



مكتف المادة النظرية / علوم الحاسوب

الفصل الدراسي الثاني 2024/2023

إعداد

أ.محمد توفيق

0786583240



1. صفحة الفيس بوك (الأستاذ محمد توفيق-حاسوب توجيهي)

<http://bit.ly/3CFmE9v>

2. حساب الإنستغرام (أ.محمد توفيق) <https://bit.ly/3XVtelX>

3. قناة اليوتيوب (محمد توفيق حاسوب)

<https://youtube.com/@user-cw7jp2sc5t>

س : اذكر مثلاً على كل مما يلي :

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

- قام العالم جورج بول بتقديم علم الجبر المنطقي للمرة الأولى في كتابه (التحليل الرياضي للمنطق)

قام بتقديم أسس الجبر المنطقي بشكل واسع في كتابه الأشهر (دراسة في قوانين التفكير)

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.

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

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

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

4. كيف نشكل بوابة NAND؟ توصيل مخرج بوابة AND بمدخل بوابة NOT

5. NAND (نفي "و" المنطقية) وهي اختصار لـ NOT AND

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

7. NOR (نفي "أو" المنطقية) وهي اختصار لـ NOT OR

الوحدة الثالثة:

الأساس المنطقي للحاسوب والبوابات المنطقية

س : ما هي أنواع البوابات المنطقية؟

1. البوابات المنطقية الأساسية وهي (AND, OR, NOT)

2. البوابات المنطقية المشتقة وهي (NAND, NOR)

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

1. تنفيذ العمليات التي بداخل الأقواس. 2. البوابة المنطقية NOT

3. البوابة المنطقية And 4. البوابة المنطقية OR

5. 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

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

1. 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.

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

البوابة المنطقية: دائرة 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 بين الاحتمالات المختلفة للمتغيرات المكونة للعبارة المنطقية، ونتيجة هذه الاحتمالات.

