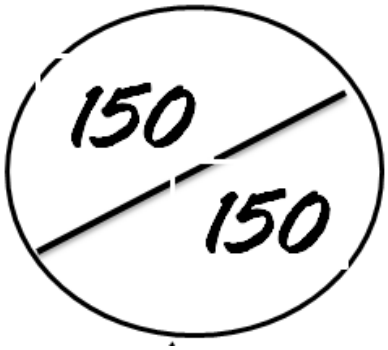
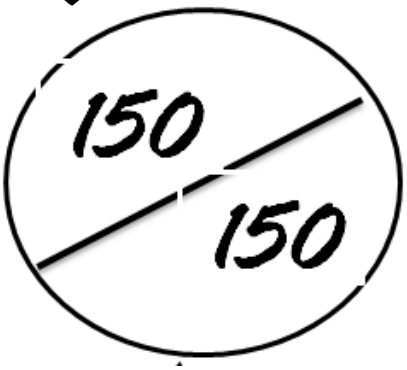
خبر عاجل



علوم الحاسوب



المراجعة المكثفة

أحمد الرّاميني

مدارس القمة

لا تنس الحصول على ملخص الرضيات الأدبي

مبدأ العد

ما هو دور العرب المسلمين في أنظمة العد

برعوا في هذا المجال حيث أخذوا عن الهنود فكرة الأعداد وحددوا لها أشكالا وأضافوا لها الصفر حتى أصبحت الارقام
(0 , 1 , 2 , 3 , 4 , 5 , 6 , 7 , 8 , 9)
وهي تسمى الأرقام العربية ولا تزال تستخدم في معظم أرجاء العالم

السؤال الثاني : علل كلا من العبارات التالية

1) يمكن التحويل من النظامين الثماني والسادس عشر دون المرور بالنظام العشري ؟

بسبب وجود ارتباط وثيق بين هذه الأنظمة ، فأساس النظام الثماني 3^2) (8 = ويساوي (8) وأساس النظام السادس عشر هو (16=4^2) ويساوي (16) أي أنهما من مضاعفات النظام الثنائي .

2) تنفيذ العمليات الحسابية في النظام الثنائي أسهل من تنفيذها في النظام العشري ؟

لأن النظام الثنائي يتكون من رقمين فقط هما (1,0) واساسه 2

3) يعد النظام الثنائي أكثر أنظمة العد ملائمة للاستعمال داخل الحاسوب

لأن بناء الحاسوب يعتمد على ملايين من الدوائر الكهربائية التي تكون إما مفتوحة واما مغلقة لذا دعت الحاجة الى استخدام نظام يمكنه التعبير عن هذه الحالة فالنظام الثنائي الذي يتكون من رمزين فقط هما (0 , 1) هو القادر على تمثيل هذه الحالة فالرمز (0) يمثل دائرة كهربائية مفتوحة والرمز (1) يمثل دائرة كهربائية مغلقة .

4) يعتبر النظام السادس عشر أحد أنظمة العد الموضعية

يسمى نظام العد موضعيا إذا كانت القيمة الحقيقة للرقم تعتمد على الخانة او المنزلة التي يقع فيها ذلك الرقم داخل العدد ما يعني أن قيمة الرقم تختلف باختلاف موقعه داخل العدد

عند إجراء عملية الضرب في النظام الثنائي كيف يمكن التحقق من صحة الحل ؟ بتحويل كل من العدد الاول والثاني والنتيجة الى النظام العشري .

بين الجمل المقبولة من غير المقبولة مع تصحيح الأخطاء في الجمل غير المقبولة ؟

1. أكثر أنظمة العد استخداما هو النظام العشري وأساس هذا النظام هو 10 نسبة الى العدد10 (×) .
2. يمكن تنفيذ عملية الضرب في النظام الثنائي على جميع الأعداد الحقيقية (×) .
3. عملية الاستلاف في النظام الثماني مشابهة تماما لعملية الاستلاف في النظام العشري (×) .
4. يمكن إجراء عمليات الجمع والطرح والضرب والقسمة في النظام الثنائي (×) .
5. عند التحويل من النظام الثنائي الى النظام الثماني نقسم العدد الثنائي الى مجموعات بحيث تتكون
6. كل مجموعة من أربعة أرقام بدءا من يسار العدد (×) .
7. يعتبر الرقم الثنائي 1001 المكافئ للعدد 9 في النظام السادس عشر (×) .
8. يمكن استخدام النظامين الثماني والسادس عشر للتسهيل على المستخدمين برمجة الحاسوب (✓) .
9. في حال وجود أي رمز تحت العدد فإن ذلك يدل على أن العدد ممثل بالنظام العشري (×) .
10. عند التحويل من النظام العشري الى أنظمة العد نقرأ بواقي القسمة من اليمين الى اليسار لايجاد الحل (✓) .
11. عند إجراء عملية الطرح في النظام الثنائي يجب أن يكون العدد المطروح أكبر من العدد المطروح منه (×) .
12. يعتبر النظام الثنائي أحد أنظمة العد الموضعية (✓) .
13. يعود سبب الاختلاف في أسماء الأنظمة العددية الى اختلاف عدد الرموز في كل نظام (✓) .
14. يمكن كتابة الرقم $(1001)_8$ بالنظام الثماني (×) .
15. الرمز 1 يمثل حالة الدائرة الكهربائية المفتوحة (×) .
16. الرمز E في النظام السادس عشر يكافئ العدد14 في النظام العشري والعدد1110 في الثنائي(✓) 16- يستخدم النظام السادس عشر لتخزين البيانات وعنونة مواقع الذاكرة في الحاسوب (×) .
17. ناتج جمع 1+1+1 يساوي 1 ويحمل الرقم 0 للمنزلة التالية (×) .
18. العدد المطروح يجب أن يكون أقل من العدد المطروح منه في النظام الثنائي (✓) .
19. ناتج ضرب العدد 10(4) × 10(5) يساوي 10(20) (✓) .
20. العدد 8(8) أكبر من العدد 2(111) (×) .

حدد الى أي نظام عد تنتمي الأعداد التالية علما بأن العدد الواحد يمكن أن ينتمي الى أكثر من نظام عد

357	01	E10	890
ثماني عشري سادس عشر	ثنائي ثماني عشري سادس عشر	سادس عشر	عشري سادس عشر

جد قيمة كل من الأعداد التالية حسب النظام المقابل لها :

إذا كانت Z=111011 ، Y = 11011 ، B = 101 A=11

جد ناتج ما يلي

-1 Z-Y ← 100000
-2 B + Z ← 1000000
-3 1111 - (A×B) ← 0000

جد ناتج كلا من التعابير العلائقية التالية

-1 $(1010)_2 <= (1010)_2$ ← صواب
-2 $(1111100)_2 >= (224)_{10}$ ← خطأ
-3 $(AC)_{16} < = (48)_{10}$ ← صواب

العدد	المكافئ له
(604)8	(110000100)2
(11101111010110)2	(3BD6)16
(730)8	(1D8)16
(B19) 16	(5431)8
(89301)10	( )2
(B5D)16	(2909)10
(1010111)2	(87)10
(777)8	(511)10
(1928)10	(788)16
(666)10	(1232)8

وضح المقصود بالمفاهيم والمصطلحات التالية

1- **النظام العددي** : مجموعة من الرموز وقد تكون هذه الرموز أرقاما او حروفا مرتبطة مع بعضها البعضبمجموعة من العلاقات وفق أسس وقواعد معينة ؛ لتشكل الأعداد ذات المعاني الواضحة والاستخدامات لمتعددة

2- **وزن الخانة (المنزلة)** : (أساس نظام العد) ترتيب الخانة

3- **نظام العد الموضعي** : يسمى نظام العد موضعيا إذا كانت القيمة الحقيقة للرقم تعتمد على الخانة المنزلة التي يقع فيها ذلك الرقم داخل العدد ما يعني أن قيمة الرقم تختلف باختلاف موقعه داخل العدد

4- **البت** : الخانة (المنزلة) التي يحتلها الرمز داخل العدد الثنائي .

