الوحدة الرّابعة

أمن المعلومات و التشفير

شامل حلّ الأنشطة و أسئلة الفصول و الوحدة و تمارين اضافيّة

أ. عيسى راجح

ماجستير في نظم معلومات الحاسوب

079 - 5676340

الفصل الأوّل
أمن المعلومات

- علل : اهتمت الشعوب قديما بالحفاظ على سرية المعلومات.
- للحفاظ على اسرارها وهيبتها ومكانتها .
- لانجاح مخططاتها العسكريه .

- على ماذا تعتمد سرّية المعلومات؟
- على موثوقيه حاملها .
- قدرته على توفير الظروف المناسبه لمنع اكتشافها .

- علل : أصبحت الحاجة أكثر إلحاحا لإيجاد طرائق جديدة لحماية المعلومات.
- نتيجة لتطوّر العلم.
- استخدام شبكات الحاسوب .

- كيف ابتدأت طرق حماية المعلومات؟ و كيف تطورت؟
- ابتدات بالطرائق المادية .
- ثم تطورت لحماية قنوات الاتصال والمعلومات ، واستخدمت اساليب لحماية المعلومات والأجهزة الخاصة فيها.
- تدريب الكادر البشري وتوعيته.

- علل: يعد أمن المعلومات من أهم الركائز التي تعتمد عليها الدول والمؤسّسات والافراد.
للحفاظ على موقفها العالمي سياسيا وماليا.

- علل : اصبح تناقل المعلومات والحصول عليها امرا سهلا.
مع التطور الهائل الذي حصل في مجالي الإنترنت و البرمجيات.

- ان وجود المخترقين والمتطفلين بشكل كبير أ وجب الاهتمام بالعديد من الأمور. عددها.
- وجب الاهتمام بكل ما يخص المعلومة من أجهزة تخزين ومعالجة .
- الاهتمام بالكادر البشري الذي يتعامل معها.
- الحفاظ على المعلومات نفسها.

- مفهوم 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 ابقائها متاحة للافراد المصرح لهم باستخدامها .

- إلى ماذا يهدف أمن المعلومات ؟ للحفاظ على خصائصه الاساسية الثلاثة(السرية و السلامة و توافر المعلومات)

- الخصائص الاساسية لأمن المعلومات:
1- السرية.
2- السلامة.
3- توافر المعلومات.

1- السرية:
تعني ان الشخص المخوّل هو الوحيد القادر على الوصول إلى المعلومات والاطلاع عليها وهو مصطلح مرادف لمفهومي الأمن والخصوصية حيث تعد المعلومات الشخصية[1] والموقف المالي لشركة ما قبل اعلانه[2] والمعلومات العسكريه[3] بيانات يعتمد أمنها على مقدار الحفاظ على سريتها.

- سرّيّة المعلومات: عدم القدرة على الحصول على المعلومات، إلّا من قبل الأشخاص المخوّل لهم بذلك.

2- السلامة:
تعني حماية الرسائل أو المعلومات التي تم تداولها والتاكد بانها لم تتعرض لاي عمليّة تعديل سواء بالاضافة ام الاستبدال ام حذف جزء منها.

مثلا عند نشر نتائج طلبة الثانوية العامة يجب الحفاظ على سلامة هذه النتائج من اي تعديلات وكذلك الامر عند صدور قوائم القبول الموحد للجامعات الاردنية والتخصصات التي قبل الطلبة فيها فلا بد من العمل على حماية هذه القوائم من اي تعديل أو حذف أو تبديل أو تغيير.

3- توافر المعلومات : هي منع المخترقين من جعل المعلومات غير متاحة اما بحذفهم لها أو الإعتداء على الأجهزة التي تخزن فيها ، لأن تلك المعلومات تكون بلا فائدة اذا لم تكن متاحة للاشخاص المصرح لهم بالتعامل معها أو ان الوصول اليها يحتاج إلى وقت كبير.

- **توافر المعلومات :** قدرة الشّخص المخوّل على الحصول على المعلومات في الوقت الذي يشاء، دون وجود عوائق.

- متى تكون المعلومات بلا فائدة ؟
- اذا لم تكن متاحة للاشخاص المصرح لهم بالتعامل معها.
- الوصول اليها يحتاج إلى وقت كبير.

تمرين: يهدف أمن المعلومات للحفاظ على ثلاث خصائص ، حدّد الى أي هذه الخصائص يتّبع كل ممّا يأتي:

#	العبارة	الخاصّية
1	الموقف المالي لشركة ما قبل اعلانه.	السرية
2	التأكد من عدم حدوث أي تعديل.	السلامة
3	الشخص المخوّل هو الوحيد القادر على الوصول للمعلومات و الطلاع عليها.	السرية
4	الوصول للمعلومات يحتاج لوقت كبير.	توافر المعلومات
5	مصطلح مرادف لمفهومي الأمن و الخصوصية.	السرية
6	المعلومات العسكرية.	السرية
7	نتائج طلبة الثانوية العامة.	السلامة
8	المعلومات الشخصية.	السرية
9	جعل المعلومات متاحة للاشخاص المصرح لهم بالتعامل معها.	توافر المعلومات

حدد عنصر أمن المعلومات الذي سيتأثّر في كل عبارة في الجدول التالي:		
1	اعتراض الرّسالة و التغيير على محتواها.	سلامة المعلومات
2	الهجوم المزوّر أو المفبرك.	سرية المعلومات و سلامتها
3	التنصت على المعلومات.	سرية المعلومات
4	الادّعاء بأنّه صديق و يحتاج إلى معلومات	سرية المعلومات و سلامتها
5	قطع قناة الاتصال.	توافر المعلومات

- أنواع المخاطر التي تهدد أمن المعلومات :
1- التهديدات.
2- الثغرات.

- أولا : التّهديدات:
- ما هي أسباب حدوث التّهديدات؟
1- أسباب طبيعية: **مثل** حدوث حريق أو انقطاع التيار الكهربائي ما يؤدي إلى فقدان المعلومات.
2- أسباب بشرية: يمكن ان تكون غير متعمدة وتحدث لإهمال أو خطأ ،أو متعمدة (غير موجهة لجهاز معين أو موجهة لجهاز معين).

- أعط أمثلة على أخطاء بشرية غير متعمدة.
- كتابة عنوان بريد الكتروني بشكل غير صحيح نتيجة الاهمال .
- كتابة اسم أحمر بدل أحمد .
- ادخال رقم 42 بدل 24 .
- ادخال تاريخ 2/30 .

- ما هي أقسام الأخطاء البشرية المتعمدة؟ مع مثال على كل منها.
1- أخطاء غير موجهة لجهاز معين: **مثل** نشر فيروس أو برنامج خبيث في موقع الكتروني.
2- أخطاء موجهة لجهاز معين (الهجوم أو الإعتداء الالكتروني): **مثل** التعديل على ملف أو حذفه.

- الهجوم (الإعتداء) الالكتروني: هو خطأ بشري (تهديد) متعمد مُوجَّه لجهاز معيّن في مكان معيّن، يقصد الإضرار به و يعدّ من أخطر أنواع التّهديدات.

- أعط ثلاثة أمثلة على الهجوم الالكتروني:(*أعط ثلاثة أمثلة على أخطاء موجهة لجهاز معين*) :
1- سرقة جهاز الحاسوب أو أحدى المعدات التي تحفظ المعلومات.
2- التعديل على ملف أو حذفه .
3- الكشف عن بيانات سرية أو منع الوصول إلى المعلومات.

