مخططات تتناول الخطوط العريضة لمنهاج علوم الحاسوب ..... وهي لا تغني عن الكتاب ولا عن دوسية **الأولى**

المادة النظرية

إعداد

أ.محمد توفيق ٠٧٨٦٥٨٣٢٤٠

أ. هيثم جميل ٠٧٨٩٧٥٦٥٩٩

- صفحتنا على الفيسبوك **https://www.facebook.com/mohammad.tawfeeq.fares**

(الأستاذ محمد توفيق)

الوحدة الأولى: أنظمة العد.

س١: ما هو الاختلاف في أسماء الأنظمة العددية؟ يعود الاختلاف إلى عدد الرموز المسموح باستخدامها في كل نظام. فالنظام العشري يستخدم ١٠ رموز/ والنظام الثنائي يستخدم رمزين/ والنظام الثماني يستخدم ٨ رموز/والسادس عشر يستخدم ١٦ رمزاً.

نظام العد الموضعي: إن القيمة الحقيقية للرقم تعتمد على الخانة أو المنزلة التي يقع فيها. فقيمة الرقم تختلف باختلاف موقعه داخل العدد.

جميع الأنظمة العددية تعتبر أنظمة موضعية.

س٢: ما هي استخدامات النظام الثنائي داخل الحاسوب؟ ١. تخزين البيانات
٢. عنونة مواقع الذاكرة

اسم النظام	أساس النظام	الرموز المستخدمة في النظام	مثال
النظام العشري	10	(9,8,7,6,5,4,3,2,1,0)	$(823)_{10}$
النظام الثنائي	2	(1,0)	$(10110)_2$
النظام الثماني	8	(7,6,5,4,3,2,1,0)	$(723)_8$
النظام السادس عشر	16	(F,E,D,C,B,A,9,8,7,6,5,4,3,2,1,0)	$(FA9)_{16}$

النظام العددي: مجموعة من الرموز (أرقاماً أو حروفاً) مرتبطة مع بعضها بمجموعة من العلاقات وفق أسس وقواعد معينة ، لتشكل الأعداد ذات المعاني الواضحة والاستخدامات المتعددة.

النظام العشري: هو أكثر الأنظمة استعمالاً، رموزه (**0,1,2,3,4,5,6,7,8,9**) وأساسه **10**

الرقم (Digit): رمز واحد من الرموز الأساسية (9,8,7,6,5,4,3,2,1,0) يستخدم للتعبير عن العدد، ويحتل منزلة واحدة من العدد.

العدد (Number): المقدار الذي يمثل برقم واحد أو أكثر (منزلة واحدة أو أكثر)

النظام الثنائي: هو نظام عد مستخدم في الحاسوب، أساسه **2** ، و رموزه (**0** ، **1**)

النظام الثماني: هو أحد أنظمة العد الموضعية، أساسه **8** ، و رموزه (7,6,5,4,3,2,1,0)

النظام السادس عشر: هو أحد أنظمة العد الموضعية، أساسه **16** ، و رموزه (F,E,D,C,B,A,9,8,7,6,5,4,3,2,1,0)

(**Bit**) على الخانة أو المنزلة التي يحتلها الرمز داخل العدد لأن كل رمز ثنائي يمثل باستخدام خانة واحدة فقط.

علل: استخدام النظام الثنائي داخل الحاسوب (لا يمكن استخدام النظام العشري داخل الحاسوب)
لأن بناء الحاسوب يعتمد على ملايين الدارات الكهربائية والتي تكون إما مفتوحة أو مغلقة

علل: استخدام النظامين الثماني والسادس عشر.
١. إن استخدام النظام الثنائي لتخزين البيانات وعنونة مواقع الذاكرة يتطلب قراءة سلسلة طويلة من الأرقام الثنائية وكتابتها. ٢. التسهيل على المبرمجين استخدام الحاسوب.

علل: إن تنفيذ العمليات الحسابية في النظام الثنائي أسهل من تنفيذها في النظام العشري. لأن النظام الثنائي يتكون من رقمين فقط هما (**0**،**1**)

الوحدة الثانية : الذكاء الاصطناعي

المنهجيات التي قام عليها موضوع الذكاء الاصطناعي

١. التفكير كالإنسان
٢. التصرف كالإنسان
٣. التفكير منطقياً
٤. التصرف منطقياً

أهداف الذكاء الاصطناعي :

١. إنشاء أنظمة خبيرة تظهر تصرفا ذكياً.
٢. تطبيق الذكاء الانساني في الآلة.
٣. برمجة الآلات لتصبح قادرة على معالجة المعلومات بشكل متواز.

مميزات برامج الذكاء الاصطناعي.

١. تمثيل المعرفة
٢. التمثيل الرمزي
٣.القدرة على التعلم أو تعلم الآلة
٤. التخطيط ٥. التعامل مع البيانات الغير مكتملة أو غير المؤكدة

تطبيقات للذكاء الاصطناعي

١. الروبوت الذكي
٢. الانظمة الخبيرة
٣.الشبكات العصبية
٤. معالجة اللغات الطبيعية
٥.الانظمة البصرية
٦. أنظمة تمييز الاصوات
٧.أنظمة تمييز خط اليد
٨. أنظمة الألعاب

لغات برمجة خاصة بالذكاء الاصطناعي

١.لغة البرمجة ليسب Lisp :
وهي لغة معالجة اللوائح .
٢. لغة البرمجة برولوج Prolog
وهي لغة البرمجة بالمنطق .

علم الروبوت

صفات آلة الروبوت

١. الاستشعار
٢. التخطيط والمعالجة
٣. الاستجابة وردة الفعل

الاجزاء التي يتكون منها الروبوت

١. الذراع الميكانيكية
٢. المستجيب النهائي
٣. المتحكم
٤. المشغل الميكانيكي
٥. الحساسات

أنواع الحساسات

١. حساس اللمس
٢. حساس المسافة
٣. حساس الضوء
٥. حساس الصوت

فوائد الروبوت في مجال الصناعة .

١.يقوم بالأعمال التي تتطلب تكرارا مدة طويلة دون تعب
٢.يستطيع القيام بالأعمال التي تتطلب تجميع القطع وتركيبها في مكانها بدقة عالية .
٣.يقلل من المشكلات التي تتعرض لها المصانع مع العمال ، كالإجازات والتأخير والتعب .
٤. يمكن التعديل على البرنامج المصمم للروبوت لزيادة المرونة في التصنيع ، حسب المتطلبات التي تقتضيها عملية التصنيع.
٥. يستطيع العمل تحت الضغط ، و في ظروف غير ملائمة لصحة الإنسان ، كأعمال الدهان ورش المواد الكيميائية ودرجات الرطوبة والحرارة العاليتين.