5- **النظام الثنائي** : هو نظام عد مستخدم في الحاسوب اساسه 2 ويتكون من رمزين فقط هما 0 , 1

جد ناتج كل من العمليات الحسابية التالية في النظام الثنائي

$(10010011)2 + (110101)2$

11001000

$(11110011)_2 + (111111)_2$

100110010

$(11101)_2 + (011011)_2 + (10001)_2$

1001001

$(1101)_2+(0101011)_2-(10110101)_2$

01111101

$(1000)_2 - (0111)_2$

0001

$(1101100)_2 - (01101)_2$

1011111

$(2)_{10} \times (3)_{10} \times (7)_{10}$

01010

$(5E)_{16} - (49)_{10}$

0101101

$(101)_2 \times (111)_2$

100011

$(101)_2 \times (100)_2$

10100

$(6)_{10} \times (7)_8$

101010

$(8DB)_{16}+(11100111)_2$

100111000010

الذكاء الاصطناعي وتطبيقاته

الذكاء الاصطناعي : علم من علوم الحاسوب، يختص بتصميم وتمثيل وبرمجة نماذج حاسوبية في مجالات الحياة المختلفه ، وتحاكي في عملها طريقة تفكير الانسان وردود أفعالة في مواقف معينة

عرف بعض الباحثين أربع منهجيات يقوم عليها موضوع الذكاء الاصطناعي :

1. التفكير كالانسان
2. التصرف كالانسان
3. التفكير منطقيا
4. التصرف منطقيا

أهداف الذكاء الاصطناعي

1. انشاء انظمة خبيرة تظهر ذكيا قادرة على التعليم والادارة
2. تطبيق الذكاء الانساني في الالة (التفكير والتصرف)
3. برمجة الالات لتصبح قادرة على معالجة المعلومات

لغات الذكاء الاصطناعي

1. لغة برمجة لسب Lisp لغة معالجة اللوائح
2. لغة البرمجة برولوغ Prolog لغة البرمجة بالمنطق

ميزات برامج الذكاء الاصطناعي

1. تمثيل المعرفة
2. التمثيل الرمزي
3. القدرة على التعلم
5. التعامل مع البيانات غير المكتملة أو غير المؤكدة

تطبيقات الذكاء الاصطناعي

1. الربوت الذكي
2. الشبكات العصبية
3. الانظمة الخبيرة
4. أنظمة تميز خط اليد
5. الأنظمة البصرية

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

الروبوت فيعرف على انه الة (الكتروميكانيكية) تبرمج بوساطة برامج حاسوبية خاصة **علك** للقيام بالعديد من الاعمال ، الخطيرة والشاقة والدقيقة خاصة

كي يطلق على أي آلة مسمى الروبوت ، يجب أن تجمع ثلاث صفات :

1. الاستشعار	ويمثل المدخلات كاستشعار الحرارة
2. التخطيط والمعالجة	كأن يخطط الروبوت للتوجة الى هدف أو يغير اتجاه حركتة أو يدور
3. الاستجابة وردة الفعل	وتمثل ردة الفعل على ما تم أخذه كمدخلات

يتكون الروبوت من الاجزاء الآتية :

1. ذراع ميكانيكية	تشبه ذراع الانسان، وتحتوي على مفاصل صناعة لتسهيل حركتها عند
2. المستجيب النهائي	الجزء النهائي من الروبوت الذي ينفذ المهمة التي يصدرها الروبوت
3. المتحكم	وهو دماغ الروبوت، يستقبل البيانات ثم يعالجها ويعطي الاوامر اللازمة
4. المشغل الميكانيكي	(عضلات) الروبوت
5. الحساسات	تشبه وظيفة الحساسات في الروبوت وظيفة الحواس الخمسة في الانسان (صلة الوصل بين الروبوت والبيئة المحيطة،)

انواع الحساسات ووظيفة كل منها

اسم الحساس	الوظيفة
1. **اللمس**	يستشعر التماس بين الروبوت وأي جسم مادي خارجي
2. **المسافة**	يستشعر المسافة باطلاق موجات لتصدم في الجسم
3. **الضوء**	يستشعر شدة الضوء المنعكس من الأجسام المختلفة ويميز بين ألوانها
4. **الصوت**	يشبه الميكروفون ويستشعر شدة الأصوات المحيطة ويحولها الى نبضات كهربائية ترسل الى دماغ الروبوت

من انواع الروبوتات حسب الاستخدام والخدمات التي يقدمها :

1. الروبوت الصناعي	عمليات الطلاء بالبخ الحراري في المصانع،
2. الروبوت الطبي	يستخدم في إجراء العمليات الجراحية المعقدة
3. الروبوت التعليمي	صممت روبوتات لتحفيز الطلبة وجذب انتباهم الى التعليم وقد تكون على هيئة إنسان معلم .
4. في الفضـــــاء	المركبات الفضائية، وفي دراسة سطح المريخ
5. في المجال الأمني	مكافحة الحرائق وإبطال مفعول الالغام

تقسم الروبوتات حسب مجال حركتها، وإمكانية تجوالها ضمن مساحة معينة إلى: 1 . الروبوت الثابت 2. الروبوت الجوال أو المنتقل

فوائد الروبوت في مجال الصناعة

1. يقوم بالاعمال التي تتطلب تكراراً مدة طويلة (زيادة الانتاجية)
2. يستطيع القيام بالاعمال التي تتطلب تجميع القطع وتركيبها في مكانها بدقة عالية، (اتقان العمل)
3. يقلل من المشكلات التي تتعرض لها المصانع مع العمال،
4. يمكن التعديل عليه لزيادة المرونة في التصنيع،
5. يستطيع العمل تحت الضغط،

محددات الروبوت في مجال الصناعة

1. الاستغناء عن الموظفين في المصانع
2. لا يستطيع القيام بالاعمال التي تتطلب حسا فنيا أو ذوقا
3. تكلفة تشغيل الروبوت في المصانع العالية
4. يحتاج الموظفين الى البرامج التدريبية للتعامل مع الروبوتات

النظام الخبير هوبرنامج حاسوبي ذكي، يستخدم مجموعة من قواعد المعرفة في مجال معين لحل المشكلات التي تحتاج الى الخبرة البشرية.

المعرفة : هي حصيلة المعلومات والخبرة البشرية ، التي تجمع في عقول الأفراد عن طريق الخبرة ، وهي نتاج استخدامات المعلومات التي تنتج من معالجة البيانات ودمجها مع الخبرات.

أمثلة عملية على برامج النظم الخبيرة ومجال استخدامها

النظام الخبير	المجال
1. **ديندرال**	المركبات الكيميائية
2. **باف**	تشخيص أمراض الجهاز التنفسي
3. **بروسبكتر**	تحديد مواقع الحفر للتنقيب عن المعادن
4. **ديزاين أدمايزر**	نصائح لتصميم رقائق المعالج
5. **ليثيان**	نصائح لعلماء الاثار لفحص الأدوات الحجرية

أنواع المشكلات (المسائل) التي تحتاج الى النظام الخبيرة للنظم الخبيرة مجالات معينة أمثلة :

1. التشخيص: تشخيص أعطال المعدات
2. التصميـــم: اعطاء نصائح تصميم مكونات أنظمة الحاسوب
3. التخطـــيط: التخطيط لمسار الرحلات الجوية .
4. التفســـير: تفسير البيانات الصور الاشعاعية .
5. التنبـــــؤ: التنبؤ بالطقس او اسعار الاسهم.