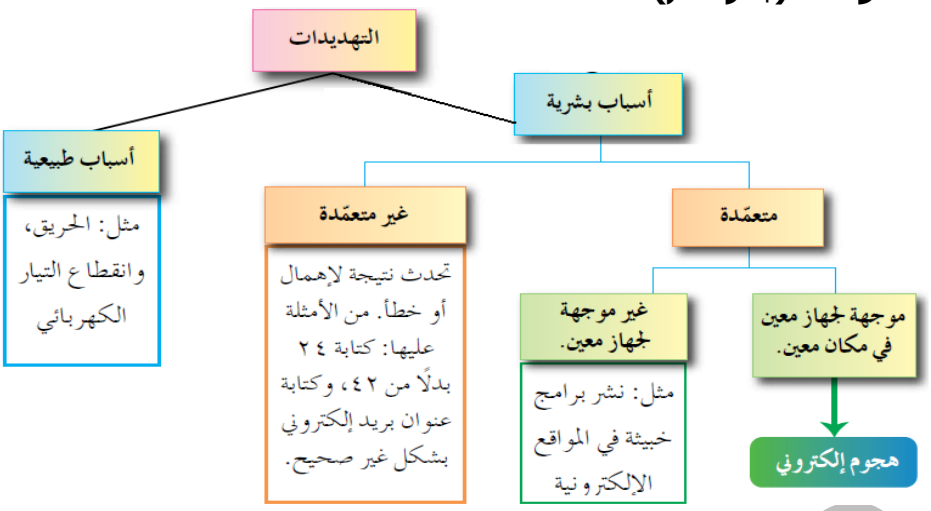
- ما هي العوامل الرئيسة التي يعتمد عليها نجاح الهجوم (الإعتداء) الالكتروني:
- *ما هي العناصر (العوامل) التي يجب اخذها في الحسبان لتقييم التهديد الذي يتعرض له النظام؟*
1- الدافع .
2- الطريقة .
3- فرصة النجاح .

1- الدافع : ما هي أنواع دوافع الافراد لتنفيذ هجوم الكتروني ؟
- الرغبة في الحصول على المال. - محأو لة لاثبات القدرات التقنيّة . - بقصد الاضرار بالاخرين .
2- الطريقة : تتضمن الطريقة كل ممّا يلي:
- المهارات التي يتميز بها المعتدي الالكتروني . - قدرة المعتدي على توفير المعدات والبرمجيات الحاسوبية التي يحتاج اليها . - معرفة المعتدي بتصميم النظام وآلية عمله . - معرفة المعتدي لنقاط القوة والضعف لهذا النظام .
3- فرصة النجاح : تتمثل فرصة نجاح الهجوم الالكتروني في كل ممّا يلي:
- تحديد الوقت المناسب للتنفيذ . - كيفية الوصول إلى الأجهزة .

تمرين: يوجد ثلاثة عوامل رئيسية تؤخذ بالحسبان لتقييم التهديد، حدد العامل لكل عبارة في الجدول التالي:

#	العبارة	العامل
1	الرغبة في اثبات القدرات.	الدافع
2	معرفة نقاط القوة و الضعف للنظام.	الطريقة
3	تحديد الوقت المناسب لتنفيذ الهجوم الالكتروني.	فرصة النجاح
4	الإضرار بالآخرين.	الدافع
5	الرغبة في الحصول على المال.	الدافع
6	القدرة على توفير المعدات والبرمجيات الحاسوبية.	الطريقة
7	كيفية الوصول إلى الأجهزة	فرصة النجاح
8	معرفة المعتدي بتصميم النظام وآلية عمله .	الطريقة

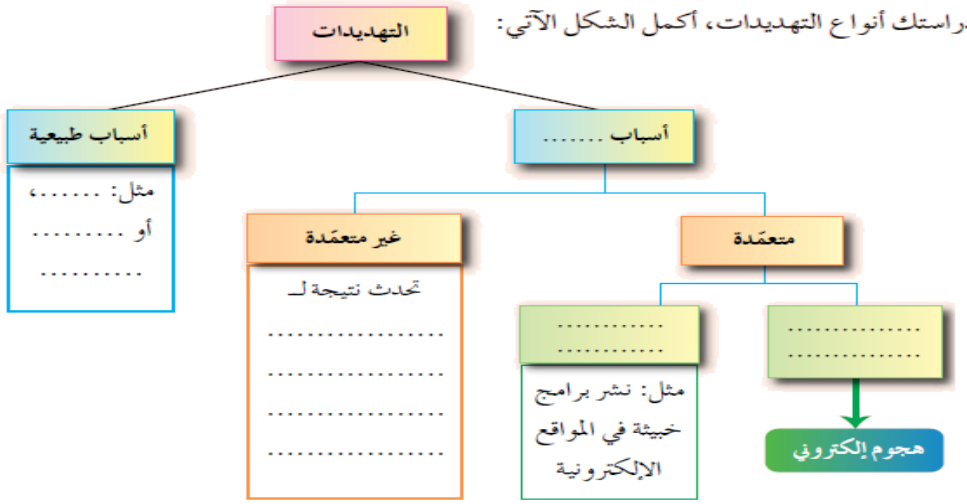
- أنواع تهديدات أمن المعلومات (بالرسم):



- <u>أنواع من الاعتداءات الالكترونية</u> التي تتعرض لها المعلومات :

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

— بناءً على دراستك أنواع التهديدات، أكمل الشكل الآتي:



1- التنصت على المعلومات :
الهدف منه الحصول على المعلومات السرية حيث يتم الاخلال بسريتها .
2- التعديل على المحتوى :
يتم اعتراض المعلومات وتغيير محتواها واعادة ارسالها للمستقبل من دون ان يعلم بتغيير محتواها (الاخلال بسلامة المعلومات) .
3- الايقاف :
يتم قطع قناة الاتصال ومن ثم منع المعلومات من الوصول إلى المستقبل فتصبح المعلومات غير متوافرة .
4- الهجوم المزور أو المفبرك :
يتمثل هذا النّوع بارسال المعتدي الالكتروني رسالة إلى أحد الأشخاص على الشبكة يخبره فيها بانه صديقه ويحتاج إلى معلومات أو كلمات سرية خاصة تتاثر بهذه الطريقة سرية المعلومات وقد تتاثر ايضا سلامتها .

- ثانيا : الثغرات: يقصد بها نقطة الضعف في النظام سواء اكانت في الاجراءات المتبعة مثل عدم تحديد صلاحيات الوصول إلى المعلومات[1] أو مشكلة بتصميم أو تنفيذ النظام[2] أو عدم كفاية الحماية المادية للأجهزة والمعلومات[3] تعدّ من نقاط الضعف التي قد تتسبب في <u>فقدان المعلومات</u> أو <u>هدم النظام</u> أو <u>تجعله عرضه للاعتداء الالكتروني</u> .

- اذكر ثلاثة أمثلة على الثغرات.

1- عدم تحديد صلاحيات الوصول إلى المعلومات.
2- مشكلة بتصميم أو تنفيذ النظام .
3- عدم كفاية الحماية المادية للأجهزة والمعلومات.

الحدّ من مخاطر أمن المعلومات

- علل: استخدام بعض الضوابط في نظام المعلومات.
يرى المختصون في مجال أمن المعلومات بان الحفاظ على المعلومات وأمنها ينبع من التوازن بين تكلفة الحماية وفعالية الرقابة من جهة مع احتمالية الخطر من جهة اخرى.

- ضوابط لتقليل المخاطر التي تتعرض لها المعلومات والحد منها:
1- الضوابط المادية.
2- الضوابط الادارية.
3- الضوابط التقنيّة.

1- الضوابط المادية.
يقصد بها مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها باستخدام (**مثل**) الجدران والاسوار والأقفال ووجود حراس الأمن وغيرها من أجهزة اطفاء الحريق.
2- الضوابط الادارية.
تستخدم مجموعة من الأوامر و الاجراءات المتفق عليها لمنع أي دخول غير مصرح فيه، **مثل** :القوانين واللّوائح والسياسات والاجراءات التّوجيهيّة وحقوق النشر وبراءات الاختراع والعقود والاتفاقيات .
3- الضوابط التقنيّة.
هي الحماية التي تعتمد على التقنيات المستخدمة سواء اكانت معدات ام برمجيات وتتضمن(**مثل**) كلمات المرور ومنح صلاحيات الوصول وبرتوكولات الشبكات والجدر النارية والتّشفير وتنظيم تدفق المعلومات في الشبكة .