محددات (سلبيات) استخدام الروبوت في الصناعة

١. الاستغناء عن الموظفين في المصانع ، سيزيد من نسبة البطالة ويقلل من فرص العمل .
٢. لا يستطيع القيام بالأعمال التي تتطلب حسا فنيا أو ذوقا في التصميم
٣. تكلفة تشغيل الروبوت في المصانع عالية ، لذا تعد غير مناسبة في المصانع المتوسطة والصغيرة .
٤. يحتاج الموظفون إلى برامج تدريبية للتعامل مع الروبوتات الصناعية وتشغيلها ، وهذا سيكلف الشركات الصناعية مالا و وقتا
٥. مساحة المصانع التي ستستخدم الروبوتات يجب أن تكون كبيرة جدا ، لتجنب الاصطدامات والحوادث في أثناء حركتها

معايير تصنيف الروبوتات

١- حسب الاستخدام و الخدمات التي تقدمها

أنواع(أصناف) الروبوتات حسب الاستخدام والخدمات التي تقدمها :

١. الروبوت الصناعي

يستخدم في١. عمليات الطلاء بالبخ الحراري في المصانع ٢. أعمال الصب وسكب المعادن

٣. عمليات تجميع القطع وتثبيتها في أماكنها

٢. الروبوت الطبي

يستخدم في ١.إجراء العمليات الجراحية المعقدة ، مثل جراحة الدماغ وعمليات القلب المفتوح .

٢. مساعدة ذوي الاحتياجات الخاصة

٣. الروبوت التعليمي:تحفيز الطلبة وجذب انتباههم الى التعليم ، وقد تكون على هيئة إنسان معلم

٤. الروبوت في الفضاء ١. استخدم في المركبات الفضائية ٢. دراسة سطح المريخ.

٥. الروبوت في المجال الامني

يستخدم في ١. مكافحة الحرائق وإبطال مفعول الألغام والقنابل. ٢. نقل المواد السامة والمشعة .

٢- حسب إمكانية تنقلها

أنواع الروبوتات حسب إمكانية نقلها

١. الروبوت الثابت

تثبيت قاعدته على أرضية ثابتة ، وتقوم ذراع الروبوت بأداء المهمة المطلوبة (نقل عناصر ، حملها ، ترتيبها بطريقة معينة)

٢١. الروبوت الجوال أو المتنقل

أنواع الروبوت الجوال أو المتنقل

١. الروبوت ذو العجلات

٢. الروبوت ذو الأرجل

٣. الروبوت السباح

٤.الروبوت على هيئة إنسان(الرجل الآلي)

تاريخ نشأة الروبوت

العصور القديمة قبل الميلاد	تصميم آلات اطلق عليها (آلات ذاتية الحركة)
القرنين الثاني عشر والثالث عشر للميلاد	العالم المسلم الجزري ، تصميم ساعات مائية وآلات أخرى مثل (آلة لغسل اليدين وتقدم الصابون والمناشف لمستخدمهاآليا) (صاحب كتاب معرفة الحيل الهندسية)
القرن التاسع عشر	ابتكار دمى آلية في اليابان ، قادرة على : تقديم الشاي ، اطلاق السهام ، الطلاء (تدعى ألعاب كاراكوري)
خمسينيات وستينيات القرن الماضي	ظهور مصطلح الذكاء الاصطناعي ، صمم : (اول نظام خبير لحل مشكلات رياضية صعبة ، اول ذراع روبوت في الصناعة)
منذ العام ٢٠٠٠م	ظهر الجيل الجديد من الروبوتات التي تشبه في تصميمها جسم الانسان ، (الانسان الآلي) ، استخدمت في أبحاث الفضاء من قبل وكالة ناسا .

النظم الخبيرة

أمثلة عملية على برامج النظم الخبيرة

اسم البرنامج	مجال الاستخدام
ديندرال	تحديد مكونات المركبات الكيميائية
باف	نظام طبي لتشخيص أمراض الجهاز التنفسي
بروسبكتر	لتحديد مواقع الحفر للتنقيب عن النفط والمعادن (يستخدم من قبل الجيولوجيين)
ديزاين أدفايزر	يقدم نصائح لتصميم رقائق المعالج
ليثيان	يعطي نصائح لعلماء الآثار لفحص الأدوات الحجرية

أنواع المشكلات (المسائل) (الفئات) التي تحتاج إلى النظم الخبيرة

الفئة	المثال
١.التشخيص	تشخيص أعطال المعدات لنوع معين من الآلات ، التشخيص الطبي لأمراض الإنسان
٢. التصميم	اعطاء نصائح عند تصميم مكونات أنظمة الحاسوب والدارات الإلكترونية .
٣. التخطيط	التخطيط لمسار الرحلات الجوية
٤. التفسير	تفسير بيانات الصور الإشعاعية
٥. التنبؤ	التنبؤ بالطقس أو أسعار الأسهم

أجزاء (مكونات) النظم الخبيرة :

١- قاعدة المعرفة

٢- محرك الاستدلال

٣- ذاكرة العمل

٤- واجهة الاستخدام

النظم الخبيرة

الأمور التي يمكن ملاحظتها في شاشة البرنامج(xpertis2Go) لتشخيص أعطال السيارة:

١. وجود خيار (لا أعرف)، ويدل ذلك على قدرة النظام على التعامل مع الإجابات الغامضة.

٢. إمكانية استخدام معطيات غير كاملة، حيث يمكن للمستخدم إدخال درجة التأكد من إجابته.

٣. إمكانية تفسير سبب طرح البرنامج هذا السؤال للمستخدم.

ميزات (فوائد) النظم الخبيرة

١. النظام الخبير غير معرض للنسيان .

٢. المساعدة على تدريب المختصين ذوي الخبرة المنخفضة

٣. توفر النظم الخبيرة مستوى عاليا من الخبرات ، عن طريق تجميع خبرة أكثر من شخص في نظام واحد .

٤. نشر الخبرة النادرة إلى أماكن بعيدة للاستفادة منها .

٥. القدرة على العمل بمعلومات غير كاملة أو مؤكدة .

محددات النظم الخبيرة . (من أسئلة الوحدة)

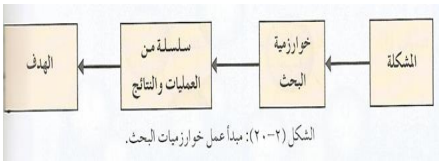
١. عدم قدرة النظام الخبير على الإدراك والحدس، بالمقارنة مع الخبير .

