مكثف علوم الحاسوب

التوجيهي الأدبي/ الفصل الدراسي الثاني

الوحدة الثالثة: البوابات المنطقية

الوحدة الرابعة: أمن المعلومات والتشفير

أعزائي الطلاب والطالبات يحتوي هذا المكثف على مكثف الوحدة الأولى والوحدة الثانية من مبحث علوم الحاسوب / الثاني عشر (التوجيهي) /الفرع الأدبي

أرجو منكم دراسته جيداً ليلة الامتحان مع حل جميع الأسئلة الواردة بالمكثف بالإضافة للأسئلة من نمط ضع دائرة التي سيتم إرسالها لكم لاحقاً متمنياً من الله العلي القدير أن يوفقكم ويسعدني بنجاحكم وتفوقكم

الأستاذ إبراهيم الكردي0798237344

2024/2023

التعريفات الهامة في الوحدة الثالثة:

1. **التعبير العلائقي** هو جملة خبرية ناتجها إما صواب (1) وإما خطأ (0)، وتكتب هذه التعابير باستخدام عمليات المقارنة (<، >، =، =>، =<، <>).
2. **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.
3. **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).
4. **البوابة المنطقية:** دائرة الكترونية بسيطة، تقوم بعملية منطقية على مدخل واحد أو أكثر، وتنتج مخرجا منطقياً واحداً، وتستخدم في بناء معالجات الأجهزة الالكترونية والحواسيب.
5. **البوابة المنطقية AND:**
هي إحدى البوابات المنطقية الأساسية التي تدخل في بناء معظم الدوائر المنطقية ولها مدخلان ومخرج واحد وتسمى بوابة (**و**) المنطقية.
6. **البوابة المنطقية OR:**
هي إحدى البوابات المنطقية الأساسية التي تدخل في بناء معظم الدوائر المنطقية ولها مدخلان ومخرج واحد وتسمى (**أو**) المنطقية.
7. **البوابة المنطقية NOT:**
هي إحدى البوابات المنطقية الأساسية التي تدخل في بناء معظم الدوائر المنطقية، ولها مدخل واحد فقط ومخرج واحد ويطلق عليها **العاكس** أي أنها تغير القيمة المنطقية للمدخل إلى عكسه.(العاكس/ النفي/المتمم)
8. **جدول الحقيقة:** هو تمثيل لعبارة منطقية يبين الاحتمالات المختلفة للمتغيرات المكونة للعبارة المنطقية، ونتيجة هذه الاحتمالات، فعدد الاحتمالات في الجدول = 2^n حيث أن n تمثل عدد المتغيرات في العبارة المنطقية وكل متغير يأخذ قيمتين إما 0 أو 1. ما عدد احتمالات جدول الحقيقة للعبارة (x and y) ؟ **4**
9. **البوابة المنطقية المشتقة NAND :**
هي اختصار ل NOT AND أي نفي (AND) وتتشكل بوابة NAND بتوصيل مخرج بوابة AND بمدخل بوابة NOT وتسمى بوابة نفي (و) المنطقية.
10. **البوابة المنطقية المشتقة NOR :**
هي اختصار ل NOT OR أي نفي (OR) وتتشكل بوابة NOR بتوصيل مخرج بوابة OR بمدخل بوابة NOTوتسمى بوابة نفي (أو) المنطقية.
11. **الجبر البوولي (المنطقي):**
هو أحد فروع علم الجبر في الرياضيات، وهو الأساس الرياضي اللازم لدراسة التصميم المنطقي للأنظمة الرقمية ومنها الحاسوب وتعود تسميته إلى العالم الرياضي الانجليزي جورج بوول (George Boole).
12. **العبارة الجبرية المنطقية:**
هي ثابت منطق (0,1) أو متغير منطق مثل (X,Y) أو مزيج من الثوابت والمتغيرات المنطقية يجمع بينها عمليات منطقية، ويمكن أن تحتوي العبارة الجبرية المنطقية على أقواس وعلى أكثر من عملية منطقية.
13. **تمثيل العبارة المنطقية** يعني تحويل العبارة المنطقية رياضيا أي تمثيلها بالرسم باستخدام التعابير الجبرية المنطقية وعند تمثيلها يجب تطبيق قواعد الأولوية في الرسم.

تدريب1: استخرج من العبارة الآتية A> B OR NOT 0 ما يلي:

1) ثابت منطقي: 0
2) متغير منطقي: A
3) بوابة منطقية: OR
4) تعبير علائقي: A> B

تدريب 2: أعط مثالاً واحداً من عندك لكل مما يلي:

1)ثابت منطقي: 0	7) بوابة منطقية أساسية: and
2) متغير منطقي: a	8) بوابة منطقية مشتقة: nand
3) عملية مقارنة: <	9) تعبير منطقي بسيط: a and b
4) تعبير علائقي: a<b	10) تعبير منطقي مركب: a and b or c
5) معامل منطقي: and	11) رمز لعملية جبرية منطقية(بوولية): +
6) بوابة منطقية: and	12) تعبير /عبارة جبرية منطقية: a+ b

التعليلات الهامة في الوحدة الثالثة:

1) **تسميت البوابات المشتقة بهذا الاسم.**
لأنها اشتقت من البوابات المنطقية الأساسية AND,OR,NOT

2) **وجود دائرة صغيرة عند مخرج بوابة NAND.**
لأنها ترمز إلى البوابة NOT

3) **تسمية الجبر البوولي بهذا الإسم.**
نسبة للعالم الرياضي الإنجليزي جورج بوول.

4) **يطلق على عملية NOT بالجبر المنطقي اسم المتمم.**
لأن متممة 0 تساوي 1 ومتممة 1 هي 0

الملاحظات الهامة في الوحدة الثالثة:

1) يتكون **الحاسوب** من الكثير من **الدوائر المنطقية** التي تستخدم في معالجة البيانات الممثلة بالنظام الثنائي (1,0) وتتكون الدوائر المنطقية من عدد من **البوابات المنطقية.**

2) تعتمد البوابات المنطقية في عملها على مبدأ الصواب أو الخطأ أو ما يسمى رقميا 1 أو 0 (رموز النظام الثنائي) وهذا هو المبدأ الأساسي المستخدم في مدخلات هذه البوابات، والذي يتحكم بمخرجات الدوائر المنطقية.
وأقرب مثال على ذلك، الدارة الكهربائية البسيطة التي تحتوي مصباحاً كهربائياً ومفتاح توصيل، فعند **غلق الدارة** بواسطة المفتاح يضيء المصباح، وتمثل الحالة بالرمز الثنائي **(1)**، وعند **فتح الدارة** بواسطة المفتاح؛ ينطفئ المصباح، وتمثل هذه الحالة بالرمز الثنائي **(0)**.

3) 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).**

4) تستطيع تصميم دائرة كهربائية تمثل البوابة المنطقية **AND** بمفتاحي توصيل في وضعية **التوالي** بحيث يضيء المصباح عندما يكون **كلا** المفتاحين في حالة **إغلاق** فقط.

5) 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)**

6) تستطيع تصميم دائرة كهربائية تمثل البوابة المنطقية **OR** بمفتاحي توصيل في وضعية **التوازي** بحيث يضيء المصباح عندما يكون **أي** من المفتاحين أو **كلاهما** في حالة **إغلاق**.

7) يمكن أن يكون جدول الحقيقية بدلالة (0) و(1) ويمكن أن يكون بدلالة (F) و (T)

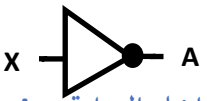
8) عدد **الخطوات** بعد تعويض قيم المتغيرات المنطقية يساوي عدد **البوابات** المنطقية في العبارة المنطقية.