تمرين: يوجد ثلاثة ضوابط لتقليل المخاطر التي تتعرض لها المعلومات والحد منها ، حدّده لكل عبارة بالجدول:

#	العبارة	الضوابط
1	التّشفير ومنح صلاحيات الوصول.	الضوابط التقنيّة
2	أجهزة اطفاء الحريق.	الضوابط المادية
3	حقوق النشر وبراءات الاختراع.	الضوابط الادارية
4	القوانين واللّوائح والسياسات والاجراءات التّوجيهيّة.	الضوابط الادارية
5	برتوكولات الشبكات.	الضوابط التقنيّة
6	العقود والاتفاقيات.	الضوابط الادارية
7	الجدران والاسوار والأقفال	الضوابط المادية
8	الجدر النارية.	الضوابط التقنيّة

- كيف يمكن الوصول إلى أفضل النتائج لتقليل المخاطر التي تتعرض لها المعلومات ؟
تعمل الضوابط الثلاثة جميعها بشكل متكامل للحد من الاخطار التي تتعرض لها المعلومات.

- يعدّ العنصر البشري من اهم مكونات الانظمة والاهتمام به من أهم المجالات للحفاظ على أمن المعلومات ، فكيف يتم اختيار(اعتماد) الكادر البشري المسؤول عن حماية الانظمة؟
يعتمد على كفايته العلمية ، واختبارات شفوية وورقية ومقابلات واخضاعهم إلى ضغوط نفسية حسب موقعهم للتاكد من قدرتهم على حماية النظام.

- مفهوم الهندسة الاجتماعية :
هي الوسائل والأساليب التي يستخدمها المعتدي الالكتروني لجعل مستخدم الحاسوب في النظام يعطي معلومات سرية أو يقوم بعمل ما يسهل علية الوصول إلى أجهزة الحاسوب أو المعلومات المخزنة فيها

- علل: تعد الهندسة الاجتماعية من أنجح و وأسهل الوسائل للحصول على المعلومات (غير المصرّحه)
- بسبب قلة اهتمام المتخصصين في مجال أمن المعلومات.
- عدم وعي مستخدمي الحاسوب بالمخاطر المترتبة عليها.

- أجب بنعم أم لا:
- مفهوم أمن الشبكات هو فرع من فروع أمن المعلومات . نعم
- يعد العنصر البشري من اهم مكونات الانظمة . نعم
- من اخطر ما يهدد نظم المعلومات ما يسمى الهندسة الاجتماعية . نعم

- <u>مجالات</u> الهندسة الاجتماعية :

1- البيئة المحيطة . (و <u>تشمل</u> مكان العمل [1]، الهاتف[2]، النّفايات الورقية[3]، الإنترنت[4]).

2- الجانب النفسي . (و <u>وسائلها</u> هي الاقناع[1] ، انتحال الشخصية والمداهنة[2]).

#	**(البيئة المحيطة) *<u>وتشمل:</u>***	#	**(الجانب النفسي) *<u>أساليب و وسائل:</u>***
1	**مكان العمل :**	**1**	**الاقناع :**
	آليّة العمل : يكتب بعض الموظفين كلمات المرور على أو راق ملصقة بشاشة الحاسوب . وعند دخول الشخص غير المخوّل له الاستخدام كزبون أو حتى عامل نظافة أو عامل صيانة يستطيع معرفة كلمات المرور ومن ثم يتمكن من الدخول إلى النظام بسهولة ليحصل على المعلومات التي يريدها .		**آليّة العمل :** اقناع المعتدي للموظف أو مستخدم الحاسوب بطريقة <u>مباشرة</u> بتقديم الحجج المنطقية والبراهين، أو <u>غير مباشرة</u> بتقديم ايحاءات نفسية تحثّ المستخدم على قبول المبررات دون تحليلها أو التفكير بها والتأثير عليه بإظهار نفسه بمظهر صاحب السّلطة، أو اغراء المستخدم بامتلاك خدمة نادرة بتقديم عرض معين بالموقع الالكتروني لمدة محددة للحصول على كلمة المرور، أو إبراز أوجه التشابه مع الشخص المستهدف لاقناعه بانه يحمل الصفات والاهتمامات نفسها فيصبح الشخص أكثر ارتياحا واقل حذرا للتعامل معه فيقدم له ما يريد من معلومات .
2	**الهاتف :**	**2**	**انتحال الشخصية والمداهنة :**
	آليّة العمل : يتّصل الشخص غير المخوّل بمركز الدعم الفني هاتفيا ويطلب منه بعض المعلومات الفنية ويستدرجه للحصول على كلمات المرور وغيرها من المعلومات ليستخدمها في ما بعد		**آليّة العمل :** حيث يتقمص شخص شخصيّة آخر، وهذا الشخص قد يكون حقيقيا أو وهميّا فقد ينتحل شخصية فني صيانة معدات الحاسوب أو عامل نظافة أو مدير أو سكرتير وبما ان الشخصية المنتحلة غالبا تكون <u>ذات سلطة</u> يبدي اغلب الموظفين خدماتهم ولن يترددوا بتقديم اي معلومات للشخص المسؤول .
3	**النّفايات الورقية :**	**3**	**مسايرة الرّكْب :**
	آليّة العمل : يدخل الشخص غير المخوّل لمكان العمل ، ويجمع النفايات التي قد تحتوي على كلمات المرور ومعلومات تخصّ الموظفين وارقام هواتفهم وبياناتهم الشخصية وقد تحتوي على تقويم العام السابق وكل ما يحتويه من معلومات يمكن استغلالها في تتبّع أعمال الموظّفين أو الحصول على المعلومات المرغوبة		**آليّة العمل :** حيث يرى الموظف بانه اذا قام زملاؤه جميعهم بأمر ما فمن غير اللائق ان يأخذ هو موقفا مغايرا .فعندما يقدم شخص نفسه على انه إداري من فريق الدعم الفني ويرغب بعمل تحديثات على الأجهزة فاذا سمح له أحد الموظفين بعمل تحديث على جهازه فان باقي الموظفين يقومون بمسايرة زميلهم غالبا والسماح للمعتدي بتحديث أجهزتهم والاطلاع على المعلومات المخزنة التي يريدها.
4	**الإنترنت :**		
	آليّة العمل : <u>من أكثر الوسائل شيوعا</u>(علل) بسبب استخدام الموظفين أو مستخدمي الحاسوب عادة كلمة المرور <u>نفسها</u> للتطبيقات <u>جميعها</u> حيث ينشئ المعتدي الالكتروني موقعا على الشبكة يقدم خدمات معينة ويشترط التسجيل فيه للحصول على هذه الخدمات يتطلب التسجيل في الموقع اسم مستخدم وكلمة المرور وهي كلمة المرور نفسها التي يستخدمها الشخص عادة فيحصل المعتدي الالكتروني عليها.		

- ملاحظة:

يسعى المعتدي الالكتروني في الجانب النفسي لكسب ثقة مستخدم الحاسوب ومن ثم الحصول على المعلومات التي يرغب بها .

الفصل الثاني
أمن الإنترنت

- ما أسباب ايجاد وسائل تقنيّة لحماية الإنترنت (الويب) ؟
للحد من الإعتداءات والاخطار التي تهدده بسبب انتشار البرامج القرصنة والمعلومات الخاصة بكيفية اقتحام المواقع.

- علل: انتشار البرامج والتطبيقات (المجانية وغير معروف المصدر والمفتوحة) بشكل كبير.
لاعتماد الافراد والمؤسسات والحكومات على تكنولوجيا المعلومات والاتصالات بشكل واسع وفي شتّى المجالات .

- علل: لا يحسّ المستخدم بالكثير من الإعتداءات الإلكترونية التي تتعرض لها المواقع الإلكترونية .
كون تلك الإعتداءات غير مرئية .