٢. عدم قدرة النظام الخبير على التجاوب مع المواقف غير الاعتيادية أو المشكلات خارج نطاق التخصص .

٣. صعوبة جمع الخبرة والمعرفة اللازمة لبناء قاعدة المعرفة من الخبراء .

خوارزميات البحث

مبدأ عمل خوارزميات البحث :



الشكل (٢-٢٠): مبدأ عمل خوارزميات البحث.

ملاحظة : يتم أخذ المشكلة على أنها مدخلات

صفات المشكلات التي تحتاج لخوارزميات البحث في الذكاء الاصطناعي

١- لا يوجد للحل طريقة تحليلية واضحة ، أو ان الحل مستحيل بالطرائق العادية .

٢- يحتاج الحل إلى عمليات حسابية كثيرة ومتنوعة لإيجاده مثل (الألعاب ، التشفير).

٣- يحتاج الحل إلى حدس عالي ، مثل (الشطرنج)

عناصر شجرة البحث (أهم المفاهيم في شجرة البحث) .

أ- مجموعة من النقاط أو العقد ب- جذر الشجرة

ج- الأب د- النقطة الهدف(الحالة الهدف) هـ- المسار

أنواع خوارزميات البحث في الذكاء الاصطناعي

١- خوارزمية البحث في العمق أولا

٢- خوارزمية البحث في العرض أولا

٣- الخوارومية الحدسية

الذكاء الاصطناعي : علم من علوم الحاسوب ، يختص بتصميم وتمثيل وبرمجة نماذج حاسوبية في مجالات الحياة المختلفة ، تحاكي في عملها طريقة تفكير الإنسان وردود أفعاله في مواقف معينة

المحاكاة: تقليد لأحداث أو عمليات من واقع الحياة، كي يتيسر عرضها والتعمق فيها لاستكشاف أسرارها، والتعرف إلى نتائجها المحتملة عن قرب.

برنامج يوجين غوستمان ؟ هو برنامج حاسوبي للذكاء الاصطناعي لطفل من أوكرانيا عمره ١٣ عاما استطاع ان يخدع ٣٣% من محاوريه مدة ٥ دقائق ، ولم يميزوا أنه برنامج بل ظنوا أنه إنسان.

تمثيل المعرفة: تنظيم المعرفة و ترميزها و تخزينها إلى ما هو موجود في الذاكرة

التمثيل الرمزي: تعامل برامج الذكاء الاصطناعي مع البيانات الرمزية (الأرقام و الحروف و الرموز) ، التي تعبر عن المعلومات عن طريق عمليات المقارنة المنطقية والتحليل

القدرة على التعلم أو تعلم الآلة: قدرة برنامج الذكاء الاصطناعي على التعلم آليا عن طريق الخبرة المخزنة داخله

التخطيط: قدرة برنامج الذكاء الاصطناعي على وضع أهداف و العمل على تحقيقها ، والقدرة على تغيير الخطة إذا اقتضت الحاجة إلى ذلك

التعامل مع البيانات الغير مكتملة أو غير المؤكدة: قدرة برامج الذكاء الاصطناعي على إعطاء حلول مقبولة ، حتى لو كانت المعلومات لديها غير مكتملة أو غير مؤكدة

علم الروبوت : العلم الذي يهتم بتصميم وبناء وبرمجة الروبوتات لتتفاعل مع البيئة المحيطة .

الروبوت : آلة (إلكترو-ميكانيكية) تبرمج بوساطة برامج حاسوبية خاصة ، للقيام بالعديد من الأعمال الخطرة والشاقة والدقيقة خاصة .

الذراع الميكانيكية: تشبه في شكلها ذراع الانسان ، وتحتوي على مفاصل صناعية لتسهيل حركتها عند تنفيذ الاوامر الصادرة إليها ، حسب الغرض الذي صمم الروبوت من أجله

المستجيب النهائي: هو الجزء النهائي من الروبوت الذي ينفذ المهمة التي يصدرها الروبوت ، فقد تكون قطعة المستجيب يدا أو مخاخا أو مطرقة ، وقد تكون أداة لخياطة الجروح

المتحكم: وهو دماغ الروبوت ، يستقبل البيانات من البيئة المحيطة ، ثم يعالجها عن طريق التعليمات البرمجية المخزنة داخله ، ويعطي الأوامر اللازمة للاستجابة لها

المشغل الميكانيكي: وهو الجزء المسؤول عن حركة الروبوت حيث يحول أوامر المتحكم إلى حركة فيزيائية (عضلات الروبوت) .

الحساسات: تعد صلة الوصل بين الروبوت والبيئة المحيطة ، حيث تكون وظيفتها جمع البيانات من البيئة المحيطة ، ومعالجتها ليتم الاستجابة لها من قبل الروبوت بفعل معين

حساس اللمس: يستشعر التماس بين الروبوت وأي جسم مادي خارجي كالجدار مثلا ، أو بين أجزاء الروبوت الداخلية كذراع الروبوت واليد.

حساس المسافة: يستشعر المسافة بين الروبوت والاجسام المادية ، عن طريق إطلاق موجات لتصطدم في الجسم وترتد عنه ، وبناءا عليه يحسب المسافة ذاتيا

حساس الضوء: يستشعر شدة الضوء المنعكس من الاجسام المختلفة ويميز ألوانها .

حساس الصوت: يشبه الميكروفون ، يستشعر شدة الأصوات المحيطة ، ويحولها إلى نبضات كهربائية ترسل إلى دماغ الروبوت

النظام الخبير: هو برنامج حاسوبي ذكي ، يستخدم مجموعة من قواعد المعرفة في مجال معين لحل المشكلات التي تحتاج إلى الخبرة البشرية

المعرفة: هي حصيلة المعلومات والخبرة البشرية التي تجمع في عقول الأفراد من خلال الخبرة وهي نتاج استخدام المعلومات التي تنتج من معالجة البيانات ودمجها مع الخبرات.

