مراجعة مكثفة

في

علوم الحاسوب

الوحدة الرابعة (أمن المعلومات والتشفير)

توزيع العلامات الوزارية حسب الدورات تقريبيا

2018 شتوي	32 علامة
2018 صيفي	31 علامة
2019 شتوي	38علامة

المراكز المعتمدة لمكثف النيرد

المنطقة	اسم المركز	التاريخ	الوقت	هاتف
طبربور	زاوية الاذكياء	5/16-15-14	9-11.30 بعد الافطار	0797783000
المنارة	محمد مشعل	5/25-24-23	9-11.30 بعد الافطار	0796588890
نزال	وجية والفقية	5/19-18-17	9-11.30 بعد الافطار	0790793936
نزال	عبسي ومشعل	5/22-21-20	9-11.30 بعد الافطار	0779860606
موقع وتد التعليمي أون لاين 0788334399				

إعداد

الاستاذ احمد شهاب (صيفي 2019) 0796459006

هنا عزيزي اضعلك بعض تعاريف الوحدة الرابعة

• أمن المعلومات	هو العلم الذي يعمل على حماية المعلومات والمعدات المستخدمة لتخزينها ومعالجتها ونقلها , من السرقة أو التطفل أو من الكوارث الطبيعية أو جميعها . ويعمل على إبقائها متاحة للأفراد المصرح لهم استخدامها .
• الثغرات	يقصد بها نقطة الضعف في النظام سواء أكانت في الإجراءات المتبعة مثل تحديد صلاحيات الوصول ،أو مشكلة في تصميم النظام ، أو في مرحلة التنفيذ ، كما أن عدم كفاية الحماية المادية للإجهزة والمعلومات تعتبر من نقاط الضعف التي قد تتسبب في فقدان المعلومات أو هدم النظام أو تجعله عرضة للإعتداء الإلكتروني
• سرية المعلومات	عدم القدرة على الحصول على المعلومات ،إلا من قبل الأشخاص المخول لهم ذلك
• توافر المعلومات	قدرة الشخص المخول الحصول على المعلومات في الوقت الذي يشاء ، من دون وجود عوائق
• الهجوم الإلكتروني او الاعتداء الإلكتروني	تهديد موجه ومتعمد لجهاز معين ؛بقصد الإضرار به
• الضوابط المادية	مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها ؛باستخدام الجدران والأسوار والأقفال ،ووجود حراس الأمن ، وغيرها من أجهزة أطفاء الحريق
• الضوابط الإدارية	الأوامر والإجراءات المتفق عليها لمنع أي دخول غير مصرح به ، وتشمل القوانين واللوائح والسياسات،والإجراءات التوجيهية ،وحقوق النشر ،وبراءات الاختراع والعقود والاتفاقيات
• النمط الثابت لتحويل العناوين الرقمية	طريقة يتم من خلالها تخصيص عنوان رقمي خارجي لكل جهاز داخلي ،وهذا العنوان الرقمي ثابت لا يتغير ،يستخدمه الجهاز في كل مرة يرغب فيها بالاتصال مع الاجهزة خارج الشبكة
• 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 متاحاً للأجهزة الأخرى
• التشفير بالتعويض	طريقة لتشفير النصوص وتعني استبدال حرف مكان حرف أو مقطع مكان مقطع
• التشفير بالتبديل	طريقة لتشفير النصوص وتعني تبديل أماكن الأحرف ،وذلك عن طريق إعادة ترتيب أحرف الكلمة ؛بشرط استخدام الأحرف نفسها من دون إجراء أي تغيير عليها
• التشفير	هو تغيير محتوى الرسالة الأصلية سواء أكان التغيير بمزجها بمعلومات أخرى ، أم استبدال الأحرف الأصلية والمقاطع بغيرها ،أم تغير بطريقة لن يفهمها إلا مرسل الرسالة ومستقبلها فقط باستخدام خوارزمية معينة ومفتاح خاص
• الهندسة الاجتماعية	هي الوسائل والأساليب التي يستخدمها المعتدي الإلكتروني ؛لجعل مستخدم الحاسوب في النظام يعطي معلومات سرية ؛ أو يقوم بعمل ما ،يسهل عليه الوصول إلى أجهزة الحاسوب أو المعلومات المخزنة فيها
IP Address*	هو عنوان رقمي مميز لكل جهاز حاسوب أو هاتف خلوي
• العنوان الرقمي الخارجي	هو ناتج تحويل العنوان الرقمي الداخلي الخاص بجهاز ما باستخدام تقنية تحويل العناوين (NAT) من خلال جهاز وسيط ،ليمكنه من الاتصال بشبكة الإنترنت او بالأجهزة الأخرى .
• متصفح الإنترنت	هو برنامج ينقل المستخدم إلى صفحة (الويب) التي يريدها بمجرد كتابة العنوان والضغط على زر الذهاب ، ويمكنه من مشاهدة المعلومات على الموقع
** خوارزمية التشفير	مجموعة من الخطوات المستخدمة لتحويل الرسالة الأصلية الى راسلة مشفرة
• المفتاح العام	هو مفتاح الرسالة ويكون معروفاً لكل من المُرسل والمُستقبل
• المفتاح الخاص	هو مفتاح فك التشفير ويكون معروفاً فقط للمستقبل
********الخوارزمية	هي عبارة عن مجموعة من الخطوات المتسلسلة منطقيا ورياضيا لحل مشكلة ما
• السلامة	حماية الرسائل أو المعلومات التي تم تداولها والتأكد بأنها لم تتعرض لأي عملية تعديل سواءا : الإضافة ، أو استبدال أو حذف جزء منها

- علل : أهتمت الشعوب قديما بالحفاظ على سرية المعلومات؟
  - للحفاظ على اسرارها وهيبتها ومكانتها ولإنجاح مخططاتها العسكرية
- عرف أمن المعلومات :هو العلم الذي يعمل على حماية المعلومات والمعدات المستخدمة لتخزينها ومعالجتها ونقلها , من السرقة أو التطفل أو من الكوارث الطبيعية أو جميعها . ويعمل على إبقائها متاحة للأفراد المصرح لهم استخدامها .
- يهدف أمن المعلومات للحفاظ على ثلاثة خصائص أساسية ،أذكرها ؟
  1. السرية
  2. سلامة المعلومات — هام جدا جدا
  3. توافر المعلومات
- عرف السرية (سرية المعلومات) : وتعني أن الشخص المخول هو الوحيد القادر على الوصول إلى المعلومات والاطلاع عليها
- ☒ السرية : مصطلح مرادف لمفهومي الأمن (Security) والخصوصية (Privacy)