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

إضافات	مخرجات البوابة	جدول الحقيقة	الرمز	اسم البوابة															
<p>التعبير الجبري لبوابة OR: $X+Y$ (توازي)</p> <p>الدارة الكهربائية لـ OR (توازي)</p>  <p>دارة كهربائية تمثل البوابة المنطقية OR</p>	<p>تعطي البوابة المنطقية OR مخرجاً قيمته (1) إذا كانت قيمة أي من المدخلين أو كلاهما (1) وتعطي مخرجاً قيمته (0) إذا كانت قيمة كلا المدخلين (0)</p>	<table border="1"> <thead> <tr> <th>X</th> <th>Y</th> <th>A=X OR Y</th> </tr> </thead> <tbody> <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> </tbody> </table>	X	Y	A=X OR Y	1	1	1	1	0	1	0	1	1	0	0	0		OR
X	Y	A=X OR Y																	
1	1	1																	
1	0	1																	
0	1	1																	
0	0	0																	
<p>التعبير الجبري لبوابة AND: $X.Y$ أو XY (توالي)</p> <p>الدارة الكهربائية لـ AND (توالي)</p>  <p>دارة كهربائية تمثل البوابة المنطقية AND</p>	<p>تعطي البوابة المنطقية AND مخرجاً قيمته (1) إذا كانت قيمة المدخل جميعها (1) فقط. وتعطي مخرجاً قيمته (0) إذا كانت قيمة أي من المدخلين أو كلاهما (0)</p>	<table border="1"> <thead> <tr> <th>X</th> <th>Y</th> <th>Z = X AND Y</th> </tr> </thead> <tbody> <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> </tbody> </table>	X	Y	Z = X AND Y	1	1	1	1	0	0	0	1	0	0	0	0		AND
X	Y	Z = X AND Y																	
1	1	1																	
1	0	0																	
0	1	0																	
0	0	0																	
<p>التعبير الجبري لبوابة NOT: \bar{X}</p>	<p>المخرجات عكس المدخلات تعطس مخرجاً قيمته 1 إذا كان المدخل 0 وتعطي مخرجاً قيمته 0 إذا كان المدخل 1</p>	<table border="1"> <thead> <tr> <th>X</th> <th>A=NOT X</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>0</td> </tr> <tr> <td>0</td> <td>1</td> </tr> </tbody> </table>	X	A=NOT X	1	0	0	1		NOT									
X	A=NOT X																		
1	0																		
0	1																		
<p>يكافئها بالعبارة المنطقية: $\overline{X \text{ AND } Y}$</p> <p>يكافئها بالتعبير الجبري $\bar{X} \cdot \bar{Y}$</p> <p>يكافئها بالبوابة الأساسية</p> 	<p>تعطي مخرجاً قيمته (1) إذا كانت قيمة أي من المدخلين أو كلاهما (0). تعطي مخرجاً قيمته (0) إذا كانت قيمة المدخل جميعها (1).</p>	<table border="1"> <thead> <tr> <th>X</th> <th>Y</th> <th>Z = X NAND Y</th> </tr> </thead> <tbody> <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> </tbody> </table>	X	Y	Z = X NAND Y	1	1	0	1	0	1	0	1	1	0	0	1		NAND
X	Y	Z = X NAND Y																	
1	1	0																	
1	0	1																	
0	1	1																	
0	0	1																	
<p>يكافئها بالعبارة المنطقية: $\overline{X \text{ OR } Y}$</p> <p>يكافئها بالتعبير الجبري $\bar{X} + \bar{Y}$</p> <p>يكافئها بالبوابة الأساسية</p> 	<p>تعطي مخرجاً قيمته (1) إذا كانت قيمة كلا المدخلين (0). تعطي مخرجاً قيمته (0) إذا كانت قيمة أي من المدخلين أو كلاهما (1).</p>	<table border="1"> <thead> <tr> <th>X</th> <th>Y</th> <th>Z = X NOR Y</th> </tr> </thead> <tbody> <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> </tbody> </table>	X	Y	Z = X NOR Y	1	1	0	1	0	0	0	1	0	0	0	1		NOR
X	Y	Z = X NOR Y																	
1	1	0																	
1	0	0																	
0	1	0																	
0	0	1																	

الوحدة الرابعة أمن المعلومات والتشفير

عناصر (خصائص) أمن المعلومات.

1. السرية 2. السلامة 3. توافر المعلومات (التوافر)

أمثلة على بيانات يعتمد أمنها على مقدار الحفاظ على سريتها:

أ. المعلومات الشخصية ب. المعلومات العسكرية

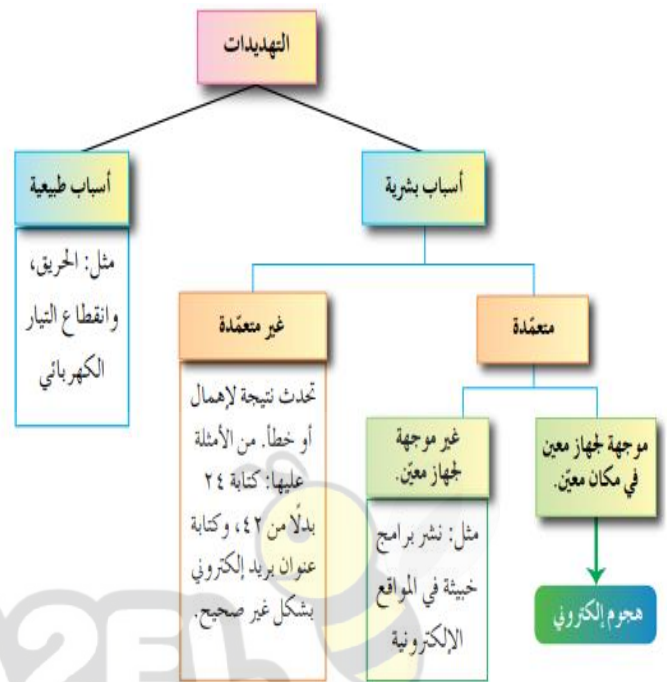
ج. الموقف المالي لشركة ما قبل إعلانه

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: 1. الثغرات 2. التهديدات



تقسم التهديدات البشرية المتعمدة إلى قسمين: 1. موجهة لجهاز معين

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

أمثلة على الهجومات (الاعتداء) الإلكتروني

1. سرقة جهاز الحاسوب أو أحد معدات حفظ المعلومات

2. التعديل على ملف أو حذفه 3. الكشف عن بيانات سرية

4. منع الوصول إلى المعلومات

عوامل نجاح الهجومات الإلكترونية:

عوامل رئيسية يجب أخذها بالحسبان لتقييم التهديد:

1- الدافع 2- الطريقة 3- فرصة النجاح

تنوع دوافع الأفراد عند تنفيذ الهجومات الإلكترونية:

1. الرغبة في إثبات القدرات التقنية 2. الإضرار بالآخرين

3. الرغبة في الحصول على المال

تتضمن الطريقة

1. معرفة نقاط القوة والضعف للنظام 2. المعرفة بتصميم النظام وآلية عمله

3. القدرة على توفير المعدات و البرمجيات الحاسوبية

4. المهارات التي يتميز بها المعتدي الإلكتروني

تتمثل فرصة النجاح في:

1. تحديد الوقت المناسب لتنفيذ الهجوم الإلكتروني

2. المعرفة بكيفية الوصول للأجهزة

أنواع الاعتداءات الإلكترونية على المعلومات:

1. التنصت على المعلومات 2. التعديل على المحتوى

3. الايقاف

4. الهجوم المفبرك او المزور

نوع الاعتداء الإلكتروني	الهدف من الاعتداء
1. التنصت على المعلومات	الحصول على المعلومات السرية (تؤثر على السرية)
2. التعديل على المحتوى	اعتراض المعلومات وتغيير محتواها وإعادة إرسالها للمستقبل (تؤثر على السلامة)
3. الايقاف	قطع قناة الاتصال ، لمنع المعلومات من الوصول للمستقبل (تؤثر على التوافر)
4. الهجوم المفبرك او المزور	ارسال المعتدي الإلكتروني رسالة إلى أحد الأشخاص على الشبكة يخبره فيها بأنه صديقه ويحتاج إلى معلومات أو كلمات سرية خاصة (تؤثر على السرية والسلامة)

أمثلة على الثغرات: 1- عدم تحديد صلاحيات الوصول إلى المعلومات

2- مشكلة في تصميم النظام

3- عدم كفاية الحماية المادية للأجهزة 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: 1. استخدام الجدران الاسوار و الاقفال