- ما أشهر الإعتداءات على (الويب) ؟
1- الإعتداء على متصفّح الإنترنت .
2- الإعتداء على البريد الالكتروني .

أولا: الإعتداءات الإلكترونية على متصفّحات الإنترنت :

- متصفّح الإنترنت : هو برنامج ينقل المستخدم الى صفحة الويب التي يريدها بمجرد كتابة العنوان والضغط على زرّ الذهاب ويمكنه من مشاهدة المعلومات على الموقع .

- علل: يتعرض متصفّح الإنترنت الى الكثير من الاخطار.
لانها قابلة للتغيير من دون ملاحظة المستخدم لذلك .

- ما هي طرق الإعتداءات الإلكترونية على متصفّحات الإنترنت ؟
1- الإعتداء عن طريق (كود) بسيط يضاف الى المتصفّح وباستطاعته القراءة والنسخ وإعادة ارسال أي شيء يتم إدخاله من المستخدم ويتمثّل التّهديد بالقدرة على الوصول للحسابات الماليّة والبيانات الحسّاسة الأخرى .
2- توجيه المستخدم إلى صفحة أخرى غير الصّفحة التي يريدها .

ثانيا: الإعتداءات الإلكترونية على البريد الالكتروني :

- وضّح العبارة التّالية: تحدث الإعتداءات الإلكترونية على الويب من خلال البريد الالكتروني .
لأن بعض الرسائل الإلكترونية تحمل عروض وهميّة بأسعار زهيدة ، و روابط تحمل عناوين جذّابة مزيّفة (كيف تصبح ثريّا) لا يمكن للأشخاص القليلي الخبرة اكتشافها تحمل روابط تنقل المستخدم لصفحات أخرى .

#	- تمرين: حدّد نوع الإعتداء في كل ممّا يلي:	نوع الإعتداء
1	- توجيه المستخدم إلى صفحة اخرى غير الصّفحة التي يريدها .	*إعتداء على متصفّح الإنترنت*
2	- كود بسيط يضاف إلى المتصفّح وباستطاعته القراءة والنّسخ وإعادة إرسال أي شيء يتم إدخاله من المستخدم .	*إعتداء على متصفّح الإنترنت*
3	- يتضمّن عروضا وهميّة و مضلّلة، و يحتوي رابط يتمّ الضّغط عليه للحصول على معلومات إضافيّة.	*إعتداء على البريد الالكتروني*

تقنيّة تحويل العناوين الرّقمية

- تقنيّة تحويل العناوين الرّقمية : هي التقنيّة التي تخفي العنوان الرّقمي للجهاز في الشّبكة الدّاخلية ليتوافق مع العنوان الرقمي المعطى للشّبكة فيصبح الجهاز الدّاخلي غير معروف بالنّسبة للجهات الخارجيّة، لتحميه من أي هجوم قد يُشنّ عليه بناء على معرفه العناوين الرّقمية ، وهي إحدى طرق حماية المعلومات من الإعتداءات الإلكترونيّة

- علل(وضّح): تحافظ تقنيّة تحويل العناوين الرّقمية على أمن المعلومات في الويب.
من خلال إخفاء العنوان الرقمي الدّاخلي لجهاز الحاسوب ، فيمنع ذلك من الإعتداء عليه.

- العناوين الرّقمية الإلكترونية :

عنوان رقمي خاص بكل جهاز ولكل حاسوب او هاتف خلوي يميزه عن غيره يسمى (IP address) يتكوّن من 32 خانة ثنائية تتوزع على اربعة مقاطع يفصل بينها نقاط وهذا ما يسمى (ip4) وكل مقطع من هذه المقاطع يتضمن رقما من (0) الى (255) .

- مثال: 215.002.004.216

- تمرين: بيّن سبب الخطأ في كل من عناوين (ip4) التالية:		
#	**العنوان**	**سبب الخطأ**
1	224.002.004.302	*الرقم أعلى من 255*
2	215.002.004	*ثلاثة مقاطع بدل أربعة*
3	215.002.004،216	*وجود فاصلة بدل نقطة*

- علل: طوّرت عناوين (ip4) لما يسمّى (ipv6) ؟

نظرا للتّطور الهائل في أعداد مستخدمي الإنترنت ظهرت الحاجة الى عناوين الكترونية اكثر ، فعنوان ipv6 يتكون من ثمانية مقاطع بدلا من اربعة.

- ما الفرق بين العناوين الرّقمية (ip4) و (ipv6) ؟

- (ip4) تتكون من اربعة مقاطع.
- (ipv6) تتكون من ثمانية مقاطع.

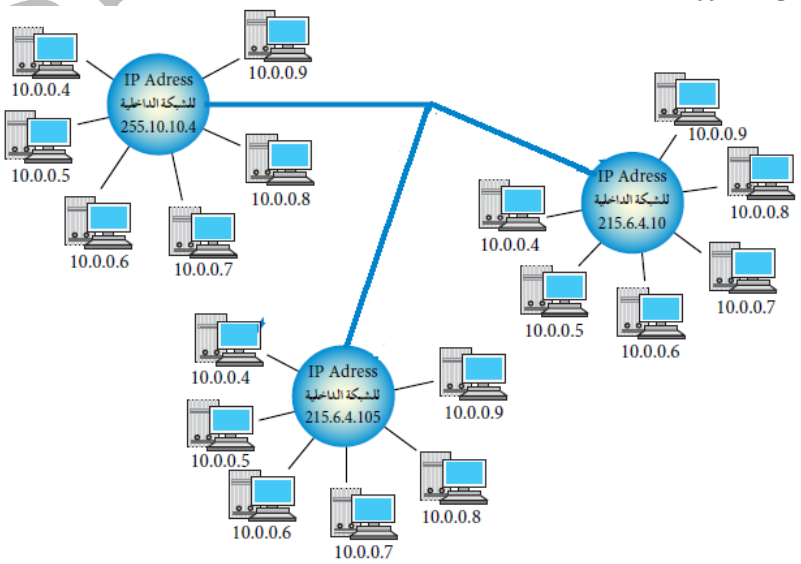
- علل: وجد ما يسمى بتقنيّة تحويل العناوين الرّقمية (Nat) ؟

على الرغم من استخدام ipv6 (ثمانية مقاطع)الا انه لا يكفي لإتاحة عدد هائل من العناوين الرّقمية .

- مفهوم تقنيّة تحويل العناوين الرّقمية (Nat) :

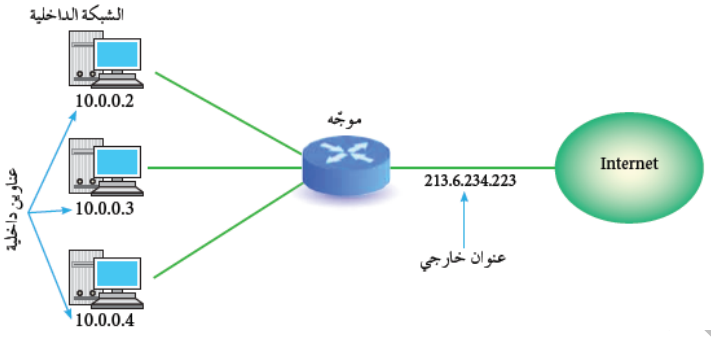
تتمتع ايانا (IANA) بالسلطة المسؤولة عن منح ارقام الإنترنت المخصصة لاعطاء العناوين الرّقمية للاجهزة على الإنترنت وبسبب قلة اعداد هذه العناوين مقارنة بعدد المستخدمين فانها تعطي الشبكة الداخلية عنوانا واحدا (او مجموعه عناوين) ويكون معرفا لها عند التعامل في شبكة الإنترنت .