قاعدة المعرفة: قاعدة بيانات تحتوي على مجموعة من الحقائق والمبادئ والخبرات بمجال معرفة معين ، وتستخدم من قبل الخبراء لحل المشكلات

محرك الاستدلال : برنامج حاسوبي يقوم بالبحث في قاعدة المعرفة لحل مسألة ، عن طريق آلية استنتاج تحاكي آلية عمل الخبير عند الاستشارة في مسألة ما لإيجاد الحل ، واختيار النصحية المناسبة

ذاكرة العمل: جزء من الذاكرة ،مخصص لتخزين المشكلة المدخلة بوساطة مستخدم النظام ، والمطلوب إيجاد حل لها

واجهة المستخدم: وسيلة تفاعل بين المستخدم والنظام الخبير ، حيث تسمح بإدخال المشكلة والمعلومات إلى النظام الخبير وإظهار النتيجة

خوارزمية البحث:سلسلة من الخطوات غير المعروفة مسبقا ، للعثور على الحل الذي يطابق مجموعة من المعايير من بين مجموعة من الحلول المحتملة

شجرة البحث : هي الطريقة المستخدمة للتعبير عن المشكلة لتسهيل عملية البحث عن الحلول الممكنة من خلال خوارزميات البحث

العقد: النقاط التي تنظم بشكل هرمي (مستويات مختلفة).

فضاء البحث: الحالات الممكنة جميعها لحل المشكلة

جذر الشجرة: نقطة البداية ، وهي الموجودة أعلى الشجرة وتمثل الحالة الابتدائية للمشكلة

الاب:النقطة التي تتفرع منها نقاط اخرى/ **الأبناء :**النقاط المتفرعة من الأب

النقطة الميتة:النقطة التي ليس لديها أبناء

النقطة (الحالة)الهدف: الحالة النهائية للمشكلة ، وهي الهدف المطلوب الوصول إليه

المسار: مجموعة من النقاط المتتالية في شجرة البحث

مسار الحل:اتباع خوارزمية البحث للوصول إلى المسار الصحيح لحل المشكلة من الحالة الابتدائية او جذر المشكلة إلى الحالة الهدف

الخوارزمية الحدسية تعمل على حساب معامل حدسي (بعد النقطة الحالية عن النقطة الهدف) وعليه تقرر المسار الأقصر للحل .

خوارزمية البحث في العرض أولا: خوارزمية البحث في العرض أولا تقوم بفحص النقاط جميعها في مستوى واحد للبحث عن الحل قبل الانتقال إلى النقاط بالمستويات التالية (بشكل أفقي)

علل كل من العبارات الآتية :

س١ : أ. لجأ الإنسان إلى إيجاد نماذج حاسوبية تحاكي قدرة العقل البشري على التفكير).

١.مجاراة تطور العالم الرقمي والحاسوب للاستفادة منه ٢.ايجاد الحلول التي تناسب أعقد المشكلات

ب. شرع الخبراء في دراسة القدرات العقلية للانسان وكيفية تفكيره ومحاولة محاكاتها عن طريق الحاسوب لإنتاج بعض صفات الذكاء من قبل الآلة في ما يعرف بالذكاء الاصطناعي

س٢ : لا تستطيع أن تطلق على برنامج يقوم بحل مسألة تربيعية أنه من ضمن برامج الذكاء الاصطناعي لانه يتبع خوارزمية محددة الخطوات للوصول إلى الحل .

س٣ : من أجزاء الروبوت ذراع ميكانيكية تشبه في شكلها ذراع الانسان ، وتحتوي على مفاصل صناعية .لتسهيل حركتها عند تنفيذ الأوامر الصادرة إليها ، حسب الغرض الذي صمم الروبوت من اجله .

س٤ :أ. استخدام الروبوت الصناعي في عمليات الطلاء بالبخ الحراري في المصانع .

لتقليل تعرض العمال لمادة الدهان التي تؤثر في صحتهم.

ب. استخدام الروبوت الصناعي في أعمال الصب وسكب المعادن .

لأن هذ العمليات تتطلب التعرض لدرجة حرارة عالية جدا ، لا يستطيع الإنسان تحملها .

س٥. لا يستطيع الروبوت القيام بالاعمال التي تتطلب حسا فنيا أو ذوقا في التصميم أو إبداعا

لأن عقل الانسان له القدرة على ابتداع الافكار

س٦ : يعد من غير المناسب استخدام الروبوت في المصانع الصغيرة والمتوسطة . لأن تكلفة تشغيل الروبوت في المصانع عالية .

س٧ : مساحة المصانع التي ستستخدم الروبوتات يجب أن تكون كبيرة جدا . لتجنب الاصطدامات والحوادث في أثناء حركتها .

س٨ : نظام خبير لتشخيص امراض الدم ، لا يستخدم لتشخيص أمراض اخرى .

أو (إن عملية تصميم نظام خبير جديد من البداية لحل مشكلة ما ، اسهل من التعديل على نظام خبير موجود) لأن النظم الخبيرة مرتبطة بمجال معين ، فإذا صممت لحل مشكلة معينة فلا يمكن تطبيقها أو تغييرها لحل مشكلة أخرى .

س٩ :يتم إدخال المعلومات إلى واجهة المستخدمين خلال الاختيار من مجموعة من الخيارات المصاغة على شكل أسئلة وإجابات لتزويد النظام بمعلومات عن موقف محدد.

س١٠ : النظام الخبير غير معرض للنسيان . لأنه يوثق قراراته بشكل دائم

س١١ : النظام الخبير يساعد على تدريب المختصين ذوي الخبرة المنخفضة .

بسبب وسائل التفسير وقواعد المعرفة التي تخدم بوصفها وسائل للتعليم .

س١٢ : توفر النظم الخبيرة مستوى عاليا من الخبرات . عن طريق تجميع خبرة أكثر من شخص في نظام واحد

س١٣ : يمكن للمستخدم إدخال درجة التأكد من إجابته على بعض الأسئلة في واجهة المستخدم للنظام الخبير . لقدرة النظام الخبير على التعامل مع الإجابات الغامضة أو غير الكاملة أو المؤكدة

س١٤ : لا يمكن للنظم الخبيرة أن تحل محل الخبير نهائيا .

(لأن هذه النظم تعمل جيدا فقط ضمن موضوع محدد ،وكلما اتسع نطاق المجال ، ضعفت قدرتها الاستنتاجية)

س١٥ : صمم باستخدام الذكاء الاصطناعي العديد من خوارزميات البحث.

لحل أصعب المشكلات في الكثير من التطبيقات مثل عمليات الملاحة

س١٦ :استخدام خوارزمية البحث في العمق أولاً ، لا يعطي المسار الأقصر للحل دائماً

لأن هذه الخوارزمية تأخذ المسار أقصى اليسار في شجرة البحث وتفحصه بالاتجاه للأمام ، حتى تصل إلى نقطة ميتة ، ثم تعود للخلف لأقرب نقطة في الشجرة يكون فيها تفرع آخر لم يفحص ويختبرذلك المسار حتى نهايته، ثم تكرر العملية للوصول الى الهدف، وبالتالي ليس بالضرورة أن يكون هو المسار الأقصر.