2. وجود حراس الأمن 3. أجهزة إطفاء الحريق

أمثلة على الضوابط الإدارية: 1. القوانين واللوائح و السياسات

2. الاجراءات التوجيهية 3. حقوق النشر

4. براءات الاختراع و العقود و الاتفاقيات

أمثلة على الضوابط التقنية: 1. كلمات المرور 2. التشفير

3. منح صلاحيات الوصول 4. بروتوكولات الشبكات والجدر النارية

5. تنظيم تدفق المعلومات في الشبكة

<p>وظيفة الجهاز الوسيط (موجهاً أو جداراً نارياً):</p> <p>1. تحويل العنوان الرقمي الداخلي إلى عنوان رقمي خارجي (عند التواصل خارج الشبكة) 2. تحويل العنوان الرقمي الخارجي إلى عنوان داخلي (عند الرد على رسالة الجهاز المرسل) من خلال سجل المتابعة لديه</p> <p>آليات عمل تقنية تحويل العناوين الرقمية.</p> <p>1. النمط الثابت للتحويل . 2. النمط المتغير للتحويل</p> <p>توضيح النمط الثابت للتحويل</p> <p>- تخصيص عنوان رقمي خارجي لكل جهاز داخلي</p> <p>- العنوان الرقمي ثابت لا يتغير.</p> <p>توضيح النمط المتغير للتحويل</p> <p>يتم إعطاء الجهاز عنوان رقمي مؤقت للتواصل خارج الشبكة وحين انتهاء الاتصال يفقد الجهاز الداخلي هذا العنوان ويصبح هذا العنوان متاحاً لأي جهاز آخر وقد يعطى عنواناً مختلفاً عند التراسل مرة أخرى</p>	<p>الهندسة الاجتماعية (التفصيل في الصفحة الأخيرة)</p> <p>تتركز الهندسة الاجتماعية في مجاله: البيئة المحيطة/الجانب النفسي</p> <p>تشمل البيئة المحيطة:</p> <p>أ. مكان العمل ب. الهاتف ج. النفايات الورقية د. الإنترنت</p> <p>الإنترنت أكثر الوسائل شيوعاً.</p> <p>الوسائل والأساليب التي يستخدمها المعتدي الإلكتروني للتأثير في الجانب النفسي على مستخدم الحاسوب وكسب ثقته:</p> <p>1- الاقناع 2- انتحال الشخصية والمداينة 3- مسابرة الركب</p>
<p>الهدف من علم التشفير:</p> <p>- الحفاظ على <u>سرية</u> المعلومات في أثناء تبادلها بين مرسل المعلومة ومستقبلها</p> <p>- عدم الاستفادة منها أو فهم محتواها حتى لو تم الحصول عليها من قبل أشخاص معترضين</p> <p>عناصر عملية التشفير: أ- خوارزمية التشفير ب- مفتاح التشفير ج- النص الأصلي د- نص الشيفرة</p>	<p>أهم الإنترنت</p> <p>الاعتداءات الإلكترونية على المواقع الإلكترونية (الويب)</p> <p>1. الاعتداء على متصفح الانترنت 2. الاعتداء على البريد الإلكتروني</p> <p>يتم الاعتداء على متصفح الانترنت بطريقتين:</p> <p>1. عن طريق كود بسيط يمكن إضافته إلى المتصفح وبإستطاعته القراءة والنسخ وإعادة الارسال لأي شيء يتم إدخاله من قبل المستخدم</p> <p>2. توجيه المستخدم إلى صفحة أخرى غير الصفحة التي يريدنا (الوصول إلى الحسابات المالية والبيانات الحساسة)</p> <p>توضيح الاعتداء على البريد الإلكتروني:</p> <p>يحاول المعتدي الإلكتروني التعامل مع الاشخاص قليلي الخبرة، حيث يقدم عروض شراء بعض المنتجات بأسعار زهيدة، أو رسائل مزيفة ومضللة "كيف تصبح ثرياً" وهذه الرسائل تحتوي روابط يتم الضغط عليه للحصول على معلومات إضافية</p>
<p>معايير تصنيف خوارزميات التشفير</p> <p>1- الآلية المستخدمة في التشفير 2- المفتاح المستخدم 3- كمية المعلومات المرسله</p> <p>يقسم التشفير المعتمد على آلية التشفير إلى نوعيه (طريقتيه):</p> <p>1. خوارزميات التعويض 2. خوارزميات التبديل</p> <p>يقسم التشفير المعتمد على المفتاح إلى نوعيه (قسميه):</p> <p>أ- خوارزميات المفتاح الخاص ب- خوارزميات المفتاح العام</p> <p>يقسم التشفير المعتمد على كمية المعلومات المرسله إلى نوعيه (قسميه)</p> <p>أذكرهما؟ 1- شيفرات التدفق 2- شيفرات الكتل</p>	<p>تقنية تحويل العناوين الرقمية (NAT)</p> <p>أيانا: السلطة المسؤولة عن منح أرقام الانترنت المخصصة لإعطاء العناوين الرقمية للأجهزة على الإنترنت</p> <p>مفهوم تقنية تحويل العناوين الرقمية NAT</p> <p>- 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).</p> <p>- تعطي الشبكة الداخلية كل جهاز داخل الشبكة عنوانا رقميا لغرض الاستخدام الداخلي فقط : أ. لا يعترف بهذا العنوان خارج الشبكة ب. يمكن أن يُلكر العناوين الرقمي للجهاز في أكثر من شبكة داخلية</p> <p>- 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)</p>
<p>مميزات خوارزمية الخط المتعرج:</p> <p>1. سهلة وسريعة 2. يمكن فك تشفيرها بسهولة 3. يمكن تنفيذها يدويا باستخدام ورقة وقلم</p>	<p>مميزات خوارزمية الخط المتعرج:</p> <p>1. سهلة وسريعة 2. يمكن فك تشفيرها بسهولة 3. يمكن تنفيذها يدويا باستخدام ورقة وقلم</p>