مثلا الشكل يبيّن وجود ثلاث شبكات داخلية وكل شبكة منحت عنوانا خاصا بها على الإنترنت مختلفا عن العناوين الاخرى مثلا العنوان 255.10.10.4 هو لشبكة على الإنترنت وهذا العنوان لا يمكن ان يمنح لشبكة اخرى وكذلك الامر بالنسبة الى العنوانين 215.6.4.10 او 215.6.4.165 تعطي الشبكة الداخلية كل جهاز داخل الشبكة عنوانا رقميا لغرض الاستخدام الداخلي فقط ولا يعترف بهذا العنوان خارج الشبكة وهذا يعني ان العنوان الرقمي للجهاز داخل الشبكة كما يظهر الشكل يمكن ان يتكرر في اكثر من شبكة داخلية مثل العنوان (10.0.0.8) لكنّ العنوان الرقمي للشبكة الداخلية لن يتكرّر .



وعند رغبة أحد الاجهزة بالتواصل مع جهاز خارج الشبكة الداخلية يعدّل العنوان الرّقمي الخاص به بإستخدام تقنيّة تحويل العناوين الرّقمية (NAT) وذلك يتمّ باستخدام جهاز وسيط يكون غالبا موجّها أو جدارا ناريا يحوّل العنوان الرّقمي الدّاخلي إلى عنوان رقمي خارجي ويسجّل ذلك في سجلّ خاص للمتابعة .

يتم التّواصل مع الجهاز الهدف في الشّبكة الأخرى عن طريق هذا الرقم الخارجي على انه العنوان الخاص بالجهاز المرسل وعندما يقوم الجهاز الهدف بالرد على رسالة الجهاز المرسل تصل الى الجهاز الوسيط الذي يحول العنوان الرقمي الخارجي الى عنوان داخلي من خلال سجل المتابعة لديه ويعيده بذلك الى الجهاز المرسل كما بالشكل :



- من السُّلطة المسؤولة عن منح أرقام الإنترنت المخصصة لإعطاء العناوين الرّقمية ؟ ايانا IANA

- ما وظيفة الجهاز الوسيط ؟
يحول العنوان الرقمي الداخلي الى عنوان رقمي خارجي ويسجل ذلك في سجل خاص للمتابعة .

- اعط أمثلة على الجهاز الوسيط ؟
- مُوجِّه.
- جدارا ناري .

- آليّة عمل تقنيّة تحويل العناوين الرّقمية (تعمل بطريقتين) :

1- النمط الثابت للتحويل :
طريقة (نمط) تقوم بتخصيص عنوان رقمي خارجي لكل جهاز داخلي وهذا العنوان الرقمي ثابت لا يتغير ، يستخدمه الجهاز في كل مرة يرغب فيها الاتصال مع الأجهزة خارج الشبكة.

2- النمط المتغيّر للتحويل : طريقة (نمط) تقوم بتخصيص عنوان رقمي للجهاز عند رغبته في التواصل مع جهاز خارج الشبكة يستخدمه، و عند انتهاء عملية الاتصال، يصبح هذا العنوان الرقمي متاحا للأجهزة الأخرى.

- آلية عمل النمط المتغيّر للتحويل : بهذه الطريقة يكون لدى الجهاز الوسيط عدد من العناوين الرّقمية الخارجية ولكنها غير كافية لعدد الاجهزة في الشبكة، هذه العناوين تبقى متاحة لجميع الاجهزة على الشبكة وعند رغبة احد الاجهزة بالتراسل خارجيا فانه يتواصل مع الجهاز الوسيط الذي يعطيه عنوانا خارجيا مؤقتا يستخدمه لحين الانتهاء من عمليّة التراسل ويعد هذا العنوان عنوانا رقميا خاصا بالجهاز عند انتهاء عمليّة التراسل يفقد الجهاز الداخلي هذا العنوان ويصبح العنوان متاحا للتراسل مرة اخرى وعند رغبة الجهاز نفسه بالتراسل مره اخرى قد يعطي عنوانا مختلفا عن المرة السابقة وهذا ما يفسر اختلاف IP address للجهاز نفسه عند تراسله اكثر من مرة.

- قارن بين طريقتي العمل لكل من:
- النمط الثابت لتحويل العناوين الرقمية : يقوم بتخصيص عنوان رقمي خارجي لكل جهاز داخلي وهذا العنوان الرقمي ثابت لا يتغير .
- النمط المتغيّر لتحويل العناوين الرقمية : يعطي الوسيط لكل جهاز عنوان رقمي مؤقت للتواصل مع الأجهزة خارج الشبكة، و حين انتهاء الاتصال يصبح هذا الرقم متاحا لأي جهاز آخر.

- فسّر اختلاف للجهاز عند تراسله أكثر من مرّه ؟
بسبب النمط المتغيّر لتحويل العناوين الرقمية بحيث يتم أعطاء الجهاز عنوانا رقميا مختلفا في كل مرّه يتواصل فيها مع أجهزة خارج الشبكة الداخليّة.

الفصل الثالث
التّشفير

- متى ظهرت الحاجة للحفاظ على سرّية المعلومات ؟
ظهرت الحاجة للحفاظ على السّرية منذ قدم البشريّة في المجالين العسكري والدبلوماسي بايجاد وسائل تنقل الرّسالة وتحافظ على سريتها بالوقت نفسه. ومع تطوّر العلم والتّكنولوجيا الحديثة كان لا بد من ايجاد طرق لحمايتها

- عرّف التّشفير : هو تغيير محتوى الرّساله الأصليه سواء أكان التغيير بمزجها بمعلومات أُخرى أم إستبدال الأحرف الأصليّة والمقاطع بغيرها أم تغيير لمواقع الأحرف بطريقة لن يفهمها إلا مرسل الرّسالة ومستقبلها فقط , بإستخدام خوارزميّة معيّنة ومفتاح خاص .

- فكّ التّشفير: عمليّات إعادة الرّسالة المشفّرة إلى المحتوى الأصلي .

- إلى ماذا يهدف التّشفير ؟
1- الحفاظ على سرّيّة المعلومات أثناء تبادلها بين مرسل المعلومة ومستقبلها.
2- عدم الإستفادة منها أو فهم محتواها حتى لو تمّ الحصول عليها من قبل أشخاص معترضين.

- علل: يعدّ التّشفير من أفضل طرق الحفاظ على أمن المعلومات.
لأنّه يخفيها عن الأشخاص غير المصرّح لهم بالإطّلاع عليها، و في حال تمّ ايجادها من قبل أشخاص آخرين فلن يتمكّنوا من فهم محتواها.

- عناصر علم التّشفير :
1- خوارزميّة التّشفير .
2- مفتاح التّشفير .
3- النّص الأصلي .
4- نص الشّيفرة.

1- خوارزمية التّشفير : مجموعة من الخطوات المتسلسلة منطقيّا ورياضيّا لحلّ مشكلة ما، ويقصد بخوارزميّة التّشفير مجموعة الخطوات المستخدمة لتحويل الرّسالة الأصليّة إلى رسالة مشفّرة .

2- مفتاح التّشفير : سلسلة الرّموز المستخدمة في خوارزميّة التّشفير،وتعتمد قوة التّشفير على قوّة هذا المفتاح

3- النّص الأصلي : يقصد بها محتوى الرّسالة الأصليّة قبل التّشفير وبعد عمليّة فك التّشفير .

4- نص الشّيفرة: الرّسالة بعد عمليّة التّشفير .

