مكثف المادة النظرية / علوم الحاسوب

الفصل الدراسي الثاني ٢٠٢٢/٢٠٢٣

إعداد

أ.محمد توفيق

٠٧٨٦٥٨٣٢٤٠

س: اذكر مثالاً على كل مما يلي:

أ.	بوابات منطقية أساسية	AND أو OR أو NOT
ب.	بوابات منطقية مشتقة	NOR أو NAND
ج.	رمز لعملية جبرية منطقية	+ أو . أو ــ
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	$\bar{A}$ + B . C
ح.	عبارة منطقية مركبة	A AND B OR C
ط.	معامل منطقي	AND أو OR أو NOT
ي.	ثابت منطقي	0 أو 1

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.

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

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

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

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

٥. **NAND** (نفي "و" المنطقية) وهي اختصار لـِ **NOT AND**

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

٧. **NOR** (نفي " أو" المنطقية) وهي اختصار لـِ **NOT OR**

الوحدة الثالثة: الأساس المنطقي للحاسوب والبوابات المنطقية

س: 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 **A ..... Z**

(لا أهمية لكون الحروف كبيرة أم صغيرة).

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

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

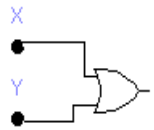
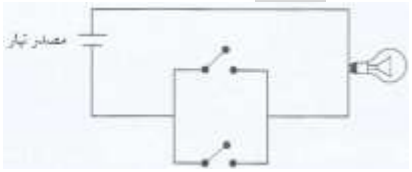
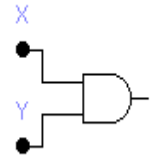
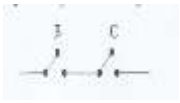
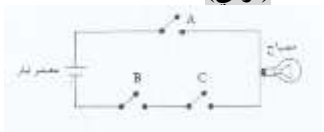
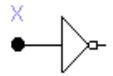
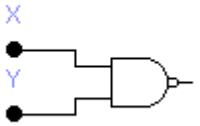
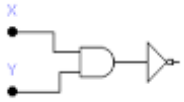
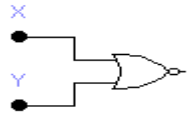
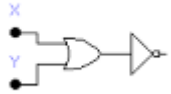
١. **المعامل المنطقي:** هو رابط يستخدم للربط بين تعبيرين علائقيين أو أكثر لتكوين عبارة منطقية مركبة ، ومن أهمها **AND** و **OR**، أو نفي تعبير منطقي باستخدام **NOT**.

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.

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 لـ 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 أو AB الدارة الكهربائية لـ AND (توالي)  
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 بالعبارة المنطقية: NOT(X AND) 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 بالعبارة المنطقية: NOT(X OR Y) يكافئها بالتعبير الجبري $\overline{X+Y}$ يكافئها بالبوابات الأساسية 

عناصر (خصائص) أمن المعلومات.

١. السرية ٢. السلامة ٣. توافر المعلومات (التوافر)

أمثلة على بيانات يعتمد أمنها على مقدار الحفاظ على سريتها :

أ. المعلومات الشخصية ب. المعلومات العسكرية

ج.الموقف المالي لشركة ما قبل إعلانه

أمثلة على بيانات يجب الحفاظ على سلامتها من الحذف أو التبديل أو التعديل أو التغيير : أ.عند نشر نتائج طلبة الثانوية العامة

ب.عند صدور قوائم القبول الموحد للجامعات الأردنية

أنواع المخاطر التي تهدد أمن المعلومات : ١. الثغرات ٢. التهديدات

الشكل (٤- ١): أنواع تهديدات أمن المعلومات.

تقسم التهديدات البشرية المتعمدة إلى قسمين : ١. موجهة لجهاز معين

٢. غير موجهة لجهاز معين مثل: نشر فيروس بين الأجهزة

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 عند تنفيذ الهجوم الإلكتروني،

١. الرغبة في إثبات القدرات التقنية ٢. الإضرار بالآخرين

٣. الرغبة في الحصول على المال

تتضمن الطريقة

١. معرفة نقاط القوة والضعف للنظام ٢المعرفة بتصميم النظام وآلية عمله

٣. القدرة على توفير المعدات و البرمجيات الحاسوبية

٤. المهارات التي يتميزبها المعتدي الإلكتروني

تتمثل فرصة النجاح في :

١. تحديد الوقت المناسب لتنفيذ الهجوم الإلكتروني

٢. المعرفة بكيفية الوصول للأجهزة

أنواع الاعتداءات الإلكترونية على المعلومات:

١. التنصت على المعلومات ٢. التعديل على المحتوى

٣. الايقاف ٤.الهجوم المفبرك او المزور

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)**

أمثلة على الثغرات : ١– عدم تحديد صلاحيات الوصول إلى المعلومات

٢– مشكلة في تصميم النظام

٣– عدم كفاية الحماية المادية للاجهزة والمعلومات

وضعت مجموعة من الضوابط لتقليل المخاطر التي تتعرض لها المعلومات والحد منها وهي:

أ–الضوابط المادية ب–الضوابط الادارية ج– الضوابط التقنية

أمثلة على الضوابط المادية : ١. استخدام الجدران والاسوار و الاقفال

٢.وجود حراس الأمن ٣. أجهزة إطفاء الحريق

أمثلة على الضوابط الإدارية : ١. القوانين واللوائح و السياسات

٢. الاجراءات التوجيهية ٣. حقوق النشر

٤. براءات الاختراع و العقود و الاتفاقيات

أمثلة على الضوابط التقنية : ١. كلمات المرور ٢. التشفير

٣. منح صلاحيات الوصول ٤. بروتوكولات الشبكات والجدر النارية

٥. تنظيم تدفق المعلومات في الشبكة

الهندسة الاجتماعية (التفصيل في الصفحة الأخيرة)

تتركز الهندسة الاجتماعية في مجالين :البيئة المحيطة/الجانب النفسي

تشمل البيئة المحيطة :

أ. مكان العمل ب. الهاتف ج. النفايات الورقية د. الإنترنت

الإنترنت أكثر الوسائل شيوعاً.

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

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

أمن الإنترنت

الاعتداءات الإلكترونية على المواقع الإلكترونية (الويب)

١– الاعتداء على متصفح الانترنت

٢– الاعتداء على البريد الإلكتروني

يتم الاعتداء على متصفح الانترنت 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

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)

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

مفهوم تقنية تحويل العناوين الرقمية NAT

– تمنح (أيانا) الشبكة الداخلية عنوانا واحدا (أو مجموعة عناوين) مختلفاً عن عناوين الشبكات الأخرى ويكون معرفاً لها عند التعامل في شبكة الانترنت . (كل شبكة داخلية تمنح عنواناً خاصاً بها على الإنترنت مختلفاً عن العناوين الأخرى).

– 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

– 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) (هنا يذكر الطالب وظيفة الجهاو الوسيط)

وظيفة الجهاز الوسيط (موجهاً أو جداراً نارياً):

١. تحويل العنوان الرقمي الداخلي إلى عنوان رقمي خارجي(عند التواصل خارج الشبكة) ٢. تحويل العنوان الرقمي الخارجي إلى عنوان داخلي (عند الرد على رسالة الجهاز المرسل) من خلال سجل المتابعة لديه

آلية (طرق) عمل تقنية تحويل العناوين الرقمية.

١. النمط الثابت للتحويل . ٢. النمط المتغير للتحويل

توضيح النمط الثابت للتحويل

– تخصيص عنوان رقمي خارجي لكل جهاز داخلي

– العنوان الرقمي ثابت لا يتغير.

توضيح النمط المتغير للتحويل

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

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

١– الآلية المستحدمة في التشفير ٢– المفتاح المستخدم

٣– كمية المعلومات المرسلة

يقسم التشفير المعتمد على آلية التشفير إلى نوعين (طريقتين):

١. خوارزميات التعويض ٢. خوارزميات التبديل

يقسم التشفير المعتمد على المفتاح إلى نوعين (قسمين) :

أ– خوارزميات المفتاح الخاص ب– خوارزميات المفتاح العام

يقسم التشفير المعتمد على كمية المعلومات المرسلة إلى نوعين (قسمين)

أذكرهما؟ . ١– شيفرات التدفق ٢– شيفرات الكتل

مميزات خوارزمية الخط المتعرج :

١. سهلة وسريعة ٢. يمكن فك تشفيرها بسهولة

٣. يمكن تنفيذها يدويا باستخدام ورقة وقلم

مصطلحات الوحدة

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؛ يقصد 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 الاجتماعية هي 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 أربعة مقاطع يفصل بينها نقاط ، وهذا يسمى (**IPV4**) وكل مقطع من هذه المقاطع يتضمن رقما من **0** إلى **255**

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 مجموعةمن 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

أسئلة علل

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

ظهور الحاجة إلى تقنية تحويل العناوين الرقمية NAT .

بسبب التطور الهائل في أعداد مستخدمي الإنترنت

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

أسئلة إضافية

س : ما الفرق بين العناوين الرقمية IPv4 **و** IPv6 **؟**

IPv4 تتوزع على أربعة مقاطع بينما **IPv6** تتوزع على ثمانية مقاطع

س : على ماذا تعتمد خوارزميات التشفير المعتمد على المفتاح؟

تعتمد على عدد المفاتيح.