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

التوافر: 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. **(أخطر أنواع التهديدات)**

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 أو هدم النظام أو جعله عرضة للاعتداء الإلكتروني

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

الضوابط الإدارية: مجموعة من الأوامر والإجراءات 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 والأساليب التي يستخدمها المعتدي الإلكتروني، 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 الإلكترونية IP Address :عنوان رقمي خاص

لجهاز الحاسوب أو الهاتف الخليوي ، 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 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، كالتبديل 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

تعرض لها المعلومات والحد منها

تعد الهندسة الاجتماعية من أنجح الوسائل وأسهلها 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 . 1. للحد من الاعتداءات

والأخطار التي تهدده بسبب انتشار البرامج المقرصنة والمعلومات الخاصة

بكيفية اقتحام المواقع الالكترونية

علل: انتشرت البرامج والتطبيقات بشكل كبير منها (المجاني/المتنوع/غير

معروف المصدر)

بسبب اعتماد الأفراد على تكنولوجيا 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 الإنترنت

ظهور الحاجة إلى تقنية تحويل العناوين الرقمية NAT .

بسبب التطور الهائل في أعداد مستخدمي الإنترنت

علل : اختلاف IP Address للجهاز عند ترأسله 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 أبسطاً من شيفرات التدفق في عملية التشفير .

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

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 أو المعلومة في خوارزميات التشفير

المعتمد على المفتاح؟ على سرية المفتاح وليس على تفاصيل الخوارزمية

س : كيف يتم إنتاج المفاتيح في الخوارزميات اللاتناظرية ؟

يتم إنتاج المفاتيح من خلال عمليات رياضية ، ولا يمكن معرفة

المفتاح الخاص من خلال المفتاح العام

لحل مشكلة التطور الهائل في أعداد مستخدمي الإنترنت والحاجة إلى

عناوين إلكترونية أكثر :

1. طورت عناوين IPV4 إلى IPV6

2. 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 اللدري)	*. 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	شيفرات الكتل
تقسيم الرسالة إلى مجموعة أجزاء ، يشفر كل جزء منها على حدة ومن ثم يرسله	تقسم الرسالة إلى أجزاء ، ولكن بحجم معلومات أكبر ، 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 5 مقاطع بدلاً من 4 مقاطع
255,254,30,1	خطأ	تم الفصل بين المقاطع ب (,) بدلاً من (.)

ملاحظة : تعرض المواقع الإلكترونية لكثير من الاعتداءات الإلكترونية.