9) عند كتابة العبارة المنطقية التي تمثلها البوابات المنطقية، يجب البدء من اليسار إلى اليمين، مع مراعاة قواعد الأولوية، فإذا أردت تنفيذ ORقبل AND ؛ فإنه يجب وضعها بين أقواس.

10)	تعطى بوابة NAND مخرجا قيمته(1) إذا كانت قيمة **أي** من المدخلين أو **كلاهما** (0). تعطي NAND مخرجا قيمته (0) إذا كانت قيمة المداخل **جميعها** (1) فقط . تكون مخرجات البوابة NAND عكس مخرجات البوابة AND.
11)	تعطى بوابة NOR مخرجاً قيمته (0) إذا كانت قيمة **أي** من المدخلين أو **كلاهما** (1) تعطي NOR مخرجاً قيمته (1) إذا كانت قيمة المداخل **جميعها** (0) تكون مخرجات البوابة NOR عكس مخرجات البوابة OR
12)	أولوية NAND تكافئ أولوية AND، وعدد الخطوات يساوي عدد البوابات.
13)	في حالة وجود أكثر من NAND في العبارة المنطقية تنفذ من اليسار إلى اليمين.
14)	العبارات المنطقية المكونة من بوابات مشتقة وبوابات أساسية (ما عدا NOT)، غير مطلوبة.
15)	يتكون جهاز **الحاسوب** من **مكونات مادية** مرتبطة معاً لتنفيذ مجموعة من **الوظائف**، ولتحديد هذه الوظائف وتنفيذها لا بد من فهم وظائف كل جزء من المكونات المادية وكيفية ارتباطه بالأجزاء الأخرى لتبادل المعلومات، وتحدد الوظائف وعمليات الربط من خلال **نموذج رياضي** (يمكن أن يمثل بعلاقات منطقية أو جبرية).
16)	قدم العالم **جورج بوول** الجبر البوولي للمرة الأولى في كتابه **(التحليل الرياضي للمنطق)**، وقام بتقديم أسس الجبر المنطقي بشكل واسع في كتابة الأشهر **(دراسة في قوانين التفكير)**، وأكد على أن استخدام صيغة جبرية في وصف عمل الحاسوب الداخلي أسهل من التعامل مع البوابات المنطقية.
17)	يسمى المتغير **متغيراً منطقياً** إذا عينت له إحدى الحالتين: صواب (True) أو خطأ (False).
18)	تستخدم أرقام نظام العد الثنائي 0 أو 1 لتمثيل حالات المتغير المنطقي فيمثل الرقم (1) الحالة الصحيحة والرقم (0) الحالة الخطأ.
19)	يرمز للمتغير المنطقي بأحد الحروف (A ... Z) لا أهمية لكون الحروف كبيرة أم صغيرة.

تمييز رموز البوابات المنطقية:

البوابة NOT



يشير X إلى مداخل البوابة و A مخرج البوابة
يعبر عنها بالعبارة المنطقية **A = NOT X**

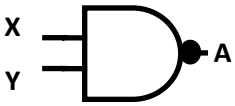
البوابة AND

تشير X,Y إلى مداخل البوابة و A مخرج البوابة
يعبر عنها بالعبارة المنطقية **A = X AND Y**

البوابة OR

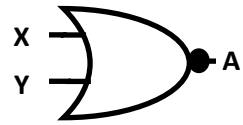
تشير X,Y إلى مداخل البوابة و A مخرج البوابة
يعبر عنها بالعبارة المنطقية **A = X OR Y**

البوابة NAND



تشير X,Y إلى مداخل البوابة و A مخرج البوابة
يعبر عنها بالعبارة المنطقية **A = X NAND Y**

البوابة NOR



تشير X,Y إلى مداخل البوابة و A مخرج البوابة
يعبر عنها بالعبارة المنطقية **A = X NOR Y**

أولويات التنفيذ للبوابات المنطقية الأساسية :

1 - ()
2 - NOT
3 - AND
4 - OR
5 - عند التكافؤ من اليسار لليمين

أولويات التنفيذ للبوابات المنطقية المشتقة :

1 - ()
2 - NOT
3 - NAND
4 - NOR
5 - عند التكافؤ من اليسار لليمين

جدول الحقيقة للبوابات المنطقية في الوحدة الثالثة:

A	B	A AND B اضرب	A OR B اجمع	A NAND B اضرب واعكس	A NOR B اجمع واعكس	NOT A اعكس
1	1	1	1	0	0	0
1	0	0	1	1	0	0
0	1	0	1	1	0	1
0	0	0	0	1	1	1

تدريب1: حدد اسم المعامل المناسب لكل من العبارات الآتية:

1) تعطي الناتج عكس المدخل: not
2) تعطي الناتج 0 فقط إذا كانت أحد المداخل 0 أو كلاهما 0: and
3) تعطي الناتج 1 فقط إذا كانت المداخل 1 فقط: and
4) تعطي الناتج 1 إذا كانت أحد المداخل 1 أو كلاهما 1: or
5) تعطي الناتج 0 إذا كانت المداخل 1 فقط: nand
6) تعطي الناتج 1 إذا كانت أحد المداخل 0 أو كلاهما 0: nand
7) تعطي الناتج 0 إذا كانت أحد المداخل 1 أو كلاهما 1: nor
8) تعطي الناتج 1 إذا كانت المداخل 0 فقط: nor

س3) تأمل العبارة الجبرية المنطقية الآتية

$$\overline{\overline{A} + \overline{B} + \overline{C} \cdot \overline{D}}$$

ثم أجب عن الأسئلة التي تليها:

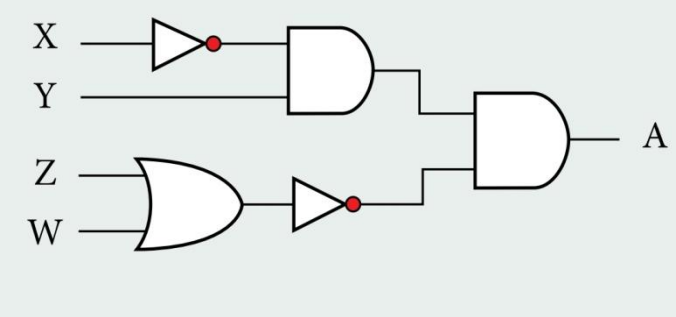
1) كم عدد المتغيرات المنطقية في العبارة؟ 4
2) كم عدد البوابات المنطقية في العبارة السابقة؟ 9
3) كم عدد الاحتمالات في جدول الحقيقة؟ 16
4) كم عدد خطوات الحل بعد تعويض قيم المتغيرات؟ 9

---

5) أوجد ناتج العبارة السابقة عندما: A=1,B=1,C=0,D=0؟

6) مثل العبارة المنطقية السابقة باستخدام البوابات المنطقية.

