سلسلة النور التعليمية

علوم الحاسوب

التوجيهي/الفرع الأدبي

الفصل الدراسي الثاني

الوحدة الثالثة/الأساس المنطقي للحاسوب والبوابات المنطقية

الوحدة الرابعة/ أمن المعلومات والتشفير

2020/2021

إعداد الأستاذ
إبراهيم الكردي
0798237344

الوحدة الثالثة: الأساس المنطقي للحاسوب، والبوابات المنطقية

البوابات المنطقية

الفصل الأول : البوابات المنطقية

يتكون الحاسوب من الكثير من الدوائر المنطقية التي تستخدم في معالجة البيانات الممثلة بالنظام الثنائي (1,0)

تتكون الدوائر المنطقية من عدد من البوابات المنطقية.

مفاهيم هامة :

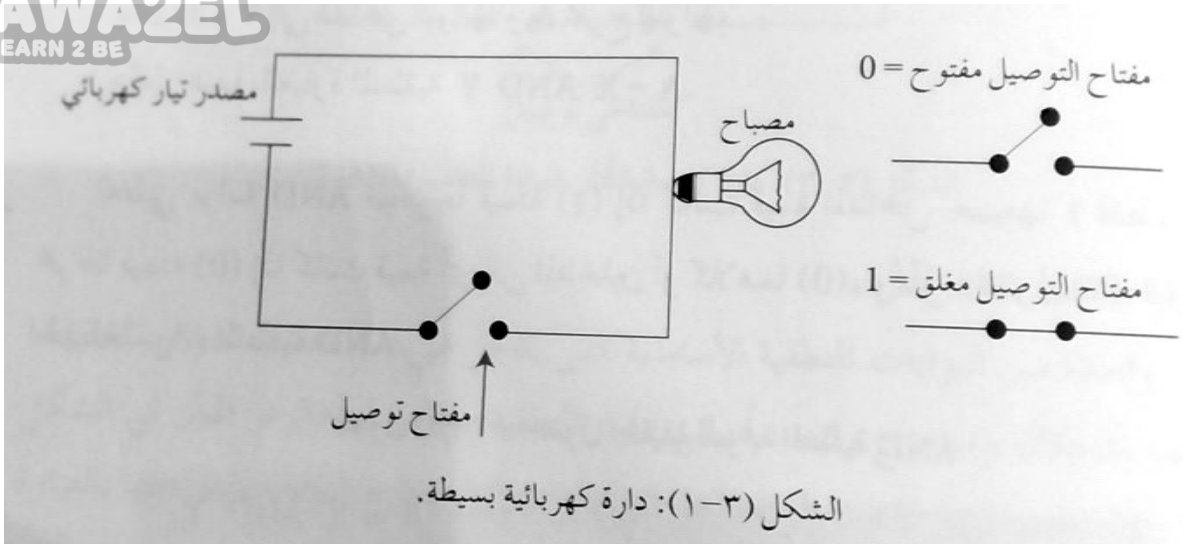
- **التعبير العلائقي:** هو جملة خبرية ناتجها إما صواب (1) وإما خطأ (0)، وتكتب هذه التعابير باستخدام عمليات المقارنة (>، <، =، <=، =>، <>).
- **المعامل المنطقي:** هو رابط يستخدم للربط بين تعبيرين علائقيين أو أكثر؛ لتكوين عبارة منطقية مركبة ومن أهمها AND،OR أو نفي تعبير منطقي باستخدام NOT.
- **العبارة المنطقية المركبة:** جملة خبرية تتكون من تعبيرين علائقيين أو أكثر، يربط بينهما معاملات منطقية (And , Or) وتكون قيمتها إما صوابا (1) أو خطأ (0).

أولاً مفهوم البوابات المنطقية:

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

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)، انظر الشكل (3-1)



الشكل (٣–١): دارة كهربائية بسيطة.

ثانياً أنواع البوابات المنطقية:

تعرف البوابات المنطقية، أنواعها وآلية عملها

تقسم البوابات المنطقية إلى:

- البوابات المنطقية الأساسية (NOT, AND, OR)
- البوابات المنطقية المشتقة (NAND, NOR)

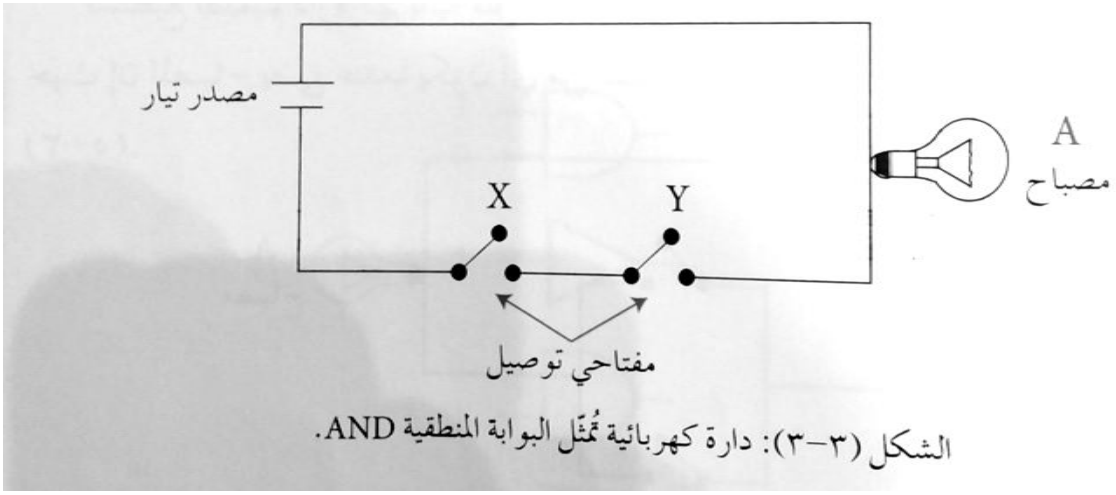
البوابة المنطقية AND:

- هي إحدى البوابات المنطقية الأساسية التي تدخل في بناء معظم الدوائر المنطقية ولها مدخلان ومخرج واحد وتسمى بوابة (**و**) المنطقية.

آلية 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).

- تستطيع تصميم دائرة كهربائية تمثل البوابة المنطقية AND بمفتاحي توصيل في وضعية **التوالي** بحيث يضيء المصباح عندما يكون كلا المفتاحين في حالة إغلاق فقط انظر الشكل (3-3)



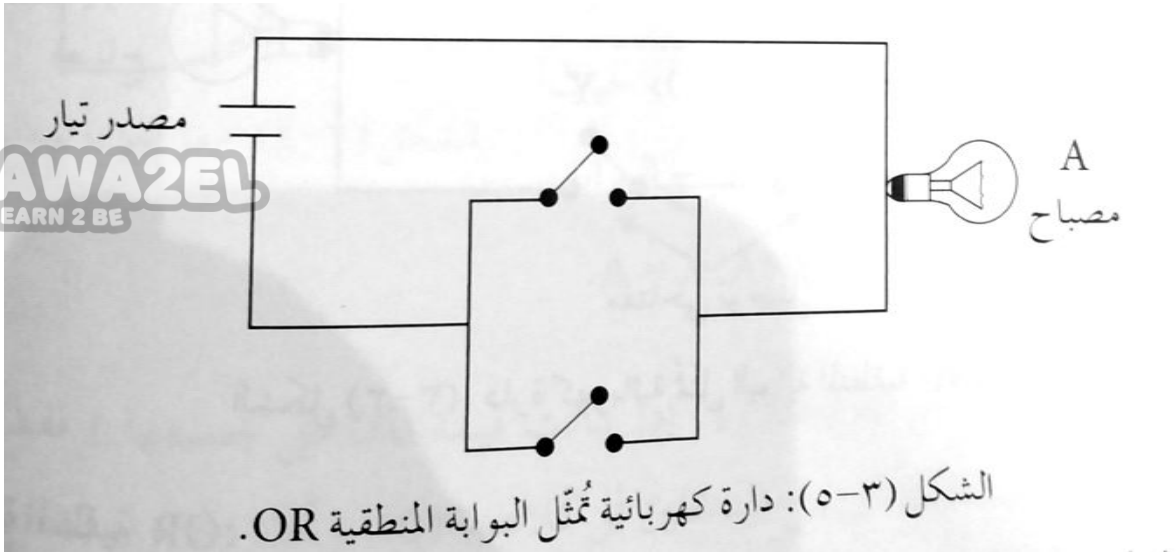
الشكل (٣–٣): دارة كهربائية تُمثّل البوابة المنطقية AND.

البوابة المنطقية OR:

- هي إحدى البوابات المنطقية الأساسية التي تدخل في بناء معظم الدوائر المنطقية ولها مدخلان ومخرج واحد وتسمى (**أو**) المنطقية.

آلية 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)
- 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، انظر الشكل (3-5)



الشكل (٣-٥): دارة كهربائية تُمثّل البوابة المنطقية OR.

