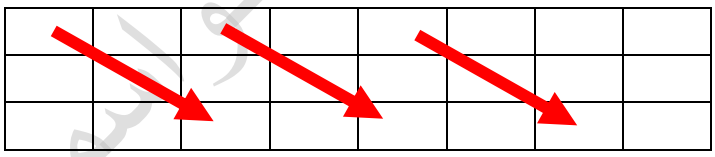
أ) سهلة وسريعة
ب) يُمكن تنفيذها يدوياً باستخدام الورقة والقلم
ج) يُمكن فك تشفيرها بسهولة

سؤال : خوارزمية الخط المتعرج تستخدم آلية التشفير بالتبديل .

الجواب (عبارة صحيحة)

أ التشفير

(أ) خطوات التشفير حسب خوارزمية الخط المتعرج :

١)	حدد **عدد** الأسطر التي ستستخدم لتشفير النص	[عدد الأسطر **يُعد** مفتاح التشفير] [لا يلزمنا معرفة عدد الأعمدة] [ابدأ بأي عدد من الأعمدة و يُمكن الزيادة عند الحاجة]
٢)	املأ الفراغ في النص الأصلي بمثلث مقلوب ▽	
٣)	أنشئ جدولاً يعتمد على عدد الأسطر (**مفتاح التشفير**)	
٤)	وزع أحرف النص المراد تشفيرة بشكل قطري	
٥)	ضع مثلث مقلوب ▽ في الفراغ الأخير	[حتى تكون الأطوال متساوية] **أي عدد الرموز في كل سطر متساوياً**
٦)	اكتب النص المُشفَّر **سطراً سطراً**	

لاحظ

* مفتاح التشفير يتم الاتفاق عليه مسبقاً (من قبل مرسل الرسالة ومستقبلها فقط) [في الامتحان ستزود به]
* استخدام المثلث المقلوب بديلاً للفراغ لغايات تسهيل الحل فقط

لاحظ

* يُمكن تشفير أحرف اللغة العربية ... غير مطالب به الطالب
* نص يحتوي علامات ترقيم ... غير مطالب به الطالب
* لا فرق في منهاجنا بين الحروف الكبيرة والحروف الصغيرة

مثال (1) // صفحة(150) :

شفّر النص الآتي ، علماً بأنّ مفتاح التشفير سطران .
I love my country

١-	حدد مفتاح التشفير (سطران)

1 — المفتاح = ٢

٢-	املأ الفراغ بالنص الأصلي بمثلث مقلوب ▽ I▽love▽my▽country

2 — كل فراغ نضع فيه ▽

3 — أنشئ جدولاً وزع أحرف النص قطرياً

٣-	I		l		v		▽		y		c		u		t		y
		▽		o		e		m		▽		o		n		r	

4

نضع ▽ للفراغ الأخير (تصبح الأطوال متساوية)

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

٤-

5

نكتب النص المشفر سطراً سطراً

٥-

النص الأصلي :

I love my country

النص المشفر :

Ilv▽ycuty▽oem▽onr

Ilv ycuty oem onr

النتيجة :

١) النص المُشفّر ، أخفى الرسالة

٢) لن يستطيع أي شخص مُتطفل أن يفهم محتواها

مثال (2) // صفحة(152) :

جد النص المشفر للنص الأصلي الآتي ، علماً بأنّ مفتاح التشفير هو خمسة أسطر

Stay positive this year makes you happy all life

راجع من صفحة 152 إلى صفحة 153

نشاط (٤-١) /ص١٥٣

التشفير باستخدام خوارزمية الخط المتعرج

(١) Stop thinking about your past mistakes

١) مفتاح التشفير (٤ أسطر)

٢) نملأ الفراغ الأصلي بمثلث مقلوب ▽

Stop▽thinking▽about▽your▽past▽mistakes

٣) وزع أحرف النص الأصلي بشكل قطري ... كما يلي :

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	▽

٤) اكتب النص المشفر سطراً سطراً على التوالي :

- النص الأصلي Stop thinking about your past mistakes
- النص المشفر :

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** ▽

٥) النص المشفر

S▽ngoy▽tsettk▽uop▽tsohiatuama▽pinb▽rsik▽
S ngoy tsettk uop tsohiatuama pinb rsik

- Never give up on your goals

١) مفتاح التشفير (٣ أسطر)
٢) نملأ الفراغ في النص الأصلي بمثلث مقلوب ▽

Never▽give▽up▽on▽your▽goals

٣) وزع أحرف النص الأصلي بشكل قطري ... كما يلي :

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

٤) اكتب النص المشفر سطراً سطراً على التوالي:

- النص الأصلي Never give up on your goals
- النص المشفر :