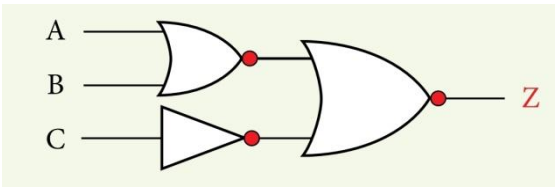
س4) تأمل البوابات المنطقية الآتية



ثم أجب عن الأسئلة الآتية:

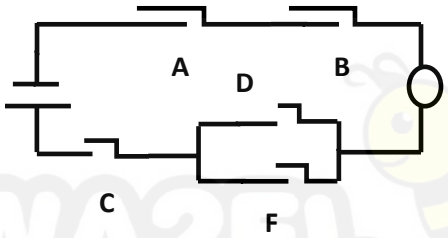
1) كم عدد المتغيرات المنطقية؟ 4
2) كم عدد البوابات المنطقية؟ 5
3) اكتب العبارة المنطقية المناسبة؟
4) اكتب العبارة الجبرية المنطقية؟
5) أوجد الناتج النهائي عندما: X=0,Y=0,Z=1,W=0

س5) تأمل البوابات المنطقية الآتية



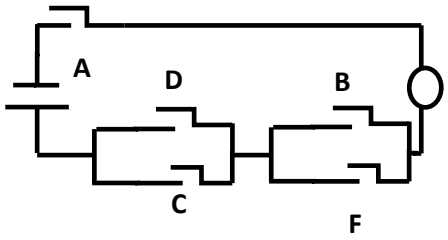
ثم أجب عن الأسئلة الآتية:

1) كم عدد المتغيرات المنطقية؟ 3
2) كم عدد البوابات المنطقية؟ 3
3) كم عدد البوابات المنطقية الأساسية؟ 1
4) كم عدد البوابات المنطقية المشتقة؟ 2
5) اكتب العبارة المنطقية المناسبة؟
6) ما قيمة Z عندما : A=0,B=1,C=0؟
7) أعد رسم البوابات المنطقية باستخدام البوابات المنطقية الأساسية فقط.



1) اكتب اسم العبارة المنطقية المناسبة للدارة الكهربائية السابقة. a and b and (d or f) and c

2) اكتب اسم العبارة الجبرية المنطقية للدارة الكهربائية السابقة. a.b.(d+f).c
3) أوجد الناتج النهائي عندما:
A=0,B=1,C=0,D=1,F=0



1) اكتب اسم العبارة المنطقية المناسبة للدارة الكهربائية السابقة.a and (b or f) and (d or c)
2) اكتب اسم العبارة الجبرية المنطقية للدارة الكهربائية السابقة. a.(b+f).(d +c)
3) أوجد الناتج النهائي عندما:
A=0,B=0,C=0,D=1,F=1

أكمل جدول الحقيقة الآتي:

A	B	C	NOT A OR NOT(B AND C)	NOT A NAND(B NAND C)	$\overline{(A+C)} \cdot \overline{B}$
1	1	1			
1		1	1		
	1	1	1		

س1) حول العبارات المنطقية الآتية إلى عبارات جبرية منطقية:

1) NOT C OR B AND NOT A OR NOT D
2) NOT (((NOT A OR NOT B) AND NOT C OR NOT D) OR NOT F)
3) NOT A OR NOT(((B OR NOT D AND C)AND NOT F)OR (K OR L))

س2) حول العبارات الجبرية المنطقية الآتية إلى عبارات منطقية:

1) $X = \overline{A} + B \cdot \overline{C + D}$

X= not a or not(b and not(c or d))

2) $X + \overline{Y} + (Z + \overline{W}) \cdot \overline{F}$

Not (x or not y) or not ((z or not w)and not f)

3) $(A + \overline{B}) + \overline{\overline{C} + \overline{D} \cdot F}$

Not((a or not b)or not(not c or not d)and f)

س3) حول العبارات المنطقية الآتية إلى عبارات منطقية باستخدام البوابات المنطقية الأساسية فقط:

1) **X= a nand b**

X= not(a and b)

2) **X= not (a nor not b)**

X= not(not (a or not b))

3) **X= not a nand not b**

X= not (not a and not b)

س4) حدد قيم Aو B و C: إذا كان ناتج العبارة المنطقية NOT A NAND NOT (B NAND C) يساوي (0)

س5) حدد قيمة C إذا علمت أن A=1,B=1 وناتج العبارة NOT(A AND (B OR NOT C)) يساوي (0)

مكثف علوم الحاسوب/الفصل الدراسي الثاني
إعداد الأستاذ إبراهيم الكردي 0798237344

الوحدة الرابعة: أمن المعلومات والتشفير

التعريفات الهامة في الوحدة الرابعة:

1. **أمن المعلومات:** هو العلم الذي يعمل على حماية المعلومات والمعدات المستخدمة لتخزينها ومعالجتها ونقلها من السرقة أو التطفل أو من الكوارث الطبيعية أو غيرها من المخاطر ويعمل على إبقائها متاحة للأفراد المصرح لهم باستخدامها.
2. **السرية:** السرية مصطلح مرادف لمفهومي **الأمن والخصوصية**، وتعني عدم القدرة على الحصول على المعلومات إلا من قبل الأشخاص المخول لهم ذلك. (أن الشخص المخول هو الوحيد القادر على الوصول إلى المعلومات والاطلاع عليها)
3. **السلامة:** حماية الرسائل أو المعلومات التي تم تداولها والتأكد بأنها لم تتعرض لأي عملية تعديل سواء: بالإضافة أم الاستبدال، أم حذف جزء منها.
4. **توافر المعلومات:** قدرة الشخص المخول الحصول على المعلومات في الوقت الذي يشاء من دون وجود عوائق.
5. **الهجوم الإلكتروني/ الاعتداء الإلكتروني : :** هو تهديد موجه ومتعمد لجهاز معين؛ بقصد الإضرار به.
6. **الثغرات:** هي نقطة الضعف في النظام سواء أكانت في الإجراءات المتبعة مثل عدم تحديد صلاحيات الوصول إلى المعلومات، أم مشكلة في تصميم النظام، كما أن عدم كفاية الحماية المادية للأجهزة والمعلومات.
7. **الضوابط المادية:** هي مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها باستخدام :
   1. الجدران والأسوار والأقفال.
   2. ووجود حراس الأمن.
   3. أجهزة إطفاء الحريق.
8. **الضوابط الإدارية:** هي مجموعة من الأوامر والإجراءات المتفق عليها مثل:
   1. القوانين واللوائح والسياسات.
   2. الإجراءات التوجيهية.
   3. حقوق النشر.
   4. براءات الاختراع والعقود والاتفاقيات.
9. **الضوابط التقنية:** هي الحماية التي تعتمد على التقنيات المستخدمة، سواء كانت معدات أو برمجيات وتتضمن:
   1. كلمات المرور.
   2. منح صلاحيات الوصول، وبرتوكولات الشبكات.
   3. الجدر النارية.
   4. التشفير.
   5. تنظيم تدفق المعلومات في الشبكة.
10. **الهندسة 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 .
11. **متصفح الانترنت:** هو برنامج ينقل المستخدم إلى صفحة (الويب) التي يريدها بمجرد كتابة العنوان والضغط على زر الذهاب ويمكّنه من استعراض المعلومات على الموقع.
12. **تقنية تحويل العناوين الرقمية:** هي تقنية تعمل على إخفاء العنوان الرقمي للجهاز في الشبكة الداخلية ليتوافق مع العنوان الرقمي المعطى للشبكة، ومن ثم فإن الجهاز الداخلي غير معروف بالنسبة إلى الجهات الخارجية وهذا يسهم في حمايته من أي هجوم قد يشن عليه بناء على معرفة العناوين الرقمية، وهي إحدى الطرائق المستخدمة لحماية المعلومات من الاعتداءات الالكترونية.
13. **العناوين الرقمية الإلكترونية:(IP Address)**
هو عنوان رقمي خاص لكل جهاز حاسوب أو أي هاتف خلوي يميزه عن غيره يرتبط بشبكة الانترنت، يتكون من 32 خانة ثنائية تتوزع على أربعة مقاطع يفصل بينها نقاط وكل مقطع من هذه المقاطع يتضمن رقماً من 0 إلى 255
14. **IANA:** هي السلطة المسؤولة عن منح أرقام الإنترنت المخصصة لإعطاء العناوين الرقمية للأجهزة على الإنترنت.