البوابة المنطقية NOT:

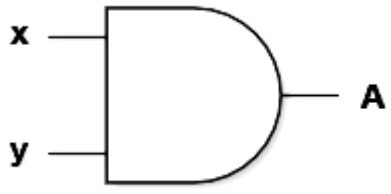
- هي إحدى البوابات المنطقية الأساسية التي تدخل في بناء معظم الدوائر المنطقية، ولها مدخل واحد فقط ومخرج واحد ويطلق عليها **العاكس** أي أنها تغير القيمة المنطقية للمدخل إلى عكسه.

آلية عمل البوابة المنطقية NOT:

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

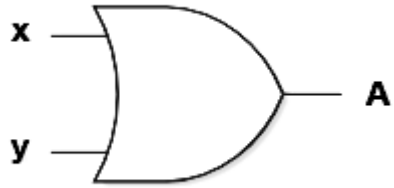
تمييز رموز البوابات المنطقية

البوابة المنطقيةAND



حيث يشير X و Y إلى مداخل البوابة و A مخرج البوابة
ويعبر عنها بالعبارة المنطقية **A = X AND Y**

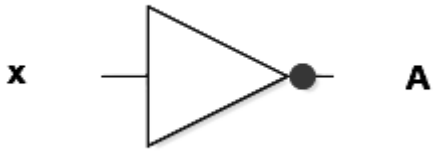
البوابة المنطقيةOR



حيث يشير X و Y إلى مداخل البوابة و A مخرج البوابة

ويعبر عنها بالعبارة المنطقية**A = X OR Y**

البوابة المنطقيةNOT



حيث يشير X إلى مداخل البوابة و A مخرج البوابة

ويعبر عنها بالعبارة المنطقية**A = NOT X**

كتابة جداول الحقيقة للبوابات المنطقية

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. مثلاً عدد احتمالات جدول الحقيقة للعبارة (x and y) يساوي**4**

ملاحظة:

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

يمكن معرفة عدد الاحتمالات من خلال القاعدة التالية:

عدد الاحتمالات = 2^N

حيث أن:

n تمثل عدد المتغيرات في العبارة المنطقية

الأساس= 2 لأن كل متغير يأخذ قيمتين إما 0 أو 1

جدول الحقيقة للبوابات المنطقية:

جدول الحقيقة للبوابة المنطقية AND

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

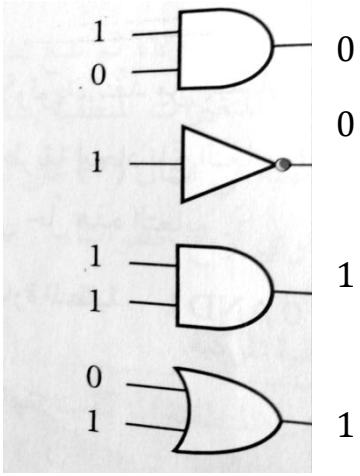
جدول الحقيقة للبوابة المنطقية OR

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

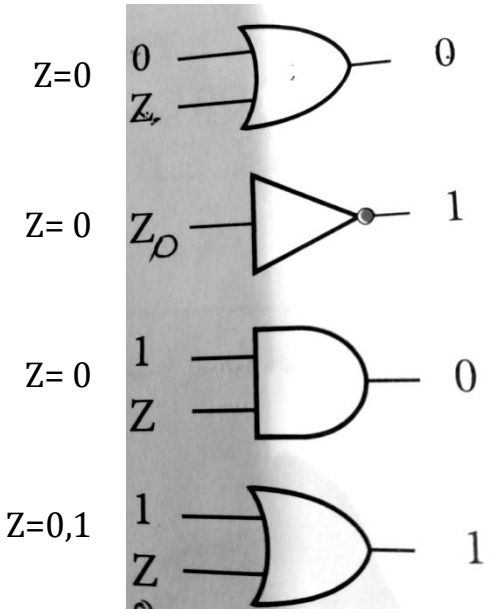
جدول الحقيقة للبوابة المنطقية NOT

X	A= NOT X
0	1
1	0

سؤال1: جد ناتج كل من البوابات المنطقية الآتية:



سؤال2: حدد قيمة z في كل من البوابات الآتية:



ثالثاً إيجاد ناتج العبارات المنطقية المركبة:

تضم العبارات المنطقية المركبة أكثر من بوابة منطقية، وفي هذه الحالة

- **يجب تطبيق قواعد الأولوية وحسب التسلسل التالي:**

1. في حالة وجود الأقواس تنفذ العمليات بداخلها أولاً.
2. البوابة المنطقيةNOT
3. البوابة المنطقيةAND
4. البوابة المنطقيةOR
5. في حالة التكافؤ في الأولوية، نبدأ من اليسار إلى اليمين.

ملاحظة: يجب تعويض قيم المتغيرات المنطقية أولاً، ثم تتبع تسلسل التنفيذ بتطبيق قواعد الأولوية، وأن عدد الخطوات بعد تعويض قيم المتغيرات المنطقية يساوي عدد البوابات المنطقية في العبارة المنطقية.

مثال 1: جد الناتج النهائي إذا كانتA=0, B=0 , C=1 , D=1 , F=0

NOT (A AND B OR C) OR D AND F

NOT (0 AND 0 OR1) OR 1 AND 0

NOT (0 OR 1) OR 1 AND 0

NOT 1 OR 1 AND 0

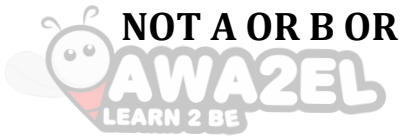
0 OR 1 AND 0

0 OR 0

0

مثال 2: جد الناتج النهائي إذا كانت A=1, B=1 , C=0 , D=0 , F=1

NOT A OR B OR C OR D AND F



مثال 3: جد الناتج النهائي إذا كانت A=0, B=1 , C=1 , D=0 , F=1

NOT(NOT (A AND B OR C) OR D OR F)

ملاحظة:

عند كتابة جدول الحقيقة يجب الحل حسب الأولويات و تذكر أن عدد الاحتمالات في جدول الحقيقة= 2^n

مثال1: اكتب جدول الحقيقة للعبارة 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

مثال2: اكتب جدول الحقيقة للعبارة A OR NOT (B OR NOT C)

مثال3: أكمل جدول الحقيقة للعبارة(NOT A OR NOT(B AND C

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

رابعاً تمثيل العبارات الجبرية المنطقية المركبة، باستخدام البوابات المنطقية

تمثيل العبارة المنطقية يعني تحويل العبارة المنطقية رياضيا إلى تمثيلها بالرسم باستخدام البوابات المنطقية

وعند تمثيلها يجب تطبيق قواعد الأولوية في الرسم

- **قواعد الأولوية:**

1. في حالة وجود الأقواس تنفذ العمليات بداخلها أولاً.
2. البوابة المنطقيةNOT
3. البوابة المنطقيةAND
4. البوابة المنطقيةOR
5. في حالة التكافؤ في الأولوية، نبدأ من اليسار إلى اليمين.

مثال1 : مثل العبارة المنطقية الآتية باستخدام البوابات المنطقية:

NOT (A AND B OR C) OR D AND F

مثال2 : مثل العبارة المنطقية الآتية باستخدام البوابات المنطقية:

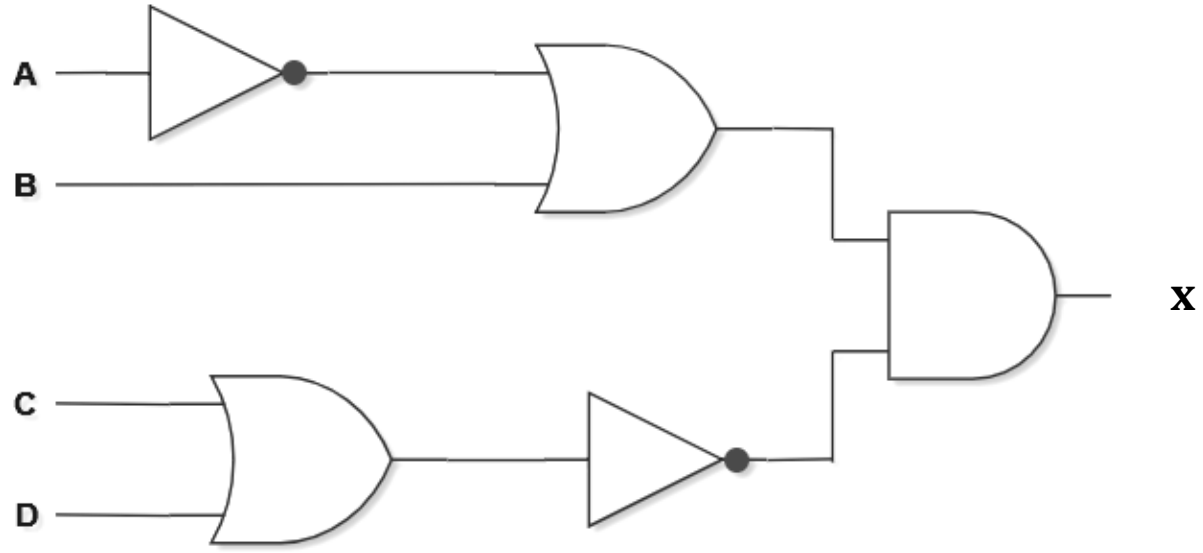
NOT A OR B OR C OR D AND F

مثال3 : مثل العبارة المنطقية الآتية باستخدام البوابات المنطقية:

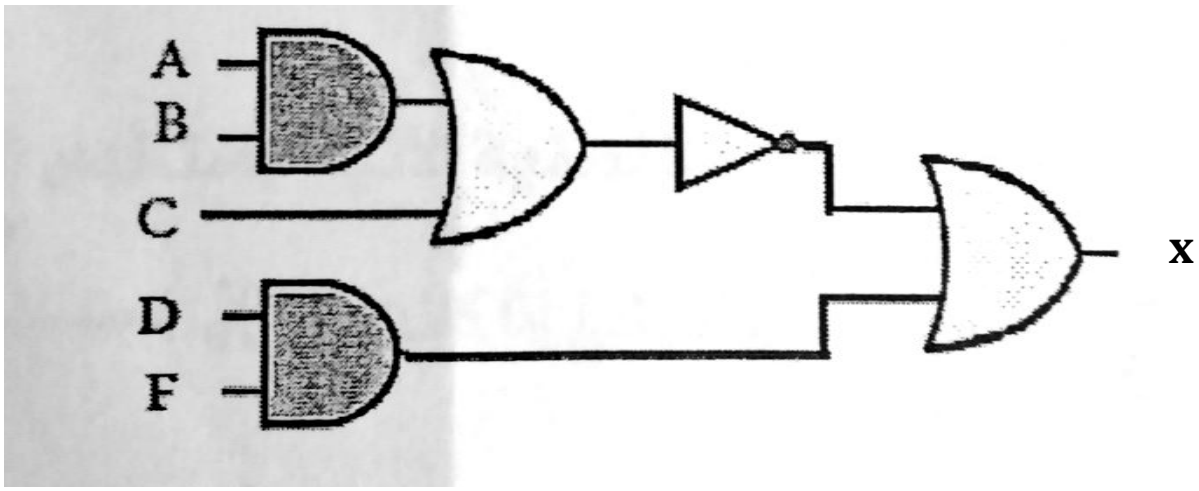
NOT(NOT (A AND B OR C) OR D OR F)

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

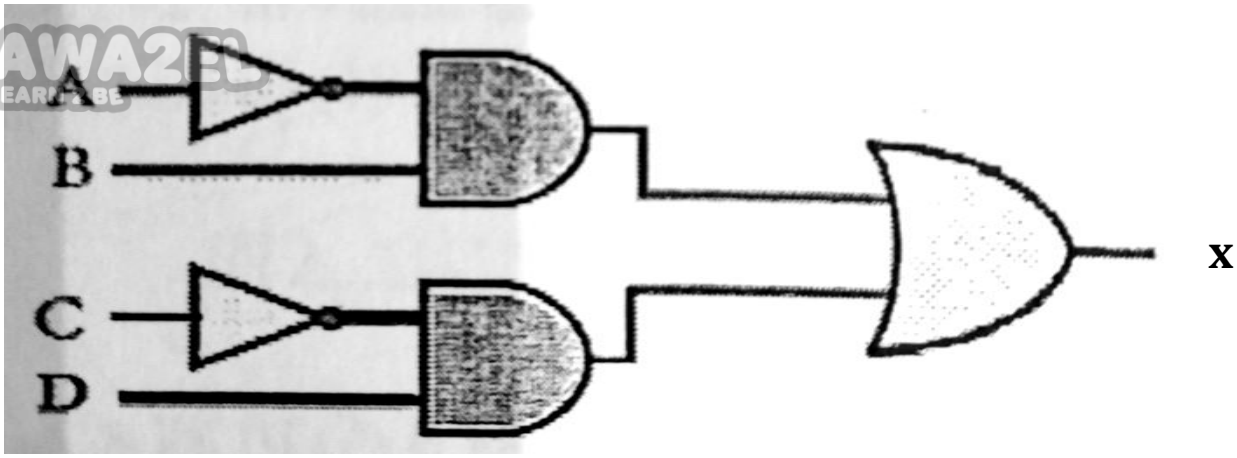
مثال1: اكتب اسم العبارة المنطقية المناسبة للبوابات المنطقية الآتية:



مثال2: اكتب اسم العبارة المنطقية المناسبة للبوابات المنطقية الآتية:



مثال3: اكتب اسم العبارة المنطقية المناسبة للبوابات المنطقية الآتية:

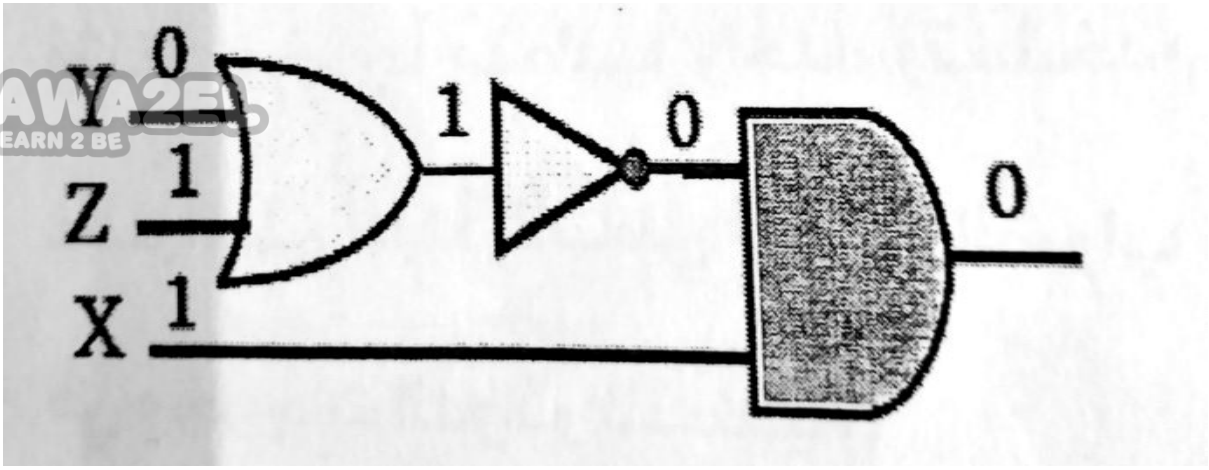


أسئلة شاملة ومهمة

س1) تأمل العبارة المنطقية الآتية (A AND B) AND ((NOT C) OR (NOT D))، ثم أجب عن الأسئلة التي تليها:

1) **كم عدد المتغيرات المنطقية في العبارة السابقة؟ 4**
2) **كم عدد البوابات المنطقية في العبارة السابقة؟ 5**
3) **كم عدد الاحتمالات في جدول الحقيقة للعبارة السابقة؟ 16**
4) **أوجد ناتج العبارة السابقة عندما: A=1,B=1,C=0,D=0؟ 1**
5) **مثل العبارة المنطقية السابقة باستخدام البوابات المنطقية.**
6) **استخرج مثالاً واحداً من العبارة السابقة لكل مما يلي(متغير منطقي، بوابة منطقية أساسية، عبارة منطقية بسيطة)**

س2)تأمل الشكل التالي ثم أجب عما يليه من أسئلة:



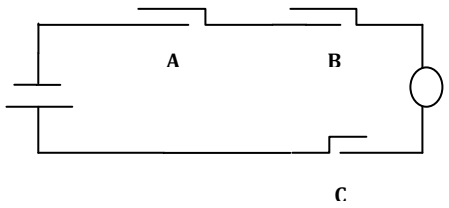
1- كم عدد المتغيرات المنطقية؟

2- كم عدد البوابات المنطقية؟

3- اكتب اسم العبارة المنطقية المناسبة للبوابات المنطقية السابقة؟

4- أوجد ناتج البوابات المنطقية السابقة عندما X=1,Y=0,Z=1

س3) تأمل الدارات الكهربائية الآتية ثم أجب عما يليها من أسئلة:

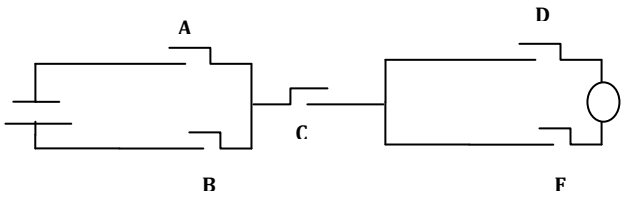


1 -اكتب العبارة المنطقية المناسبة للدارة الكهربائية السابقة.