Negepno▽a
eri▽▽▽ugl
v▽vuoyros

٥) النص المشفر

Negepno▽aeri▽▽▽uglv▽vuoyros
Negepno aeri uglv vuoyros

في خوارزمية الخط المتعرج إذا كان لدينا فراغ في آخر الجدول ، فإنه يتم وضع :
أ) +
ب) ▽
ج) مثلث
د) يبقى فراغ
الإجابة

في خوارزمية الخط المتعرج يتم وضع مثلث مقلوب في الفراغ الأخير في جدول التشفير حتى تُصبح الأطوال متساوية :
أ) نعم
ب) لا
الإجابة

في خوارزمية الخط المتعرج يلزمنا معرفة مفتاح التشفير وعدد الأعمدة :
أ) نعم
ب) لا
الإجابة

مثال على طريقة تشفير التعويض شيفرة الإزاحة ، يلزمنا معرفة مفتاح التشفير :
أ) نعم
ب) لا
الإجابة

في خوارزمية الخط المتعرج إذا كان لدينا فراغ في آخر الجدول بعد توزيع حروف الرسالة، فإنه يتم وضع ▽ مثلث مقلوب لكي :
أ) نملأ الفراغ ب) لإخفاء نص الرسالة الأصلية
ج) يُصبح عدد الرموز متساوياً في كل سطر
د) يُصبح عدد ▽ متساوي في كل سطر
الإجابة

في خوارزمية الخط المتعرج وبعد توزيع نص الرسالة الأصلية داخل جدول التشفير ، فإنه يتم كتابة نص الشيفرة سطراً سطراً ومرتب على التوالي :
أ) نعم
ب) لا
الإجابة

آخر خطوة في خوارزمية الخط المتعرج هو كتابة نص الرسالة المشفرة سطراً سطراً ومرتب على التوازي فوق بعضها البعض :
أ) نعم
ب) لا
الإجابة

الخطوة الثانية في تشفير نص الرسالة الأصلية وتحويلها إلى نص الشيفرة ، هي :
أ) تحديد عدد الأسطر
ب) إنشاء جدول التشفير
ج) توزيع النص الأصلي قطرياً
د) نضع ▽ مكان الفراغ
الإجابة

مفتاح التشفير يجب الاتفاق عليه مسبقاً قبل عملية التشفير ، ويتم الاتفاق عليه مق قبل :
أ) مرسل الرسالة ومستقبلها فقط
ب) مرسل الرسالة فقط
ج) مستقبل الرسالة فقط
د) عناصر عملية التشفير
الإجابة

الخطوة الأخيرة (السادسة) في تشفير النص الأصلي إلى رسالة مشفرة ، هي :
أ) نضع مثلث مقلوب مكان الفراغ
ب) نضع ▽ في الفراغ الأخير
ج) نكتب النص المشفر سطراً سطراً
د) إنشاء جدول
الإجابة

ب فك التشفير

(ب) عملية فك التشفير:

١)	املأ الفراغات بمثلث مقلوب ▽	
٢)	قسم النص المشفر إلى أجزاء	[اعتماداً على عدد الأسطر [مفتاح التشفير]]
		[أي عدد الأجزاء = عدد الأسطر]
	نقوم بتحديد عدد الأحرف في كل جزء **((نجمع المثلثات المقلوبة مع الأحرف))**	[مجموع أحرف النص المشفر مع الفراغات ÷ عدد الأجزاء]
		((إذا ناتج القسمة كسراً ... نُقربه إلى أقرب عدد صحيح أكبر منه))
٣)	أكتب الحرف الأول من كل جزء ... ثم الحرف الثاني ... ثم الحرف الثالث ... وهكذا ... الخ	**((بشكل عمودي))**

في عملية فك التشفير ، يتم تقسيم النص المشفر إلى أجزاء ، وهذه الأجزاء تساوي :
أ) عدد الرموز
ب) الحرف الأول لكل جزء
ج) عدد الأسطر
د) الحروف والمثلثات المقلوبة
الإجابة

الطريقة المتبعة في تقسيم النص المشفر إلى أجزاء هي :
أ) مجموع الأحرف والفراغات مقسمة على عدد الأجزاء
ب) مجموع الأحرف مقسمة على عدد الأجزاء
ج) عدد الأجزاء مقسمة على مجموع الأحرف
د) مجموع ▽ والأجزاء تقسيم مجموع الأحرف
الإجابة

في عملية فك التشفير ، يتم تقسيم النص المشفر إلى أجزاء ، إذا كان ناتج القسمة كسراً فنقوم بما يلي :
أ) نقرب إلى أقرب عدد صحيح أقل منه
ب) كل جزء مساوياً للجزء الأول
ج) يتم توزيع الحروف عمودياً
د) نقرب إلى أقرب عدد صحيح أكبر منه
الإجابة

إذا كان مجموع الحروف والمثلثات 17 وعدد الأسطر هو 3 ، فإن عدد الرموز في كل جزء يساوي :
أ) 5.6
ب) 5
ج) 6.6
د) 6
الإجابة