مكونات الانظمة الخبيرة

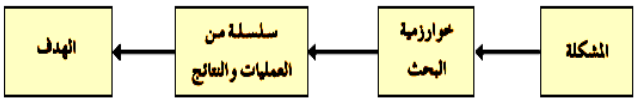
1. قاعدة المعرفة 2. ذاكرة العمل 3. محرك الاستدلال 4. واجهة المستخدم

مزايا النظم الخبيرة (فوائد)	محددات النظم الخبيرة
1) غير معرض للنسيان، لانه يوثق قرارتة بشكل دائم .	1) عدم القدرة على الادراك والحدس
2) المساعده على تدريب المختصين ذوي الخبرة المنخفضة	2) عدم القدرة على التجاوب مع الموقف غيرالاعتيادية
3) توفر مستوى عاليا من الخبرات	3) صعوبة جمع الخبرة والمعرفة اللازمة لبناء
4) نشر الخبرة النادرة الى اماكن بعيدة	قاعدة المعرفة من
5) القدرة على العمل. بمعلومات غير كاملة او مؤكده	الخبراء

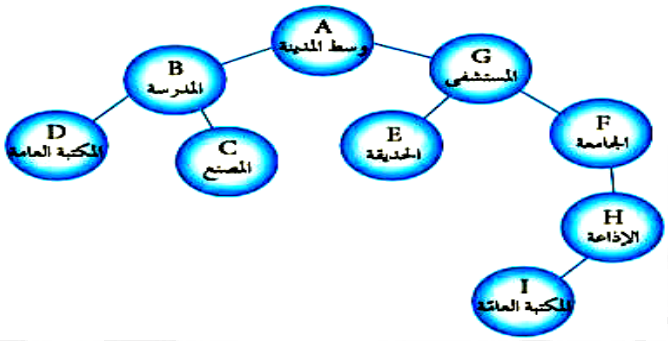
مفهوم خوارزميات البحث

خوارزميات البحث سلسلة من الخطوات غير معرفة مسبقا للعثور على الحل الذي يطابق مجموعة من المعايير من بين المجموعة من الحلول المحتملة .

مبدأ عمل خوارزميات البحث (انتبه لاتجاه الأسهم)



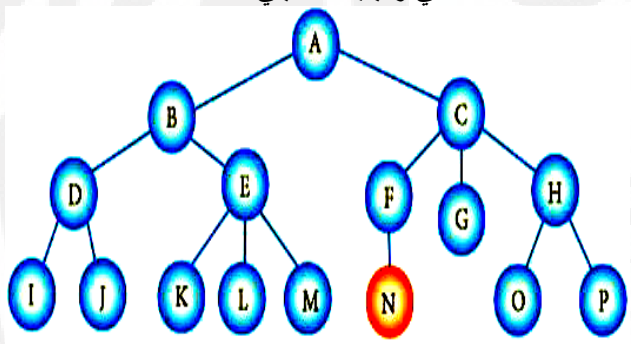
مثال توضيحي لشجرة البحث وأهم المفاهيم المرتبطة فيها(هيكلية الشجرة)



- النقطة A في المستوى الأول والنقطتان B, G في المستوى الثاني
- النقاط A,B,C,D,G,E,F,H,I تمثل حالات فضاء البحث .
- النقطة A تمثل جذر الشجرة (الحالة الابتدائية للمشكلة)
- النقطة G هي الأب للنقاط F , E والنقط D تمثل الابن للنقطة B

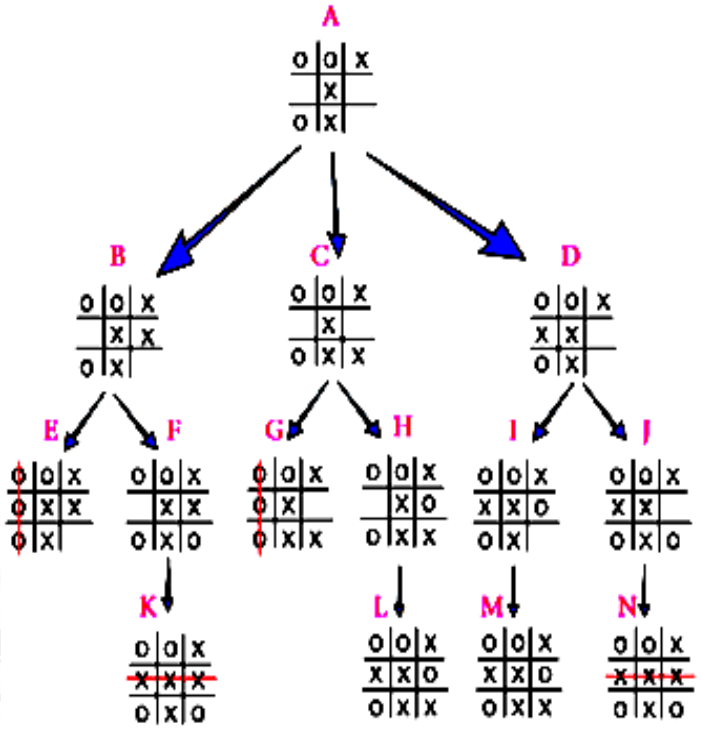
- النقطة C نقطة ميتة (ليس لديها أبناء)
- النقطة D أو النقطة I هي النقطة (الحالة) الهدف
- النقاط المتتالية مثل G-F-H تعتبر مسار
- النقاط A-B-D هي مسار الحل (وهو ليس المسار الوحيد لكنه الأفضل لأنه الأقصر مسافة)

تأمل الشكل التالي واجب عما يلي



1. عدد حالات فضاء البحث التي تمثلها هذه الشجرة:
2. ما الحالة الابتدائية للمشكلة (A)
3. ما جذر الشجرة (A)
4. أذكر أمثلة تحتوي على علاقة (الأب – الأبناء
   النقطة (A) هي الأب للنقطة(B) النقطة (A) هي الأب ل (C)
5. عدد أمثلة على مسار ضمن الشجرة: A-B-E-K
6. أذكر مثالا على نقطة ميتة G

تأمل الشكل التالي والذي يمثل جزء من شجرة بحث للعبة (X O) بين لاعبين ويقوم اللاعبان باللعب بالتناوب حيث يقوم اللاعب الأول (الحاسوب) بوضع الحرف (X) ، واللاعب الثاني(المستخدم) بوضع الحرف (O) ثم أجب عن ما يليه ؟



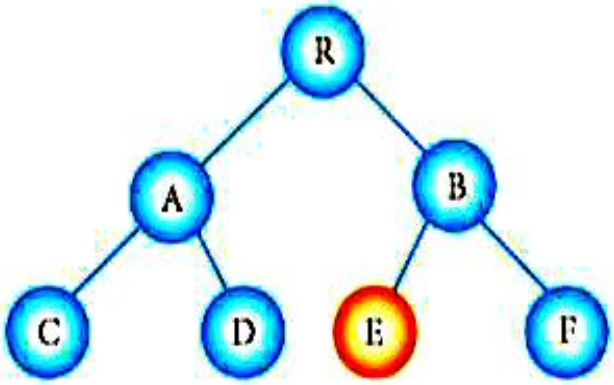
1. مالنقطة التي تمثل جذر الشجرة
2. كم عدد حالات فضاء البحث ؟(A,B,C,D,E,F,G,H,I,J,K,L,M,N)
3. أذكر أمثلة على مسار A-B-F-K
4. ما عدد النقاط الميتة : 6 نقاط
5. ما الحالة الهدف في هذه الشجرة ؟ ولماذا ؟

أنواع الخوارزميات البحث

1. خوارزمية البحث في العمق أولا
2. خوارزمية البحث بالعرض أولا
3. الخوارزمية الحدسية