A AND B AND C

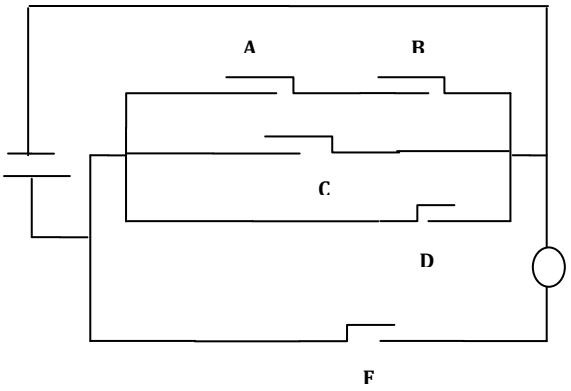
2 -أوجد ناتج الدارة الكهربائية عندما A=0,B=0,C=1

0



1 -اكتب العبارة المنطقية المناسبة للدارة الكهربائية السابقة.

2 -أوجد ناتج الدارة الكهربائية عندما
A=0,B=0,C=1,D=0,F=1



1 -اكتب العبارة المنطقية المناسبة للدارة الكهربائية السابقة.

2 -أوجد ناتج الدارة الكهربائية عندما
A=0,B=0,C=1,D=0,F=0

الفصل الثاني: البوابات المنطقية المشتقة

- **علل:سميت البوابات المشتقة بهذا الاسم.**

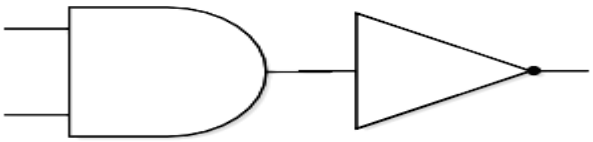
لأنها اشتقت من البوابات المنطقية الأساسية AND,OR,NOT

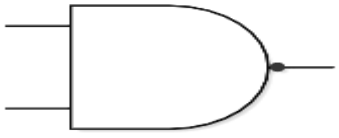
أولاً: البوابة المنطقية المشتقةNAND :

هي اختصار ل NOT AND أي نفي (AND) وتتشكل بوابة NAND بتوصيل مخرج بوابة AND بمدخل بوابة NOT وتسمى بوابة نفي (و) المنطقية.

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

علل: وجود دائرة صغيرة عند مخرج بوابة NAND. لأنها ترمز إلى البوابة NOT





- **جدول الحقيقة للبوابة المنطقية NAND:**

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

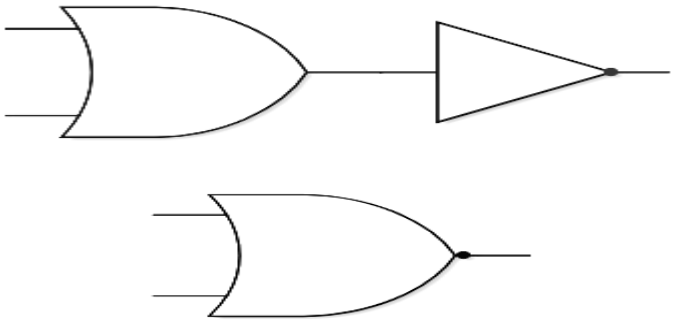
ملاحظات:

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

ثانياً: البوابة المنطقية المشتقةNOR

هي اختصار ل NOT OR أي نفي (OR) وتتشكل بوابة NOR بتوصيل مخرج بوابة OR بمدخل بوابة NOTوتسمى بوابة نفي (أو) المنطقية.

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



- **جدول الحقيقة للبوابة المنطقيةNOR**

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

ملاحظات:

- **تعطي بوابة NOR مخرجاً قيمته (0) إذا كانت قيمة أي من المدخلين أو كلاهما (1)**
- **تعطي مخرجاً قيمته (1) إذا كانت قيمة المداخل جميعها (0)**
- **مخرجات NOR عكس مخرجات بوابة.OR**

إيجاد ناتج العبارات المنطقية، التي تتكون من بوابات منطقية مشتقة من النوع نفسه

- **قواعد الأولوية وحسب التسلسل التالي:**

1. في حالة وجود الأقواس تنفذ العمليات بداخلها أولاً
2. البوابة المنطقية NOT
3. البوابة المنطقية NAND
4. البوابة المنطقية NOR
5. في حالة تساوي الأولوية، نبدأ من اليسار إلى اليمين.

ملاحظات:

- **أولوية NAND تكافئ أولوية AND، وعدد الخطوات يساوي عدد البوابات.**
- **في حالة وجود أكثر من NAND في العبارة المنطقية تنفذ من اليسار إلى اليمين.**
- **العبارات المنطقية المكونة من بوابات مشتقة وبوابات أساسية (ما عدا NOT)، غير مطلوبة في هذا المنهاج.**

تمارين : أوجد ناتج العبارات المنطقية المشتقة الآتية عندما A=0.B=0,C=1,D=1، ثم مثلها باستخدام البوابات المنطقية المشتقة :

1) **NOT A NAND NOT B**

   NOT 0 NAND NOT 0

   1 NAND NOT 0

   1 NAND 1

   0

---

2) **NOT(A NAND B)NAND C**

---

3) NOT A NAND NOT (B NAND C)

---

4) NOT(NOT(A NAND NOT B)NAND C)NAND NOT D

---

5) NOT(A NAND NOT(NOT B NAND NOT C)NAND D)

---

6) NOT A NOR NOT B

---

7) NOT(A NOR B)NOR C

---

8) NOT A NOR NOT (B NOR C)

---

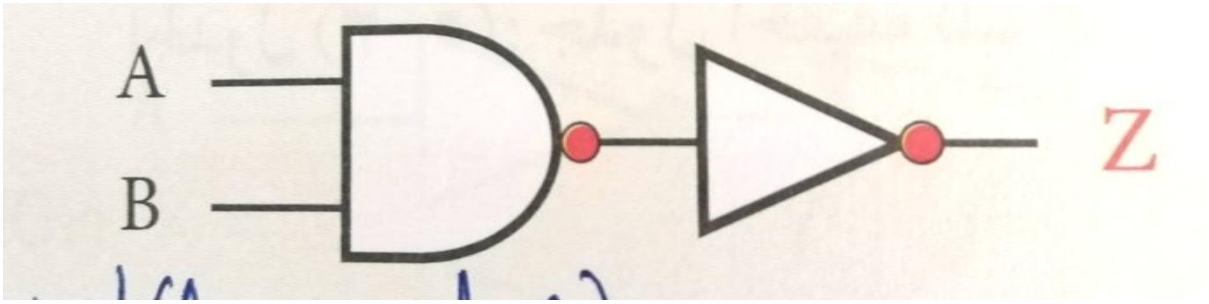
9) NOT(NOT(A NOR NOT B)NOR C)NOR NOT D

---

10)NOT(A NOR NOT(NOT B NOR NOT C)NOR D)

كتابة العبارات المنطقية التي تمثلها البوابات المنطقية المشتقة

أسئلة مهمة: تأمل البوابات المنطقية الآتية ثم أجب عما يليها من أسئلة:



1 -كم عدد المتغيرات المنطقية؟ 2

2 -كم عدد البوابات المنطقية؟ 2

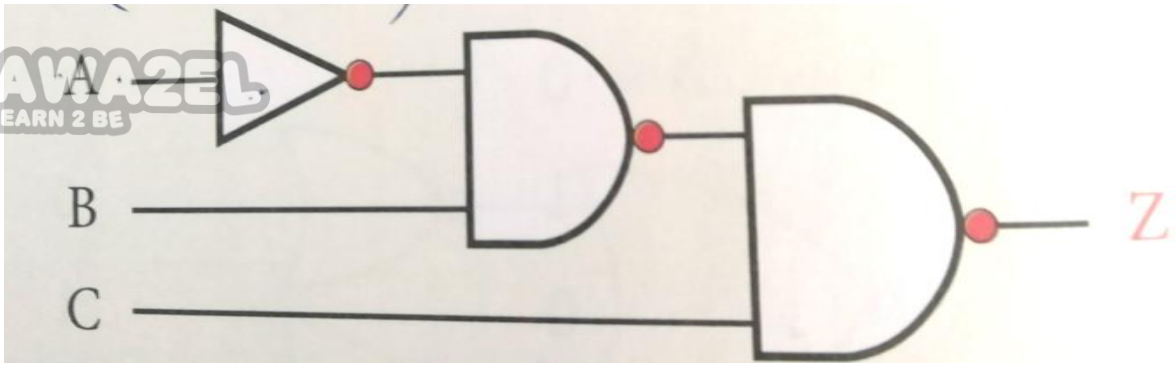
3 -كم عدد البوابات المنطقية الأساسية؟ 1

4 -كم عدد البوابات المنطقية المشتقة؟ 1

5 -اكتب العبارة المناسبة للبوابات السابقة. Z= NOT (A NAND B)

6 -ما قيمة Z عندما A=0,B=1؟ Z= 0

7 -أعد رسم البوابات المنطقية السابقة باستخدام البوابات المنطقية الأساسية فقط.