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

لحل مشكلة التطوررالهائل في أعداد مستخدمي الإنترنت والحاجة إلى عناوين إلكترونية أكثر :

١. طورت عناوين **IPV4** إلى **IPV6**
٢. تم إيجاد تقنية تحويل العناوين الرقمية **NAT**

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 .

العنوان الرقمي	الجواب	سبب الخطأ إن وجد
255.254.30.1	صحيح	
255.256.30.1	خطأ	أحد مقاطع العنوان تجاوز 255
255.255.30.1.2	خطأ	احتوى العنوان على ٥ مقاطع بدلاً من ٤ مقاطع
255,254,30,1	خطأ	تم الفصل بين المقاطع بـ (,) بدلاً من (.)

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

لا تنس مكثف المادة العملية.

الهندسة الاجتماعية

تتركز الهندسة الاجتماعية في مجالين : ١. البيئة المحيطة ٢. الجانب النفسي

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

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

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

مجال (البيئة المحيطة)	آلية العمل
مكان العمل	كتابة الموظفين لكلمات المرور على أوراق ملصقة بشاشة الحاسوب ، وعند دخول الشخص غير المخول له الاستخدام (زبون ،عامل نظافة،عامل صيانة) يستطيع معرفة كلمات المرور ومن ثم يتمكن من الدخول الى النظام بسهولة ليحصل على المعلومات التي يريدها
الهاتف	يتصل الشخص غير المخول بمركز الدعم الفني هاتفياً ، و يطلب إليه بعض المعلومات الفنية و يستدرجه للحصول على كلمات المرور وغيرها من المعلومات
النفايات الورقية	يدخل الاشخاص غير المخولين الى مكان العمل ويجمعون النفايات التى قد تحتوى على (كلمات المرور و معلومات تخص الموظفين و أرقام هواتفهم و بياناتهم الشخصية) ، وقد تحتوى على تقويم العام السابق وكل ما يحتويه من معلومات يمكن استغلالها في تتبع أعمال الموظفين أو الحصول على المعلومات المرغوبة
الأنترنت سؤال صح خطأ (ص٢٠١٨)	من أكثر الوسائل شيوعا؛ (**علل**)وذلك بسبب استخدام الموظفين عادة كلمة المرور نفسها للتطبيقات جميعها ، حيث ينشئ المعتدي الإكتروني موقعاً على الشبكة يقدم خدمات معينة، ويشترط التسجيل فيه للحصول على هذه الخدمات. يتطلب التسجيل اسم مستخدم و كلمة المرور وهي كلمة المرور نفسها الذي يستخدمها الشخص عادة، وبهذه الطريقة يتمكن المعتدي الإلكتروني من الحصول عليها.

مجال (الجانب النفسي)	آلية العمل
	– طريقة مباشرة : يستطيع المعتدي اقناع مستخدم الحاسوب من خلال تقديم الحجج و البراهين – طريقة غير مباشرة: بحيث يعمد الى تقديم إيحاءات نفسية تحث المستخدم على قبول المبررات من دون تحليلها أو التفكير فيها ، وذلك عن طريق: ١. إظهار نفسه بمظهر صاحب السلطة أو إغراء المستخدم إمتلاك خدمة نادرة(كأن يقدم له عرضاً معيناً من خلال موقعه الإلكتروني لمدة محددة) ، يمكنه ذلك من الحصول على كلمة المرور ٢. إبراز أوجه التشابه مع الشخص المستهدف(علل) لإقناعه بأنه يحمل الصفات والإهتمامات نفسها فيرتاح له الشخص فيقدم له ما يريد من معلومات
انتحال الشخصية والمداهنة	يتقمص شخص شخصية آخر، فقد ينتحل شخصية (فني صيانة الحاسوب ، عامل نظافة ، المدير ، السكرتير) وغالباً تكون ذات سلطة ولن يتردد الموظفين بتقديم المعلومات و الخدمات لهذا الشخص
مسايرة الركب	يرى الموظف بأنه إذا قام زملاؤه جميعهم بأمر ما ،فمن غير اللائق أن يأخد هو موقفا مغايراً. مثال : يقدم شخص على انه إداري من فريق الدعم الفني و يرغب بعمل تحديثات على الاجهزة فإذا سمح له أحد الموظفين بذلك ، فإن باقي الموظفين يقومون بمسايرة زميلهم غالبا ومن ثم يتمكن من الاطلاع على المعلومات التى يريدها.