تمرين : تأمل الشكل التالي ثم أوجد مسار البحث عن الحالة الهدف باستخدام خوارزمية البحث في العمق أولا علما بأن E هي الحالة الهدف ؟ مسار البحث باستخدام خوارزمية البحث في العمق أولا

(R-A-C-D-B-E)



الوحدة الثالثة : البوابات المنطقية

سؤال : مم يتكون الحاسوب ؟
من الكثير من الدوائر المنطقية التي تستخدم في معالجة البيانات الممثلة بالنظام الثنائي (0 و 1)

سؤال : مم تتكون الدوائر المنطقية ؟ من عدد من البوابات المنطقية

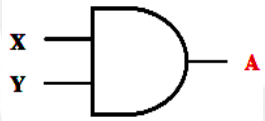
التعبير العلائقي جملة خبرية ناتجها إما صواب 1 وإما خطأ 0 ، وتكتب هذه التعابير باستخدام عمليات المقارنة (=! , <> , => , =< , < , >)

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

العبارة المنطقية المركبة : جملة خبرية تتكون من تعبيرين علائقيين أو أكثر ، يربط بينهما معاملات منطقية (And , Or) وتكون قيمتها إما صوابا (1) أو خطأ. (0)

البوابة المنطقية: دائرة الكترونية بسيطة ، تقوم بعملية منطقية على مدخل واحد أو أكثر وتنتج مخرجا منطقيا واحدا وتستخدم في بناء معالجات الأجهزة الالكترونية والحواسيب.

◊ 1- البوابة االمنطقية AND



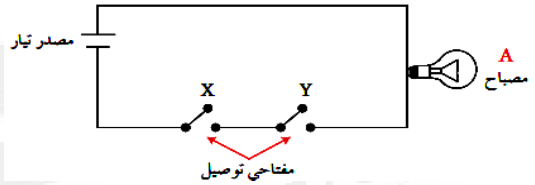
يرمز للبوابة المنطقية AND بالشكل التالي ⟵
حيث يشير X و Y الى مداخل البوابة و A مخرج البوابة

اشرح الية عمل البوابة المنطقية : AND تعطي بوابة AND مخرجا قيمته (1) إذا كانت قيمة جميع المداخل 1 فقط وتعطي مخرجا قيمته (0) إذا كانت قيمة أي من المدخلين أو كلاهما (0)

جدول الحقيقة للبوابة المنطقية AND

X	Y	A = X AND Y
1	1	1
1	0	0
0	1	0
0	0	0

تستطيع تصميم دائرة كهربائية تمثل البوابة المنطقية AND بمفتاحي توصيل في وضعية التوالي بحيث يضيء المصباح عندما يكون كلا المفتاحين في حالى إغلاق فقط



◊ 2- البوابة المنطقية : OR

واحدة من البوابات المنطقية الأساسية التي تدخل في بناء معظم الدوائر المنطقية ، ولها مدخلان ومخرج واحد وتسمى((أو))المنطقية.

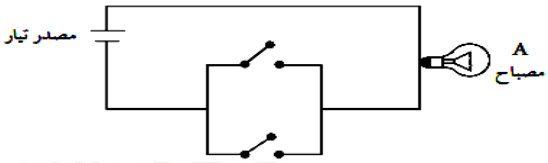
يرمز للبوابة المنطقية OR بالشكل التالي
حيث يشير X و Y الى مداخل البوابة و A مخرج البوابة

اشرح الية عمل البوابة المنطقية : OR
تعطي بوابة OR مخرجا قيمته (1) إذا كانت قيمة أي من المدخلين أو كلاهما 1 فقط وتعطي مخرجا قيمته (0) إذا كانت قيمة كلا المدخلين (0)

جدول الحقيقة للبوابة المنطقية OR

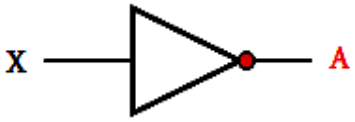
X	Y	A = X OR Y
1	1	1
1	0	1
0	1	1
0	0	0

تستطيع تصميم دائرة كهربائية تمثل البوابة المنطقية OR بمفتاحي توصيل في وضعية التوازي بحيث يضيء المصباح عندما يكون كلا المفتاحين في حالى إغلاق فقط



◊ البوابة المنطقية : NOT

واحدة من البوابات المنطقية الأساسية التي تدخل في بناء معظم الدوائر المنطقية ،ولها مدخل واحد فقط ومخرج واحد ويطلق عليها العاكس (INVERTER)أي أنها تغير القيمة المنطقية للمدخل إلى عكسه.



يرمز للبوابة المنطقية NOT بالرمز التالي
حيث يشير X الى مداخل البوابة و A مخرج البوابة

اشرح الية عمل البوابة النطقية: NOT

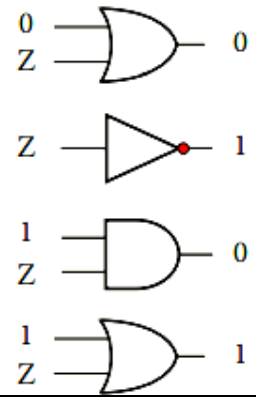
إذا كانت قيمة المدخل (1) فإن قيمة المخرج (0) وإذا كانت قيمة المدخل (0)فإن قيمة المخرج (1)

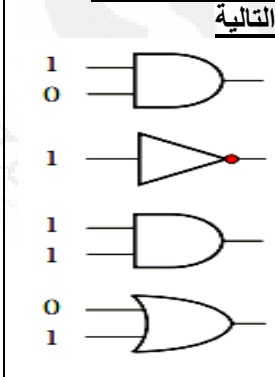
جدول الحقيقة للبوابة المنطقية NOT

X	A = NOT X
1	0
0	1

جدول الحقيقة :
هو تمثيل لعبارة منطقية يبين الاحتمالات المختلفة للمتغيرات المكونة للعبارة المنطقية ، ونتيجة هذه الاحتمالات فعدد الاحتمالات 2^n حيث أن n تمثل عدد المتغيرات في ونتيجة هذه العبارة المنطقية وكل متغير يأخذ قيمتين إما (1) أو(0)

أوجد ناتج كل من البوابات المنطقية التالية





جد ناتج العبارة المنطقية 1 OR 0 AND 1

1 OR 0 AND 1

1 OR 0

1

أوجد ناتج العبارة المنطقية A AND NOT B OR C علما بأن A=1 , B=0 , C=0

A AND NOT B OR C
1 AND NOT 0 OR 0
1 AND 1 OR 0
1 OR 0
1

اوجد ناتج العبارة المنطقية NOT A AND (NOT B OR C)

NOT A AND (NOT B OR C)
NOT 0 AND (NOT 1 OR 0)
NOT 0 AND (0 OR 0)
NOT 0 AND 0
1 AND 0
0

أكتب جدول الحقيقة للعبارة المنطقية التالية A OR NOT B

A	B	NOT B	A OR NOT B
1	1	0	1
1	0	1	1
0	1	0	0
0	0	1	1

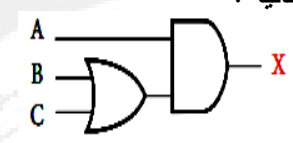
مثل العبارة المنطقية NOT A OR NOT B ثم جد الناتج النهائي اذا كانت A=1 , B=0 , C=1 , D=0

مثل العبارة المنطقية AND C OR NOT B ثم جد الناتج النهائي اذا كانت A=1 , B=0 , C=1 , D=0

0 , C=1 , D=0

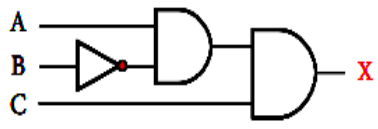
مثل العبارة المنطقية A AND NOT (B OR NOT C) ثم جد الناتج النهائي اذا كانت A=1 , B=0 , C=1 , D=0