مثال (3) // صفحة(154) :

جد النص الأصلي المُشفر الآتي، علماً بأنّ مفتاح التشفير سطران.
Ilv ycuty oem onr

1
ملأ الفراغات ▽

١-	Ilv▽ycuty▽oem▽onr

2
قسّم النص لجزأين
المفتاح=2

٢-	يتم عدّ حروف النص مع المثلثات المقلوبة، ثم القسمة: 17 ÷ 2 = 8.5

3
الكسر =ناتج القسمة
نُقربه لأكبر عدد صحيح
هنا (9)

٣-	كل جزء يتكون من (9) رموز، كما يلي :	
	الجزء الأول	Ilv▽ycuty
	الجزء الثاني	▽oem▽onr

4
نأخذ أول حرف من كل
جزء بشكل عمودي
(رأسي)

٤-	نستمر بأخذ الحروف بشكل رأسي من الجزئين على التوالي ، فينتج : I▽love▽my▽country

5
النص الأصلي بدون
مثلثات مقلوبة

٥-	النص الأصلي : I love my country

مثال (4) // صفحة(155) :

جد النص الأصلي للنص المشفر الآتي ، باستخدام خوارزمية الخط المتعرج ، علماً بأنّ مفتاح التشفير هو خمسة أسطر .

Spiheayaaitoviakoplfasesreupleyi▽▽▽s▽y▽▽▽ttym▽h▽l▽

راجع الكتاب صفحة (155)

في عملية التشفير وعملية فك التشفير ، يتم استخدام خوارزمية خاصة بذلك ، هي :
أ) التعويض
ب) التبديل
ج) الإزاحة
د) الخط المتعرج
الإجابة

في عملية التشفير وعملية فك التشفير ، يتم استخدام خوارزمية خاصة بذلك ، تتبع طريقه تشفير ، هي :
أ) التعويض
ب) التبديل
ج) الإزاحة
د) الخط المتعرج
الإجابة

نشاط (٤-٣) /ص١٥٦

فك التشفير باستخدام خوارزمية الخط المتعرج

- Bieno▽itsee▽▽uali▽lviyrbie▽

١) مفتاح التشفير (٣ أسطر)
٢) قسّم النص المُشفّر إلى ٣ أجزاء = ٣ أسطر
٣) نُحدد عدد الحروف في كل جزء :
مجموع حروف النص المشفر ÷ عدد الأجزاء
٢٧ ÷ ٣ = ٩ حروف في كل سطر

B	i	e	n	o	▽	i	t	s
e	e	▽	▽	u	a	l	i	▽
l	v	i	y	r	b	i	e	▽

السطر الأول
السطر الثاني
السطر الثالث

٤) نأخذ الحرف الأول من كل جزء ثم الحرف الثاني ثم الثالث وهكذا حتى النهاية (عمودي) .

- النص مع المثلثات المقلوبة
- النص الأصلي :

Believe▽ in▽your▽abilities▽▽

Believe in your abilities

- Eoterkodnhmon▽u▽eemelci▽n▽siasmtdsgt▽o▽a▽hi▽vfrtt

١) مفتاح التشفير (٧ أسطر)
٢) قسم النص المشفر إلى ٧ أجزاء = ٧ أسطر
٣) يتم عدّ النص المشفر مع المثلثات المقلوبة
٤) نُحدد عدد الحروف في كل جزء :
مجموع حروف النص المشفر ÷ عدد الأجزاء
٤٩ ÷ ٧ = ٧ حروف في كل سطر

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

٤) نأخذ الحرف الأول من كل جزء ثم الحرف الثاني ثم الثالث وهكذا حتى النهاية (عمودي) .

- النص مع المثلثات المقلوبة

Education▽is▽▽▽the▽movement▽from▽darkness▽to▽light

- النص الأصلي :

Education is the movement from darkness to light

يا فرحتي
والله قربت
الأمور في خواتيمها

2 التشفير المعتمد على المفتاح

- يُصنف هذا النوع على عدد المفاتيح المستخدمة في عملية التشفير
- أي :: أنَّ أمن الرسالة والمعلومة **يعتمد** على سرية المفتاح
  [**وليس على تفاصيل الخوارزمية**]

سؤال : أذكر أقسام التشفير المعتمد على المفتاح ؟

أ) خوارزمية المفتاح الخاص (**Private**-key Algorithms)
ب) خوارزمية المفتاح العام (**Public**-key Algorithms)