15.النمط الثابت لتحويل العناوين الرقمية:
طريقة يتم خلالها تخصيص عنوان رقمي خارجي لكل جهاز داخلي، وهذا العنوان الرقمي ثابت لا يتغير، يستخدمه الجهاز في كل مرة يرغب فيها بالاتصال مع الأجهزة خارج الشبكة.

16.النمط المتغير لتحويل العناوين الرقمية:
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.

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

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

19.الخوارزمية: مجموعة من الخطوات المتسلسلة منطقيا ورياضيا والتي تقوم بوصف حل مشكلة ما.

20.مفتاح التشفير: سلسلة من الرموز المستخدمة في خوارزمية التشفير وتعتمد قوة التشفير على قوة هذا المفتاح.

21.النص الأصلي في التشفير: محتوى الرسالة الأصلية قبل التشفير وبعد عملية فك التشفير.

22.نص الشيفرة: الرسالة بعد عملية التشفير.

23.تشفير التعويض: هي استبدال حرف مكان حرف أو مقطع مكان مقطع.

24.تشفير التبديل: يتم فيها تبديل أماكن الأحرف عن طريق إعادة ترتيب أحرف الكلمة بشرط استخدام الأحرف نفسها من دون إجراء أي تغيير عليها، وعند تنفيذ عملية التبديل يختفي معنى النص الحقيقي وهذا يشكل عملية التشفير شريطة أن تكون قادرا على استرجاع النص الأصلي منها وهذا ما يسمى عملية فك التشفير.

25.فك التشفير: عمليات إعادة الرسالة المشفرة إلى المحتوى الأصلي.

26.خوارزمية الخط المتعرج: هي خوارزمية تتميز بأنها سهلة وسريعة ويمكن تنفيذها يدوياً باستخدام الورقة والقلم، كما أنه يمكن فك تشفيرها بسهولة.

27.خوارزميات المفتاح الخاص (المفتاح السري):ويطلق عليها اسم الخوارزمية التناظرية:
يستخدم المفتاح نفسه لعمليتي التشفير وفك التشفير ويتم الاتفاق على اختياره قبل بدء عملية التراسل بين المرسل و المستقبل.

28.خوارزميات البحث العام (الخوارزميات اللاتناظرية)
تستخدم هذه الخوارزميات مفتاحين، أحدهما يستخدم لتشفير الرسالة ويكون معروفاً (للمرسل والمستقبل) ويسمى المفتاح العام والآخر يكون معروفاً لدى المستقبل فقط ويستخدم لفك التشفير ويسمى المفتاح الخاص
يتم إنتاج المفتاحين من خلال عمليات رياضية ولا يمكن معرفة المفتاح الخاص من خلال معرفة المفتاح العام.

29.شيفرات التدفق:
يعمل هذا النوع من الخوارزميات على تقسيم الرسالة إلى مجموعة أجزاء ويشفر كل جزء منها على حدة ومن ثم يرسله.

30.شيفرات الكتل:
تقسم الرسالة إلى أجزاء ولكن بحجم أكبر 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.

التعليلات الهامة في الوحدة الرابعة:

1) اهتمت الشعوب قديما بالحفاظ على سرية المعلومات.
أ - للحفاظ على أسرارها وهيبتها ومكانتها. ب- لإنجاح مخططاتها العسكرية.

2) كانت الحاجة أكثر إلحاحاً لإيجاد طرائق جديدة لحماية المعلومات.
لتطور العلم واستخدام شبكات الحاسوب.

3) يعد أمن المعلومات من أهم الركائز التى تعتمد عليها الدول والمؤسسات والأفراد .
للحفاظ على موقفها العالمي سياسياً ومالياً.

4) أصبح تناقل المعلومات والحصول عليها أمراً سهلاً.
للتطور الهائل الذي حصل في مجالي الانترنت والبرمجيات.

5) وجوب الاهتمام بكل ما يخص المعلومة.
بسبب وجود المخترقين والمتطفلين بشكل كبير.

6) استخدام مجموعة من الضوابط في نظم المعلومات.
لتقليل المخاطر التي تتعرض لها المعلومات والحد منها .

7) تعد الهندسة الاجتماعية من أنجح الوسائل وأسهلها للحصول على معلومات غير مصرح بالاطلاع عليها .
أ-بسبب قلة اهتمام المتخصصين في مجال أمن المعلومات. ب- عدم وعي مستخدمي الحاسوب بالمخاطر المترتبة عليها .

8) الانترنت من أكثر وسائل الهندسة الاجتماعية شيوعا.
بسبب استخدام الموظفين أو مستخدمي الحاسوب عادة كلمة المرور نفسها للتطبيقات جميعها .

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

10)غالبا ما تكون الشخصية المنتحلة ذات سلطة.
ليبدي الموظفين خدماتهم ولن يترددوا بتقديم أي معلومات لهذا الشخص المسؤول .

11)انتشار البرامج والتطبيقات بشكل واسع.
لاعتماد الأفراد والمؤسسات والحكومات على تكنولوجيا المعلومات والاتصالات والانترنت بشكل واسع وفي شتى المجالات.

12)لا بد من إيجاد وسائل تقنية تعمل على حماية الانترنت (الويب) والحد من الاعتداءات والأخطار التي تهددها.
أ-لانتشار البرامج والتطبيقات بشكل كبير . ب- لانتشار البرامج المقرصنة والمعلومات الخاصة بكيفية اقتحام المواقع.

13)الاعتداءات التي تتعرض لها المواقع الالكترونية التي لا يحس بها المستخدم.
كونها غير مرئية.

14)يتعرض متصفح الانترنت إلى الكثير من الأخطار.
لأنها قابلة للتغير من دون ملاحظة ذلك من قبل المستخدم.

15)ظهور IPv6 .
للتطور الهائل في أعداد المستخدمين ظهرت الحاجة إلى عناوين إلكترونية أكثر، يتكون من ثمانية مقاطع بدلا من أربعة .

16)عند استخدام تقنية تحويل العناوين الرقمية NAT تعطى الشبكة الداخلية عنوانا واحد (أو مجموعة عناوين) ويكون معرفا لها عند التعامل في شبكة الانترنت.
بسبب قلة أعداد هذه العناوين مقارنة بعدد المستخدمين.

17)اختلاف العنوان الرقمي للجهاز نفسه عند تراسله أكثر من مرة.
عند رغبة أحد الأجهزة بالتراسل خارجيا فإنه يتواصل مع الجهاز الوسيط الذي يعطيه عنوانا خارجيا مؤقتا يستخدمه لحين الانتهاء من عملية التراسل، ويعد هذا العنوان عنوانا رقميا خاصا بالجهاز.
عند انتهاء عملية التراسل يفقد الجهاز الداخلي هذا العنوان ويصبح العنوان متاحا للتراسل مرة أخرى.
عند رغبة الجهاز نفسه بالتراسل مرة أخرى قد يعطى عنوانا مختلفا عن المرة السابقة.

18)يعد التشفير من أفضل الطرق المستخدمة للحفاظ على أمن المعلومات.
حيث يعمل على إخفاء المعلومات عن الأشخاص غير المصرح لهم بالاطلاع عليها وعدم الاستفادة منها أو فهم محتواها حتى لو تم الحصول عليها من قبل أشخاص معترضين.

19)خوارزميات المفتاح الخاص يطلق عليها اسم الخوارزمية التناظرية:
يستخدم المفتاح نفسه لعمليتي التشفير وفك التشفير ويتم الاتفاق على اختياره قبل بدء عملية التراسل بين المرسل والمستقبل.

