أمن المعلومات : هو العلم الذي يعمل على حماية المعلومات والمعدات المستخدمة لتخزينها ومعالجتها ونقلها من السرقة أو التطفل أو من الكوارث الطبيعية أو غيرها من المخاطر ويعمل على إبقاءها متاحة للأفراد المصرح لهم باستخدامها

الخصائص الأساسية لأمن المعلومات ؟ (مهم)

1-السرية 2- السلامة 3- توافر المعلومات

الخصائص الأساسية لأمن المعلومات ؟1-السرية 2- السلامة 3- توافر المعلومات

علل: ظهور مصطلح أمن المعلومات .

لحماية المعلومات والمعدات المستخدمة إبقاءها متاحة للأفراد المصرح لهم باستخدامها**ما**

المخاطر التي تهدد المعلومات .

1.السرقة 2.التطفل 3. الكوارث الطبيعية

	التعريف	أمثلة	ملاحظات
السرية	أن الشخص المخول هو الوحيد القادر على الوصول إلى المعلومات والاطلاع عليها.	• المعلومات الشخصية • الموقف المالي لشركة ما قبل إعلانه • المعلومات العسكرية	مصطلح السرية مرادف لمفهومي (الأمن و الخصوصية) (مهمم للأسئلة الموضوعية)
السلامة	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	
توافر المعلومات	قدرة الشخص المخول الحصول على المعلومات في الوقت الذي يشاء ، دون وجود عوائق	• حذف المعلومات • أو الاعتداء على الأجهزة التي تخزن فيها هذه المعلومات	**متى تكون المعلومات بلا فائدة .** • إذا لم تكن متاحة للأشخاص المصرح لهم بالتعامل معها • أو أن الوصول إليها يحتاج إلى وقت كبير

تقسم المخاطر التي تهدد أمن المعلومات إلى نوعين رئيسين هما:

1-التهديدات 2- الثغرات .

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

الأسباب البشرية : و تقسم إلى نوعين:

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

ب. أن تكون متعمدة وتقسم إلى قسمين

1.غير موجهة لجهاز معين كأن ينشر فيروس

2. موجهة لجهاز معين وهذا ما يسمى **الهجوم الإلكتروني** ,أو **الاعتداء الإلكتروني ومثال عليه الاعتداء الالكتروني ؟** سرقة جهاز الحاسوب

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

الدافع 2. الطريقة 3. فرصة النجاح

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

دوافع الأفراد لتنفيذ هجوم إلكتروني .

1. الرغبة في الحصول على المال 2. محاولة لإثبات القدرات التقنية 3. بقصد الإضرار بالآخرين .

الأمور التي تتضمنها الطريقة في الهجوم الالكتروني ؟

1.المهارات التي يتميز بها المعتدي الإلكتروني .

2. قدراته على توفير المعدات والبرمجيات التي يحتاج إليها .

3. معرفته بتصميم النظام وآلية عمله 4.معرفة نقاط القوة والضعف لهذا النظام

على ماذا تعتمد فرصة نجاح الهجوم الإلكتروني؟

1. تحديد الوقت المناسب للتنفيذ 2. كيفية الوصول إلى الأجهزة

أنواع الاعتداءات الإلكترونية .

1.التنصت على المعلومات 2. التعديل على المحتوى

3. الإيقاف 4. الهجوم المزور أو المفبرك

التنصت على المعلومات :الهدف منه الحصول على المعلومات السرية حيث يتم الإخلال بسرية المعلومات .

التعديل على محتوى المعلومات : يتم اعتراض المعلومات وتغيير محتواها وإعادة إرسالها للمستقبل من دون أن يعلم بتغيير محتواها وفي هذا النوع يكون الإخلال بسلامة المعلومات

الإيقاف :يتم قطع قناة الاتصال ومن ثم منع المعلومات من الوصول إلى المستقبل وفي هذه الحالة الاخلال بتوافر المعلومات

الهجوم المفبرك : يتمثل هذا النوع بإرسال المعتدي الالكتروني رسالة إلى أحد الأشخاص على الشبكة ويخبره فيها بأنه صديقه ويحتاج إلى معلومات أو كلمات سرية خاصة والاخلال يكون بسرية المعلومات وسلامة المعلومات

علل : قام المختصون في أمن المعلومات بوضع مجموعة من الضوابط.
لتقليل المخاطر التي تتعرض لها المعلومات والحد منها .

قام المختصون في أمن المعلومات بوضع مجموعة من الضوابط لتقليل المخاطر التي تتعرض لها المعلومات والحد منها . أذكر هذه الضوابط .
1.الضوابط المادية . 2.الضوابط الإدارية . 3.الضوابط التقنية

الضوابط المادية	مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها (مثل)**باستخدام الجدران والأسوار واستخدام الأقفال ووجود حراس الأمن وغيرها من أجهزة لإطفاء الحريق .**
الضوابط الإدارية	استخدام مجموعة من الأوامر والإجراءات المتفق عليها **مثل : القوانين واللوائح والسياسات والإجراءات التوجيهية وحقوق النشر وبراءات الاختراع والعقود والاتفاقيات**
الضوابط التقنية	وهي الحماية التي تعتمد على التقنيات المستخدمة سواء أكانت معدات (hardware) أو برمجيات (software) وتتضمن (مثل)**كلمات المرور ومنح صلاحيات الوصول و بروتوكولات الشبكات والجدار الناري والتشفير وتنظيم تدفق المعلومات في الشبكة .**

يعتمد اختيار الكادر البشري المسؤول عن حماية الأنظمة على عدة أمور . اذكرها .
1. كفايته العلمية .
2. اختبارات شفوية و ورقية و مقابلات
3. إخضاعهم إلى ضغوط نفسية كل حسب موقعهم للتأكد من قدرتهم على حماية النظام .