(أ) خوارزمية المفتاح الخاص

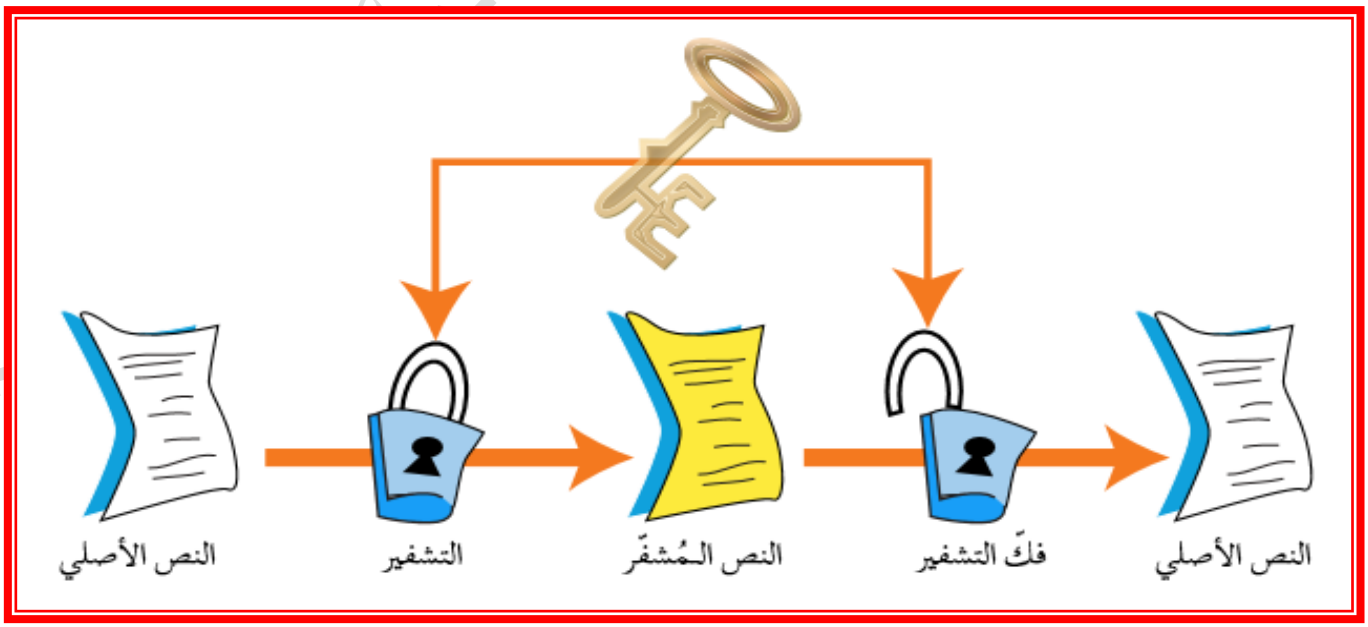
سؤال : علل ... خوارزمية التشفير المفتاح الخاص تُسمى الخوارزمية التناظرية ؟

لأنَّ ... المفتاح نفسه يُستخدم لعمليتي التشفير و فك التشفير

سؤال : علل ... خوارزمية التشفير المفتاح الخاص تُسمى بخوارزمية المفتاح السري ؟

لأنَّه ... يتم الإتفاق على اختياره قبل بدء عملية التراسل بين المُرسل والمُستقبِل

خوارزمية المفتاح الخاص



(ب) خوارزمية المفتاح العام

- تستخدم هذه الخوارزميات **مفتاحين**
  - أحدهما :
    يُستخدم لتشفير الرسالة
    [ويكون معروفاً – للمرسل والمستقبل –]
    ويُسمى **المفتاح العام** .
  - والآخر :
    يكون معروفاً لدى المستقبل **فقط**
    ويُستخدم لفك التشفير
    ويُسمى **المفتاح الخاص** .

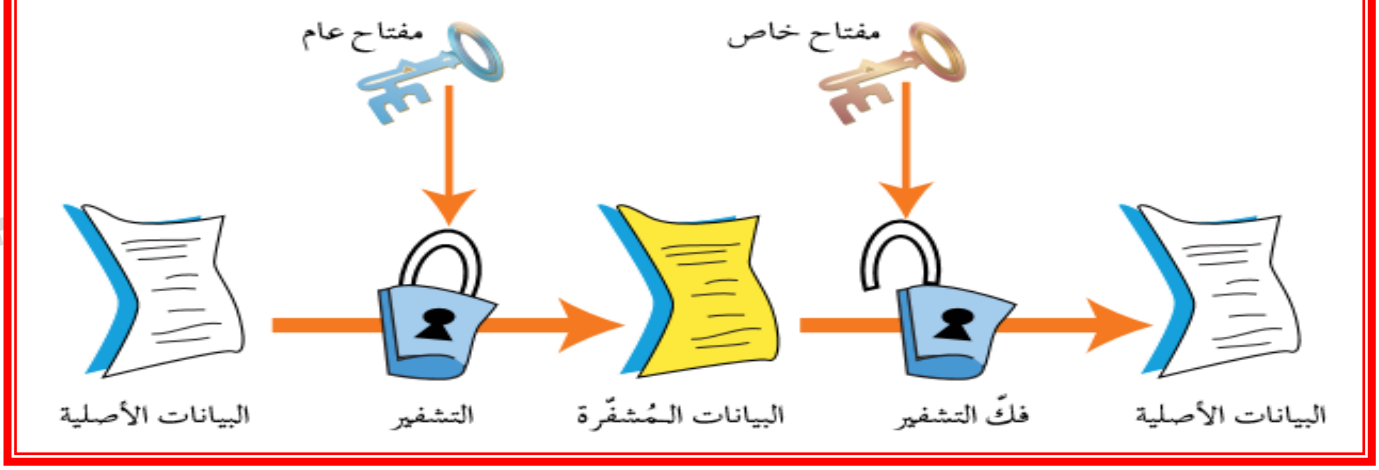
سؤال : كيف يتم إنتاج المفتاحين في خوارزمية المفتاح العام ؟