أكتب العبارة المنطقية التي تمثلها البوابات التالية ؟



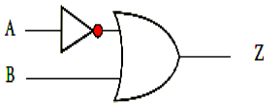
X = (B OR C) AND A

أكتب العبارة المنطقية التي تمثلها البوابات التالية ؟
لاحظ هنا أننا سنبدأ بالبوابة NOT حسب الأولويات ثم البوابة AND ثم البوابة



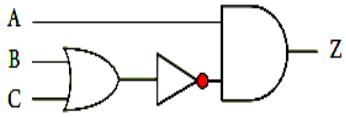
NOT B AND A AND C

أكتب العبارة المنطقية التي تمثلها البوابات التالية ؟
الأولوية للبوابة NOT ثم البوابة OR



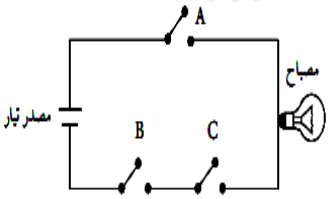
Z = NOT A OR B

أكتب العبارة المنطقية التي تمثلها البوابات التالية ؟



Z = NOT (B OR C) AND A

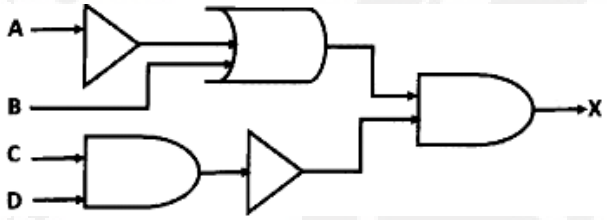
أكتب العبارة المنطقية التي تمثلها البوابات التالية ؟



في هذا النوع من الأسئلة نقوم بتحول الدائرة الكهربائية الى بوابات منطقية اعتمادا على مبدأ التوالي والتوازي بحيث نمثل التوالي بالبوابة المنطقية AND والتوازي بالبوبة المنطقية OR لاحظ أن المفتاح B والمفتاح C في حاله توالي لذا سيعبر عنهم بالبوابة AND وهما متوازيان مع البوابة A والتي سنعبر عنها بالبوابة OR وعليه يكون الحل كما يلي

(B AND C) OR A

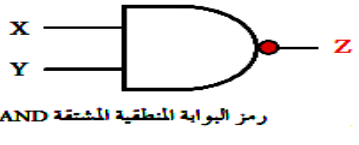
أكتب العبارة المنطقية التي تمثلها البوابات التالية ؟ ثم جد الناتج النهائي اذا علمت أن
A = 0 , B = 1 , C = 0, D = 1



X = (NOT A OR B) AND NOT(C AND D)
X = (NOT 0 OR 1) AND NOT(0 AND 1)
X = (1 OR 1) AND NOT(0 AND 1)
X = 1 AND NOT (0 AND 1)
X = 1 AND NOT 0
X = 1 AND 1
X = 1

البوابة المنطقية المشتقة NAND

هي اختصار ل NOT AND اي نفي AND وتتشكل بوابة NAND بتوصيل مخرجبوابة AND بمدخل بوابة NOTوتسمى بوابة نفي و المنطقية.



رمز البوابة المنطقية المشتقة NAND.

تمثل البوابة المنطقية NAND برمز بوابة AND مع دائرة صغيرة عند المخرج ترمز إلى بوابة NOT

اشرح الية عمل البوابة المنطقية: NAND

® تعطي بوابة NAND مخرجا قيمته (1) إذا كانت قيمة أي من المدخلين أو كلاهما (0)
® وتعطي مخرجا قيمته(0) إذا كانت قيمة المداخل جميعها (1) عكس مخرجات بوابة. AND

جدول الحقيقة للبوابة المنطقية المشتقة NAND

X	Y	Z = X NAND Y
1	1	0
1	0	1
0	1	1
0	0	1

البوابة المنطقية المشتقة NOR

هي اختصار ل NOT OR اي نفي OR وتتشكل بوابة NOR بتوصيل مخرج بوابة OR بمدخل بوابة NOT وتسمى بوابة نفي((أو))المنطقية

رمز البوابة المنطقية المشتقة NOR

تمثل البوابة المنطقية NOR برمز بوابة OR مع دائرة صغيرة عند المخرج ترمز إلى بوابةNOT

اشرح الية عمل البوابة النطقية : NOR

تعطي بوابة NOR مخرجا قيمته (0) إذا كانت قيمة أي من المدخلين أو كلاهما (1) وتعطي مخرجا قيمته(1) إذا كانت قيمة المداخل جميعها (0) عكس مخرجات بوابة OR

جدول الحقيقة للبوابة المنطقية المشتقة NOR

X	Y	Z = X NOR Y
1	1	0
1	0	0
0	1	0
0	0	1

أوجد ناتج العبارة المنطقية A NAND NOT B علما بأن A = 1 , B = 0

A NAND NOT B
1 NAND NOT 0
1 NAND 1
0

1. أوجد ناتج العبارة المنطقية NOT A NAND B NAND C علما بأن , C=0 A=0 , B=1

NOT A NAND B NAND C
NOT 0 NAND 1 NAND 0
1 NAND 1 NAND 0
0 NAND 0
1

2. أوجد ناتج العبارة المنطقية NOT A NAND NOT B علما بأن C=1 , A=0 , B=0

NOT 0 NAND NOT 0
1 NAND NOT 0
1 NAND 1
0

3. أوجد ناتج العبارة المنطقية NOT (A NAND B) NAND C علما بأن , C=1 A=0 , B=0

NOT (0 NAND 0) NAND 1
NOT 1 NAND 1
0 NAND 1
1

4. أوجد ناتج العبارة المنطقية NOT A NAND NOT (B NAND C) علما بأن C=1 A=0 , B=0 ,

NOT A NAND NOT (B NAND C)
NOT 0 NAND NOT (0 NAND 1)
NOT 0 NAND NOT 1
1 NAND NOT 1
1 NAND 0
1

5. أوجد ناتج العبارة المنطقية NOT (A NOR B) NOR C علما بأن , C=0 A=1 , B=1

NOT (1 NOR 1) NOR 0
NOT 0 NOR 0
1 NOR 0
0

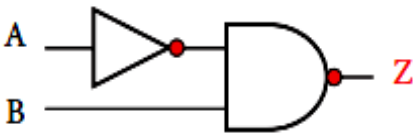
6. أوجد ناتج العبارة المنطقية NOT A NOR B علما بأن , C=0 A=1 , B=0

NOT 1 NOR 0
0 NOR 0
1

7. أوجد ناتج العبارة المنطقية A NOR NOT (B NOR NOT C) علما بأن C=0 A=1 , B=0 ,

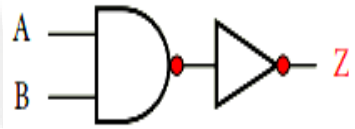
1 NOR NOT (0 NOR NOT 0)
1 NOR NOT (0 NOR 1)
1 NOR NOT 0
1 NOR 1
0

8. أكتب العبارة المنطقية التي تمثلها البوابات المنطقية التالية نبدأ من جهة اليسار بكتابة العبارة المنطقية للبوابة NOT ثم نجعلها مدخلا للبوابة NAND



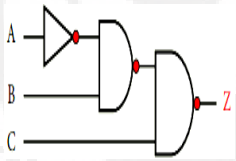
Z = NOT A NAND B

9. أكتب العبارة المنطقية التي تمثلها البوابة المنطقية الاتية ثم جد قيمة Z علما بأن A=1 , B=0 , C=1