20)خوارزميات المفتاح العام (الخوارزميات اللاتناظرية)
تستخدم هذه الخوارزميات مفتاحين، أحدهما يستخدم لتشفير الرسالة ويكون معروفاً (للمرسل والمستقبل) ويسمى المفتاح العام والآخر يكون معروفاً لدى المستقبل فقط ويستخدم لفك التشفير ويسمى المفتاح الخاص.
يتم إنتاج المفتاحين من خلال عمليات رياضية ولا يمكن معرفة المفتاح الخاص من خلال معرفة المفتاح العام .

21)شيفرات الكتل بأن حجم المعلومات أكبر، لذا فإنها أبطأ.
تقسم الرسالة إلى أجزاء ولكن بحجم أكبر من حجم الأجزاء في شيفرات التدفق ويشفر أو يفك تشفير كل كتلة على حدة.

اعتمدت سرية المعلومات على:
1) موثوقية حاملها. 2) قدرته على توفير الظروف المناسبة لمنع اكتشافها.

طرق حماية المعلومات:
1. الطرق المادية.
2. الطرق لحماية قنوات الاتصال والمعلومات.
3. استخدام أساليب كثيرة لحماية المعلومات والأجهزة الخاصة فيها.
4. تدريب الكادر البشري وتوعيته.

- يجب الاهتمام بكل ما يخص المعلومات من **أجهزة التخزين، الاهتمام بالكادر البشري** الذي يتعامل معها، بالإضافة إلى **الحفاظ على المعلومات نفسها.**

الخصائص الأساسية لأمن المعلومات والتي يهدف أمن المعلومات للحفاظ عليها:
1. السريـة.
2. السلامـة.
3. توافر المعلومات.

أمثلة على معلومات سرية:
1)المعلومات الشخصية. 2) الموقف المالي لشركة ما قبل إعلانه. 3) المعلومات العسكرية.
4) بيانات يعتمد أمنها على مقدار الحفاظ على سريتها.

قد تتعرض الرسائل أو المعلومات الى عدة عمليات قد تؤثر على سلامتها، من هذه العمليات:
1) الإضافة. 2) الاستبدال. 3) الحذف (أي جزء منها).

أمثلة على سلامة المعلومات:
1. عند نشر نتائج طلبة الثانوية العامة يجب الحفاظ على سلامة هذه النتائج من أي تعديلات.
2. عند صدور قوائم القبول الموحد للجامعات الأردنية والتخصصات التي قبل بها الطلبة لابد من العمل على حماية هذه القوائم من أي حذف أو تبديل أو تغيير.

متى تكون المعلومات بلا فائدة:
1. إذا لم تكن متاحة للأشخاص المصرح لهم بالتعامل معها. 2. الوصول إليها يحتاج إلى وقت كبير .

من الوسائل التي يقوم بها المخترقون لجعل المعلومات غير متاحة:
1. حذفها. 2. الاعتداء على الأجهزة التي تخزن فيها هذه المعلومات .

تقسم المخاطر التي تهدد أمن المعلومات إلى نوعين رئيسيين: 1)التهديـدات. 2) الثغـرات.

تحدث التهديدات :

1 - لأسباب طبيعية: مثل (حدوث حريق) أو (انقطاع التيار الكهربائي) ، مما **يؤدي إلى فقدان المعلومات.**

2 - لأسباب بشرية:

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

ب - متعمدة وتقسم إلى قسمين:1) غير موجهة لجهاز معين، كأن ينشر فيروس. 2)موجهة لجهاز معين وهذا ما يسمى بالهجوم الإلكتروني أو الاعتداء الإلكتروني، ومن الأمثلة عليها سرقة جهاز الحاسوب، أو إحدى المعدات التي تحفظ المعلومات، أو التعديل على ملف أو حذفه، أو الكشف عن بيانات سرية أو منع الوصول إلى المعلومات.

يعد الاعتداء الإلكتروني من أخطر أنواع التهديدات، ويعتمد نجاح هذا الهجوم على ثلاثة عوامل رئيسة يجب أخذها في الحسبان لتقييم التهديد الذي يتعرض له النظام وهي:

1) الدافـــع. 2) الطريقـــة. 3)فرصـة النـــجاح.

ما هي دوافع الأفراد لتنفيذ الهجوم الإلكتروني؟

1) رغبة في الحصول على المال.
2) محاولة لإثبات القدرات التقنية.
3) الإضرار بالآخرين.

ماذا تتضمن الطريقة لتنفيذ الهجوم الإلكتروني؟

1) المهارات التي يتميز بها المعتدي الإلكتروني.
2) قدرة المعتدي على توفير المعدات والبرمجيات الحاسوبية التي يحتاج إليها.
3) معرفة المعتدي بتصميم النظام وآلية عمله.
4) معرفة نقاط القوة والضعف لهذا النظام.

ماذا تتضمن فرصة نجاح الهجوم الإلكتروني؟

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

تتعرض المعلومات إلى أربعة أنواع من الاعتداءات الإلكترونية،اذكرها مع التوضيح.

1) **التنصت على المعلومات:** والهدف منه الحصول على **المعلومات السرية**، حيث يتم الإخلال بسريتها.
2) **التعديل على المحتوى:** يتم اعتراض المعلومات وتغيير محتواها وإعادة إرسالها للمستقبل، من دون أن يعلم بتغيير محتواها، وفي هذا النوع يكون الإخلال **بسلامة المعلومات**.
3) **الإيقاف:** يتم قطع قناة الاتصال ومن ثم منع المعلومات من الوصول إلى المستقبل وفي هذه الحالة تصبح المعلومات **غير متوافرة**.
4) **الهجوم المزور أو المفبرك:** يتمثل هذا النوع بإرسال المعتدي الإلكتروني رسالة إلى أحد الأشخاص على الشبكة يخبره فيها بأنه صديقه ويحتاج إلى معلومات أو كلمات سرية خاصة. تتأثر بهذه الطريقة **سرية المعلومات** وقد تتأثر أيضاً **سلامتها**.

ماذا تسبب نقاط الضعف ؟

1) فقدان المعلومات. 2) هدم النظام. 3) تجعله عرضة للاعتداء الإلكتروني.

حسب رأي المختصون في مجال أمن المعلومات فإن الحفاظ على المعلومات وأمنها ينبع من التوازن بين:

1) تكلفة الحماية وفعالية الرقابة من جهة. 2) احتمالية الخطر من جهة أخرى.

هناك مجموعة من الضوابط التي وضعت لتقليل المخاطر التي تتعرض لها المعلومات والحد منها، اذكرها.

1) الضوابط المادية. 2) الضوابط الإدارية. 3) الضوابط التقنية.

عدد أمثلة على الضوابط المادية.

1) الجدران والأسوار والأقفال. 2) ووجود حراس الأمن. 3) أجهزة إطفاء الحريق.

عدد أمثلة على الضوابط الإدارية.

1) القوانين واللوائح والسياسات. 2) الإجراءات التوجيهية. 3) حقوق النشر. 4) براءات الاختراع والعقود والاتفاقيات.

عدد أمثلة على الضوابط التقنية.

1) كلمات المرور. 2) منح صلاحيات الوصول، وبرتوكولات الشبكات. 3) الجدر النارية. 4) التشفير.
5) تنظيم تدفق المعلومات في الشبكة.

ملاحظة:

للوصول إلى أفضل النتائج، وللحد من الأخطار التي تتعرض لها المعلومات، يجب أن تعمل ضوابط التقليل من المخاطر التي تتعرض لها المعلومات بشكل متكامل.