س : ما الفرق بين البيانات الرمزية والبيانات الرقمية ؟البيانات الرمزية تستخدم (الارقام والحروف والرموز) بينما البيانات الرقمية تتمثل (بالنظام الثنائي)

س : متى يوصف أن البرنامج الحاسوبي برنامجا ذكيا أو أن الحاسوب حاسوبا مفكرا ؟

إذا نجح في اختبار تورينغ

ما الفرق بين قاعدة البيانات وقاعدة المعرفة ؟ قاعدة البيانات تتكون من مجموعة من البيانات والمعلومات المترابطة في ما بينها ، بينما قاعدة المعرفة تبنى بالاعتماد على الخبرة البشرية ، بالإضافة إلى المعلومات و البيانات. وتتميز قاعدة المعرفة بالمرونة حيث يمكن الإضافة عليها أو الحذف منها أو التعديل عليها من دون التأثير في المكونات الأخرى للنظام الخبير .

س : ما هي متطلبات بناء برامج الذكاء الاصطناعي ؟ ١– كميات هائلة من المعارف الخاصة بمجال معين . ٢– الربط بين المعارف المتوافرة والنتائج

الوحدة الثالثة: الأساس المنطقي للحاسوب والبوابات المنطقية

ما هي أنواع البوابات المنطقية؟

١. البوابات المنطقية الأساسية وهي **(AND , OR , NOT)**

٢.البوابات المنطقية المشتقة وهي **(NAND , NOR)**

أولويات إيجاد ناتج العبارات المنطقية، وتمثيلها باستخدام البوابات المنطقية، حسب التسلسل:

١. ننفذ العمليات التي بداخل الأقواس. ٢. البوابة المنطقية **NOT** ٣. البوابة المنطقية **And**

٤. البوابة المنطقية **OR** ٥. في حالة التكافؤ في الأولوية، تنفذ من اليسار إلى اليمين

ما هي رموز المتغير المنطقي؟ أحد الحروف **Z ..... A** (لا أهمية لكون الحروف كبيرة أم صغيرة).

اذكر ثلاثاً من العمليات المنطقية الأساسية المستخدمة في الجبر المنطقي، موضحاً رمز كل عملية

	العملية المنطقية	رمزها في الجبر المنطقي
أ.	**NOT**	ـــــ
ب.	**AND**	.
ج.	**OR**	+

١. **التعبير العلائقي:** هي جملة خبرية جوابها إما صواباً (**1**) أو خطأ (**0**)، وتكتب هذه التعابير باستخدام عمليات المقارنة ($\leq , \geq , \neq , = , < , >$)

٢. **المعامل المنطقي**:هو رابط يستخدم للربط بين تعبيرين علائقيين أو أكثر لتكوين عبارة منطقية مركبة ، ومن أهمها **AND** و **OR**، أو نفي تعبير منطقي باستخدام **NOT**.

٣. **العبارة المنطقية المركبة**.هي جمل خبرية تتكون من تعبيرين علائقيين أو أكثر، يربط بينها معاملات منطقية مختلفة، (**AND,OR**) وتكون إما صواباً (**1**) أو خطأ (**0**) .

البوابة المنطقية: دارة إلكترونية بسيطة، تقوم بعملية منطقية على مدخل واحد أو أكثر، وتنتج مخرجاً منطقياً واحداً، وتستخدم في بناء معالجات الأجهزة الإلكترونية والحواسيب.

جدول الحقيقة: تمثيل لعبارة منطقية يبين الاحتمالات المختلفة للمتغيرات المكونة للعبارة المنطقية، ونتيجة هذه الاحتمالات.

الجبر البوولي (المنطقي) :هو أحد فروع علم الجبر في الرياضيات، وهو الأساس الرياضي اللازم لدراسة التصميم المنطقي للأنظمة الرقمية ومنها الحاسوب.

المتغير المنطقي:هو متغير تعين له إحدى الحالتين صواب **(True)** أو خطأ **(False)**.

العبارة الجبرية المنطقية :هي ثابت منطقي **(0,1)** أو متغير منطقي مثل **(X,Y)** أو مزيج من الثوابت والمتغيرات المنطقية، يجمع بينها عمليات منطقية./ **س١: اكتب مثالاً واحداً على كل مما يأتي:**

أ.	بوابات منطقية أساسية	AND **أو** OR **أو** NOT
ب.	بوابات منطقية مشتقة	NOR **أو** NAND
ج.	رمز لعملية جبرية منطقية	+ **أو** . **أو** ـــ
د.	متغير منطقي	A (**أي حرف**)
هـ.	عبارة منطقية	A OR B
و.	عبارة جبرية منطقية	A + B **أو** A . B .... **الخ**
ز.	عبارة جبرية منطقية مركبة	$\overline{A}$ + B . C
ح.	تعبير علائقي	**A<B**
ط.	عبارة منطقية مركبة	**A>B AND C < D أو A AND B OR C**
ي.	معامل منطقي	AND **أو** OR **أو** NOT
ك	عملية مقارنة	< **أو** > **أو** = أو ≠ أو ≤ أو ≥
ل	ثابت منطقي	0 **أو** 1

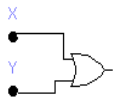
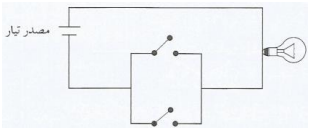
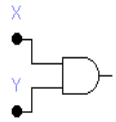
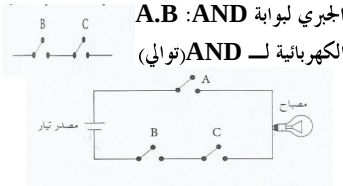
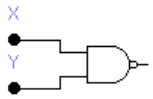
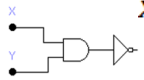
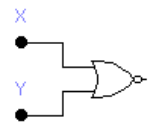
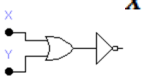
علل: تسمية البوابات المشتقة.لأنها اشتقت من البوابات المنطقية الأساسية**(NOT, AND , OR)**

علل: وجود دائرة صغيرة عند مخرج بوابة NAND. الدائرة الصغيرة على مخرج بوابة **NAND** لكي ترمز إلى بوابة **NOT**

علل: عملية NOT تسمى المتمم : لأن متممة **0** تساوي **1** ومتممة **1** تساوي **0**

كيف نشكل بوابة NAND؟ توصيل مخرج بوابة **AND** بمدخل بوابة **NOT**

كيف نشكل بوابة NOR؟ **توصيل مخرج بوابة** OR **بمدخل بوابة** NOT.