1 -كم عدد المتغيرات المنطقية؟

2 -كم عدد البوابات المنطقية؟

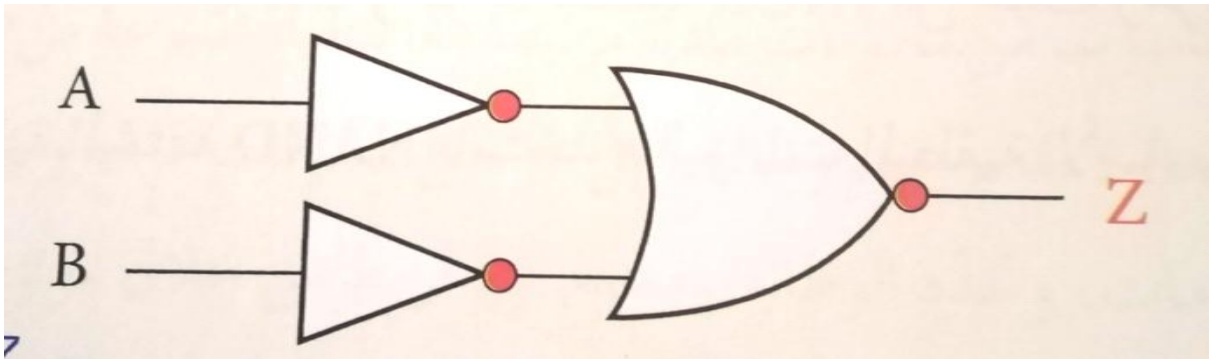
3 -كم عدد البوابات المنطقية الأساسية؟

4 -كم عدد البوابات المنطقية المشتقة؟

5 -اكتب العبارة المناسبة للبوابات السابقة.

6 -ما قيمة Z عندما A=0,B=1,C=0؟

7 -أعد رسم البوابات المنطقية السابقة باستخدام البوابات المنطقية الأساسية فقط.



1 -كم عدد المتغيرات المنطقية؟

2 -كم عدد البوابات المنطقية؟

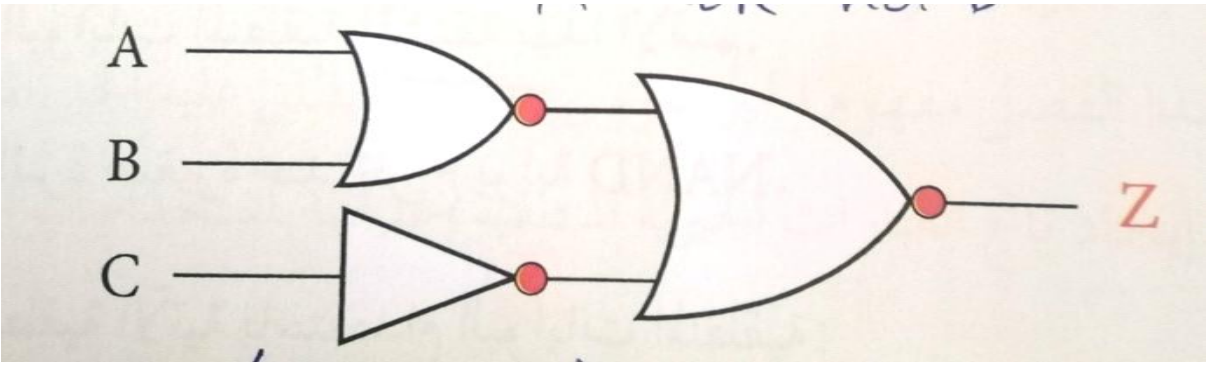
3 -كم عدد البوابات المنطقية الأساسية؟

4 -كم عدد البوابات المنطقية المشتقة؟

5 -اكتب العبارة المناسبة للبوابات السابقة.

6 -ما قيمة Z عندما A=0,B=1؟

7 -أعد رسم البوابات المنطقية السابقة باستخدام البوابات المنطقية الأساسية فقط.



1 -كم عدد المتغيرات المنطقية؟

2 -كم عدد البوابات المنطقية؟

3 -كم عدد البوابات المنطقية الأساسية؟

4 -كم عدد البوابات المنطقية المشتقة؟

5 -اكتب العبارة المناسبة للبوابات السابقة.

6 -ما قيمة Z عندما A=0,B=1,C=0؟

7 -أعد رسم البوابات المنطقية السابقة باستخدام البوابات المنطقية الأساسية فقط.

الفصل الثالث : الجبر المنطقي (البوولي)

أولاً: مفهوم الجبر المنطقي (البوولي)

AWA2EL LEARN TO BE

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).

- **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)، وقد قدمه 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.

ملاحظة:

- يسمى المتغير متغيراً منطقياً إذا عينت له إحدى الحالتين: صواب (True) أو خطأ (False).
- تستخدم أرقام نظام العد الثنائي 0 أو 1 لتمثيل حالات المتغير المنطقي فيمثل الرقم (1) الحالة الصحيحة والرقم (0) الحالة الخطأ.
- يرمز للمتغير المنطقي بأحد الحروف (A ... Z) لا أهمية لكون الحروف كبيرة أم صغيرة.

ثانياً: العبارات الجبرية المنطقية، والعمليات المنطقية

- **العبارة الجبرية المنطقية:**

هي ثابت منطقي (0,1) أو متغير منطقي 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.

عمليةNOT

يطلق على عملية NOT اسم المتمم، لأن متممة 0 تساوي 1 ومتممة 1 هي 0

العبارة الجبرية المنطقية لعملية NOT:

$A=\overline{X}$

حيث تعني _ المتممة

عمليةAND

يعبر عن عملية AND في الجبر المنطقي بالرمز(.)

العبارة الجبرية المنطقية لعمليةAND :

$A= X . Y$

استخدام (.) يشبه الضرب الثنائي وغالباً ما يهمل الرمز (.) في التعبير المنطقي، وتكتب XY بدلاً منX.Y

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

عمليةOR

يعبر عن عملية OR في الجبر المنطقي بالرمز(+)

العبارة الجبرية المنطقية لعمليةOR :

A= X+Y

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

ثالثاً: إيجاد ناتج التعابير الجبرية المنطقية المركبة

قواعد الأولوية حسب التسلسل التالي:

1. في حالة وجود الأقواس تنفذ العمليات بداخلها أولاً.
2. البوابة المنطقيةNOT
3. البوابة المنطقيةAND
4. البوابة المنطقيةOR
5. في حالة تكافؤ الأولوية، نبدأ من اليسار إلى اليمين

رابعاً: تمثيل العبارات الجبرية المنطقية المركبة، باستخدام البوابات المنطقية

تمثيل العبارة المنطقية يعني تحويل العبارة المنطقية رياضيا إلى تمثيلها بالرسم باستخدام التعابير الجبرية المنطقية وعند تمثيلها يجب تطبيق قواعد الأولوية في الرسم.

قواعد الأولوية:

1. في حالة وجود الأقواس تنفذ العمليات بداخلها أولاً
2. البوابة المنطقيةNOT
3. البوابة المنطقيةAND
4. البوابة المنطقيةOR
5. في حالة تساوي الأولوية، نبدأ من اليسار إلى اليمين.

أسئلة مهمة:

س1) أوجد ناتج العبارات الجبرية المنطقية الآتية: عندما A=0,B=0,C=1,D=1، ثم مثل كلاً منها باستخدام البوابات المنطقية.

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

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

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

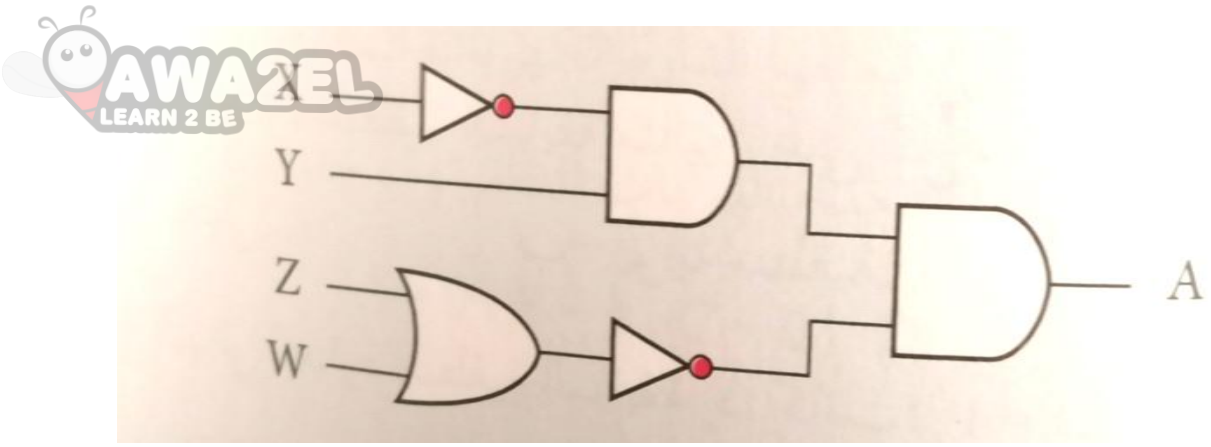
4) $\overline{A \cdot B} + \overline{C + D}$