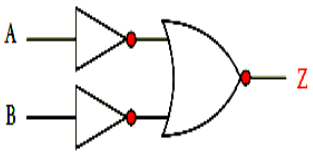
Z = NOT (A NAND B)
Z = NOT (1 NAND 0)
Z = NOT 1
Z = 0

10. أكتب العبارة المنطقية التي تمثلها البوابة المنطقية الاتية ثم جد قيمة Z علما بأن A=1 , B=0 , C=1



Z = (NOT A NAND B) NAND C
Z = (NOT 1 NAND 0) NAND 1
Z = (0 NAND 0) NAND 1
Z = 1 NAND 1
Z = 0

11. أكتب العبارة المنطقية التي تمثلها البوابة المنطقية الاتية ثم جد قيمة Z علما بأن A=0 , B=0 , C=1



Z = NOT A NOR NOT B
Z = NOT 0 NOR NOT 0
Z = 1 NOR NOT 0
Z = 1 NOR 1
Z = 0

الجبر المنطقي (البوولي)

الجبر البوولي(المنطقي:)

هو أحد فروع علم الجبر في الرياضيات ، وهو الأساس الرياضي اللازم لدراسة التصميم المنطقي للأنظمة الرقمية ومنها الحاسوب وتعود تسميته الى العالم الرياضي الانجليزي جورج بوولى (George Boole)

متى يسمى المتغير متغيرا منطقيا ؟ إذا عينت له إحدى الحالتين : صواب (True)أو خطأ. (False)

العبارات الجبرية المنطقية والعمليات المنطقية

وضح المقصود بالعبارة الجبرية المنطقية ؟

هي ثابت منطقي (0,1) أو متغير منطقي مثل (X,Y) أو مزيج من الثوابت والمتغيرات المنطقية يجمع بينها عمليات منطقية ، ويمكن ان تحتوي العبارة الجبرية المنطقية على أقواس وعلى أكثر من عملية منطقية

جدول ناتج متممة X

X	$A=\overline{X}$
1	0
0	1

جدول ناتج عملية AND المنطقية

X	Y	A=X+Y
1	1	1
1	0	1
0	1	1
0	0	0

جدول ناتج عملية AND المنطقية

X	Y	A=X.Y
1	1	1
1	0	0
0	1	0
0	0	0

1. أوجد ناتج العبارة الجبرية المنطقية $A+\overline{B}.C$ علما بأن A=1 , B=0 , C=1

2. أوجد ناتج العبارة الجبرية المنطقية $\overline{A . B + C + D}$ علما بأن A=0 , B=1 , C=1 , D=0

3. أوجد ناتج العبارة الجبرية المنطقية $\overline{A + B . C + D}$ علما بأن A=1 , B=0 , C=0 , D=1

4. جد ناتج العبارة الجبرية المنطقية $(\overline{A} . \overline{B}) + (A . \overline{B})$ علما بأن , D=1 A=1 , B=0 , C=0

5. أوجد ناتج العبارة الجبرية المنطقية $\overline{\overline{A} + B . C + D}$ علما بأن A=1 , B=0 , C=0 , D=1

أكتب جدول الحقيقة للعبارة المنطقية التالية NOT A NAND NOT B

الوحدة الرابعة / أمن المعلومات والتشفير

أمن المعلومات ؟

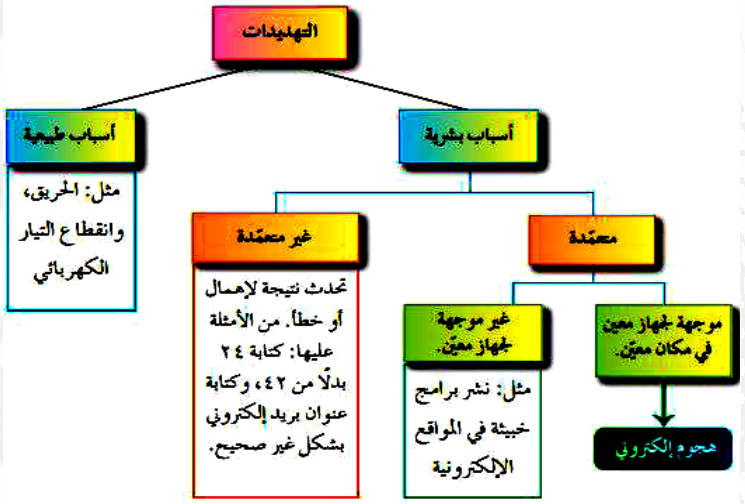
العلم الذي يعمل على حماية المعلومات والمعدات المستخدمة لتخزينها ومعالجتها ونقلها من السرقة او التطفل أو من الكوارث الطبيعية أو غيرها من المخاطر ويعمل على إبقائها متاحة للأفراد المصرح لهم باستخدامها.

سؤال : ما هي الخصائص الأساسية لأمن المعلومات ؟

1. السرية 2. السلامة 3. توافر المعلومات

السرية(سرية المعلومات)	أمثلة على معلومات سرية
عدم القدرة على الحصول على المعلومات إلا من قبل الأشخاص المخول لهم ذلك .	1. المعلومات الشخصية 2. الموقف المالي لشركة ما 3. المعلومات العسكرية
السلامة(سلامة المعلومات)	**أمثلة على سلامة المعلومات:**
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 سلامة هذه النتائج من أي تعديلات.

المخاطر التي تهدد أمن المعلومات(أنواع تهديدات أمن المعلومات)



سؤال : ما أثر الأسباب الطبيعية مثل حدوث حريق أو انقطاع التيار الكهربائي كتهديد على أمن المعلومات ؟ تؤدي الى فقدان المعلومات

اعط مثال عن اخطاء نتيجة الاهمال أو الخطأ.

1. سرقة جهاز الحاسوب 2. سرقة المعدات التي تحفظ المعلومات

ما هي العوامل الرئيسية التي يجب أخذها في الحسبان لتقييم التهديد الذي يتعرض له النظام ؟

1. الدافع 2. الطريقة. 3. فرصة النجاح.

1. الدافع	**اذكر ثلاثة دوافع** 1. رغبة في الحصول على المال 2. محاولة لاثبات القدرات التقنية 3. بقصد الاضرار بالاخرين.
2. الطريقة	**تتضمن عدة أمور أذكرها** 1. المهارات التي يتميز بها المعتدي الالكتروني 2. معرفته بتصميم النظام وآلية عمله. 3. معرفة نقاط القوة والضعف لهذا النظام.
3. فرصة النجاح	**تتمثل بأمرين اثنين ، أذكرهما !** 1. تحديد الوقت المناسب للتنفيذ. 2. كيفية الوصول الى الأجهزة.

تتعرض المعلومات إلى أربعة أنواع من الاعتداءات الالكترونية ، أذكرها ؟

1. التنصت على المعلومات 3. التعديل على المحتوى
2. الإيقاف 4. الهجوم المزور أو المفبرك.

التنصت على المعلومات	الحصول على المعلومات السرية حيث يتم الاخلال بسريتها
الإيقاف	يتم قطع قناة الاتصال ، ومن ثم منع المعلومات من الوصول الى المستقبل ، وفي هذه الحالة تصبح المعلومات غير متوافرة.
التعديل على المحتوى	يتم اعتراض المعلومات وتغيير محتواها واعادة ارسالها للمستقبل ، من دون أن يعلم بتغير محتواها وفي هذا النوع يكون الاخلال بسلامة المعلومات.
الهجوم المزور أو المفبرك	يتمثل هذا النوع بارسال المعتدي الالكتروني رسالة الى أحد الأشخا على الشبكة يخبره فيها بأنه صديقه ويحتاج إلى معلومات أو كلمات سرية خاصة

سؤال : وضح المقصود بالثغرات ؟

نقطة ضعف في النظام سواء أكانت في الاجراءات المتبعة

مثل :

1> عدم تحديد صلاحيات الوصول الى النظام
2> مشكلة في تصميم النظام
3> عدم كفاية الحماية المادية للأجهزة والمعلومات

تعد من نقاط الضعف لأنها قد تتسبب في فقدان المعلومات ، أو هدم النظام ، أو تجعله عرضة للاعتداء الالكتروني.