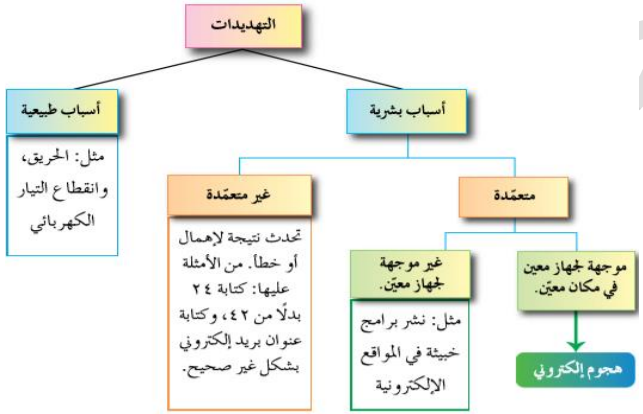
الاستاذ احمد شهاب كل التوفيق

- اذكر أمثلة على معلومات تحتاج إلى سرية ؟
  - المعلومات الشخصية
  - والموقف المالي لشركة ما قبل إعلانه
  - المعلومات العسكرية
  - بيانات يعتمد أمنها على مقدار الحفاظ على سريتها .
- عرف السلامة (سلامة المعلومات) : وتعني حماية الرسائل أو المعلومات التي تم تداولها , و التأكد بأنها لم تتعرض لأي عملية تعديل سواء : بالإضافة أم الاستبدال أم حذف جزء منها
- اذكر أمثلة على معلومات تحتاج الى الحفاظ على سلامتها؟
  - عند نشر نتائج طلبة الثانوية العامة ،يجب الحفاظ على سلامة هذه النتائج من أي تعديلات
  - عند صدور قوائم القبول الموحد للجامعات الأردنية والتخصصات التي قبل فيها الطلبة ، فلا بد من العمل على حماية هذه القوائم من أي تعديل أو حذف أو تبديل أو تغير .
- عرف توافر المعلومات: قدرة الشخص المخول الحصول على المعلومات في الوقت الذي يشاء من دون وجود عوائق
- متى تكون المعلومات بلا فائدة ؟
  - إذا لم يمكن متاحة للأشخاص المصرح لهم بالتعامل معها
  - أو أن الوصول إليها يحتاج إلى وقت كبير

- اذكر الوسائل التي يقوم بها المخترقون لجعل المعلومات غير متاحة؟
  1. حذفها
  2. الاعتداء على الاجهزة التي تخزن فيه هذه المعلومات

أنواع تهديدات أمن المعلومات ...

- تتقسم المخاطر التي تهدد أمن المعلومات إلى نوعين رئيسين ،إذكرهما ؟
  - التهديدات — الاستاذ احمد شهاب
  - الثغرات



- من المخاطر التي تهدد أمن المعلومات التهديدات ولها سببين ،اذكرهما ؟
  - أسباب بشرية — 0796459006
  - أسباب متعمدة
- ما آثر التهديدات الناتجة عن الأسباب الطبيعية ؟
  - تؤدي الى فقدان المعلومات
- اذكر مثال على تهديدات من الاسباب طبيعية ؟
  - حدوث الحريق
  - انقطاع التيار الكهربائي .
- اذكر أنواع المسببات البشرية للتهديدات ؟
  - متعمدة
  - غير متعمدة
- تقسم التهديدات البشرية المتعمدة الى قسمين ، اذكرهما ؟
  - موجهة لجهاز معين
  - غير موجهة لجهاز معين

- تسمى التهديدات لأسباب بشرية الموجهة لجهاز معين في مكان معين اسمين ،اذكرهما ؟
  - الهجوم الالكتروني
  - الأعتداء الالكتروني
- اذكر مثال على تهديدات بشرية متعمدة وموجه لجهاز معين
  - هجوم الكتروني
- اذكر مثال على تهديدات بشرية غير موجهة لجهاز معين
  - نشر برامج خبيثة في المواقع الإلكترونية
- اذكر مثال على تهديدات بشرية متعمدة موجهة لجهاز معين في مكان معين ؟ // مثال على هجوم الكتروني او الاعتداء الالكتروني ..
  - سرقة جهاز الحاسوب
  - سرقة إحدى المعدات التي تحفظ المعلومات
  - التعديل على ملف أو حذفة
  - الكشف عن بيانات سرية أو منع الوصول إلى المعلومات .
- عرف الهجوم الإلكتروني : تهديد موجه ومتعمد لجهاز معين ،بقصد الإضرار به
- ما هو أخطر أنواع التهديدات ؟
  - الهجوم الالكتروني
- يعتمد نجاح الاعتداء الإلكتروني على ثلاثة عوامل رئيسية ، اذكرهما ؟
  - الدافع — هام جدا جدا
  - الطريقة
  - فرصة النجاح
- تتنوع دوافع الأفراد لتنفيذ هجوم إلكتروني ؟ اذكر هذه الدوافع ؟
  - رغبة الحصول على المال
  - محاولة لإثبات القدرات التقنية
  - بقصد الإضرار بالآخرين
  -

النجاح هو حليفك عزيزي : تأكد ان الملخص تم عمله بعناية
خوفا عليكم اتمنى لكم كل التوفيق والناجح دائما

ان شاء الله بشوفك بالجامعة عزيزي

- ماهي الطريقة (المهارات) التي يتميز بها المعتدي الإلكتروني ؟
  - قدرته على توفير المعدات والبرمجيات الحاسوبية التي يحتاج إليها
  - معرفة بتصميم النظام وآلية عمله
  - معرفة نقاط القوة والضعف لهذا النظام
- تتمثل فرصة نجاح الهجوم الإلكتروني بعملين ،إذكرهما ؟
  - تحديد الوقت المناسب للتنفيذ
  - ومعرفة كيفية الوصول إلى الإجهزة
- هام) يهدف أمن المعلومات للحفاظ على ثلاث خصائص أساسية هي : (سرية المعلومات ،وسلامة المعلومات ،وتوافر المعلومات) حدد إلى أي هذه الخصائص يتبع كل مما يأتي :
  - التأكد من عدم حدوث أي تعديل ؟
    - ✓ الاجابة سلامة المعلومات
  - الشخص المخول هو الوحيد القادر على الوصول إلى المعلومات والاطلاع عليها
    - ✓ الاجابة سرية المعلومات
  - الوصول إلى المعلومات يحتاج إلى وقت كبير
    - ✓ الاجابة : توافر المعلومات
  - مصطلح مرادف لمفهومي الأمن والخصوصية
    - ✓ الاجابة: سرية المعلومات
  - المعلومات العسكرية
    - ✓ الاجابة :سرية المعلومات
- تتعرض المعلومات إلى أربعة أنواع من الاعتداءات الإلكترونية ،أذكرها ؟
  - التنصت على المعلومات
  - التعديل على المحتوى
  - الإيقاف هام جدا
  - الهجوم المزور أو المفبرك هام جدا
- يهدف الاعتداءات الإلكترونية (الإخلال بسرية المعلومات ، الإخلال بسلامة المعلومات ،عدم توافر المعلومات) صنف الآتي :
  - التنصت على المعلومات ؟_____ ؟ الإجابة :الإخلال بسرية المعلومات
  - التعديل على المحتوى ؟_____ ؟ الإجابة :الإخلال بسلامة المعلومات
  - الإيقاف ؟_____ ؟ الإجابة :عدم توافر المعلومات
  - الهجوم المزور أو المفبرك ؟ _____ ؟ الإجابة : الإخلال بسرية المعلومات وسلامتها