من خلال عمليات رياضية
و**لا يُمكن** معرفة المفتاح الخاص من خلال معرفة المفتاح العام

سؤال : ما هو الاسم الآخر لخوارزمية المفتاح العام ؟

اللاتناظرية

خوارزمية المفتاح العام



3 التشفير المعتمد على كمية المعلومات المرسلة

سؤال : أذكر أقسام التشفير المعتمد على كمية المعلومات المرسلة ؟

أ) شيفرات التدفق
ب) شيفرات الكتل

خوارزمية شيفرات التدفق :
- يعمل هذا النوع على تقسيم الرسالة إلى مجموعة أجزاء
- ويُشفر كل جزء منها على حدة
- ومن ثم يُرسله .

خوارزمية شيفرات الكتل :
- تُقسم الرسالة إلى أجزاء - ولكن بحجم أكبر من حجم الأجزاء في شيفرات التدفق
- ويُشفر ثم يُفّك كل كتلة على حدة .

نتيجة :

- شيفرات الكتل تختلف عن شيفرات التدفق ، بما يلي :
  - بأنَّ حجم المعلومات أكبر
  - لذلك هي – أبطأ

إجابات أسئلة الفصل الثالث

أسئلة الفصل

١ – وضّح المقصود بكلٍّ من: التشفير، فكّ التشفير.

إجابة (١)

التشفير	هو تغيير محتوى الرسالة الأصلية ...سواء كان التغيير بمزجها بمعلومات أخرى ...أم استبدال الأحرف الأصلية والمقاطع بغيرها ...أم تغيير لمواقع الأحرف بطريقة لن يفهمها إلا مُرسل الرسالة و مستقبلها فقط ... باستخدام خوارزمية معينة و مفتاح خاص
فك التشفير	هو إعادة الرسالة إلى نصها الأصلي باستخدام خطوات محددة ومفاتيح خاصة تكون معلومة لدى المرسل والمستقبل أو ... **عمليات إعادة الرسالة المشفرة إلى المحتوى الأصلي**

٢ – فسّر ما يأتي:

يُعدّ التشفير من أفضل الوسائل الـمُستخدمة للحفاظ على أمن المعلومات.

إجابة (٢)

لأنه يعمل على إخفاء محتوى الرسالة عن الأشخاص غير المصرح لهم مشاهدتها، وفي حال وجدها أشخاص آخرون (المعترضين لها) فإنهم لن يتمكنوا من الاستفادة منها أو فهم محتواها.

٣ – إلامَ يهدف علم التشفير؟ وما عناصره؟

إجابة (٣)

هدف علم التشفير	١) الحفاظ على سرية المعلومات أثناء تبادلها بين مرسل المعلومة ومستقبلها ٢) عدم الاستفادة من المعلومات أو فهم محتواها ، حتى لو تم الحصول عليها من قبل أشخاص معترضين
عناصره	أ) خوارزمية التشفير ب) مفتاح التشفير ج) النص الأصلي د) نص الشيفرة

٤ – حدّد إلى أي من عناصر التشفير يتبع كل مما يأتي:

أ – مجموعة من الخطوات الـمُستخدمة لتحويل الرسالة الأصلية إلى رسالة مُشفّرة .....

ب– الرسالة بعد عملية التشفير .....

جـ– سلسلة من الرموز التي تُستخدم من خلال خوارزمية التشفير .....

د – الرسالة قبل عملية التشفير .....

إجابة (٤)

(أ)	(ب)	(ج)	(د)
خوارزمية التشفير	نص الشيفرة	مفتاح التشفير	النص الأصلي

٥ – عدّد المعايير التي تُصنّف خوارزميات التشفير بناءً عليها.

إجابة (٥)

المعايير	١) التشفير المعتمد على نوع عملية التشفير ٢) التشفير المعتمد على استخدام المفتاح ٣) التشفير المعتمد على كمية المعلومات المرسلة

٦ – ما الفرق بين طريقتي التشفير باستخدام عملية التبديل وعملية التعويض.