اختيار الكادر البشري المسؤول عن حماية الأنظمة يعتمد على عدة أمور:

1) الكفاية العلمية.
2) اختبارات شفوية وورقية.
3) المقابلة.
4) إخضاعهم إلى ضغوط نفسية كل حسب موقعهم ويكون ذلك للتأكد من قدرتهم على حماية النظام.

المجالات التي ترتكز عليها الهندسة الاجتماعية:

1) البيئة المحيطة : **تشمل ما يأتي:**(مكان العمل/ الهاتف/ النفايات الورقية/الإنترنت)
2) الجانب النفسي: **تشمل ما يأتي**(الإقناع/انتحال الشخصية/ مسايرة الركب أو المداهنة)

أولاً: البيئة المحيطة:

مكان العمل: مثال توضيحي

يكتب بعض الموظفين كلمات المرور على أوراق ملصقة بشاشة الحاسوب وعند دخول الشخص غير المخول له الاستخدام كزبون أو عامل نظافة أو عامل صيانة، يستطيع معرفة كلمات المرور ومن ثم يتمكن من الدخول إلى النظام بسهولة ليحصل على المعلومات التي يريدها.

الهاتف: مثال توضيحي

تصل الشخص غير المخول بمركز الدعم الفني هاتفيا، ويطلب إليه بعض المعلومات الفنية ويستدرجه للحصول على كلمات المرور وغيرها من المعلومات؛ ليستخدمها في ما بعد.

النفايات الورقية: مثال توضيحي

يدخل الأشخاص غير المخولين إلى مكان العمل ويجمعون النفايات التي قد تحتوي على كلمات المرور ومعلومات تخص الموظفين وأرقام هواتفهم وبياناتهم الشخصية، وقد تحتوي على تقويم العام السابق وكل ما يحتويه من معلومات، يمكن استغلالها في تتبع أعمال الموظفين أو الحصول على المعلومات المرغوبة.

الانترنت: مثال توضيحي

آلية عمل الهندسة الاجتماعية في مجال الانترنت:

حيث ينشئ المعتدي الالكتروني موقعا على الشبكة، يقدم خدمات معينة ويشترط التسجيل فيه للحصول على هذه الخدمات. يتطلب التسجيل في الموقع اسم مستخدم وكلمة مرور وهي كلمة المرور نفسها التي يستخدمها الشخص عادة وبهذه الطريقة يتمكن المعتدي الالكتروني من الحصول عليها.

ثانياً: الجانب النفسي:

الاقناع: مثال توضيحي

يسعى المعتدي من خلال الجانب النفسي إلى:

1) كسب ثقة مستخدم الحاسوب. 2) الحصول على المعلومات التي يرغب بها.

يقنع المعتدي الموظف أو مستخدم الحاسوب ب:

أ - **طريقة مباشرة** : يقدم الحجج المنطقية والبراهين.

ب - **طريقة غير مباشرة**:

1 -تقديم إيحاءات نفسية، تحث المستخدم على قبول المبررات من دون تحليلها أو التفكير فيها ويحاول التأثير بهذه الطريقة .

2 - إظهار نفسه بمظهر صاحب السلطة .

3 - إغراء المستخدم بامتلاك خدمات نادرة (يقدم له عرضا معينا من خلال موقعه الالكتروني لمدة محدد يمكنه ذلك من الحصول على كلمة المرور).

4 -إبراز أوجه التشابه مع الشخص المستهدف لإقناعه بأنه يحمل الصفات والاهتمامات نفسها فيصبح الشخص أكثر ارتياحا وأقل حذرا للتعامل معه فيقدم له ما يريد من معلومات.

انتـحال الشخــصية: مثال توضيحي

آلية عمل الهندسة الاجتماعية في مجال انتحال الشخصية:

يتقمص شخص شخصية آخر وهذا الشخص قد يكون **شخصا حقيقيا** أو **وهميا**، فقد ينتحل شخصية فني صيانة معدات الحاسوب أو عامل نظافة أو حتى المدير أو السكرتير.

غالبا ما تكون الشخصية المنتحلة ذات سلطة، حتى يبدي الموظفين خدماتهم ولن يترددوا بتقديم أي معلومات لهذا الشخص المسؤول.

مسايرة الركب أو المداهنة: مثال توضيحي

آلية عمل الهندسة الاجتماعية في مجال مسايرة الركب التي يستخدمها المعتدي للاطلاع على المعلومات:

1) يرى الموظف بأنه إذا قام زملاؤه جميعا بأمر ما فمن غير اللائق أن يأخذ هو موقفا مغايراً.
2) 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 زميلهم غالبا والسماح لهذا المعتدي باستخدام أجهزتهم لتحديثها ومن ثم يتمكن من الاطلاع على المعلومات التي يريدها والمخزنة على الأجهزة.

أصناف البرامج والتطبيقات المستخدمة:

1) مجاني.
2) غير معروف المصدر.
3) مفتوح. التطبيقات (البرامج) المفتوحة: هي التي يمكن استخدامها على الأجهزة المختلفة.

أنواع الاعتداءات التي تتعرض لها المواقع الالكترونية التي لا يحس بها المستخدم كونها غير مرئية:

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

يتم الاعتداء على متصفح الانترنت بطريقتين:

1) الاعتداء عن طريق (كود) بسيط، يمكن إضافته إلى المتصفح وباستطاعته القراءة، والنسخ، وإعادة إرسال أي شيء يتم إدخاله من قبل المستخدم.
2) توجيه المستخدم إلى صفحة أخرى غير الصفحة التي يريدها.

يتمثل التهديد بالاعتداء على متصفح الانترنت عن طريق (كود) بسيط بـ :

القدرة على الوصول إلى الحسابات المالية والبيانات الحساسة الأخرى.

يتم الاعتداء الالكتروني على البريد الالكتروني بعدة طرق منها:

1) تصل الكثير من الرسائل الالكترونية إلى البريد الالكتروني، بعض هذه الرسائل الالكترونية مزيفة وبعضها يسهل اكتشافه وبعضها الآخر استخدم بطريقة احترافية.
2) يحاول المعتدي الالكتروني التعامل مع الأشخاص القليلي الخبرة حيث يقدم عروض شراء لمنتجات بعض المصممين

بأسعار زهيدة أو رسائل تحمل عنوان كيف تصبح ثرياً.

3) هذه الرسائل تحتوي روابط للمزيد من المعلومات يرجى الضغط عليه ، وغيرها من الرسائل المزيفة والمضللة التي تحتاج إلى وعي من المستخدم.

العناوين الرقمية الإلكترونية:(IP Address)

هو عنوان رقمي خاص لكل جهاز حاسوب أو أي هاتف خلوي يميزه عن غيره يرتبط بشبكة الانترنت، يتكون من 32 خانة ثنائية تتوزع على أربعة مقاطع يفصل بينها نقاط وكل مقطع من هذه المقاطع يتضمن رقماً من 0 إلى 255 ويشكل (IPv4) أو يتكون من ثمانية مقاطع ويشكل(IPv 6)

أنواع IP Address :(ipv6/ ipv4)

IPv4 : يتكون من (32) خانة ثنائية تتوزع على أربعة مقاطع يفصل بينها نقاط كل مقطع من هذه المقاطع يتضمن رقم من (0 إلى 255)

مثال: 215.005.006.153

علل: ظهورIPv6 : نظرا للتطور الهائل في أعداد المستخدمين ظهرت الحاجة إلى عناوين إلكترونية أكثر وطورت هذه العناوين لما يسمىIPv6 ، يتكون من ثمانية مقاطع بدلا من أربعة.