- ما الهدف من هجمة التنصت على المعلومات ؟
  - الحصول على المعومات السرية ،حيث يتم الإخلال بسرية المعلومات
- وضح كيف يتم هجمة التعديل على المحتوى ؟
  - اعتراض المعلومات وتغيير محتواها وإعادة إرسالها للمستقبل من دون أن يعلم بتغير المحتوى ويتم الإخلال بسلامة المعلومات
- وضح عملية هجمة الإيقاف ؟
  - يتم قطع قناة الإتصال ومن ثم، منع المعلومات من الوصول إلى المستقبل وهنا يتم الإخلال بتوافر المعلومات
- وضح عملية الهجوم المزور أو المفبرك ؟
  - يقوم إرسال المعتدي الإلكتروني رسالة إلى أحد الإشخاص على الشبكة ،ويخبر فيها أنه صديقه ويحتاج إلى معلومات أو كلمات سرية خاصة.. وهنا يتم الإخلال بسرية المعلومات وقد تتأثر بسلامتها . ما الذي يمكن ان يتأثر في هذه العملية
- عرف الثغرات : نقطة الضعف في النظام سواء أكانت في الإجراءات المتبعة مثل تحديد صلاحيات الوصول ،أو مشكلة في تصميم النظام ، أو في مرحلة التنفيذ ، كما أن عدم كفاية الحماية المادية للإجهزة والمعلومات تعتبر من نقاط الضعف التي قد تتسبب في فقدان المعلومات أو هدم النظام أو تجعله عرضة للإعتداء الإلكتروني
- اذكر الأماكن المحتملة لوجود الثغرات في النظام ؟ // اذكر امثلة؟
  1. الإجراءات المتبعة في النظام
  2. مشكلة في تصميم النظام
  3. عدم كفاية الحماية المادية للإجهزة والمعلومات
- علل: إن عدم كفاية الحماية المادية للإجهزة والمعلومات ، تعد من نقاط الضعف ؟
  - لإنها قد تتسبب في فقدان المعلومات أو هدم النظام ،وتجعلة عرضة للاعتداء الالكتروني .
- يرى المختصون في مجال أمن المعلومات , بأن الحفاظ على المعلومات وأمنها ينبع من التوازن بين تكلفة الحماية وفعالية الرقابة من جهة , مع احتمالية الخطر من جهة أخرى , لذا ، وضعت مجموعة من الضوابط لتقليل من المخاطر التي تتعرض لها المعلومات والحد منها علل

- هناك مجموعة من الظوابط التي وضعت لتقليل المخاطر التي تتعرض لها المعلومات والحد منها ، أذكر هذه الظوابط ؟
  1. الظوابط مادية.
  2. الظوابط الادارية.
  3. الظوابط التقنية .
- عرف الظوابط المادية : مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها باستخدام الجدران والأسوار واستخدام الأقفال ووجود حراس الأمن وغيرها من أجهزة إطفاء الحريق .
- أعط مثال على استخدام ظوابط مادية ؟
  - باستخدام الجدران والأسوار
  - واستخدام الأقفال
  - ووجود حراس الأمن وغيرها من أجهزة إطفاء الحريق .
- عرف الظوابط الادارية : الأوامر والإجراءات المتفق عليها القوانين واللوائح والسياسات ،والإجراءات التوجيهية ، و حقوق النشر وبراءات الاختراع والعقود والاتفاقيات .
- إعط مثال على ظوابط إدارية ؟
  - القوانين واللوائح والسياسات
  - الإجراءات التوجيهية
  - حقوق النشر وبراءات الاختراع والعقود والاتفاقيات
- عرف الظوابط التقنية : وهي الحماية التي تعتمد على التقنيات المستخدمة , سواء أكانت معدات أو برمجيات وتتضمن كلمات المرور ، ومنح صلاحيات الوصول ، وبروتوكولات الشبكات والجدر النارية ، والتشفير ، وتنظيم تدفق المعلومات في الشبكة .
- إعط مثال على ظوابط تقنية ؟
  1. كلمات المرور
  2. ومنح صلاحيات الوصول
  3. وبروتوكولات الشبكات والجدر النارية
  4. التشفير
  5. وتنظيم تدفق المعلومات في الشبكة
- ❖ معلومة : للوصول إلى أفضل النتائج ،تعمل الضوابط السابقة بشكل متكامل ،للحد من الأخطار التي تتعرض لها المعلومات

علل : يعد العنصر البشري من أهم مكونات الأنظمة , والاهتمام به من أهم المجالات ؟

- للحفاظ على أمن المعلومات .

يعتمد اختيار الكادر البشري المسؤول عن حماية الانظمة على مهارات (أمور) أذكر هذه الامور (المهارات) ؟

1. الكفاية العلمية
2. اختبارات شفوية وورقية
3. اخضاعهم لضغوط نفسية كل حسب موقعهم

علل | يعتمد اختيار الكادر البشري المسؤول عن حماية الانظمة على الكفاية العلمية واختبارات شفوية واخضاعهم لضغوط نفسية كل حسب موقعهم ؟

- للتاكد من قدرتهم على حماية هذا النظام .

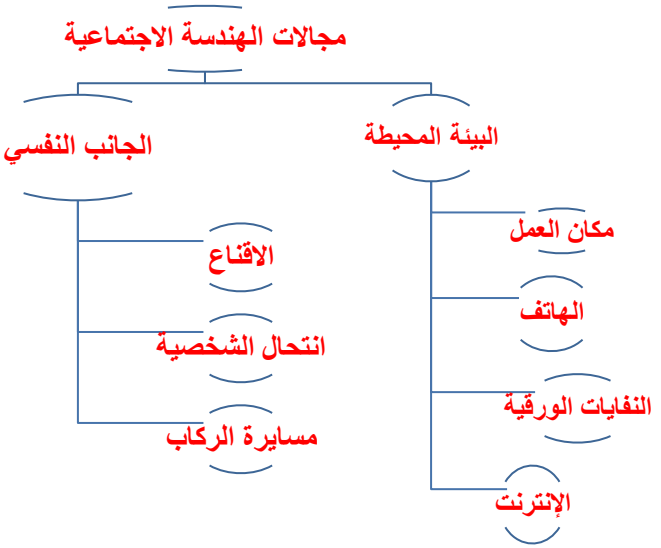
عرف الهندسة الاجتماعية : هي الوسائل والأساليب التي يستخدمها المعتدي الإلكتروني ؛لجعل مستخدم الحاسوب في النظام يعطي معلومات سرية ؛ أو يقوم بعمل ما ،يسهل عليه الوصول إلى أجهزة الحاسوب أو المعلومات المخزنة فيها .