التي لا يشعر بها المستخدم كونها غير مرئية

- يعتمد اختيار الكادر البشري المسؤول عن أمن المعلومات و حماية الانظمة

1- الكفاية العلمية 2- الخضوع لاختبارات شفوية وورقية

3- المقابلات

4-أخضاعهم إلى ضغوط نفسية حسب موقعهم للتأكد من قدرتهم

على حماية النظام

الهندسة الإجتماعية / 1. يعد العنصر البشري من أهم مكونات أنظمة المعلومات

2- تعد الهندسة الاجتماعية من أخطر ما يهدد نظم المعلومات 3- تعد الهندسة الاجتماعية من أخطر الوسائل وأسهلها للحصول على المعلومات

تتركز الهندسة الاجتماعية في مجاله: 1. البيئة المحيطة 2. الجانب النفسي (يسعى المعتدي الإلكتروني لكسب ثقة مستخدم الحاسوب)

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

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

1- الإقناع 2- انتحال الشخصية والمداهنة 3- مسايرة الركب

آلية العمل	مجال (البيئة المحيطة)
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	1. مكان العمل
يتصل الشخص غير المخول بمركز الدعم الفني هاتفياً ، و يطلب إليه بعض المعلومات الفنية و يستدرجه للحصول على كلمات المرور وغيرها من المعلومات	2. الهاتف
يدخل الاشخاص غير المخولين الى مكان العمل ويجمعون النفايات التي قد تحتوي على (كلمات المرور و معلومات تخص الموظفين و أرقام هواتفهم و بياناتهم الشخصية) ، وقد تحتوي على تقييم العام السابق وكل ما يحتويه من معلومات يمكن استغلالها في تتبع أعمال الموظفين أو الحصول على المعلومات المرغوبة	3. النفايات الورقية
من أكثر الوسائل شيوعاً؛ (علل) وذلك بسبب استخدام الموظفين عادة كلمة مرور نفسها للتطبيقات جميعها ، حيث يثق المعتدي الإلكتروني موقفاً على الشبكة يقدم خدمات معينة، ويشترط التسجيل فيه للحصول على هذه الخدمات. يتطلب التسجيل اسم مستخدم وكلمة المرور وهي كلمة المرور نفسها الذي يستخدمها الشخص عادة، وبهذه الطريقة يتمكن المعتدي الإلكتروني من الحصول عليها.	4. الأترنت
آلية العمل	مجال (الجانب النفسي)
<p>– طريقة مباشرة: يستطيع المعتدي اقناع مستخدم الحاسوب من خلال تقديم الحجج والبراهين</p> <p>– طريقة غير مباشرة: بحيث يعتمد الى تقديم إبداءات نفسية تحت المستخدم على قبول المبررات من دون تحليلها أو التفكير فيها، وذلك عن طريق:</p> <p>1. إظهار نفسه بمظهر صاحب السلطة أو إغراء المستخدم امتلاك خدمة نادرة (كأن يقدم له عرضاً معيناً من خلال موقعه الإلكتروني لمدة محددة)، يمكنه ذلك من الحصول على كلمة المرور</p> <p>2. إبراز أوجه التشابه مع الشخص المستهدف(علل) لإقناعه بأنه يحمل الصفات والاهتمامات نفسها فيرتاح له الشخص فيقدم له ما يريد من معلومات</p>	1. الإقناع
يتقمص شخص شخصية آخر، فقد ينتحل شخصية (فني صيانة الحاسوب، عامل نظافة، المدير، السكرتير) وغالباً تكون ذات سلطة ولن يتردد الموظفين بتقديم المعلومات والخدمات لهذا الشخص	2. انتحال الشخصية والمداهنة
يرى الموظف بأنه إذا قام زملاؤه جميعهم بأمر ما، فمن غير اللائق أن يأخذ هو موقفاً مغايراً. مثال: يقدم شخص على انه إداري من فريق الدعم الفني ويرغب بعمل تحديثات على الاجهزة فإذا سمح له أحد الموظفين بذلك، فإن باقي الموظفين يقومون بمسايرة زميلهم غالباً ومن ثم يتمكن من الاطلاع على المعلومات التي يريدها.	3. مسايرة الركب