اسم البوابة	الرمز	جدول الحقيقة	مخرجات البوابة	إضافات
OR		<table><tr><th>X</th><th>Y</th><th>A=X OR Y</th></tr><tr><td>1</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>0</td><td>0</td><td>0</td></tr></table>	تعطي البوابة المنطقية **OR** مخرجاً قيمته **(1)** إذا كانت قيمة أي من المدخلين أو كلاهما **(1)**. و تعطي مخرجاً قيمته **(0)** إذا كانت قيمة كلا المدخلين **(0)**	التعبير الجبري لبوابة **OR**: **A+B** الدارة الكهربائية لـــ **OR**(توازي) 
AND		<table><tr><th>X</th><th>Y</th><th>Z = X AND Y</th></tr><tr><td>1</td><td>1</td><td>1</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>0</td><td>0</td><td>0</td></tr></table>	تعطي البوابة المنطقية **AND** مخرجاً قيمته **(1)** إذا كانت قيمة المداخل جميعها **(1)** فقط. و تعطي مخرجاً قيمته **(0)** إذا كانت قيمة أي من المدخلين أو كلاهما **(0)**	التعبير الجبري لبوابة **AND**: **A.B** الدارة الكهربائية لـــ **AND**(توالي) 
NOT		جدول (جدول الحقيقة) للبوابة المنطقية NOT <table><tr><th>X</th><th>A=NOT X</th></tr><tr><td>1</td><td>0</td></tr><tr><td>0</td><td>1</td></tr></table>	المخرجات عكس المدخلات تعطس مخرجاً قيمته **1** إذا كان المدخل **0** وتعطي مخرجاً قيمته **0** إذا كان المدخل **1**	التعبير الجبري لبوابة **NOT**: $\overline{X}$
NAND		<table><tr><th>X</th><th>Y</th><th>Z = X NAND Y</th></tr><tr><td>1</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>1</td></tr><tr><td>0</td><td>1</td><td>1</td></tr><tr><td>0</td><td>0</td><td>1</td></tr></table>	تعطي مخرجاً قيمته **(1)** إذا كانت قيمة أي من المدخلين أو كلاهما **(0)**. تعطي مخرجاً قيمته **(0)** إذا كانت قيمة المداخل جميعها **(1)**.	يكافئها العبارة المنطقية: **NOT(X AND Y)** يكافئها بالتعبير الجبري $\overline{X.Y}$ يكافئها بالبوابات الأساسية 
NOR		<table><tr><th>X</th><th>Y</th><th>Z = X NOR Y</th></tr><tr><td>1</td><td>1</td><td>0</td></tr><tr><td>1</td><td>0</td><td>0</td></tr><tr><td>0</td><td>1</td><td>0</td></tr><tr><td>0</td><td>0</td><td>1</td></tr></table>	تعطي مخرجاً قيمته **(1)** إذا كانت قيمة كلا المدخلين **(0)**. تعطي مخرجاً قيمته **(0)** إذا كانت قيمة أي من المدخلين أو كلاهما**(1)**.	يكافئها العبارة المنطقية: **NOT(X OR Y)** يكافئها بالتعبير الجبري $\overline{X+Y}$ يكافئها بالبوابات الأساسية 

الوحدة الرابعة أمن المعلومات والتشفير

عناصر (خصائص) أمن المعلومات.

١. السرية

وأمثلتها:

أ. المعلومات الشخصية

ب.الموقف المالي لشركة ما قبل إعلانه

ج. المعلومات العسكرية

٢.السلامة

وأمثلتها:

أ. عند نشر نتائج الثانوية العامة

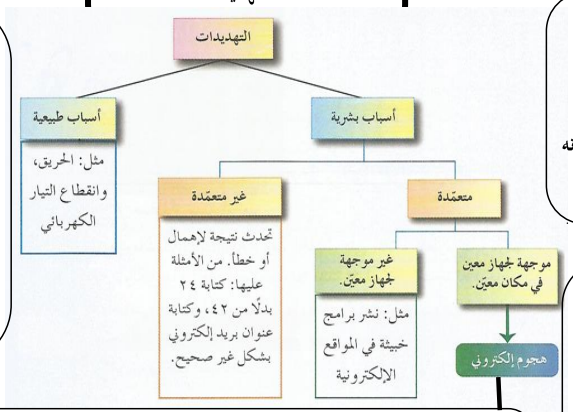
ب.عند صدور قوائم القبول الموحد للجامعات

٣. توافر المعلومات

أنواع المخاطر التي تهدد أمن المعلومات:

١- الثغرات

٢- التهديدات



أمثلة على الهجوم(الاعتداء) الالكتروني

١.سرقة جهاز الحاسوب أو أحد معدات حفظ المعلومات ٢.التعديل على ملف أو حذفه

٣. الكشف عن بيانات سرية ٤.منع الوصول إلى المعلومات

عوامل نجاح الهجوم الالكتروني :

عوامل رئيسة يجب أخذها بالحسبان لتقييم التهديد

١. الدافع	٢. الطريقة	٣. فرصة النجاح
تتنوع دوافع الأفراد: ١. الرغبة في إثبات القدرات التقنية ٢. الإضرار بالآخرين ٣. الرغبة في الحصول على المال	**وتتضمن:** ١. معرفة نقاط القوة والضعف للنظام ٢. القدرة على توفير المعدات و البرمجيات الحاسوبية ٣. المعرفة بتصميم النظام وآلية عمله ٤. المهارات التي يتميزها المعتدي الإلكتروني	**وتتمثل في:** ١. تحديد الوقت المناسب لتنفيذ الهجوم الإلكتروني ٢. المعرفة بكيفية الوصول للأجهزة

أمن المعلومات والتشفير

أنواع الاعتداءات الإلكترونية على المعلومات

نوع الاعتداء الالكتروني	الهدف من الاعتداء
١. التنصت على المعلومات	الحصول على المعلومات السرية(**تؤثر على السرية**)
٢. التعديل على المحتوى	اعتراض المعلومات وتغيير محتواها وإعادة إرسالها للمستقبل (**تؤثر على السلامة**)
٣. الايقاف	قطع قناة الاتصال ، لمنع المعلومات من الوصول للمستقبل (**تؤثر على توافر المعلومات**)
٤.الهجوم المفبرك او المزور	ارسال المعتدي الالكتروني رسالة إلى أحد الأشخاص على الشبكة يخبره فيها بأنه صديقه ويحتاج إلى معلومات أو كلمات سرية خاصة(**تؤثر على السرية والسلامة**)