علل | الهندسة الاجتماعية من أنجح الوسائل وأسهلها ،التي تستخدم للحصول على معلومات غير مصرح بها وبطريقة غير شرعية ؟

- بسبب قلة اهتمام المتخصصين في مجال أمن المعلومات ،وعدم وعي مستخدمي الحاسوب بالمخاطر المترتبة عليها

ترتكز الهندسة الأجتماعية في مجالين اثنين ، اذكرهما ؟

1. البيئة المحيطة
2. الجانب النفسي



وضح آلية عمل الهندسة الاجتماعية في مجال مكان العمل ؟

- يكتب بعض الموظفين كلمات المرور على أوراق ملصقة على الحاسوب . وعند دخول الشخص غير المخول 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.

وضح آلية عمل الهندسة الاجتماعية في مجال الهاتف ؟

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

وضح آلية عمل الهندسة الاجتماعية في مجال 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 او الحصول على المعلومات المرغوبة

علل | يعتبر الانترنت من أكثر وسائل الهندسة الاجتماعية شيوعا

- بسبب استخدام الموظفين أو مستخدمي الحاسوب عادة كلمات المرور نفسها للتطبيقات جميعها

وضح آلية عمل الهندسة الاجتماعية في مجال الانترنت

- حيث ينشئ المعتدي الإلكتروني موقعا على الشبكة , ويقدم خدمات معينة ويشترط التسجيل فيه للحصول على هذه الخدمات . ويتطلب التسجيل في المواقع اسم مستخدم وكلمة مرور ، وهي الكلمة المرور نفسها التي يستخدمها الشخص عادة ، وبهذه الطريقة يتمكن المعتدي الإلكتروني من الحصول عليها .

يسعى المعتدي من خلال الجانب النفسي الى

- كسب ثقة مستخدم الحاسوب
- الحصول على المعلومات الذي يرغب بها

اذكر اساليب التي يستخدمها المعتدي لكسب الثقة

- الاقناع
- انتحال الشخصية
- مسايرة الركب

وضح آلية عمل الهندسة الاجتماعية في الاقناع ؟

- يستطيع المعتدي إقناع الموظف أو مستخدم الحاسوب بطريقة مباشرة . بحيث يقدم الحجج المنطقية والبراهين . وقد يستخدم طريقة غير مباشرة بحيث يعتمد إلى تقديم إيحاءات نفسية ، تحث المستخدم على قبول المبررات بدون تحليلها أو التفكير فيها ،ويحاول التأثير بهذه الطريقة عن طريق إظهار نفسه بمظهر صاحب السلطة , أو إغراء المستخدم بامتلاك خدمة نادرة , حيث يقدم له عرضا معينا من خلال موقعه الإلكتروني لمدة محددة ، يمكنه ذلك من الحصول على كلمة المرور . وقد يلجا المعتدي الإلكتروني إلى إبراز أوجه التشابه مع الشخص المستهدف , لإقناعه بأنه يحمل الصفات والاهتمامات نفسها , فيصبح الشخص أكثر ارتياحا واقل حذرا للتعامل معه فيقدم له ما يريد من المعلومات .

كيف يمكن للمعتدي التأثير على مستخدم الحاسوب بطريقة غير المباشرة

- إظهار نفسه بمظهر صاحب السلطة
- إغراء المستخدم بامتلاك خدمة نادرة , حيث يقدم له عرضا معينا من خلال موقعه الإلكتروني لمدة محددة ، يمكنه ذلك من الحصول على كلمة المرور
- إبراز أوجه التشابه مع الشخص المستهدف

وضح آلية عمل الهندسة الاجتماعية في مجال انتحال الشخصية ؟

- حيث يتقمص شخص شخصية آخر , وهذا الشخص يكون حقيقيا أو وهميا . فقد ينتحل شخصية فني صيانة معدات الحاسوب , أو عامل نظافة أو حتى المدير أو السكرتير ،

علل | الشخصية المنتحلة غالبا تكون ذات سلطة ؟

- حتى يبدي أغلب الموظفين خدماتهم , ولن يترددوا بتقديم أي معلومات لهذا الشخص المسؤول.