سؤال : هناك مجموعة من الضوابط التي وضعت لتقليل المخاطر التي تتعرض لها المعلومات والحد منها ، أذكر هذه الضوابط

الضوابط	التعريف / مع مثال
1. **الضوابط المادية**	مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها باستخدام الجدران والأسوار ،
2. **الضوابط الادارية**	مجموعة من الأوامر والاجراءات المتفق عليها مثل :القوانين واللوائح والسياسات ،
3. **الضوابط التقنية**	الحماية التي تعتمد على التقنيات المستخدمة ، سواء كانت معدات أو برمجيات وتتضمن : كلمات المرور ، ومنح صلاحيات الوصول ،

سؤال : يعتمد اختيار الكادر البشري المسؤول عن حماية الأنظمة على عدة امور ، أذكرها ؟

1. الكفاية العلمية
2. اختبارات شفوية وورقية
3. اخضاعهم الى ضغوط نفسية كل حسب موقعهم

سؤال : وضح المقصود بالهندسة الاجتماعية ؟

هي الوسائل والأساليب 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.

علل : تعد الهندسة الاجتماعية من أنجح الوسائل وأسهلها للحصول على معلومات غير مصرح بالاطلاع عليها ؟

بسبب قلة اهتمام المتخصصين في مجال أمن المعلومات وعدم وعي مستخدمي الحاسوب بالمخاطر المترتبة عليها.

سؤال : ترتكز الهندسة الاجتماعية في مجالين ، ما هما ؟

1. البيئة المحيطة 2. الجانب النفسي

أولا : البيئة المحيطة

مكان العمل	يكتب بعض الموظفين كلمات المرور على أوراق ملصقة بشاشة الحاسوب وعند دخول الشخص غير المخول له يتمكن من الدخول الى النظام بسهولة
الهاتف	يتصل الشخص غير المخول بمركز الدعم الفني هاتفيا ، ويطلب إليه بعض المعلومات الفنية ويستدرجه
النفايات الورقية	يدخل الأشخاص غير المخولين الى مكان العمل ويجمعون النفايات التي قد تحتوي على كلمات المرور ومعلومات تخص الموظفين وأرقام هواتفهم وبياناتهم الشخصية
الانترنت	**من أكثر وسائل الهندسة الاجتماعية شيوعا** بسبب استخدام الموظفين أو مستخدمي الحاسوب عادة كلمة المرور نفسها للتطبيقات جميعها. # حيث ينشئ المعتدي الالكتروني موقعا على الشبكة. # يتطلب التسجيل في الموقع اسم مستخدم وكلمة مرور وهي كلمة المرور نفسها التي يستخدمها الشخص عادة

ثانيا : الجانب النفسي

الاقناع	• **بطريقة مباشرة** بحيث يقدم الحجج المنطقية والبراهين • **بطريقة الاقناع غير المباشر** 1. إظهار نفسه بمظهر صاحب السلطة. 2. إغراء المستخدم بامتلاك خدمات نادرة 3. إبراز أوجه التشابه مع الشخص المستهدف.
انتحال الشخصية	يتقمص شخص شخصية اخر وهذا الشخص قد يكون شخصا حقيقيا أو وهميا . فقد ينتحل شخصية فني صيانة معدات الحاسوب أو عامل نظافة أو حتى المدير أو السكرتير .#
مسايرة الركب	# يرى الموظف بأنه اذا قام زملاؤه جميعا بأمر ما فمن غير اللائق أن يأخذ هو موقفا مغايرا. # عندما يقدم شخص نفسه على انه إداري من فريق الدعم الفني ويرغب بعمل تحديثات على الأجهزة فإذا سمح له أحد الموظفين بعمل تحديث على جهازه فإن باقي الموظفين يقومون بمسايرة

ما هي أسباب إيجاد وسائل تقنية لحماية الانترنت (الويب) ؟

1. بسبب انتشار البرامج والتطبيقات بشكل كبير منها ما هو مجاني ومنها ما هو غير معروف المصدر
2. بسبب انتشار البرامج المقرصنة والمعلومات بكيفية اقتحام المواقع.

أذكر مثالين على الاعتداءات التي تتعرض لها المواقع الالكترونية)؟ ما هي أشهر الاعتداءات على(الويب)؟

1. الاعتداءات الالكترونية على متصفحات الانترنت.
2. الاعتداءات الالكترونية على البريد الالكتروني.

متصفح الانترنت ؟ برنامج ينقل المستخدم الى صفحة(الويب) التي يريدها بمجرد كتابة العنوان والضغط على زر الذهاب ويمكّنه من مشاهدة المعلومات على الموقع.

سؤال : يتم الاعتداء على متصفح الانترنت بطريقتين ، أذكرهما

1. الاعتداء عن طريق(كود)بسيط
2. توجيه المستخدم إلى صفحة أخرى غير الصفحة التي يريدها.

سؤال : وضح كيف يتم الاعتداء الالكتروني على البريد الالكتروني ؟

تصل الكثير من الرسائل الالكترونية الى البريد الالكتروني ، بعض هذه الرسائل الالكترونية مزيفة
هذه الرسائل تحتوي روابط للمزيد من المعلومات يرجى الضغط عليه ، وغيرها من الرسائل المزيفة والمضللة التي تحتاج وعي من المستخدم.

تقنية تحويل العناوين الرقمية ؟

هي التقنية التي تعمل على إخفاء العنوان الرقمي للجهاز في الشبكة الداخلية ليتوافق مع العنوان الرقمي المعطى للشبكة . ومن ثم فإن الجهاز الداخلي غير معروف بالنسبة الى الجهات

العناوين الرقمية الإلكترونية

يرتبط ملايين الأشخاص عبر شبكة الانترنت بملايين الأجهزة ولكل جهاز حاسوب أو هاتف خلوي عنوان رقمي خاص به يميزه عن غيره يسمى Internet Protocol Address (IP Address)

IP4	IPv6
# يتكون من (32) خانة ثنائية تتوزع على أربعة مقاطع يفصل بينها نقاط. # كل مقطع من هذه المقاطع يتضمن رقم من (0) الى (255)	# علل : سبب ظهور IPv6 ؟ نظرا للتطور الهائل في أعداد المستخدمين ظهرت الحاجة الى عناوين إلكترونية أكثر وطورت هذه العناوين لما يسمى IPv6 # يتكون من ثمانية مقاطع بدلا من أربعة.

مفهوم تقنية تحويل العناوين الرقمية NAT

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

آلية عمل تقنية تحويل العناوين الرقمية

سؤال : تعمل تقنية تحويل العناوين الرقمية بعدة طرائق ، أذكر طريقتين ؟

1. النمط الثابت للتحويل. 2. النمط المتغير للتحويل.

1. النمط الثابت للتحويل	# طريقة يتم خلالها تخصيص عنوان رقمي خارجي لكل جهاز داخلي ،وهذا العنوان الرقمي ثابت لا يتغير
2. النمط المتغير للتحويل.	# نمط يتم خلاله تخصيص عنوان رقمي للجهاز عند رغبته في التواصل مع جهاز خارج الشبكة يستخدمه وعند انتهاء عملية الاتصال يصبح هذا العنوان الرقمي متاحا للأجهزة الأخرى.

سؤال : فسر اختلاف IP Address للجهاز نفسه عند تراسله أكثر من مرة !