على الرغم من استخدام IPv6 إلا انه لا يكفي لتوفير عدد هائل من العناوين الرقمية ولحل هذه المعضلة وجد ما يسمى **تقنية تحويل العناوين الرقمية ((Network Address Tranlation (NAT)**

تقنية تحويل العناوين الرقمية:

هي تقنية تعمل على إخفاء العنوان الرقمي للجهاز في الشبكة الداخلية ليتوافق مع العنوان الرقمي المعطى للشبكة، ومن ثم فإن الجهاز الداخلي غير معروف بالنسبة إلى الجهات الخارجية وهذا يسهم في حمايته من أي هجوم قد يشن عليه بناء على معرفة العناوين الرقمية، وهي إحدى الطرائق المستخدمة لحماية المعلومات من الاعتداءات الالكترونية.

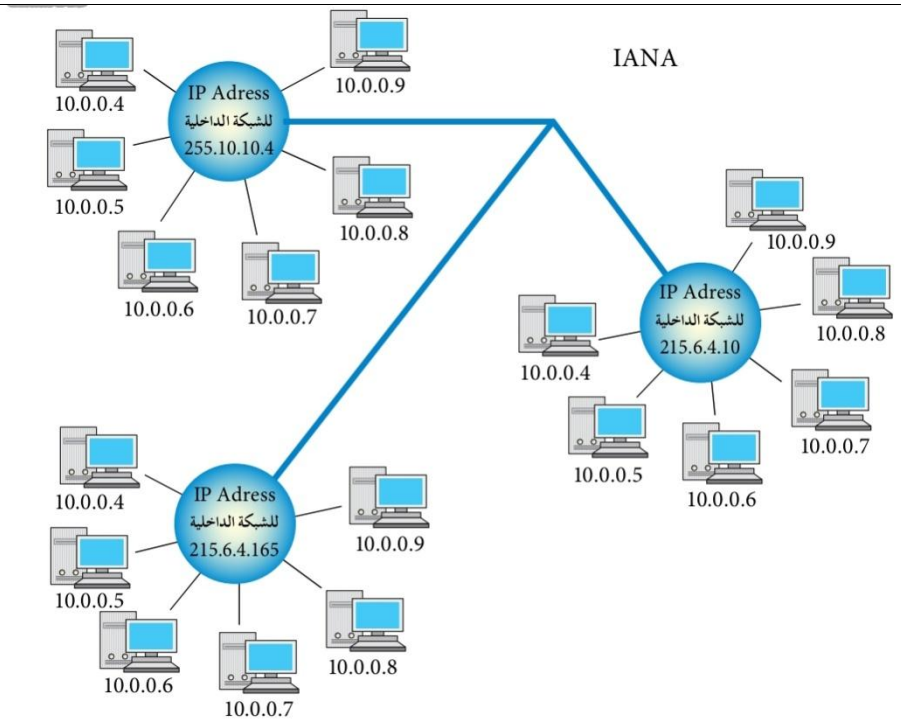
أهمية استخدام تقنية تحويل العناوين الرقمية:

هي إحدى الطرق المستخدمة لحماية المعلومات (الويب) من الاعتداءات الالكترونية.

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

علل: عند استخدام تقنية تحويل العناوين الرقمية NAT تعطى الشبكة الداخلية عنوانا واحد (أو مجموعة عناوين) ويكون معرفا لها عند التعامل في شبكة الانترنت.

بسبب قلة أعداد هذه العناوين مقارنة بعدد المستخدمين.



الشكل (٤– ٢): العناوين الرقمية للشبكات والأجهزة.

تعمل تقنية تحويل العناوين الرقمية بعدة طرق: 1)النمط الثابت للتحويل. 2)النمط المتغير للتحويل.

أولاً النمط الثابت لتحويل العناوين الرقمية:

طريقة يتم خلالها تخصيص عنوان رقمي خارجي لكل جهاز داخلي، وهذا العنوان الرقمي **ثابت لا يتغير**، يستخدمه الجهاز في كل مرة يرغب فيها بالاتصال مع الأجهزة خارج الشبكة.

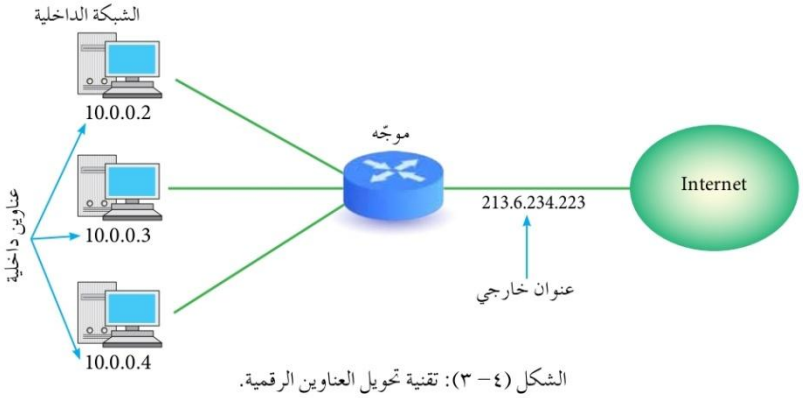
ثانياً النمط المتغير لتحويل العناوين الرقمية:

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.

وظيفة الجهاز الوسيط الموجود في الشبكة الداخلية:

عند رغبة أحد الأجهزة بالتواصل مع جهاز خارج الشبكة الداخلية يعدل العنوان الرقمي الخاص به باستخدام تقنية تحويل العناوين الرقميةNAT وذلك باستخدام **جهاز وسيط** حيث يكون غالباً **موجهاً** (Router) أو **جداراً نارياً** إلى عنوان رقمي خارجي ويسجل ذلك في سجل خاص للمتابعة.

ويتم التواصل مع الجهاز الهدف في الشبكة الأخرى عن طريق الرقم الخارجي على أنه العنوان الخاص بالجهاز المرسل، وعندما يقوم الجهاز الهدف بالرد على رسالة الجهاز المرسل تصل إلى الجهاز الوسيط الذي يحول العنوان الرقمي الخارجي إلى عنوان داخلي من خلال سجل المتابعة لديه، ويعيده بذلك إلى الجهاز المرسل.



الشكل (٤ – ٣): تقنية تحويل العناوين الرقمية.

علل: اختلاف IP Address للجهاز نفسه عند تراسله أكثر من مرة:

- عند رغبة أحد الأجهزة بالتراسل خارجيا فإنه يتواصل مع الجهاز الوسيط الذي يعطيه عنوانا خارجيا مؤقتا يستخدمه لحين الانتهاء من عملية التراسل، ويعد هذا العنوان عنوانا رقميا خاصا بالجهاز.
- عند انتهاء عملية التراسل يفقد الجهاز الداخلي هذا العنوان ويصبح العنوان متاحا للتراسل مرة أخرى.
- عند رغبة الجهاز نفسه بالتراسل مرة أخرى قد يعطى عنوانا مختلفا عن المرة السابقة وهذا ما يفسر اختلاف IP Addressللجهاز نفسه عند تراسله أكثر من مرة.

ملاحظة:

في طريقة النمط المتغير للتحويل يكون لدى الجهاز الوسيط عدد من العناوين الرقمية الخارجية ولكنها غير كافية لعدد الأجهزة في الشبكة هذه العناوين تبقى متاحة لجميع الأجهزة على الشبكة.