- وضح آلية عمل الهندسة الاجتماعية في مجال مسايرة الركب؟
  - حيث يرى الموظف بأنه إذا قام زملاءه جميعهم بأمر ما , فمن غير اللائق أن يأخذ هو موقفا مغايرا
  - عندما يقدم شخص نفسه على إنه إداري من فريق الدعم الفني ، ويرغب بالحصول بعمل تحديثات على الأجهزة ، فإذا سمح له أحد الموظفين بعمل تحديث على جهازه، فإن باقي الموظفون يقومون بمسايرة زميلهم غالبا ، والسماح لهذا المعتدي باستخدام أجهزتهم لتحديثها ، ومن ثم يتمكن من الإطلاع على المعلومات التي يريدها والمخزنة على الأجهزة .
- سؤال هام : توجد ثلاثة عوامل توخذ في الحسبان لتقيم التهديد ، حدد العامل الذي يندرج تحته كل مما يأتي ؟
  1. الرغبة في اثبات القدرات ؟ الاجابة :الدافع
  2. معرفة نقاط القوة والضعف للنظام ؟ الاجابة :الطريقة
  3. تحديد الوقت المناسب للهجوم الالكتروني ؟ الاجابة : فرصة نجاح الهجوم .
  4. الاضرار بالإخرين ؟ الاجابة: الدافع
  5. الرغبة في الحصول على المال ؟ الاجابة :الدافع
  6. القدرة على توفير المعدات والبرمجيات الحاسوبية الاجابة الطريقة .
- يعتمد الافراد والمؤسسات والحكومات على تكنولوجيا المعلومات والاتصالات بشكلٍ واسع وفي شتى المجالات
- ما هي أسباب إيجاد وسائل تعمل على حمايةالانترنت (الويب)
  - انتشار البرامج والتطبيقات بشكل كبير ، منها ما هو مجاني ،ومنها ما هو غير معروف المصدر ،ومنها ما هو مفتوح
  - انتشار البرامج المقرصنة والمعلومات الخاصة بكيفية اقتحام المواقع
- تتعرض المواقع الإلكترونية لكثير من الاعتداءات الإلكترونية ، أذكر مثال على ذلك ؟ هـــــام جدا
  1. الاعتداء على متصفحات الانترنت
  2. الاعتداء على البريد الالكتروني
- عرف متصفح الإنترنت : هو برنامج ينقل المستخدم إلى صفحة (الويب) التي يريدها بمجرد كتابة العنوان والضغط على زر الذهاب ، ويمكنه من مشاهدة المعلومات على الموقع .
- علل| يتعرض متصفح الانترنت الى الكثير من الأخطار ؟
  - لأنها غير قابلة للتغير من دون ملاحظة ذلك من قبل المستخدم
- اذكر طرق الاعتداء على متصفحات الإنترنت ؟
  - الاعتداء عن طريق (كود) بسيط
  - توجيه المستخدم إلى صفحة أخرى غير الصفحة التي يريدها
- اذكر مبدأ عمل الاعتداء عن طريق كود بسيط
  - يمكن إضافته إلى المتصفح ، وباستطاعته القراءة ، والنسخ ، وإعادة إرسال أي شيء يتم من قبل المستخدم ويتمثل التهديد بالقدرة على الوصول إلى الحسابات المالية والبيانات الحساسة الأخرى
- اذكر الخطر الناتج عن الاعتداء بإضافة كود إلى المتصفح ؟
  - القدرة على الوصول إلى الحسابات المالية والبيانات الحساسة الأخرى
- اذكر مبدأ عمل الاعتداء على البريد الإلكتروني؟
  - تصل الكثير من الرسائل الإلكترونية إلى البريد الإلكتروني ، بعض هذه الرسائل الإلكترونية مزيفة ، وبعضها يسهل اكتشافه وبعضها الآخر استخدم بطريقة احترافية
  - يحاول المعتدي الإلكتروني التعامل مع الأشخاص القليلي الخبرة ،حيث يقدم عروض شراء المنتجات بعض المصممين بأسعار زهيدة أو رسائل تحمل عنوان كيف تصبح ثرياً
  - وهذه الرسائل تحتوي على روابط يتم الضغط عليها للحصول على المزيد من المعلومات .وغيرها من الرسائل المزيفة والمضللة التي تحتاج الى وعي من المستخدم
- اذكر مثال على وقاية المستخدمين من الاعتداءات على البريد الإلكتروني ؟
  - تحتاج إلى الوقاية منها إلى وعي من المستخدمين
- عرف تقنية تحويل العناوين الرقمية
  - هي التقنية التي تعمل على إخفاء العنوان الرقمي للجهاز في الشبكة الداخلية ،ليتوافق مع العنوان الرقمي المعطى للشبكة .
- من فوائد تقنية تحويل العناوين الرقمية :أن الجهاز الداخلي غير معروف بالنسبة إلى الجهات الخارجية وهذا يسهم في حماية أي هجوم قد يشن عليه بناءً على معرفة العناوين الرقمية ،
- علل : تحافظ تقنية العناوين الرقمية على أمن المعلومات في الويب ؟
  - أن الجهاز الداخلي غير معروف بالنسبة إلى الجهات الخارجية وهذا يسهم في حماية أي هجوم قد يشن عليه بناءً على معرفة العناوين الرقمية ،

❖ يرتبط ملايين الأشخاص عبر شبكة الإنترنت بملايين الأجهزة ، ولكل حاسوب أو هاتف خلوي عنوان رقمي خاص به يميزه عن غيرة يسمى NOTS

((Internet Protocol Address (IP Address

- عرف IP Address: هو عنوان رقمي مميز لكل جهاز حاسوب أو هاتف خلوي
- ماهو IP4، اذكر مكوناته ، مع ذكر مثال على ذلك ؟
  - هو IP Address يتكون من (32) خانة تتوزع على أربعة مقاطع يفصل بينهما نقاط ، وكل مقطع من هذه المقاطع يتضمن رقما من (0) إلى (255).
  - مثال (215.002.004.216)
- علل :سبب ظهور IPV6: نظرا للتطور الهائل في أعداد مستخدمي الإنترنت .ظهرت الحاجة إلى عناوين إلكترونية أكثر وطورت هذه العناوين لما يسمى IPV6
- يتكون IPV6 : من ثمانية مقاطع بدلاً من أربعه IP4
- على الرغم من استخدام IPV6 إلا انه لا يكفي لإتاحة عدد هائل من العناوين الرقمية ولحل هذه المعضلة وجد ما يسمى تقنية تحويل العناوين الرقمية ((Network Address Translation)(NAT)
- ماهو IPv6 ،اذكر مكوناته : الجواب : هو IP Address مطور عن IP4 ، ويتكون من ثمانية مقاطع بدلاً من أربعة
- علل ظهور أو استحداث IPv6: بسبب التطور الهائل في أعداد مستخدمي الأنترنت ظهرت الحاجة إلى عناوين إلكترونية أكثر
- اذكر الفرق بين IP4 و IPv6

IP4	يتكون من أربعة مقاطع
IPv6	يتكون من ثمانية مقاطع

علل ظهور تقنية تحويل العناوين الرقمية NAT : لأنة IPv6 لا تكفي لإتاحة عدد هائل من العناوين الرقمية

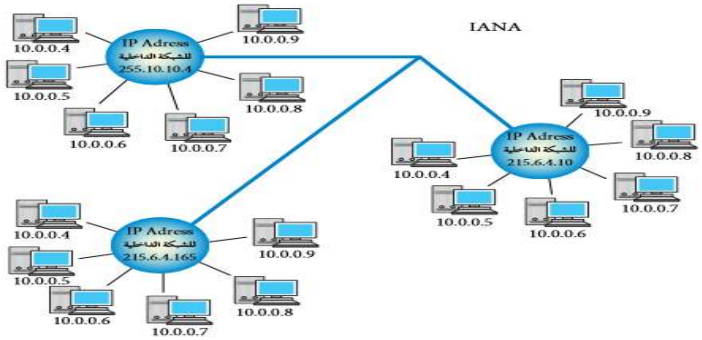
اذكر اختصار الآتي : IP Address ،NAT؟

IP Address	Internet Protocol Address
NAT	Network Address Translation

ما هو اختصار IANA: (Internet Assigned Numbers Authority)

عرف IANA: هي السلطة المسؤولة عن منح أرقام الإنترنت المخصصة لإعطاء العناوين الرقمية للأجهزة على الإنترنت