- تمرين: حدّد إلى أي من عناصر التّشفير يتبع كل ممّا يلي:

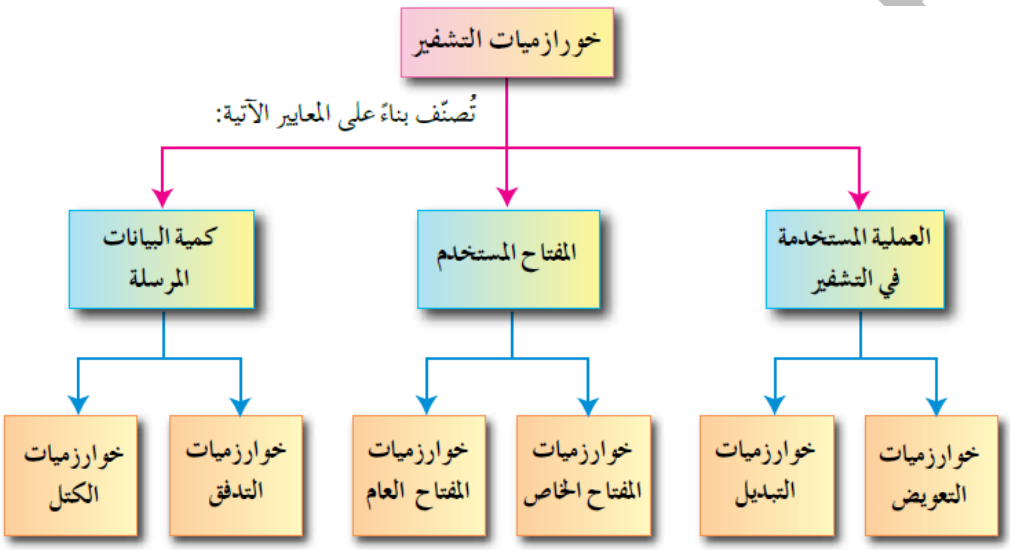
#	العبارة	العنصر
1	مجموعة من الخطوات المتسلسلة لتحويل الرّسالة الأصليّة إلى رسالة مشفّرة.	خوارزميّة التّشفير .
2	الرّسالة بعد عمليّة التّشفير .	نصّ الشّيفرة.
3	سلسلة من الرّموز تستخدم من خلال خوارزميّة التّشفير.	مفتاح التّشفير .
4	الرّسالة الأصليّة قبل عمليّة التّشفير أو بعد عمليّة فك التّشفير .	النّصّ الأصلي .

خوارزميّات التّشفير

- معايير تصنيف خوارزميّات التّشفير :
1- إستخدام المفتاح .
2- كميّة المعلومات المرسلة.
3- العمليّة المستخدمة في التّشفير. (نوع عمليّة التّشفير).

- أنواع خوارزميّات التّشفير:
1- خوارزميّات التّعويض.
2- خوارزميّات التّبديل.
3- خوارزميّات المفتاح الخاص.
4- خوارزميّات المفتاح العام.
5- خوارزميّات التّدفق.
6- خوارزميّات الكتل.

- حدّد أنواع خوارزميّات التّشفير، إذا قسّمت بناء على المعايير التّالية:
أ- المفتاح المستخدم:خوارزميّات التّشفير بإستخدام المفتاح الخاص، وخوارزميّات التّشفير بإستخدام المفتاح العام.
ب- كميّة المعلومات المرسلة: شيفرات التّدفق، و شيفرات الكتل.
ج- العمليّة المستخدمة في التّشفير: التّشفير بالتّعويض، والتّشفير بالتّبديل.



أولا: التّشفير المعتمد على نوع عمليّة التّشفير:
- يقسم هذا النّوع إلى :
أ- طريقة التّشفير **<u>بالتّعويض</u>**:طريقة لتشفير النصوص، يتم خلالها إستبدال حرف مكان حرف او مقطع مكان مقطع **ومثال** علها شيفرة الإزاحة .
ب- طريقة التّشفير **<u>بالتّبديل</u>** : طريقة تشفير تقوم على تبديل أماكن الأحرف عن طريق إعادة ترتيب أحرف الكلمة بشرط إستخدام الأحرف <u>نفسها</u> من دون إجراء أي تغيير عليها.

- ملاحظة: عند تنفيذ عمليّة التبديل يختفي معنى النّص الحقيقي، وهذا يشكّل عمليّة التّشفير شريطة أن تكون قادرا على إسترجاع النّصّ الأصلي منها .

- وفي ما يأتي توضيح لخوارزميّة الخطّ المتعرّج التي تستخدم شيفرة التّبديل :
- خوارزمية الخط المتعرّج: هي خوارزميّة تتميّز بأنّها سهلة وسريعة ويمكن تنفيذها يدويّا باستخدام الورقة والقلم،ويمكن فكّ تشفيرها بسهولة .

- خطوات تشفير النّصّ حسب خوارزميّة الخط المتعرّج :
1- حدّد عدد الأسطر التي ستستخدم لتشفير النّص حيث أنّ عدد الأسطر يعدّ مفتاح التّشفير، ولا يلزمنا معرفة عدد الأعمدة (إبدأ بأيّ عدد من الأعمدة ويمكن الزّيادة عند الحاجة).
2- إملأ الفراغ في النّص الأصلي بمثلّث مقلوب.
لاحظ : إستخدام المثلّث المقلوب بديلا للفراغ لغايات تسهيل الحلّ فقط.
3- انشئ جدولا يعتمد على عدد الأسطر (مفتاح التّشفير).
4- وزّع أحرف النّصّ المراد تشفيره بشكل <u>قطري</u> حسب إتّجاه الأسهم.
5- ضع مثلّثا مقلوبا في الفراغ الاخير وذلك كي تكون الأطوال متساوية.
6- أكتب النّص المشفّر <u>سطرا سطرا</u>.

- ملاحظة: مفتاح التّشفير يتم الاتّفاق عليه مسبقا من قبل مرسل الرّسالة ومستقبلها فقط وسيتمّ تزويدك به لغايات حلّ السّؤال .

- مثال 1: شفّر النّص التّالي، علما بأنّ مفتاح التّشفير سطران.

I love my country

1- حدّد مفتاح التّشفير و هو سطران.

2- إملأ الفراغ بالنّص الأصلي بمثلّث مقلوب.

النّص الأصلي : I▽love▽my▽country

3- أنشئ جدولا ، علما بأنّ عدد الصّفوف = **2** و أضف أعمدة عند الحاجة.

4- وزّع أحرف النّص بشكل قطري:

I		l		v		▽		y		c		u		t		y	
	▽		o		e		m		▽		o		n		r		

5- ضع مثلّثا مقلوبا ▽ في الفراغ الأخير، و ذلك كي تصبح الأطوال متساوية.

I		l		v		▽		y		c		u		t		Y	
	▽		o		e		m		▽		o		n		r		▽

6- اكتب النّص المشفّر سطرا سطرا. و رتّبه على التّوالي:

- النّصّ الأصلي : I love my country
- النّصّ المشفّر : Ilv▽ycuty▽oem▽onr▽

-مثال 2: حد النّص المشفّر للنّص الأصلي التّالي،علما بأنّ مفتاح التّشفير هو خمسة أسطر.

Stay positive this year makes you happy all life

1- حدّد مفتاح التّشفير وهو خمسة أسطر، و تذكّر بأنه لا يلزمنا معرفة عدد الأعمدة.

2- املأ الفراغ بالنّصّ الأصلي بمثلّث مقلوب.

Stay▽positive▽this▽year▽makes▽you▽happy▽all▽life

3- انشئ جدولا ، علما بأنّ عدد الصّفوف = **5** و أضف أعمدة عند الحاجة.

4- وزّع أحرف النّص بشكل قطري، و ضع مثلّثا مقلوبا ▽ في الفراغ الأخير، لكي تصبح الأطوال متساوية.

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		▽

6- اكتب النّص المشفر سطرا سطرا. و رتّبه على التّوالي:

- النّص المشفّر:

Spiheayaaitoviakoplfasesreupleyi▽▽▽s▽y▽▽▽ttym▽h▽l▽

- مثال 3: جد النّصّ المشفّر للنصّ الأصلي التّالي، بإستخدام خوارزميّة الخطّ المتعرّج ،علما بأنّ مفتاح التّشفير هو ثمانية أسطر.