وُضِعت مجموعة من الضوابط لتقليل المخاطر

	١. الضوابط المادية	٢. الضوابط الادارية	٣. الضوابط التقنية
أمثلة عليها	١. استخدام الجدران والاسوار و الاقفال ٢.وجود حراس الأمن/ ٣. أجهزة إطفاء الحريق	١. القوانين واللوائح و السياسات ٢. الاجراءات التوجيهية ٣. حقوق النشر ٤. براءات الاختراع و العقود و الاتفاقيات	١. كلمات المرور ٢. منح صلاحيات الوصول/ ٣. التشفير ٤. بروتوكولات الشبكات والجدر النارية / ٥. تنظيم تدفق المعلومات في الشبكة

الهندسة الاجتماعية

تتركز الهندسة الاجتماعية في مجالين هما :

١- البيئة المحيطة

تشمل البيئة المحيطة : أ. مكان العمل ب. الهاتف ج. النفايات الورقية د. الإنترنت

٢- الجانب النفسي

الوسائل والأساليب التي يستخدمها المعتدي الالكتروني للتأثير في الجانب النفسي على مستخدم الحاسوب وكسب ثقته :

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

راجع دوسية الأولى في الحاسوب صفحة ٧٠

أمن الإنترنت

الاعتداءات الإلكترونية على المواقع الإلكترونية (الويب)

١- الاعتداء على متصفح الانترنت

توضيح الاعتداء على متصفح الانترنت

يتم هذا الاعتداء بطريقتين :

١. عن طريق كود بسيط يمكن إضافته إلى المتصفح وباستطاعته القراءة والنسخ وإعادة الارسال لأي شيء يتم إدخاله من قبل المستخدم .

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

٢- الاعتداء على البريد الإلكتروني

توضيح الاعتداء على البريد الاكتروني :

يحاول المعتدي الالكتروني التعامل مع الاشخاص قليلي الخبرة ، حيث يقدم عروضا وهمية ومضللة ، وتحتوي روابط يتم الضغط عليه للحصول على معلومات إضافية

تقنية تحويل العناوين الرقمية (NAT)

مفهوم تقنية تحويل العناوين الرقمية NAT

١.تمنح (أيانا) الشبكة الداخلية عنوانا واحدا (أو مجموعة عناوين) مختلفاً عن عناوين الشبكات الأخرى ويكون معرفاً لها عند التعامل في شبكة الانترنت . (لن يتكرر العنوان الرقمي للشبكة الداخلية).

٢ . تعطي الشبكة الداخلية كل جهاز داخل الشبكة عنوانا رقميا لغرض الاستخدام الداخلي فقط :

أ. لا يعترف بهذا العنوان خارج الشبكة

ب.يمكن أن يتكرر العنوان الرقمي للجهاز في أكثر من شبكة داخلية

٣.عند رغبة أحد الاجهزة بالتواصل مع جهاز خارج الشبكة الداخلية ، يعدل العنوان الرقمي الخاص به ، باستخدام تقنية تحويل العناوين الرقمية **NAT** . وذلك يتم باستخدام جهاز وسيط (موجهاً أو جداراً نارياً)

آلية(طرق) عمل تقنية تحويل العناوين الرقمية.

١. النمط الثابت للتحويل .

توضيح:

– تخصيص عنوان رقمي خارجي لكل جهاز داخلي

– العنوان الرقمي ثابت لا يتغير.

٢. النمط المتغير للتحويل

توضيح:

يتم إعطاء الجهاز عنوان رقمي مؤقت للتواصل خارج الشبكة وحين انتهاء الاتصال يفقد الجهاز الداخلي هذا العنوان و يصبح هذا العنوان متاحاً لأي جهاز آخر وقد يعطى عنوانا مختلفاً عند التراسل مرة أخرى

وظيفة الجهاز الوسيط (موجهاً أو جداراً نارياً):

تحويل العنوان الرقمي الداخلي إلى عنوان رقمي خارجي(عند التواصل خارج الشبكة)

تحويل العنوان الرقمي الخارجي إلى عنوان داخلي (عند الرد على رسالة الجهاز المرسل)

أيانا: السلطة المسؤولة عن منح أرقام الانترنت المخصصة لإعطاء العناوين الرقمية

التشفير

الهدف من علم التشفير:

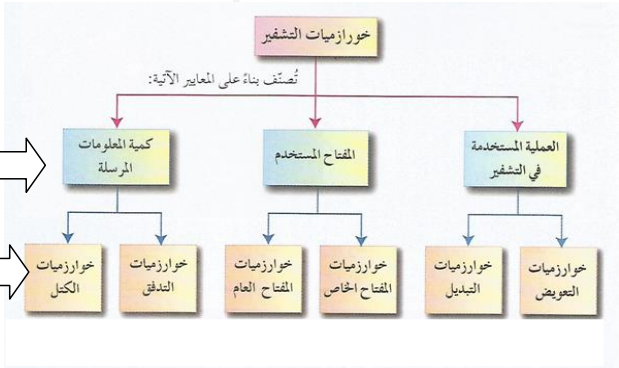
– سرية المعلومات في أثناء تبادلها بين مرسل المعلومة ومستقبلها .

– عدم الاستفادة منها أو فهم محتواها حتى لو تم الحصول عليها من قبل أشخاص معترضين

عناصر عملية التشفير:

أ–خوارزمية التشفير ب–مفتاح التشفير

ج– النص الأصلي د–نص الشيفرة



معايير تصنيف خوارزميات التشفير

أنواع خوارزميات التشفير وفقاً لكل معيار

مميزات خوارزمية الخط المتعرج :

١. سهلة وسريعة٢. يمكن فك تشفيرها بسهولة

٣. يمكن تنفيذها يدويا باستخدام ورقة وقلم

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

السرية(الأمن والخصوصية):الشخص المخول هو الوحيد القادر على الوصول إلى المعلومات والاطلاع عليها.

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

توافر المعلومات: العمل على إبقاء المعلومات متاحة للأفراد المصرح لهم التعامل معها واستخدامها ، وان الوصول إليها لا يحتاج إلى وقت كبير

الهجوم (الاعتداء)الإلكتروني: تهديد موجه ومتعمد لجهاز معين؛ بقصد الإضرار به.