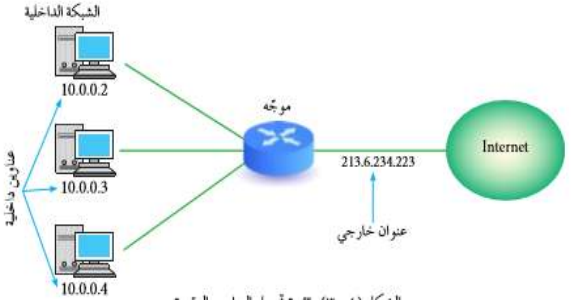
معلومة هامة : بسبب قلة أعداد أرقام الإنترنت المخصصة للعناوين الرقمية؛ فإن IANA تعطي الشبكة الداخلية عنواناً واحداً (أو مجموعة عناوين) ويكون معرفاً لها عند التعامل في شبكة الإنترنت . الرسمه هام جدا جدا



السؤال	الجواب
عدد الشبكات الداخلية لهذه الشبكة	3 شبكات
عدد العناوين الخاصة للإنترنت	255.10.10.4 215.6.4.10 215.6.4.10
هل يمكن ان يتكرر عنوان خاص للإنترنت ، لماذا	لا لا يمكن ان يتكرر في نفس اللحظة لأكثر من جهاز حول العالم ،لأنة رقم مميز وفريد ولا يجوز تكراره
مثال على عنوان رقمي داخل الشبكة	10.0.0.8
هل عناوين الأجهزة الداخلية في الشبكة تعتبر عناوين	لا

رقمية خاصة للإنترنت	
هل يمكن لأحد الأجهزة الداخلية أن يتصل بالإنترنت بدون عنوان انترنت خاص	لا
اذكر آلية اتصال أجهزة الشبكة الداخلية بالإنترنت	عند رغبة أحد الأجهزة بالتواصل مع جهاز الشبكة الداخلية ،يعدل العنوان الرقمي الخاص به ،باستخدام تقنية تحويل العناوين الرقمية NAT . وذلك يتم باستخدام جهاز وسيط يكون غالبا 1- موجهاً (Router) أو 2- جدارا نارياً (Firewall) يحول العناون الرقمي الداخلي إلى عنوان رقمي خارجي . ويسجل ذلك في سجل خاص للمتابعة
اذكر أمثلة على أجهزة وسيطة ؟	الموجه (Router) جداراً نارياً (Firewall)
اذكر مبدأ عمل الأجهزة الوسيطة	تحويل العناوين الداخلية إلى خارجية
عرف العنوان الرقمي الخارجي	هو ناتج تحويل العنوان الرقمي الداخلي الخاص بجهاز ما باستخدام تقنية تحويل العناوين (NAT) من خلال جهاز وسيط ،ليمكنه من الاتصال بشبكة الإنترنت او بالأجهزة الأخرى .

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



تعمل تقنية تحويل العناوين الرقمية بعدة طرائق ، اذكرها ؟

- النمط الثابت للتحويل
- النمط المتغير للتحويل

اذكر مبدأ عمل النمط الثابت للتحويل ؟

- يتم عن طريق هذا النمط تخصيص عنوان رقمي خارجي لكل جهاز داخلي ،وهذا العنوان ثابت لا يتغير .

اذكر مبدأ عمل النمط المتغير للتحويل ؟

- بهذه الطريقة يكون لدى الجهاز الوسيط عدد من العناوين الرقمية الخارجية ،ولكنها غير كافية لعدد الأجهزة في الشبكة . وهذه العناوين تبقى متاحة لجميع الأجهزة على الشبكة

بين آلية التراسل في مبدأ عمل النمط المتغير للتحويل ؟

- يتواصل مع الجهاز الوسيط الذي يعطيه عنواناً خارجيا مؤقتاً يستخدمة لحين الانتهاء من عملية التراسل ،ويعد هذا العنوان رقمياً خاصا بالجهاز . عند إنتهاء عملية التراسل ،يفقد الجهاز الداخلي هذا العنوان ،ويصبح العنوان متاحاً للتراسل مرة أخرى . وعند رغبة الجهاز نفسه بالتراسل مرة أخرى ، قد يعطى عنوانا مختلفاً عن المرة السابقة ، وهذا يفسر اختلاف IP Address للجهاز نفسه عند تراسله أكثر من مرة .

علل : اختلاف IP Address للجهاز نفسه عند تراسله مرة آخرى ؟

- بسبب النمط المتغير لتحويل العناوين الرقمية بحيث يتم إعطاء الجهاز عنواناً رقمياً مختلفاً في كل مرة يتواصل فيها مع أجهزة خارج الشبكة الخارجية

من أسئلة الكتاب : هام : قارن بين طريقتي العمل لكل من النمط الثابت لتحويل العناوين الرقمية ، والنمط المتغير لتحويل العناوين الرقمية ؟

النمط الثابت	يتم تخصيص عنوان رقمي خارجي لكل جهاز داخلي ، وهذا العنوان الرقمي ثابت لا يتغير
النمط المتغير	يتم إعطاء الجهاز عنوان رقمي مؤقت للتواصل مع الأجهزة خارج الشبكة وحين انتهاء الاتصال يصبح هذا الرقم متاحاً لأي جهاز آخر

الفصل الثالث : التشفير

- ظهرت الحاجة للحفاظ على سرية المعلومات منذ قدم البشرية في المجالين 1-العسكري 2-الدبلوماسي خاصة
- تم آنذاك إيجاد الوسائل التي يمكن نقل الرسائل عن طريقها والمحافظة على سريتها في الوقت نفسه
- مع تطور العلم والوسائل التكنلوجية الحديثة كان لابد من إيجاد طرائق لحمايتها

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

إلى ماذا يهدف التشفير ؟ أذكر أهداف التشفير

- الحفاظ على سرية المعلومات في أثناء تبادلها بين المرسل ومستقبلها
- عدم الاستفادة منها أو فهم محتوها .حتى لو تم الحصول عليها من قبل أشخاص معترضين

علل يعتبر التشفير من أفضل طرق حماية المعلومات وأمنها ؟

- لأنة يخفي المعلومات عن الأشخاص غير المصرح لهم بالاطلاع عليها

تتضمن عملية التشفير أربعة عناصر أساسية ، أذكرها ؟

- خوارزمية التشفير
- مفتاح التشفير
- النص الأصلي
- نص الشيفرة

حكمة : إذا لم يجد الإنسان شيئاً في الحياة يموت من أجله ، فإنه أغلب الظن لن يجد شيئاً يعيش من أجله
إنه من المخجل التعثر مرتين بالحجر نفسه..