التشفير: ظهرت الحاجة للحفاظ على سرية المعلومات منذ قدم البشرية في المجالين العسكري والدبلوماسي خاصة، تم منذ آنذاك إيجاد الوسائل التي يمكن نقل الرسائل عن طريقها والمحافظة على سريتها في الوقت نفسه، مع تطور العلم والوسائل التكنولوجية الحديثة كان لا بد من إيجاد طرائق لحمايتها.

يهدف التشفير إلى:

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

تتضمن عملية التشفير أربعة عناصر أساسية هي:

1)خوارزمية التشفير. 2) مفتاح التشفير. 3)النص الأصلي. 4) نص الشيفرة.

تصنف خوارزميات التشفير بناء على عدة معايير: (أنواع خوارزميات التشفير):

1) التشفير المعتمد على العملية(الآلية) المستخدمة في التشفير.
2) التشفير المعتمد على المفتاح المستخدم.
3) التشفير المعتمد على كمية المعلومات المرسلة.

مثال على طريقة التشفير بالتعويض: شيفرة الإزاحة.

مثال على طريقة التشفير بالتبديل: خوارزمية الخط المتعرج.

ميزات خوارزمية الخط المتعرج:

1)سهلة وسريعة. 2)يمكن تنفيذها ورقياً باستخدام الورقة والقلم. 3) يمكن فك تشفيرها بسهولة.

ملاحظات هامة:

- مفتاح التشفير يتم الاتفاق عليه مسبقاً من قبل مرسل الرسالة ومستقبلها فقط.
- استخدام المثلث المقلوب بديلاً للفراغ لغايات تسهيل الحل فقط.
- يمكن تشفير أحرف اللغة العربية باستخدام هذه الخوارزميات ولكنها غير متضمنة في الكتاب وغير مطلوبة من الطلبة.
- تشفير نص يحتوي على علامات ترقيم غير متضمن وغير مطلوب في هذا الكتاب.

خطوات التشفير باستخدام خوارزمية الخط المتعرج:

1. حدد عدد الأسطر التي ستستخدم لتشفير النص حيث أن عدد الأسطر، يعد مفتاح التشفير ويتم الاتفاق عليه مسبقا من قبل مرسل الرسالة.
2. املأ الفراغ في النص الأصلي بمثلث مقلوب.
3. أنشئ جدولا يعتمد على عدد الأسطر (مفتاح التشفير).
4. وزع أحرف النص المراد تشفيره بشكل قطري حسب اتجاه الأسهم.
5. ضع مثلث مقلوب في الفراغ الأخير كي تكون الأطوال متساوية.
6. أكتب النص المشفر سطراً سطراً.

مثال: جد النص المشفر للنص الأصلي الآتي، علماً بأن مفتاح التشفير هو خمسة أسطر.

Stay positive this year makes you happy all life

s		p		i		H		e		a		y		a		A		i		
	t		o		v		i		a		k		o		p		l		f	
		a		s		E		s		r		e		u		P		l		e
			y		i		▼		▼		▼		S		▼		y		▼		▼
				▼		T		t		y		m		▼		H		▼		l		▼

النص المشفر هو :

خطوات فك التشفير:

1) املأ الفراغات بمثلث مقلوب.
2) قسم النص المشفر إلى أجزاء، اعتماداً على عدد الأسطر (مفتاح التشفير)، أي أن عدد الأجزاء يساوي عدد الأسطر.
3) عدد الأحرف في كل جزء= مجموع أحرف النص المشفر(بما فيها الفراغات) / عدد الأجزاء.
4) اكتب الحرف الأول من كل جزء، ثم الحرف الثاني، ثم الحرف الثالث وهكذا.

مثال: جد النص الأصلي للنص المشفر الآتي، علماً بأن مفتاح التشفير ثلاثة أسطر.

sdhdtya▼u▼r▼

عدد الأعمدة= مجموع الحروف+ الفراغات /عدد الأسطر

= 12/3= 4

s	D	H	D
t	Y	A	▼
u	▼	R	▼

النص الأصلي بعد فك التشفير هو study hard

تصنيف خوارزميات التشفير المعتمد على المفتاح

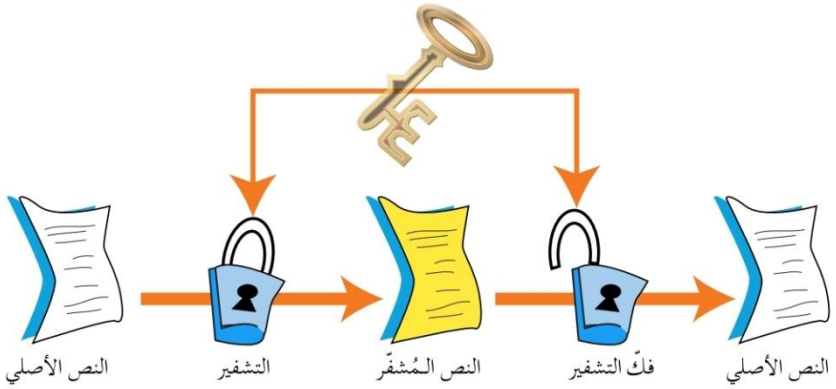
يعتمد هذا النوع من خوارزميات التشفير على عدد المفاتيح المستخدمة في عملية التشفير وعليه فإن أمن الرسالة أو المعلومة يعتمد على سرية المفتاح وليس على تفاصيل الخوارزمية .

أنواع التشفير المعتمد على المفتاح:

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

أولاً: خوارزميات المفتاح الخاص (المفتاح السري):ويطلق عليها اسم الخوارزمية التناظرية:

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

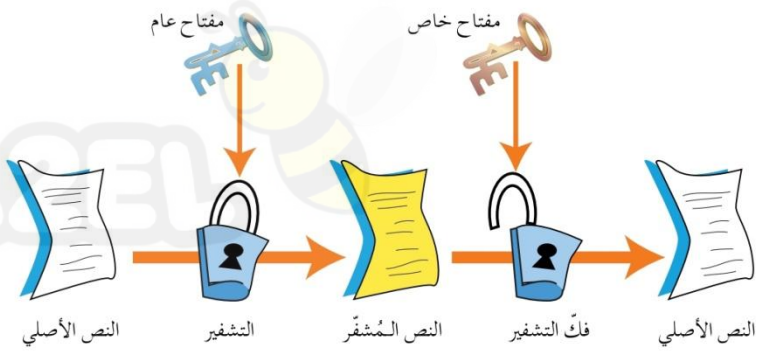


الشكل (٤–٥): خوارزمية المفتاح الخاص.

ثانياً: خوارزميات المفتاح العام (الخوارزميات اللاتناظرية)

تستخدم هذه الخوارزميات **مفتاحين**، أحدهما يستخدم لتشفير الرسالة ويكون معروفاً (للمرسل والمستقبل) ويسمى المفتاح العام والآخر يكون معروفاً لدى المستقبل فقط ويستخدم لفك التشفير ويسمى المفتاح الخاص

يتم إنتاج المفتاحين من خلال **عمليات رياضية** ولا يمكن معرفة المفتاح الخاص من خلال معرفة المفتاح العام.



الشكل (٤–٦): خوارزمية المفتاح العام.

أنواع التشفير المعتمد على كمية المعلومات المرسلة:

1) شيفرات التدفق
2) شيفرات الكتل

شيفرات التدفق: يعمل هذا النوع من الخوارزميات على تقسيم الرسالة إلى مجموعة أجزاء ويشفر كل جزء منها على حدة ومن ثم يرسله.

شيفرات الكتل: تقسم الرسالة إلى أجزاء ولكن **بحجم أكبر** 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**.

انتهى مكثف الوحدة الرابعة / كل التوفيق والنجاح لجميع الطلاب