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

علل : تعد الهندسة الاجتماعية من أنجح الوسائل وأسهلها التي تستخدم للحصول على معلومات غير مصرح بالاطلاع عليها .
- بسبب قلة اهتمام المتخصصين في مجال أمن المعلومات
- وعدم وعي مستخدمي الحاسوب بالمخاطر المترتبة عليها

مجالات الهندسة الاجتماعية

1. البيئة المحيطة 2. الجانب النفسي

الضوابط المادية	الية العمل (فهم)
مكان العمل.	يكتب بعض الموظفين كلمات على أوراق ملصقة بشاشة الحاسوب وعند دخول الشخص غير المخول له الاستخدام كزبون أو عامل نظافةيستطيع معرفة كلمات المرور
الهاتف	يتصل الشخص غير المخول بمركز الدعم الفني هاتفيا ويطلب إليه بعض المعلومات الفنية ويستدرجه للحصول على كلمات المرور ليستخدمها في ما بعد
النفايات الورقية	يدخل الأشخاص غير المخولين إلى مكان العمل ويجمعون النفايات التي قد تحتوي على كلمات المرور ومعلومات تخص الموظفين وأرقام هواتفهم وبياناتهم الشخصية وكل ما يحتويه من معلومات يمكن استغلالها في تتبع أعمال الموظفين و الحصول على المعلومات
الإنترنت	من خلال استخدام الموظفين أو مستخدمي الحاسوب عادة كلمة المرور نفسها للتطبيقات جميعها حيث ينشئ المعتدي الإلكتروني موقعا على الشبكة و يتطلب التسجيل في الموقع اسم مستخدم وكلمة المرور وهي كلمة المرور نفسها التي يستخدمها الشخص عادة وبهذه الطريقة يتمكن المعتدي الإلكتروني من الحصول عليها

الأساليب التي يستخدمها المعتدي الإلكتروني هنا لكسب ثقة مستخدم الحاسوب ومن ثم الحصول على المعلومات ؟
1.الإقناع. 2.انتحال الشخصية والمداهنة3.مسايرة الركب

	الية العمل
الاقناع	طرق الاقناع بطريقة مباشرة : بحيث يقدم الحجج المنطقية والبراهين . ب.بطريقة غير مباشرة :تقديم الايحاءات
انتحال الشخصية و المداهنة	حيث يتقمص شخص شخصية أخرى وهذا الشخص قد يكون شخصا حقيقيا أو وهميا (انتحال شخصية فني الصيانة)
مسايرة الركب	يرى الموظف بأنه إذا قام زملاؤه جميعهم بأمر ما فمن غير اللائق أن يأخذ هو موقفا مغايرا (مثل : اعطاء المدير الصلحية لشخص بتحديث الجهاز فيقوم الجميع بالسماح له بالتحديث)

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

علل :لا بد من إيجاد وسائل تعمل على حماية (الويب).
للحد من الاعتداءات والأخطار التي تهددهابسبب انتشار البرامج المقرصنة والمعلومات الخاصة بكيفية اقتحام المواقع .

أذكر انواع البرامج المنتشرة عبر الانترنت .
- البرامج المجانية .
- البرامج غير معروفة المصدر .
- البرامج المفتوحة : أي أنه يمكن استخدامه على الأجهزة المختلفة

اذكر أنواع الاعتداءات التي تتعرض لها المواقع الإلكترونية.
1. الاعتداء على متصفح الإنترنت (Browsers attack)
2. الاعتداء على البريد الإلكتروني (E- mail attack)

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

أيانا (iana) :السلطة المسؤولة عن منح أرقام الإنترنت المخصصة لإعطاء العناوين الرقمية للأجهزة على الإنترنت.

يتعرض متصفح الإنترنت إلى الكثير من الأخطار ويمكن أن يتم هذا الاعتداء بطريقتين ، اذكرهما ؟
أ- الاعتداء عن طريق (كود) بسيط يمكن إضافته إلى المتصفح وباستطاعته القراءة والنسخ وإعادة إرسال أي شيء يتم إدخاله من قبل المستخدم
ب-توجيه المستخدم إلى صفحة أخرى غير الصفحة التي يريدها

كيف تتم الاعتداءات الإلكترونية على البريد الالكتروني .
من خلال وصول الرسائل الإلكترونية المزيفة إلى البريد الإلكتروني.