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

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

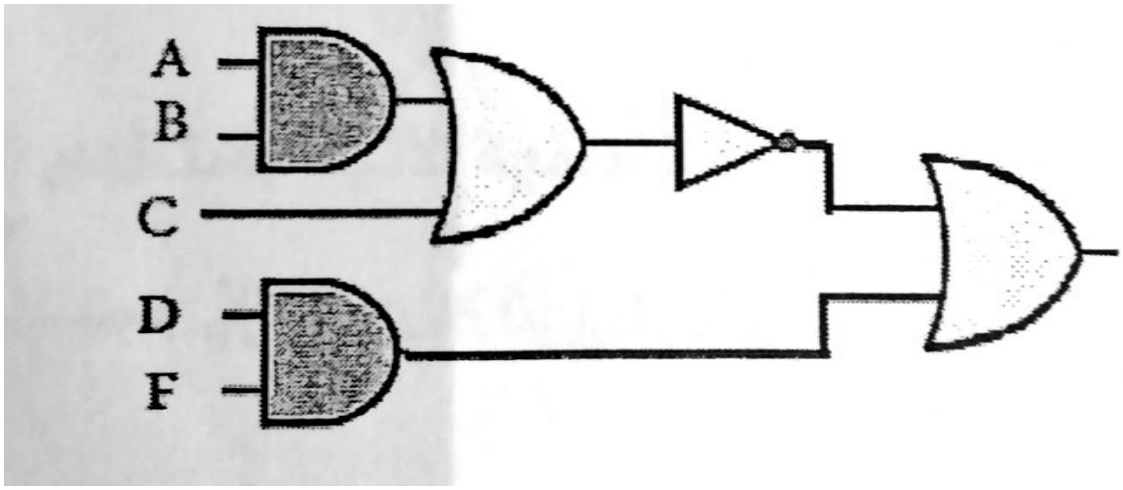
7) $\overline{\overline{A} \cdot (D \cdot \overline{C}) + \overline{B}}$

س2) اكتب العبارات الجبرية المنطقية لكل من البوابات المنطقية الآتية:



الجواب:

$$A = \overline{X} \cdot Y \cdot \overline{(Z + W)}$$



الجواب:

س3) حول العبارات المنطقية الآتية إلى عبارات جبرية منطقية:

1) F= NOT A OR NOT (B OR C) AND D

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

2) NOT C OR B AND NOT A OR NOT D

3) NOT (((NOT A OR NOT B) AND NOT C OR NOT D) OR NOT F)

4) NOT A OR NOT(((B OR NOT D AND C)AND NOT F)OR (K OR L))

س4) حول العبارات الجبرية المنطقية الآتية إلى عبارات منطقية:

1) $A = \overline{X \cdot \overline{Y} + \overline{(Z + W)}}$

A= NOT(X AND NOT Y OR NOT(Z OR W))

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

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

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

الوحدة الرابعة :أمن المعلومات والتشفير

أمن المعلومات

الفصل الأول :توضيح مفهوم أمن المعلومات

أولاً مقدمة في أمن المعلومات:

- **علل:اهتمت الشعوب قديما بالحفاظ على سرية المعلومات.**
  1) للحفاظ على أسرارها وهيبتها ومكانتها.
  2) لإنجاح مخططاتها العسكرية.
- **اعتمدت سرية المعلومات على:**

1. موثوقية حاملها.
2. قدرته على توفير الظروف المناسبة لمنع اكتشافها.

- **علل: كانت الحاجة أكثر إلحاحاً لإيجاد طرائق جديدة لحماية المعلومات.**

لتطور العلم واستخدام شبكات الحاسوب.

- **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.

ملاحظات:

- **علل: يعد أمن المعلومات من أهم الركائز التي تعتمد عليها الدول والمؤسسات والأفراد** في الحفاظ على موقفها العالمي سياسياً ومالياً.
- **علل:أصبح تناقل المعلومات والحصول عليها أمراً سهلاً،** بسبب التطور الهائل الذي حصل في مجالي الانترنت والبرمجيات.
- **علل:وجوب الاهتمام بكل ما يخص المعلومة،** بسبب وجود المخترقين والمتطفلين بشكل كبير.
- يجب الاهتمام بكل ما يخص المعلومات من **أجهزة التخزين، الاهتمام بالكادر البشري** الذي يتعامل معها، بالإضافة إلى **الحفاظ على المعلومات نفسها.**

- **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.

الخصائص الأساسية لأمن المعلومات والتي يهدف أمن المعلومات للحفاظ عليها:

1. السريـــــة.
2. السلامـــــة.
3. توافر المعلومـــات.

(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)

أمثلة على معلومات سرية:

1. المعلومات الشخصية.
2. الموقف المالي لشركة ما قبل إعلانه.
3. المعلومات العسكرية.

(السلامة)

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

- **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.

(توافر المعلومات)

قدرة الشخص المخول الحصول على المعلومات في الوقت الذي يشاء من دون وجود عوائق.

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 .

توضيح المخاطر التي تهدد أمن المعلومات

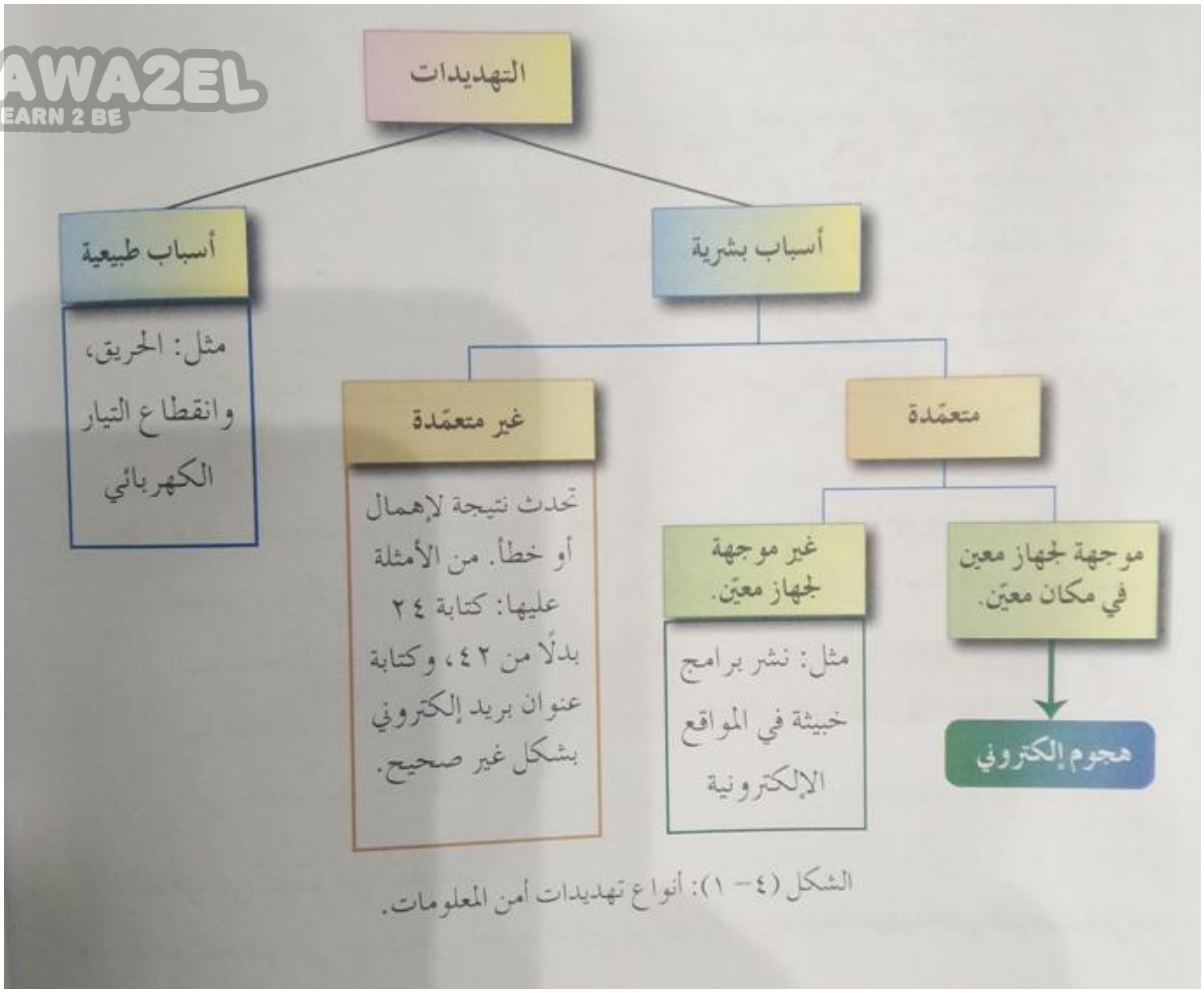
تقسم المخاطر التي تهدد أمن المعلومات إلى نوعين رئيسيين:

1 - التهديـــــدات.
2 - الثغـــــــرات.