إجابة (٦)

عملية التبديل	عملية التعويض
تبديل أماكن الأحرف وذلك بإعادة ترتيب أحرف الكلمة ، بشرط استخدام الأحرف نفسها من دون إجراء أي تغيير عليها	تعني استبدال حرف مكان حرف أو مقطع مكان مقطع ، مثال شيفرة الإزاحة

٧ – لماذا سُميّت خوارزميات المفتاح الخاص بهذا الاسم؟

إجابة (٧)

لأنَّ نفس المفتاح يُستخدم في عمليتي التشفير وفك التشفير

٨ – أوجد النص المُشفّر لكلّ نص مما يأتي، باستخدام خورازمية الخط المتعرج Zig Zag:

أ – Let us keep our home safe and united

علمًا بأن مفتاح التشفير: ثلاثة أسطر.

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

علمًا بأن مفتاح التشفير: ثمانية أسطر.

إجابة (٨) (أ)

Let us keep our home safe and united

١) مفتاح التشفير (٣ أسطر)
٢) نملأ الفراغ الأصلي بمثلث مقلوب ▽
Let▽us▽keep▽our▽home▽safe▽and▽united
٣) وزع أحرف النص الأصلي بشكل قطري ... كما يلي :

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**

٤) اكتب النص المشفر سطراً سطراً :

L▽▽eo▽**msenut**
eukpuhea▽**dne**
tse▽**ro**▽**fa**▽**id**

٥) النص المشفرفي سطر واحد :
L▽▽eo▽**msenut**eukpuhea▽**dne**tse▽**ro**▽**fa**▽**id**

٦) النص المشفر بدون ▽ :
L eo **msenut**eukpuhea **dne**tse **ro** **fa** **id**

إجابة (٨) **(ب)**

Investing in people is more important than investing in things

١) مفتاح التشفير (٨ أسطر)

٢) نملأ الفراغ الأصلي بمثلث مقلوب ▽

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

٣) وزع أحرف النص الأصلي بشكل قطري ... كما يلي :

l		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		l		s	
						i		e		▽		p		t		e		n		▽
							n		o		m		o		h		S		▽		▽

٤) اكتب النص المشفر سطراً سطراً :

lgporatt
n▽**lrtnih**
vieea▽**ni**
en▽▽**nign**
s▽**iitn**▽**g**
tpsm▽**vis**
ie▽**pten**▽
nomohs▽▽

٥) النص المشفرفي سطر واحد :

lgporattn▽**lrtnih**vieea▽**nien**▽▽**nigns**▽**iitn**▽gtpsm▽**visie**▽**pten**▽ nomohs▽▽

٦) النص المشفر بدون ▽ :

lgporattn **lrtnih**vieea **nien nigns iitn** gtpsm **visie pten** nomohs

٩ – فكّ تشفير النص الآتي؛ مستخدمًا خوارزمية الخط المتعرج Zig Zag، علمًا بأن مفتاح التشفير عشرة أسطر.

النص الـمُشفّر:

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

إجابة (٩)

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

١) مفتاح التشفير (١٠ أسطر)
٢) قسم النص المشفر إلى ١٠ أجزاء = ١٠ أسطر
٣) نُحدد عدد الحروف في كل جزء :

مجموع حروف النص المشفر ÷ عدد الأجزاء
٥٠ ÷ ١٠ = ٥ حروف في كل سطر

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

٤) نأخذ الحروف بشكل عمودي :

- النص مع المثلثات المقلوبة :

To▽ brighten▽the▽future▽**we**▽must▽invest▽**in**▽**education**

- النص الأصلي :