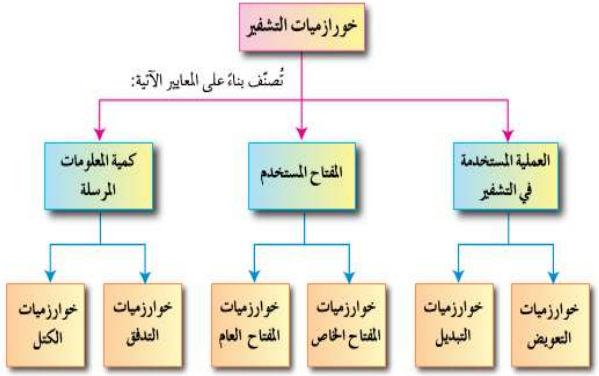
عرف عناصر عملية التشفير

1-خوارزمية التشفير : مجموعة من الخطوات المستخدمة لتحويل الرسالة الأصلية الى راسلة مشفرة .
2-مفتاح التشفير : سلسلة من الرموز المستخدمة في خوارزمية التشفير وتعتمد على قوة التشفير على قوة المفتاح
3-النص الأصلي :محتوى الرسالة الأصلية قبل التشفير وبعد فك التشفير
4-نص الشيفرة: الرسالة بعد عملية التشفير

هام جدا عرف الخوارزمية : هي عبارة عن مجموعة من الخطوات المتسلسلة منطقيا ورياضيا لحل مشكلة ما

تصنف خوارزميات التشفير بناءً على عدة معايير ، اذكرهما

- إستخدام المفتاح
- كمية المعلومات المرسلة
- العملية المستخدمة في عملية التشفير



أذكر أنواع الخوارزميات ؟

- خوارزميات التعويض
- خوارزميات التبديل
- خوارزميات المفتاح الخاص
- خوارزميات المفتاح العام
- خوارزميات التدفق
- خوارزميات الكتل

اذكر أنوع خوارزميات التشفير حسب المفتاح المستخدم

1-خوارزميات المفتاح الخاص
2- خوارزميات المفتاح العام

اذكر أنواع خوارزميات التشفير حسب العمليات المستخدمة في التشفير

- خوارزميات التعويض
- خوارزميات التبديل

اذكر انواع خوارزميات التشفير حسب كمية المعلومات المرسلة ؟

- خوارزميات التدفق
- خوارزميات الكتل

أذكر أقسام هذا النوع من التشفير ،وعرف كل منها (وآلية كل منها)؟

	التشفير بالتعويض	التشفير بالتبديل
عرف	طريقة لتشفير النصوص وتعني استبدال حرف أو مقطع مكان مقطع	طريقة لتشفير النصوص وتعني تبديل أماكن الأحرف ،وذلك عن طريق إعادة ترتيب أحرف الكلمة ؛بشرط استخدام الأحرف نفسها من دون إجراء أي تغيير عليها
مثال	شيفرة الإزاحة (تم دراستها بالصف العاشر)	خوارزمية الخط المتعرج (Zig Zag Cipher)

ما هو شرط التشفير بالتبديل ؟

- شرط استخدام الأحرف نفسها من دون إجراء أي تغيير عليها

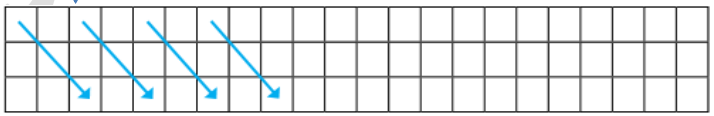
عرف فك التشفير : هو عكس عملية التشفير أي القدرة على استرجاع النص الأصلي من خلال خوارزمية

اذكر مميزات خوارزمية الخط المتعرج ؟

- خوارزمية الخط المتعرج سهلة وسريعة
- يمكن تنفيذها باستخدام الورقة والقلم
- يمكن فك تشفيرها بسهولة

حكمة : إننا نعيش لأنفسنا حياة مضاعفة، حينما نعيش للآخرين، وبقدر ما نضاعف إحساسنا بالآخرين نضاعف إحساسنا بحياتنا، ونضاعف هذه الحياة ذاتها في النهاية

- تمر خوارزمية الخط المتعرج بعدة خطوات اذكرها بالترتيب
  - تحديد عدد الأسطر التي ستستخدم لتشفير النص (عدد الأسطر يعد مفتاح التشفير)
  - املأ الفراغ (المسافة) في النص الأصلي بمثلث مقلوب ▽
  - أنشئ جدولاً يعتمد على عدد الأسطر (مفتاح التشفير)
  - وزع أحرف النص المراد تشفيره بشكل قطري حسب اتجاه السهم
  - ضع مثلثاً مقلوبا ▽ في الفراغ الأخير ،كي تكون الأطوال متساوية
  - اكتب النص المشفر سطراً سطراً



❖ معلومات هامة :
❖ لا نحتاج لمعرفة عدد الأعمدة (ابدأ بأي عدد من الأعمدة ويمكن زيادة الأعمدة حسب الحاجة)
❖ مفتاح التشفير يتم الاتفاق عليه مسبقا من قبل المرسل والمستقبل
❖ استخدام المثلث المقلوب لغاية تسهيل الحل

مثال (1): شفر النص الآتي ، علما بأن مفتاح التشفير سطران
(لاحظ هنا بعطيك بالسؤال عدد الأسطر أما الاعمدة حسب الحاجة)

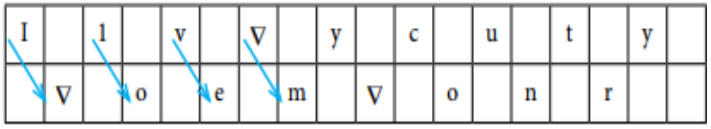
love my country

خطوات الحل : 1) حدد عدد الاسطر وهو مفتاح الحل !

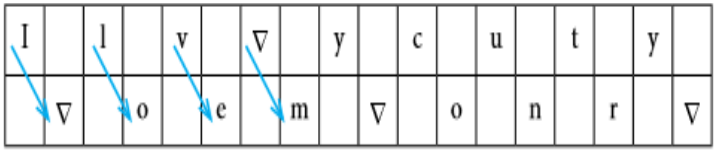
2)ضع مثلث مقلوب بين الفراغات

I ▽ love ▽ My ▽ country

3) أنشئ جدولاً علماً بأن عدد الصفوف =2 ووزع الاحرف بشكل قطري



4) ضع مثلث اخر فراغ لتكون الاطوال متساوية



الحل : خذ الاحرف سطرا سطرا مع المثلث المقلوب

النص المشفر : Ilv ▽ ycuty ▽ oem ▽ onr

النص بلا مثلث Ilv ycuty oem onr

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

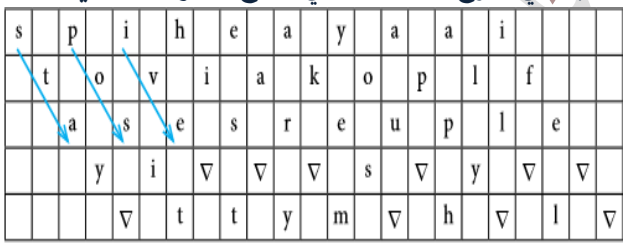
Stay positive this year makes you happy all life

خطوات الحل : 1) حدد عدد الاسطر وهو مفتاح الحل !