تقنية تحويل العناوين الرقمية : هي التقنية التي تعمل على إخفاء العنوان الرقمي للجهاز في الشبكة الداخلية ليتوافق مع العنوان الرقمي المعطى للشبكة.

مم يتكون العنوان الرقمي الإلكتروني (IP address) .
يتكون من (32) خانة ثنائية تتوزع على أربعة مقاطع يفصل بينها نقاط وهذا ما يسمى بـ ip4 وكل مقطع من هذه المقاطع يتضمن رقم من (0) إلى (255) كالآتي : 215.002.004.216

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

قارن بين IP4 / IPV6 من حيث :

	عدد المقاطع	السلطة المسؤولة عن منح العناوين
IP4	4	IANA
IPV6	8	IANA

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

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

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

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

الطرق التي تعمل بها تقنية تحويل العناوين الرقمية (مههم)
1. النمط الثابت للتحويل .
2. النمط المتغير للتحويل .

	مكان وجود العناوين الخارجية	الية العمل
النمط الثابت للتحويل	عند كل جهاز داخل الشبكة له عنوان خارجي له	ويتم عن طريق هذا النمط تخصيص عنوان رقمي خارجي لكل جهاز داخلي وهذا العنوان الرقمي ثابت لا يتغير .
النمط المتغير للتحويل .	عند الجهاز الوسيط	• عند رغبة أحد الأجهزة بالتراسل خارجيا فانه يتواصل مع الجهاز الوسيط الذي يعطيه عنوانا خارجيا مؤقتا يستخدمه لحين الانتهاء من عملية التراسل خارجيا مؤقتا يستخدمه ويعد هذا العنوان عنوانا رقميا خاصا بالجهاز • عند انتهاء عملية التراسل يفقد الجهاز الداخلي هذا العنوان ويصبح العنوان متاحا للتراسل مرة أخرى

علل (فسر) : اختلاف IP Address للجهاز نفسه عند تراسله أكثر من مرة في النمط المتغير للتحويل .
لأن العناوين تكون مخزنة لدى الجهاز الوسيط و عند القيام بعملية التراسل خارجياً يأخذ المرسل العنوان المتاح و يرسل فيه و عند رغبته بالارسال مرة أخرى من الممكن أن يكون العنوان الذي أخذه في المرة السابقة غير متوفر و بالتالي يأخذ عنواناً آخر .

AWA2EL LEARN 2 LIVE
www.awa2el.net

التشفير .

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

ما هدف التشفير. /علل : يُعدّ التشفير من أفضل الطرق المُستخدمة للحفاظ على أمن المعلومات .

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

عناصر التشفير .

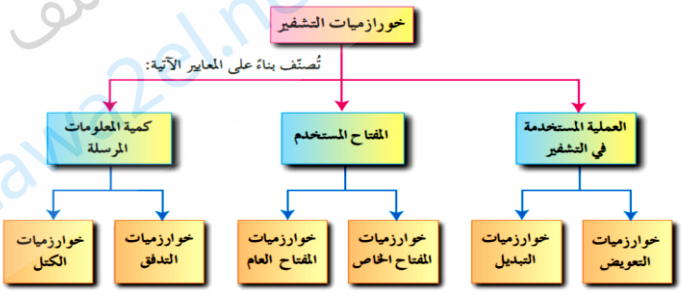
أ. خوارزمية التشفير: مجموعة الخطوات المُستخدمة لتحويل الرسالة الأصلية إلى رسالة مُشفّرة،

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

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

د - نص الشيفرة: الرسالة بعد عملية التشفير

معايير تصنيف خوارزميات التشفير



الشكل (٤– ٤): أنواع الخوارزميات.

قارن بين :

	التعريف	مثال
خوارزمية التعويض	وتعني استبدال حرف مكان حرف أو مقطع مكان مقطع	شيفرة الإزاحة
خوارزمية التبديل	وذلك عن طريق إعادة ترتيب أحرف الكلمة؛ بشرط استخدام الأحرف نفسها من دون إجراء أي تغيير عليها	خوارزمية الخط المتعرج .

عمليات التشفير .

عملية التشفير : اخفاء معنى النص الحقيقي . و تكون عند المرسل

عملية فك التشفير : استرجاع النص الأصلي من النص المشفر . و تكون عند المستقبل

مميزات خوارزمية الخط المتعرج .

أ) خوارزمية سهلة وسريعة.

ب) يمكن تنفيذها يدويًّا باستخدام الورقة والقلم .

ج) يمكن فكّ تشفيرها بسهولة.

قارن:

	عدد المفاتيح المستخدمة	اسمائها
خوارزمية المفتاح العام	2 المفتاح العام (يستخدم للتشفير) المفتاح الخاص (يستخدم لفك التشفير)	1.الخوارزميات اللاتناظرية
خوارزمية المفتاح الخاص	1 (المفتاح نفسه مستخدم للتشفير و فك التشفير)	1.الخوارزميات التناظرية . 2.خوارزميات المفتاح السري

آلية التشفير بالمفتاح العام .

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

وضح آلية التشفير باستخدام شيفرات التدفق .

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

وضح آلية التشفير باستخدام شيفرات الكتل .

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