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

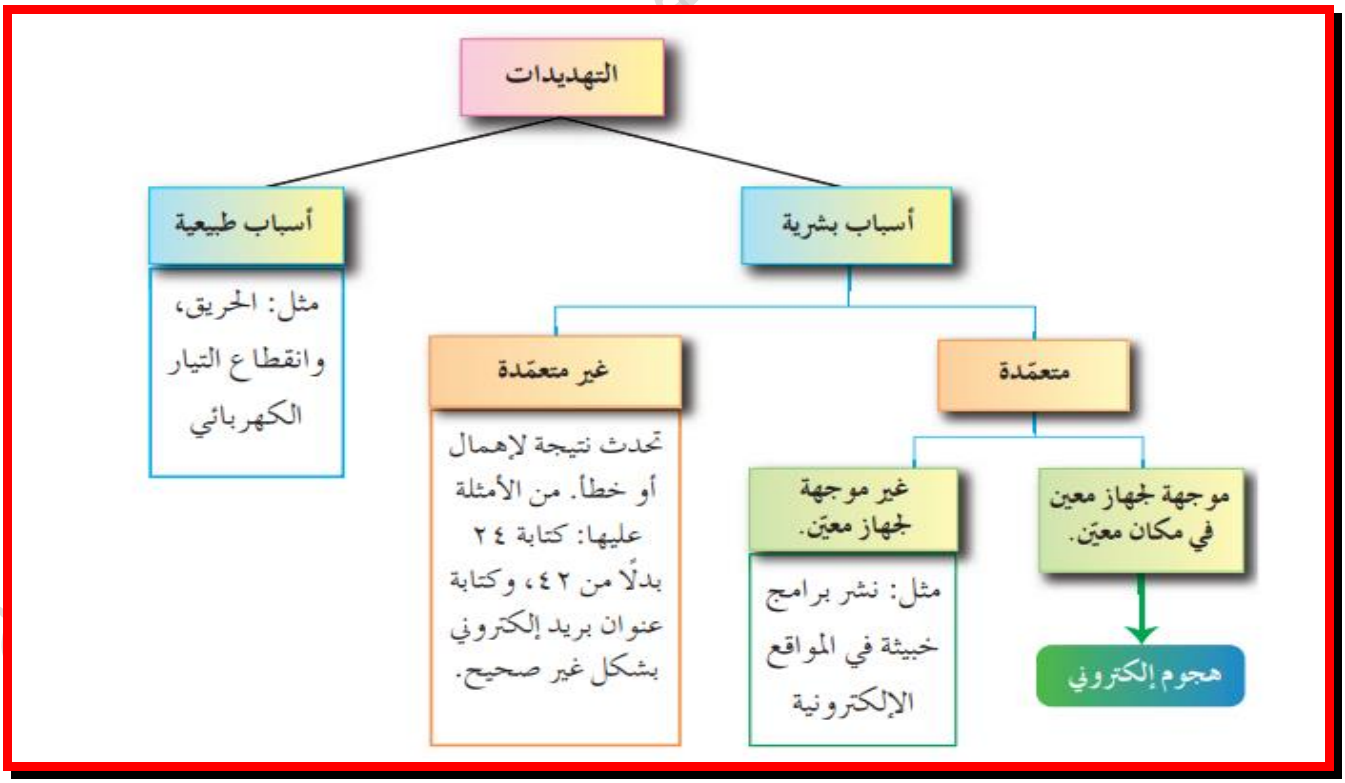
دُعائي لكم بالتوفيق

الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله
الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله الحمد لله

الرابعة

إجابات أسئلة الوحدة

إجابة السؤال الأول:..



٢ – وضّح المقصود بالمفاهيم الآتية: الهندسة الاجتماعية، السلامة، مفتاح التشفير.

إجابة السؤال الثاني :..

الهندسة الاجتماعية	هي الوسائل والأساليب التي يستخدمها المعتدي الإلكتروني لجعل مستخدم الحاسوب في النظام يُعطي معلومات سرية أو يقوم بعمل ما يُسَهِّل عليه الوصول إلى أجهزة الحاسوب أو المعلومات المُخَزَّنة فيها
السلامة	أي حماية الرسائل أو المعلومات التي تمَّ تداولها ... والتأكد بأنها لم تتعرض لأي تعديل ... سواء ((إضافة .. أم .. استبدال .. أم .. حذف جزء منها))
مفتاح التشفير	سلسلة الرموز المستخدمة في خوارزمية التشفير التي تعتمد قوة التشفير عليها

٣ – عند تعرض المعلومات للهجمات الالكترونية يتأثر واحد أو أكثر من عناصر أمن المعلومات في ما يأتي بعض الاعتراضات للبيانات، حدّد عناصر أمن المعلومات التي تتأثر بها.

أ – اعتراض الرسالة والتغيير على محتواها .....

ب– الهجوم المزوّر أو المفبرك .....

جـ– التنصّت على الرسائل .....

د – إدعاء شخص بأنه صديق ويحتاج إلى معلومات .....

هـ– قطع قناة الاتصال .....

إجابة السؤال الثالث :..

(أ)	(ب)	(ج)	(د)	(هـ)
سلامة المعلومات	سرية المعلومات وسلامتها	سرية المعلومات	سرية المعلومات وسلامتها	توافر المعلومات

٤ – فسّر، اختلاف IP address للجهاز عند تراسله أكثر من مرة.

إجابة السؤال الرابع :..

بسبب النمط المتغير لتحويل العناوين الرقمية بحيث يُعطي الجهاز عنواناً رقمياً مختلفاً في كل مرة يتصل فيها مع أجهزة خارج الشبكة الداخلية

٥ – من المخاطر التي تُهدّد الشبكات وجود الثغرات، اذكر ثلاثة أمثلة عليها.

إجابة السؤال الخامس :..