الثغرات:هي نقطة الضعف في النظام سواء أكانت في الإجراءات المتبعة،مثل عدم تحديد صلاحيات الوصول إلى المعلومات ، أو مشكلة في تصميم النظام أو عدم كفاية الحماية المادية للأجهزة والمعلومات وهذا قد يتسبب في فقدان المعلومات او هدم النظام أو جعله عرضة للاعتداء الالكتروني

الضوابط المادية: مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها باستخدام الجدران والأسوار والأقفال، ووجود حراس الأمن وأجهزة إطفاء الحريق.

الضوابط الادارية:مجموعة من الأوامر والاجراءات المتفق عليها مثل: القوانين/العقود/حقوق النشر

الضوابط التقنية:وهي الحماية التي تعتمد على التقنيات المستخدمة سواء كانت معدات ام برمجيات وتتضمن كلمات المرور والتشفير والجدر النارية ومنح صلاحيات الوصول والبروتوكولات

الهندسة الاجتماعيةهي الوسائل و الأساليب التي يستخدمها المعتدي الالكتروني ،لجعل مستخدم الحاسوب في النظام يعطي معلومات سرية أو يقوم بعمل ما يسهل عليه الوصول إلى أجهزة الحاسوب أو المعلومات المخزنة فيها

متصفح الانترنت :برنامج ينقل المستخدم إلى صفحة الويب التي يريدها بمجرد كتابة العنوان ، ويمكنه من مشاهدة المعلومات على الموقع

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

العناوين الرقمية الالكترونية IP Address :عنوان رقمي خاص لجهاز الحاسوب أو الهاتف الخلوي ،يتكون من ٣٢ خانة ثنائية تتوزع على أربعة مقاطع يفصل بينها نقاط ، وهذا يسمى (**IP4**) وكل مقطع من هذه المقاطع يتضمن رقما من **255 – 0**

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

الخوارزمية: مجموعة من الخطوات المتسلسلة منطقياً ورياضياً لحل مشكلة ما.

خوارزمية التشفير: مجموعة الخطوات المستخدمة لتحويل الرسالة الأصلية إلى رسالة مشفرة

مفتاح التشفير: سلسلة الرموز المستخدمة في خوارزمية التشفير ، وتعتمد قوة التشفير على قوة هذا المفتاح

النص الأصلي: محتوى الرسالة الاصلية قبل التشفير ، وبعد عملية فك التشفير

نص الشيفرة: الرسالة بعد عملية التشفير.

التشفير بالتعويض:طريقة تشفير تقوم باستبدال حرف مكان حرف أو مقطع مكان مقطع،كشيفرة الإزاحة

التشفير بالتبديل : طريقة تشفير تقوم على تبديل أماكن الأحرف ، وذلك بإعادة ترتيب أحرف الكلمة ، بشرط استخدام الأحرف نفسها من دون إجراء أي تغيير عليها ، ومثال عليها خوارزمية الخط المتعرج

.....

علل : استخدام بعض الضوابط في نظام المعلومات. لتقليل المخاطر التي تتعرض لها المعلومات والحد منها

تعد الهندسة الاجتماعية من أنجح الوسائل و أسهلها للحصول على المعلومات . بسبب قلة اهتمام المتخصصين في مجال أمن المعلومات وعدم وعي مستخدمي الحاسوب بالمخاطر المترتبة عليها

ما أسباب إيجاد وسائل تقنية لحماية الانترنت . ١. للحد من الاعتداءات والأخطار التي تهدده بسبب انتشار البرامج المقرصنة والمعلومات الخاصة بكيفية اقتحام المواقع الالكترونية

علل : انتشرت البرامج والتطبيقات بشكل كبير منها (المجاني/المفتوح/غير معروف المصدر)

بسبب اعتماد الأفراد على تكتولوجيا المعلومات والاتصالات

علل. يتعرض متصفح الانترنت إلى الكثير من الأخطار . لأنها قابلة للتغيير من دون ملاحظة ذلك من قبل المستخدم

علل : ظهرت الحاجة إلى عناوين إلكترونية أكثر ، وطورت هذه العناوين لما يسمى IPv6 .

بسبب التطور الهائل في أعداد مستخدمي الانترنت

علل : اختلاف IP Address **للجهاز عند تراسله أكثر من مرة .**

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

علل : يعد التشفير من أفضل الوسائل المستخدمة للحفاظ على أمن المعلومات

لأنه يعمل على إخفائها عن الأشخاص غير المصرح لهم بالاطلاع عليها

علل :تعتبر شيفرات الكتل أبطأ من شيفرات التدفق في عملية التشفير .

لأن الرسالة تقسم إلى أجزاء ولكن بحجم معلومات أكبر ، لذا فإنها أبطأ

س : قارن بين كل من خوارزميات المفتاح الخاص وخوارزميات المفتاح العام .

خوارزميات المفتاح الخاص (التناظرية)	**خوارزميات المفتاح العام** (اللاتناظرية)
*. المفتاح يستخدم لعمليتي التشفير وفك التشفير(التناظرية) *. يتم الاتفاق على المفتاح قبل بدء عملية التراسل بين المرسل والمستقبل (خوارزميات المفتاح السري)	*. تستخدم مفتاحين ، احدهما لتشفير الرسالة وهو معروف للمرسل والمستقبل (المفتاح العام) *. المفتاح الآخر يكون معروف للمستقبل فقط ، ويستخدم لفك التشفير (المفتاح الخاص)

س : قارن بين كل من شيفرات التدفق وشيفرات الكتل ؟

شيفرات التدفق	تقسيم الرسالة إلى مجموعة أجزاء ، يشفر كل جزء منها على حدة ومن ثم يرسله
شيفرات الكتل	تقسم الرسالة إلى اجزاء ، ولكن بحجم معلومات اكبر ، ويشفر او يفك تشفير كل كتلة على حدة .

س : ما الفرق بين العناوين الرقمية IP4 **و** IPv6 **؟**

IP4 تتوزع على أربعة مقاطع بينما **IPv6** تتوزع على ثمانية مقاطع

س : على ماذا يعتمد أمن الرسالة او المعلومة في خوارزميات التشفير المعتمد على المفتاح ؟

على عدد المفاتيح المستخدمة وعلى سرية المفتاح وليس على تفاصيل الخوارزمية

س : كيف يتم انتاج المفتاحين في الخوارزميات اللاتناظرية ؟

يتم انتاج المفتاحين من خلال عمليات رياضية ، ولا يمكن معرفة المفتاح الخاص من خلال المفتاح العام

ملاحظة : للحصول على تفاصيل المادة راجع الكتاب المدرسي أو دوسة الأولى في الحاسوب

إن تيسر وقت إن شاء الله نوافيكم بالمادة العملية.

بالتوفيق