Investing in people is more important than investing in things

I		g		p		o		r		a		t		t							
	n		▽		l		r		t		n		i		h						
		v		i		e		e		a		▽		n		i					
			e		n		▽		▽		n		i		g		n				
				s		▽		i		i		t		n		▽		g			
					t		p		s		m		▽		v		i		s		
						i		e		▽		p		t		e		n		▽	
							n		o		m		o		h		s		▽		▽

- النّصّ المشفّر:

Igporattn▽lrtnihvieea▽nien▽▽nigns▽iitn▽gtpsm▽visie▽pten▽nomohs▽▽

-مثال 4: جد النّص المشفّر للنّصّ التّالي، بإستخدام خوارزميّة الخط المتعرّج،ومفتاح التّشفير هو 3 أسطر

Let us keep our home safe and united

L		▽		▽		e		o		▽		m		s		e		n		u		t		
	e		u		k		p		u		h		e		a		▽		d		n		e	
		t		s		e		▽		r		o		▽		f		a		▽		i		d

- النّصّ المشفّر:

L▽▽eo▽msenuteukpuhea▽dnetse▽ro▽fa▽id

- مثال5 : جد النّص المشفّر للنصّ الأصلي التّالي، باستخدام خوارزميّة الخطّ المتعرّج،(مفتاح التّشفير 4 أسطر)

Youth is the future and the spirit of our home

Y		h		▽		▽		u		a		t		s		i		f		r		m			
	o		▽		t		f		r		n		h		p		t		▽		▽		e		
		u		i		h		u		e		d		e		i		▽		o		h		▽	
			t		s		e		t		▽		▽		▽		r		o		u		o		▽

- النّص المشفّر:

Yh▽▽uatsifrmo▽tfrnhpt▽▽euihuedei▽oh▽tset▽▽▽rouo▽

- مثال 6: شفّر النّص الأصلي التّالي،باستخدام خوارزميّة الخط المتعرّج (مفتاح التّشفير ستّة أسطر).

School is the place where great people and ideas are formed

S		▽		e		e		e		t		l		▽		▽		o					
	c		i		▽		▽		▽		▽		e		i		a		r				
		h		s		p		w		g		p		▽		d		r		m			
			o		▽		l		h		r		e		a		e		e		e		
				o		t		a		e		e		o		n		a		▽		d	
					l		h		c		r		a		p		d		s		f		▽

- النّص المشفّر:

S▽eeetl▽▽oci▽▽▽▽eiarhspwgp▽drmo▽lhreaeeeotaeeona▽dlhcrapdsf▽

- مثال 7: جد النّص المشفّر للنصّ الأصلي التّالي، بإستخدام خوارزميّة الخط المتعرّج ،علما بأنّ مفتاح التّشفير هو أربعة أسطر.

Stop thinking about your past mistakes

S		▽			n			g		o		y		▽		t		s		e		
	t		t			k			▽		u		o		p		▽		t		s	
		o		h			i			a		t		u		a		m		a		▽
			p		i			n			b		▽		r		s		i		k		▽

- النّص المشفّر:

S▽ngoy▽tsettk▽uop▽tsohiatuama▽pinb▽rsik▽

- مثال 8: جد النّص المشفّر للنصّ الأصلي التّالي، باستخدام خوارزميّة الخط المتعرّج ،علما بأنّ مفتاح التّشفير هو ثلاثة أسطر.

Never give up on your goals

N		e		g		e		p		n		o		▽		a		
	e		r		i		▽		▽		▽		u		g		l	
		v		▽		v		u		o		y		r		o		s

- النّصّ المشفّر:

Negepno▽aeri▽▽▽uglv▽vuoyros

- ملاحظات:

- نلاحظ بأن النّص المشفّر أخفى الرّسالة، ولن يستطيع أي شخص متطفّل أن يفهم محتواها.
- يمكن تشفير أحرف اللّغة العربيّة باستخدام هذه الخوارزميّات ،ولكنّها غير مطلوبة من الطّلبة في هذا الكتاب.
- تشفير نصّ يحتوي على علامات ترقيم غير مطلوب في هذا الكتاب.

فكّ التّشفير

- خطوات فك التّشفير :

1- إملأ الفراغ بمثلّث مقلوب.

2- قسّم النّص المشفّر إلى أجزاء إعتمادا على عدد الأسطر (مفتاح التّشفير) أيّ أنّ عدد الأجزاء يساوي عدد الأسطر . ولتحديد عدد الأحرف في كلّ سطر (جزء) نقوم بما يأتي :

مجموع أحرف النّص المشفّر(بما فيها الفراغات) ÷ عدد الأجزاء

- ملاحظه: إذا كان الناتج عدد كسري نقرّبه إلى أقرب عدد صحيح أكبر منه.

3- أكتب الحرف الأوّل من كل جزء ثمّ الحرف الثّاني ثمّ الحرف الثّالث وهكذا...

- مثال 9: جد النّصّ الأصلي للنصّ المشفّر التّالي، علما بأنّ مفتاح التّشفير هو سطران.

Ilv ycuty oem onr

- الحل:

1- إملأ الفراغ بمثلّث مقلوب.

Ilv▽ycuty▽oem▽onr

2- قسّم النّص المشفّر إلى جزأين، لأن مفتاح التشفير سطران،(إذا كان الناتج عدد كسري نقرّبه إلى أقرب عدد صحيح أكبر منه.)

17 ÷ 2 = 8.5 ثمّ نقرّبه إلى أقرب عدد صحيح أكبر منه ، و هو 9

- ذلك يعني أن الحل سيكون على سطران، و كل سطر (جزء) يتكوّن من تسعة رموز (أحرف).

I	l	v	▽	y	c	u	t	y	الجزء (السّطر) الأوّل
▽	o	e	m	▽	o	n	r	▽	الجزء (السّطر) الثّاني

- نأخذ الحرف الأوّل من كل جزء بشكل عمودي ثمّ الحرف الثّاني ثمّ الحرف الثّالث وهكذا...

I▽love▽my▽country▽

- النّص الأصلي: I love my country

- مثال 10: فكّ تشفير النّص التّالي باستخدام خوارزميّة الخط المتعرّج علما بأنّ مفتاح التّشفير هو ستّة أسطر

Hwote ▽ ▽ eoem ▽esp ▽meeupwl ▽etvs ▽ee ▽▽ ▽ l ▽ iea ▽ shektts ▽

- الحل:

48 ÷ **6 = 8 أحرف في كلّ سطر.**

H	w	o	t	e	▽	▽	e	السّطر الأوّل
o	e	m	▽	e	s	p	▽	السّطر الثّاني
m	e	e	u	p	w	l	▽	السّطرالثّالث
e	t	▽	s	▽	e	e	▽	السّطر الرّابع
▽	▽	l	▽	i	e	a	▽	السّطر الخامس
s	h	e	k	t	t	s	▽	السّطر السّادس

Home▽sweet▽home▽let▽us▽keep▽it▽sweet▽please▽▽▽▽▽

Home sweet home let us keep it sweet please

- مثال 11: فكّ تشفير النّص التّالي باستخدام خوارزميّة الخط المتعرّج علما بأنّ مفتاح التّشفير هو ثلاثة أسطر

Bieno ▽ itsee ▽▽ uali ▽ lviyrbie ▽

- الحل:

27 ÷ 3 = 9 أحرف في كلّ سطر.

B	i	e	n	o	▽	i	t	s	السّطر الأوّل
e	e	▽	▽	u	a	l	i	▽	السّطر الثّاني
l	v	i	y	r	b	i	e	▽	السّطرالثّالث

Believe▽in▽your▽abilities▽

Believe in your abilities

- مثال 12: فكّ تشفير النّص التّالي باستخدام خوارزميّة الخط المتعرّج (مفتاح التّشفير هو سبعة أسطر).

Eoterkodnhmon▽u▽eemelci▽n▽siasmtdsgt▽o▽a▽hltvfrtt

- الحل:

49 ÷ 7 = 7 أحرف في كلّ سطر.

E	o	t	e	r	k	o	السّطر الأوّل
d	n	h	m	o	n	▽	السّطر الثّاني
u	▽	e	e	m	e	l	السّطرالثّالث
c	i	▽	n	▽	s	i	السّطر الرّابع
a	s	m	t	d	s	g	السّطر الخامس
t	▽	o	▽	a	▽	h	السّطر السّادس
i	t	v	f	r	t	t	السّطر السّابع

Education▽is▽the▽movement▽from▽darkness▽to▽light

Education is the movement from darlness to light

- مثال 13: فكّ تشفير النّص التّالي باستخدام خوارزميّة الخط المتعرّج (مفتاح التّشفير هو عشرة أسطر).