عند رغبة أحد الاجهزة بالتراسل خارجيا فإنه يتواصل مع الجهاز الوسيط الذي يعطيه عنوانا خارجيا مؤقتا
عند انهاء عملية التراسل يفقد الجهاز الداخلي هذا العنوان
عند رغبة الجهاز نفسه بالتراسل مرة أخرى قد يعطى عنوانا مختلفا عن المرة السابقة وهذا

الفصل الثالث : التشفير

سؤال : وضح المقصود بالتشفير ؟

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

سؤال : ما هو الهدف من علم التشفير(أو)الى ماذا يهدف التشفير ؟

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

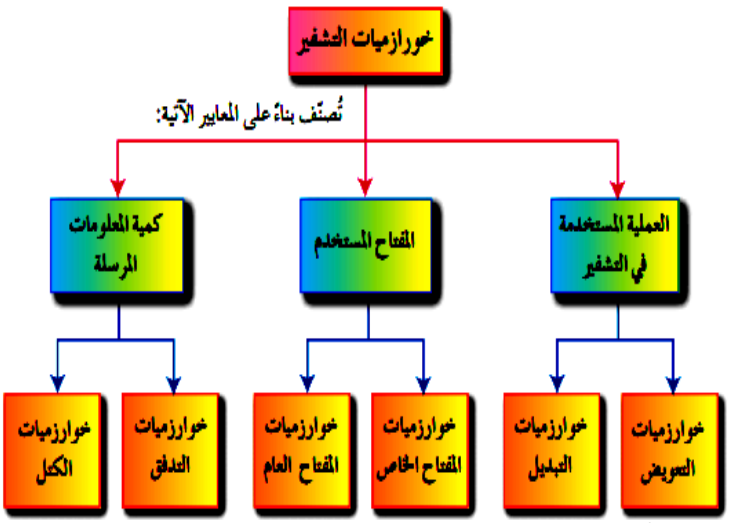
علل : يعد التشفير من أفضل الطرق المستخدمة للحفاظ على أمن المعلومات ؟ لأنه يعمل على أخفاء المعلومات عن الأشخا غير المصرح لهم بالاطلاع عليها وعدم الاستفادة منها أو فهم محتواها حتى لو تم الحصول عليها من قبل أشخا معترضين.

سؤال : تتضمن عملية التشفير أربعة عناصر أساسية ، أذكرها ؟

# خوارزمية التشفير	مجموعة من الخطوات المستخدمة لتحويل الرسالة الأصلية الى رسالة مشفرة.
# مفتاح التشفير	سلسلة من الرموز المستخدمة في خوارزمية التشفير وتعتمد قوة التشفير على قوة هذا المفتاح
# النص الأصلي	محتوى الرسالة الأصلية قبل التشفير وبعد عملية فك التشفير.
# نص الشيفرة	الرسالة بعد عملية التشفير.

سؤال : تصنف خوارزميات التشفير بناء على عدة معايير ، أذكر ثلاثا من هذه المعايير ؟

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



أولا : التشفير المعتمد على نوع عملية التشفير

1. تشفير التبديل

يتم فيها تبديل أماكن الأحرف عن طريق إعادة ترتيب أحرف الكلمة بشرط استخدام الاحرف نفسها من دون إجراء أي تغيير عليها

2. تشفير التعويض

استبدال حرف مكان حرف أو مقطع مكان مقطع ، مثال : شيفرة الازاحة

فك التشفير : عمليات إعادة الرسالة المشفرة إلى المحتوى الأصلي

خوارزمية الخط المتعرج: (Zig Zag Cipher)

هي خوارزمية تتميز بأنها سهلة وسريعة ويمكن تنفيذها يدويا باستخدام الورقة والقلم ، كما انه يمكن فك تشفيرها بسهولة.

شفر النص الاتي ، علما بأن مفتاح التشفير هو خمسة أسطر

Stay positive this year makes you happy all life

شفر النص الاتي ، علما بأن مفتاح التشفير هو ثلاثة أسطر

Never give up on your goals

أوجد النص المشفر لكل نص مما يأتي ، مستخدما خوارزمية الخط المتعرج Zig Zag علما بأن مفتاح التشفير أربعة أسطر

Youth is the future and the spirit of our home

أوجد النص المشفر لكل نص مما يأتي ، مستخدما خوارزمية الخط المتعرج علما بأن مفتاح التشفير ستة أسطر Zig Zag

School is the place where great people

فك تشفير النص الاتي مستخدما خوارزمية الخط المتعرج Zig Zag علما بأن مفتاح التشفير ستة أسطر

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

فك تشفير النص الاتي مستخدما خوارزمية الخط المتعرج Zig Zag علما بأن مفتاح التشفير خمسة أسطر

Spiheayaaitoviakoplfasesreupleyi ∇ ∇ ∇ s ∇ y ∇ ∇ ∇ ttym ∇ h ∇ l ∇

ثانيا :التشفير المعتمد على المفتاح

سؤال : كيف تصنف خوارزميات التشفير المعتمد على المفتاح ؟

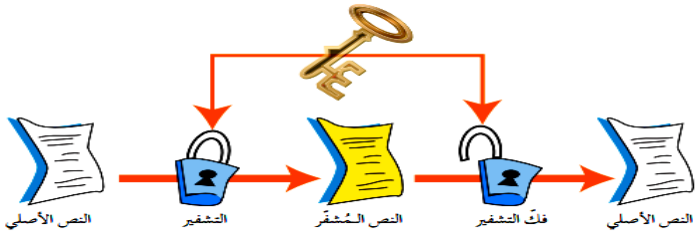
يصنف هذا النوع من خوارزميات التشفير على عدد المفاتيح المستخدمة في عملية التشفير وعليه فإن أمن الرسالة أو المعلومة يعتمد على سرية المفتاح وليس على تفاصيل الخوارزمية.

سؤال : يقسم التشفير المعتمد على المفتاح الى قسمين ، أذكرهما

1- خوارزميات المفتاح الخاص (الخوارزميات التناظرية.)
2- خوارزميات المفتاح العام (الخوارزميات اللاتناظرية.)

سؤال : وضح المقصود بخوارزميات المفتاح الخاص (أو)علل تسمى خوارزميات المفتاح الخا بالخوارزميات التناظرية ؟ (أو)علل تسمى خوارزميات المفتاح الخاص بخوارزميات المفتاح السري.

إن المفتاح نفسه يستخدم لعمليتي التشفير وفك التشفير ويتم الاتفاق على اختياره قبل بدء عملية التراسل بين المرسل والمستقبل.



سؤال : وضح المقصود بخوارزميات البحث العام (أو)علل تسمى خوارزميات المفتاح العام بالخوارزميات اللاتناظرية ! تستخدم هذه

الخوارزميات مفتاحين ، أحدهما يستخدم لتشفير الرسالة ويكون معروفا (للمرسل والمستقبل) ويسمى المفتاح العام ن والاخر يكون معروفا لدى المستقبل فقط ويستخدم لفك التشفير ويسمى المفتاح الخاص.

سؤال : كيف يتم انتاج المفاتيح في خوارزميات البحث العام ؟

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

ثالثا :التشفير المعتمد على كمية المعلومات المرسلة

سؤال : يقسم التشفير المعتمد على المفتاح الى قسمين ، أذكرهما

1- شيفرات التدفق. 2- شيفرات الكتل.

سؤال : وضح المقصود بشيفرات التدفق (كيف تعمل شيفرات التدفق)؟

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

سؤال : وضح المقصود بشيفرات الكتل (كيف تعمل شيفرات الكتل)؟

تقسم الرسالة الى أجزاء ولكن بحجم اكبر من حجم الأجزاء في شيفرات التدفق ويشفر أو يفك تشفير كل كتلة على حدة . يختلف عن شيفرات التدفق بأن حجم المعلومات أكبر ، لذا فإنها أبطأ.

تمت بحمد الله