- مثل عدم تحديد صلاحيات الوصول إلى المعلومات
- وجود مشكلة في تصميم النظام أو في مرحلة التنفيذ
- عدم كفاية الحماية المادية للأجهزة والمعلومات

٦ – ما الوسائل التي يستخدمها المعتدي الإلكتروني، للتأثير في الجانب النفسي للشخص المستهدف؟

إجابة السؤال السادس :..

١) الإقناع ٢) انتحال الشخصية والمداهنة ٣) مسايرة الركب

٧ – تُعدّ الثغرات من المخاطر التي تهدد أمن المعلومات. وضّح ذلك.

إجابة السؤال السابع :..

لأنها تُعدّ من نقاط الضعف التي قد تتسبب في فقدان المعلومات ، أو هدم النظام ، أو جعله عرضة للاعتداء الإلكتروني

٨ – أوجد النص الـمُشفّر لكلّ 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.

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

علمًا بأن مفتاح التشفير ستة أسطر.

إجابة السؤال الثامن :..

الفرع (أ) :

Youth is the future and the spirit of our home

١) مفتاح التشفير (٤ أسطر)

٢) نملأ الفراغ الأصلي بمثلث مقلوب ▽

Youth▽is▽the▽future▽and▽the▽spirit▽of▽our▽home

٣) وزع أحرف النص الأصلي بشكل قطري ... كما يلي :

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

٤) اكتب النص المشفر سطراً سطراً :

Yh▽▽**uatsifrm**
o▽**tfrnhpt**▽▽e
uihuedei▽oh▽
tset▽▽▽**rouo**▽

٥) النص المشفرفي سطر واحد :

Yh▽▽**uatsifrmo**▽**tfrnhpt**▽▽**e**uihuedei▽**oh**▽tset▽▽▽**rouo**▽

النص المشفر بدون ▽ :

Yh **uatsifrmo tfrnhpt e**uihuedei **oh** tset **rouo**

الفرع (ب) :

School is the place where great people and ideas are formed

١) مفتاح التشفير (٦ أسطر)

٢) نملأ الفراغ الأصلي بمثلث مقلوب ▽

School▽is▽the▽place▽where▽great▽people▽and▽ideas▽are▽formed

٣) وزع أحرف النص الأصلي بشكل قطري ... كما يلي :

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**		▽

٤) اكتب النص المشفر سطراً سطراً :

S▽eeetl▽▽**o**
ci▽▽▽▽**eiar**
hspwgp▽**drm**
o▽**lhreaeee**
otaeeona▽**d**
lhcrapdsf▽

٥) النص المشفرفي سطر واحد :

S▽eeetl▽▽**o**ci▽▽▽▽**eiar**hspwgp▽**drm**o▽**lhreaeee**otaeeona▽**d**lhcrapdsf▽

النص المشفر بدون ▽ :

S eeetl **o**ci **eiar**hspwgp **drm**o **lhreaeee**otaeeona **d**lhcrapdsf

٩ – فك تشفير كلّ نص من النصوص الآتية، مستخدمًا خوارزمية الخط المتعرج Zig Zag علمًا بأن مفتاح التشفير ستة أسطر.

النص الـمُشفّر:

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

إجابة السؤال التاسع:..

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

١) مفتاح التشفير (٦ أسطر)
٢) قسم النص المشفر إلى ٦ أجزاء = ٦ أسطر
٣) نُحدد عدد الحروف في كل جزء :
مجموع حروف النص المشفر ÷ عدد الأجزاء
٤٨ ÷ ٦ = ٨ حروف في كل سطر

السطر الأول	e	▽	▽	p	s	e	t	w	H
السطر الثاني	▽	p	s	e	▽	m	▽	e	o
السطر الثالث	▽	l	w	p	u	e	e	m
السطر الرابع	▽	e	e	▽	s	▽	t	e
السطر الخامس	▽	a	e	i	▽	l	▽	▽
السطر السادس	▽	s	t	t	k	e	h	s

٤) نأخذ الحروف بشكل عمودي :

- **النص مع المثلثات المقلوبة :**

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

- **النص الأصلي :**

Home sweet home let us keep it sweet please

١٠- حدّد أنواع خوارزميات التشفير، إذا قُسّمت بناءً على المعايير الآتية:

أ - المفتاح الـمُستخدم.

ب- كمية المعلومات الـمُرسلَة.

جـ- العملية الـمُستخدمة في التشفير.

إجابة السؤال العاشر:..

(أ) المفتاح المستخدم	(ب) كمية المعلومات المرسلة	(ج) العملية المستخدمة في التشفير
أ) خوارزمية المفتاح الخاص	أ) شيفرات التدفق	أ) تشفير التعويض
ب) خوارزمية المفتاح العام	ب) شيفرات الكتل	ب) تشفير التبديل

200 ستكون من نصيبكم بعون الله

تمّ بحمد الله

من طلب العلا سهر الليالي