Tnr∇∇o∇eie∇t∇ndbhwvureeeci∇∇sagfmtthuu∇ittsioeutnn

أ- تقسيم النص إلى عشرة أجزاء.

عدد أحرف النص 50 حرف ÷ 10 = 5 أحرف في كل جزء.

T n r ∇ ∇	الجزء الأول
o ∇ e i e	الجزء الثاني
∇ t ∇ n d	الجزء الثالث
b h w v u	الجزء الرابع
r e e e c	الجزء الخامس
i ∇ ∇ s a	الجزء السادس
g f m t t	الجزء السابع
h u u ∇ i	الجزء الثامن
t t s i o	الجزء التاسع
e u t n n	الجزء العاشر

ب- أخذ الحرف الأول من كل جزء لتشكيل النص الاصلي.

To∇brighten∇the∇future∇we∇must∇invest∇in∇education

- مثال 14 : فكّ تشفير النّص التّالي باستخدام خوارزميّة الخط المتعرّج (مفتاح التّشفير هو خمسة أسطر).

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

الحلّ: ٥٠ ÷ ٥ = ١٠ أحرف في كل جزء.

S p i h e a y a a i	السطر الأول
t o v i a k o p l f	السطر الثاني
a s e s r e u p l e	السطر الثالث
y i ∇ ∇ ∇ s ∇ y ∇ ∇	السطر الرابع
∇ t t y m ∇ h ∇ l ∇	السطر الخامس

Stay ∇ positive ∇ this ∇ year ∇ makes ∇ you ∇ happy ∇ all ∇ life

النص الأصلي:

Stay positive this year makes you happy all life

- ثانيا: التّشفير المعتمد على المفتاح :

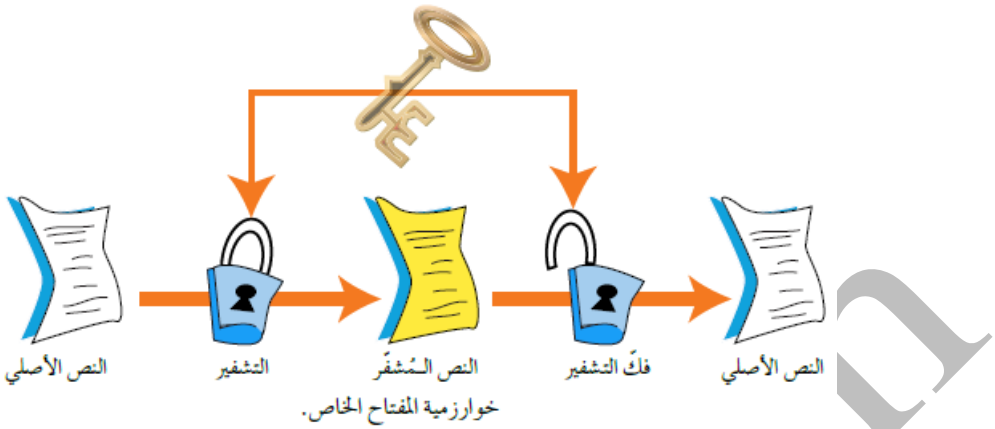
يعتمد هذا النّوع من خوارزميّات التّشفير على عدد المفاتيح المستخدمة في عمليّة التّشفير، وعليه فان امن الرّسالة او المعلومة يعتمد على سرية المفتاح وليس على تفاصيل الخوارزمية.

- على ماذا يعتمد أمن الرّسالة أو المعلومة عند تشفيرها بنوع " التّشفير المعتمد على المفتاح " ؟

يعتمد على سرية المفتاح وليس على تفاصيل الخوارزمية.

- يقسم هذا النّوع إلى قسمين :

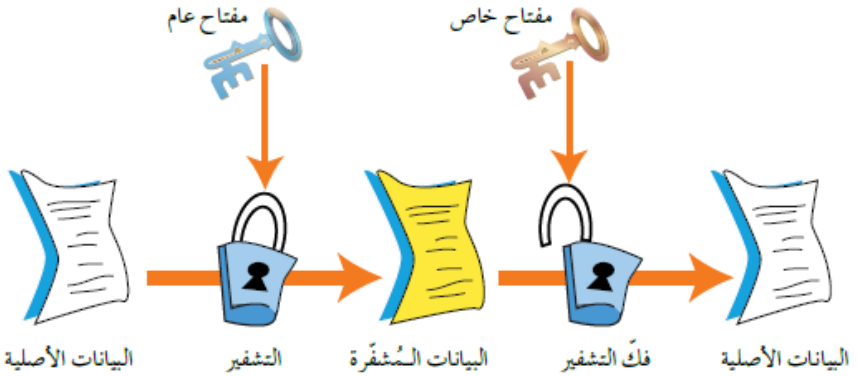
أ- خوارزميّات المفتاح الخاص : يطلق عليها أيضا اسم الخوارزميّات الّتناظريّة حيث أن المفتاح نفسه يستخدم لعمليتيّ التّشفير وفك التّشفير، ويتمّ الإتّفاق على إختياره قبل بدء عمليّة التّراسل بين المرسل والمستقبل، لذا تسمّى أيضا خوارزميّات المفتاح السّري. انظر الشكل:



خوارزمية المفتاح الخاص.

- علل: لماذا سمّيت خوارزميّات المفتاح الخاص (الّتناظريّة) بهذا الإسم ؟
نتيجة لإستخدام نفس المفتاح في عمليّتيّ التّشفير و فكّ التّشفير.

ب- خوارزميّات المفتاح العام : تستخدم هذه الخوارزميّات مفتاحين احدهما يستخدم لتشفير الرّسالة ويكون معروفا (للمرسل والمستقبل)، ويسمى المفتاح العام والآخر يكون معروفا لدى المستقبل فقط ويستخدم لفك التّشفير ويسمى المفتاح الخاص يتم إنتاج المفتاحين خلال عمليّات رياضيّة ولا يمكن معرفة المفتاح الخاص من خلال معرفة المفتاح العام . يسمى هذا النّوع ايضا الخوارزميّات اللاتناظرية . انظر الشكل :



خوارزمية المفتاح العام.

- علل: لماذا سمّيت خوارزميّات المفتاح العام (اللاتناظرية) بهذا الإسم ؟
نتيجة لإستخدامها لمفتاحين أحدهما عامّ ،لتشفير الرّسالة ويكون معروفا (للمرسل والمستقبل)، والآخر خاصّ، لفك التّشفير ويكون معروفا للمستقبل فقط، يتمّ إنتاج المفتاحين خلال عمليّات رياضيّة.

- ثانيا: التّشفير المعتمد على كمية المعلومات المرسلة:

- يقسم التّشفير المعتمد على كمية المعلومات المرسلة الى قسمين :

أ- شيفرات التدفّق : يعمل هذا النّوع من الخوارزميّات على تقسيم الرّسالة إلى مجموعة أجزاء ويشفّر كل جزء منها على حدة ومن ثم يرسله.

ب- شيفرات الكتل : تقسم الرّسالة أيضا إلى أجزاء ولكن بحجم أكبر من حجم الأجزاء في شيفرات التدفّق، ويشفّر أو يفكّ تشفير كل كتلة على حدة' يختلف عن شيفرات التدفق بان حجم المعلومات أكبر لذا فانّها أبطأ.

- علل: يعد استخدام التشفير ب "شيفرات الكتل" أبطأ من شيفرات التّدفّق ؟
تقسم الرّسالة فيها إلى أجزاء ولكن بحجم أكبر من حجم الأجزاء في شيفرات التدفّق، ويشفّر أو يفكّ تشفير كل كتلة على حدة (ان حجم المعلومات أكبر لذا فانّها أبطأ).