التهديدات: يحدث التهديد لأسباب طبيعية، مثل حدوث حريق أو انقطاع التيار الكهربائي، مما **يؤدي إلى فقدان المعلومات،** أو لأسباب بشرية يمكن أن تكون غير متعمدة وتحدث نتيجة لإهمال أو خطأ مثل: كتابة عنوان بريد إلكتروني بشكل غير صحيح وأحياناً تكون متعمدة وتقسم إلى قسمين غير موجهة لجهاز معين، كأن ينشر فيروس، أو 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.

- **الهجوم الإلكتروني/ الاعتداء الإلكتروني:** هو تهديد موجه ومتعمد لجهاز معين؛ بقصد الإضرار به.

الشكل (4-1) يبين أنواع التهديدات.



الشكل (٤– ١): أنواع تهديدات أمن 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) الدافـــــع.
  2) الطريقـــة.
  3) فرصـــة 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**.

- **الثغـــــرات:** 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.

- **ماذا تسبب نقاط الضعف ؟**

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

- **تعرف كيفية الحد من مخاطر أمن المعلومات**

(علل) يتم استخدام مجموعة من الضوابط في نظم المعلومات، لتقليل المخاطر التي تتعرض لها المعلومات والحد منها.

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

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، ومن هذه الضوابط:**

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

الضوابط المادية: هي مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها باستخدام:
1. الجدران والأسوار والأقفال.
2. ووجود حراس الأمن.
3. أجهزة إطفاء الحريق.

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.

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.

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.

توضيح المقصود من الهندسة الاجتماعية

يعد العنصر البشري من أهم مكونات الأنظمة والاهتمام به من أهم المجالات للحفاظ على أمن المعلومات.

- **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.

ثانياً: الهندسة الاجتماعية

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.

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

1) بسبب قلة اهتمام المتخصصين في مجال أمن المعلومات
2) عدم وعي مستخدمي الحاسوب بالمخاطر المترتبة عليها.

تحديد مجالات الهندسة الاجتماعية

- **ترتكز الهندسة الاجتماعية في مجالين:**

1. البيئة المحيطة
2. الجانب النفسي

أولاً البيئة المحيطة

تشمل ما يأتي:(مكان العمل/ الهاتف/ النفايات الورقية/الإنترنت)

مكان العمل:

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:

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:

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:

علل: تعتبر الانترنت من أكثر وسائل الهندسة الاجتماعية شيوعا.

بسبب استخدام الموظفين أو مستخدمي الحاسوب عادة كلمة المرور نفسها للتطبيقات جميعها.

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

- **يسعى المعتدي من خلال الجانب النفسي إلى:**
  1. كسب ثقة مستخدم الحاسوب.
  2. الحصول على المعلومات التي يرغب بها.

- **الوسائل التي يستخدمها المعتدي الالكتروني للتأثير في الجانب النفسي للشخص المستهدف:**

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

- **آلية عمل الهندسة الاجتماعية في المجال النفسي:**

يقنع المعتدي الموظف أو مستخدم الحاسوب **بطريقة مباشرة** ويقدم الحجج المنطقية والبراهين

وقد يستخدم **طريقة غير مباشرة** بحيث يعمد إلى تقديم إيحاءات نفسية، تحث المستخدم على قبول المبررات من دون تحليلها أو التفكير فيها ويحاول التأثير بهذه الطريقة من خلال إظهار نفسه بمظهر صاحب السلطة أو إغراء المستخدم بامتلاك خدمات نادرة (يقدم له عرضا معينا من خلال موقعه الالكتروني لمدة محدد يمكنه ذلك من الحصول على كلمة المرور).

وقد 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.

علل: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.

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.

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.

الفصل الثاني: أمن الانترنت

أولاً: الاعتداءات الإلكترونية على الويب وإعطاء أمثلة عليها

أمن الإنترنت

- **علل : انتشار البرامج والتطبيقات بشكل واسع.**
لاعتماد الأفراد والمؤسسات والحكومات على تكنولوجيا المعلومات والاتصالات والانترنت بشكل واسع وفي شتى المجالات.

- **علل: كان لا بد من إيجاد وسائل تقنية تعمل على حماية الانترنت (الويب) والحد من الاعتداءات والأخطار التي تهددها:**

1. بسبب انتشار البرامج والتطبيقات بشكل كبير منها ما هو مجاني ومنها ما هو غير معروف المصدر ومنها ما هو مفتوح المصدر (أي يمكن استخدامه على الأجهزة المختلفة).
2. بسبب انتشار البرامج المقرصنة والمعلومات الخاصة بكيفية اقتحام المواقع.

- **أصناف البرامج والتطبيقات المستخدمة:**

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

الاعتداءات الالكترونية على الويب

- **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.

أولاً الاعتداءات الالكترونية على متصفحات الانترنت

- **متصفح الانترنت:** هو برنامج ينقل المستخدم إلى صفحة (الويب) التي يريدها بمجرد كتابة العنوان والضغط على زر الذهاب ويمكّنه من استعراض المعلومات على الموقع.

- **علل : يتعرض متصفح الانترنت إلى الكثير من الأخطار.**
لأنها قابلة للتغير من دون ملاحظة ذلك من قبل المستخدم.

- **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.

ثانياً الاعتداءات الالكترونية على البريد الالكتروني

يتم الاعتداء الالكتروني على البريد الالكتروني بعدة طرق منها:

- تصل الكثير من الرسائل الالكترونية إلى البريد الالكتروني ، بعض هذه الرسائل الالكترونية مزيفة بعضها يسهل اكتشافه وبعضها الآخر استخدم بطريقة احترافية.
- يحاول المعتدي الالكتروني التعامل مع الأشخاص القليلي الخبرة حيث يقدم عروض شراء لمنتجات بعض المصممين بأسعار زهيدة أو رسائل تحمل عنوان كيف تصبح ثريا.
- هذه الرسائل تحتوي روابط للمزيد من المعلومات يرجى الضغط عليه ، وغيرها من الرسائل المزيفة والمضللة التي تحتاج إلى وعي من المستخدم.

- **أصناف الرسائل التي قد تصل إلى البريد الالكتروني:**

1. رسائل مزيفة.
2. رسائل يسهل اكتشافها.
3. رسائل استخدمت بطريقة احترافية.

ثانياً: توضيح مفهوم تقنية تحويل العناوين الرقمية

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.

توضيح مفهوم العناوين الرقمية الالكترونيةIP Address

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 (IP4) أو يتكون من ثمانية مقاطع ويشكل (IPv 6) ويسمى (IP Address) Internet Protocol Address.

أنواع:IP Address

IP4 : 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))

توضيح مفهوم تقنية تحويل العناوين الرقميةNAT

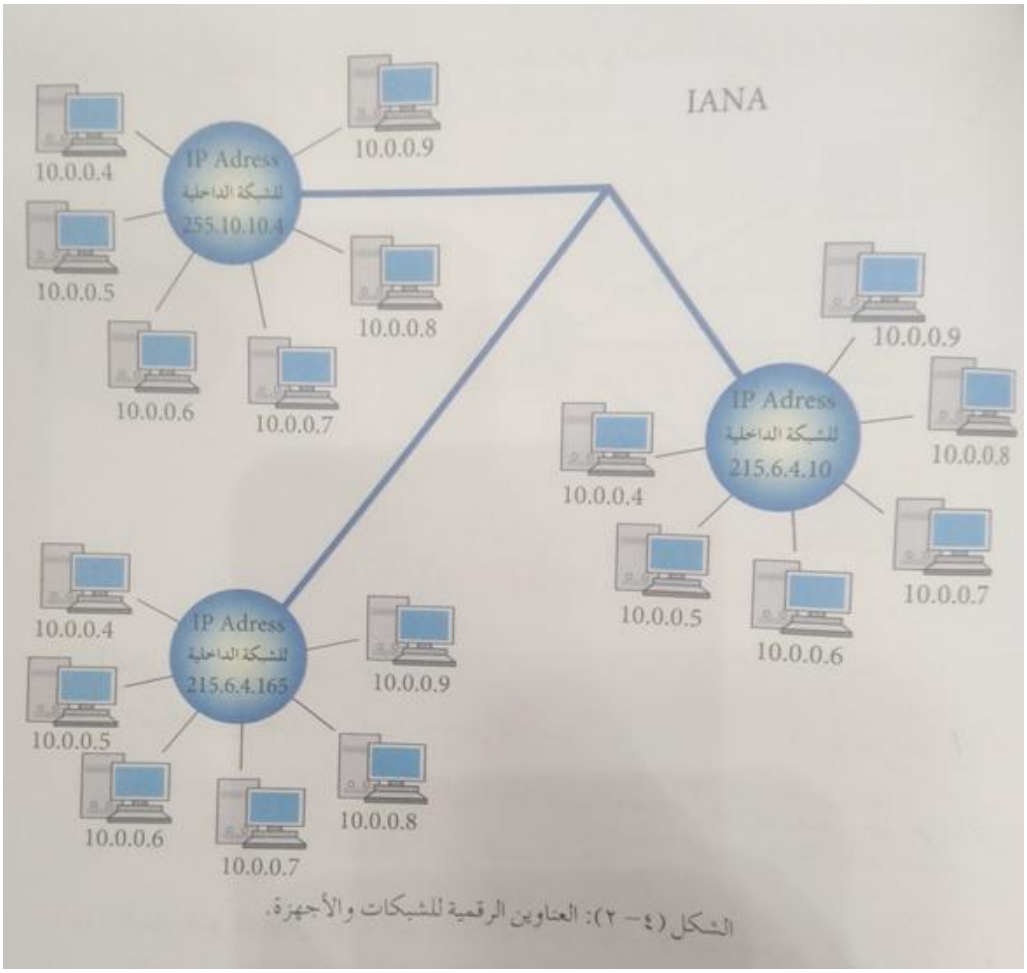
مفهوم تقنية تحويل العناوين الرقمية(NAT) Network Address Translation

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.

(IANA): هي السلطة المسؤولة عن منح أرقام الإنترنت المخصصة لإعطاء العناوين الرقمية للأجهزة على الإنترنت.



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

توضيح آلية عمل تقنية تحويل العناوين الرقمية وتعديد أنماطها

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.

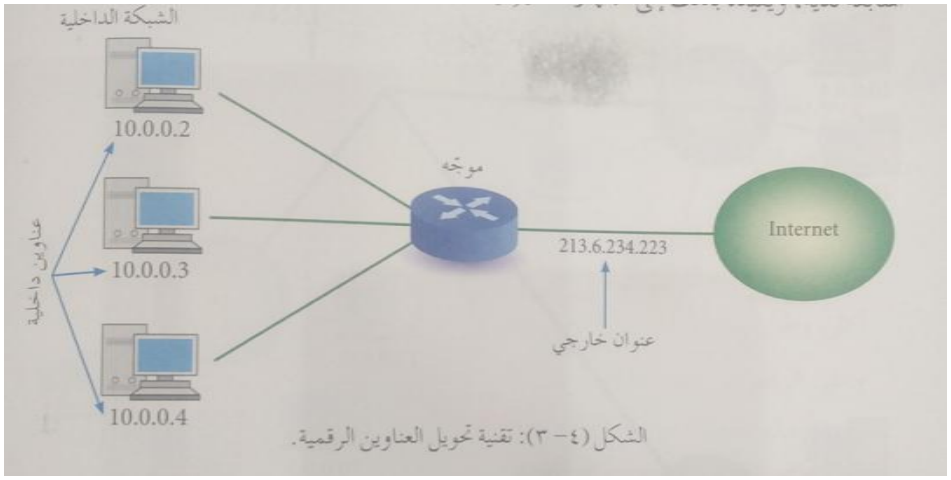
ثانياً النمط المتغير لتحويل العناوين الرقمية:

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 Address للجهاز 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.

الفصل الثالث: التشفير

أولاً :توضيح مفهوم التشفير والهدف منه وعناصره

AWA2EL LEARN 2 LIVE

ظهرت الحاجة للحفاظ على سرية المعلومات منذ قدم البشرية في المجالين العسكري والدبلوماسي خاصة، ثم 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.

- **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.
- **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.

- **علل: 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.

تحديد عناصر عملية التشفير والمقصود بكل عنصر

تتضمن عملية التشفير أربعة عناصر أساسية:

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

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

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

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

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

نص الشيفرة: الرسالة بعد عملية التشفير.

ثانياً: تعرف أنواع خوارزميات التشفير

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

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

توضيح المقصود بالتشفير المعتمد على نوع عملية التشفير

أنواع التشفير المعتمد على نوع عملية التشفير:

- **تشفير التعويض:** هي استبدال حرف مكان حرف أو مقطع مكان مقطع.

مثال على طريقة التشفير بالتعويض: شيفرة الإزاحة.

- **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.
- **فك التشفير:** عمليات إعادة الرسالة المشفرة إلى المحتوى الأصلي.

مثال على طريقة التشفير بالتبديل: خوارزمية الخط المتعرج

تشفير نص معين

ميزات خوارزمية الخط المتعرج:

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

خوارزمية الخط المتعرج: هي خوارزمية تتميز بأنها سهلة وسريعة ويمكن تنفيذها يدوياً باستخدام الورقة والقلم، كما أنه 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 1: شفر النص الآتي I LOVE MY COUNTRY ، علما بأن مفتاح التشفير سطران.

I		L		V		▽		Y		C		U		T		Y	
	▽		O		E		M		▽		O		N		R		▽

ويكون النص المشفر هو:

ILV▽YCUTY▽OEM ▽ONR▽

مثال 2: جد النص المشفر للنص الأصلي الآتي، علماً بأن مفتاح التشفير هو خمسة أسطر.

Stay positive this year makes you happy all life

النص المشفر هو----------

مثال3: جد النص المشفر للنص الأصلي الآتي باستخدام خوارزمية الخط المتعرج، علماً بأن مفتاح التشفير هو سطران

Time is gold

إيجاد النص الأصلي لنص مشفر

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.

عدد الأحرف في كل جزء= مجموع أحرف النص المشفر(بما فيها الفراغات) / عدد الأجزاء.

3. اكتب الحرف الأول من كل جزء، ثم الحرف الثاني، ثم الحرف الثالث وهكذا.

مثال1: جد النص الأصلي للنص المشفر الآتي باستخدام خوارزمية الخط المتعرج، علماً بأن مفتاح التشفير سطران.

ILV▽YCUTY▽OEM▽ONR

عدد الأحرف في كل جزء = 2/17=8.5 ونقرب العدد ليصبح 9

نفصل كل 9 خانات من النص المشفر معا ونكتب بالجدول المكون من 9 أعمدة وصفين النص المشفر بشكل أفقي ونكتب النص الأصلي بشكل عمودي.

استخراج النص الأصلي ↓ كتابة النص المشفر →

I	L	V	▽	Y	C	U	T	Y
▽	O	E	M	▽	O	N	R	

النص الأصلي هو: I LOVE MY COUNTRY

مثال2: جد النص الأصلي للنص المشفر الآتي، علماً بأن مفتاح التشفير ثلاثة أسطر.

Sdhdtya ▽ u▽r▽

توضيح المقصود بالتشفير المعتمد على المفتاح ومعرفة أنواعه

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).

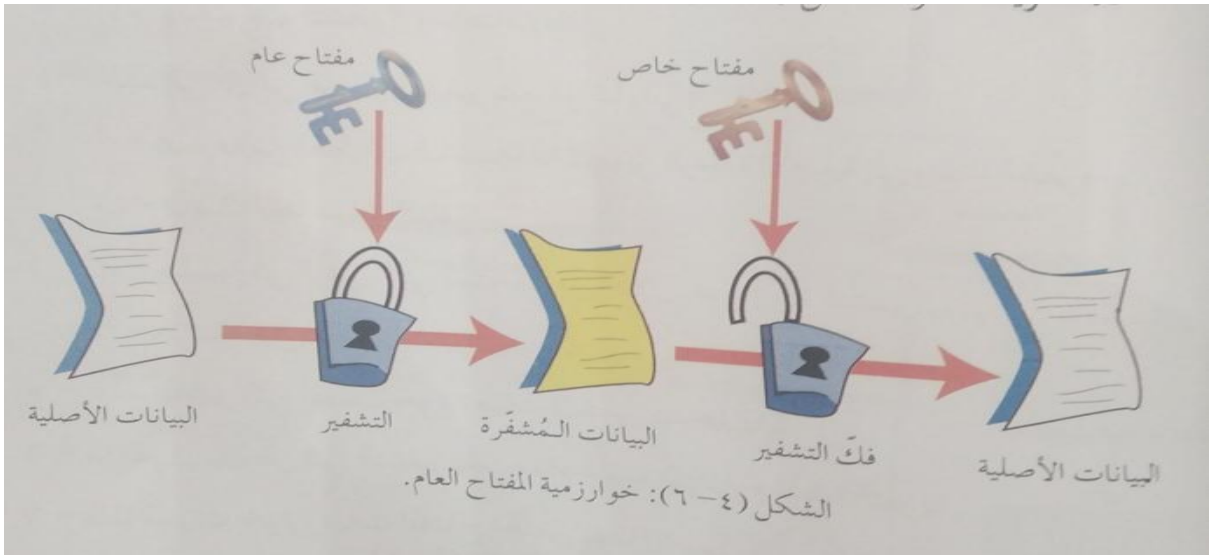
خوارزميات المفتاح الخاص (المفتاح السري):ويطلق عليها اسم الخوارزمية التناظرية:

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

الشكل (٤–٥): خوارزمية المفتاح الخاص.

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



الشكل (٤– ٦): خوارزمية المفتاح العام.

توضيح المقصود بالتشفير المعتمد على كمية المعلومات المرسلة ومعرفة أنواعه

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.

محبكم الأستاذ إبراهيم الكردي
0798237344