2)ضع مثلث مقلوب بين الفراغات

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

وزع الأحرف بشكل قطري حسب إتجاه الأسهم . - ضع مثلثاً مقوباً ▽ في الفراغ الأخير وذلك كي تصبح الأطوال متساوية



نكتب النص المشفر سطرًا سطرّ ،ونرتبه على التوالي

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

النص المشفر

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

Spiheayaaitoviakoplfasesreupleyi s y ttym h l

☒ وجبة سريعه : تدرب : شفر النصوص الاتية // ابعتها على الفيس بأسم الاستاذ احمد شهاب

ب-عملية فك التشفير

تمر عملية فك التشفير بعدة خطوات ،أذكرها ؟

1. املأ الفراغات بمثلث مقلوب ▽
2. قسم النص المشفر الى أجزاء اعتمادا على مفتاح التشفير . أي أن عدد الأجزاء يساوي عدد الأسطر

ولتحديد عدد الأحرف في كل جزء ؛ نقوم بما يأتي :

مجموع أحرف النص المشفر (بما فيها الفراغات)
÷ (مقسوم)
عدد الاجزاء (الاسطر)

مثال (٣):

جد النص الأصلي للنص المُشفّر الآتي، علمًا بأن مفتاح التشفير سطران.

Ilv ycuty oem onr

الحل:

لإيجاد النص الأصلي، اتبع الخطوات الآتية:

أ – املأ الفراغات بمثلث مقلوب.

Ilv ▽ ycuty ▽ oem ▽ onr

ب– قسّم النص المُشفّر إلى جزأين؛ لأن مفتاح التشفير سطران. إذا كان الناتج عددًا كسريًّا نقرّبه إلى أقرب عدد صحيح أكبر منه.

١٧ ÷ ٢ = ٨,٥

٨,٥ عدد صحيح نقرّبه إلى العدد ٩ . ومن ثم، فإن الجزء الأول يتكوّن من تسعة رموز.

Ilv ▽ ycuty	الجزء الأول
▽ oem ▽ onr	الجزء الثاني

جـ– نأخذ الحرف الأول من كلّ جزء بشكل عمودي (حرف I من الجزء الأول والمثلث المقلوب من الجزء الثاني)، ثم الحرف الثاني من كل جزء (l من الجزء الأول و o من الجزء الثاني)، نضمّ للأحرف السابقة، وهكذا...

I ▽ love ▽ my ▽ country

النص الأصلي: I love my country

- Stop thinking about your past mistakes.

مفتاح التشفير أربعة أسطر.

- Never give up on your goals.

مفتاح التشفير ثلاثة أسطر.

مثال (٤):

جد النص الأصلي للنص المُشفّر الآتي؛ باستخدام خوارزمية الخط المتعرج، علمًا بأن مفتاح التشفير هو خمسة أسطر.

النص المُشفّر:

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

الحل:

لإيجاد النص الأصلي، قم بما يأتي:

أ – قسّم النص المُشفّر إلى أجزاء، اعتمادًا على عدد الأسطر (مفتاح التشفير).

مفتاح التشفير = عدد الأسطر = خمسة

لتحديد حدد الأحرف في كلّ جزء، قم بما يأتي:

مجموع أحرف النص المُشفّر ÷ عدد الأجزاء

٥٠ ÷ ٥ = ١٠ أحرف في كل جزء.

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

٢ – يؤخذ الحرف الأول من كل جزء: الحرف S من الجزء الأول، والحرف i من الجزء الثاني، و a من الجزء الثالث، و y من الجزء الرابع، والمثلث المقلوب من الجزء الخامس، ونضمّها إلى بعضها بعضًا، ثم الحرف الثاني من كل جزء، ثم الثالث وهكذا...

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

النص الأصلي:

Stay positive this year makes you happy all life

- وجبة سريعه : تدرب ~~ابعتلي الحل على الفيس الاستاذ احمد شهاب
- جد النص الأصلي للنص المشفر الآتي باستخدام خوارزمية الخط المتعرج
  - Bieno ▽ its ee ▽ ▽ uali ▽ lviyrbie ▽.

علما بإن مفتاح التشفير ثلاثة أسطر .

☒ الحل النهائي : Believe in your abilities

- Eoterkodnhmon▽u▽eemelci▽n▽siasmtdsgt▽o▽a▽hItvfrtt.

علما بإن مفتاح التشفير هو سبعة أسطر ..

☒ الحل النهائي : Education is tthe movement from darkeness to light

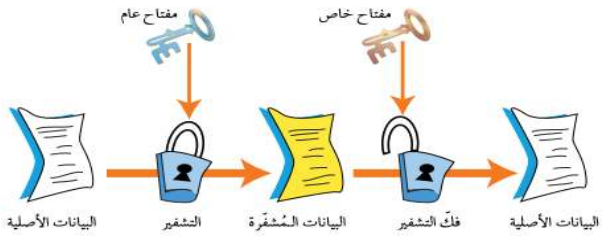
النجاح يحتاج شخص واثق لدية الكثير من التحدي

فكر بفرحة امك وابوك يوم ما ترفع راسهم

2-التشفير المعتمد على المفتاح

- على ماذا يعتمد التشفير المعتمد على المفتاح ؟
  - يعتمد على عدد المفاتيح المستخدمة في عملية التشفير
- معلومة هامة ----> أمن الرسالة أو المعلومة يعتمد على سرية المقتاح ، وليس على تفاصيل الخوارزمية
- يقسم التشفير المعتمد على المفتاح إلى نوعين ،إذكرهما ؟
  1. خوارزميات المفتاح الخاص
  2. خوارزميات المفتاح العام
- معلومة هامة -----> يطلق على خوارزميات المفتاح الخاص اسم الخوارزميات التناظرية أيضا
- معلومة هامة -----> يطلق على خوارزميات المفتاح العام اسم الخوارزميات اللاتناظرية أيضا
- ما هي آلية عمل خوارزمية المفتاح الخاص ؟
  - لها مفتاح واحد فقط ، يستخدم لعمليتي التشفير وفك التشفير ، يتم الاتفاق على اختياره قبل بدء عملية التراسل بين المرسل والمستقبل .

- علل : تسمية خوارزمية المفتاح الخاص بخوارزمية المفتاح السري ؟
  - لأنة يتم اختيار مفتاح تشفير وفك التشفير قبل بدء عملية التراسل بين المرسل والمستقبل
- ماهي آلية عمل خوارزمية المفتاح العام
  - لها مفتاحين ، أحدهما يستخدم لتشفير الرسالة ويكون معروفاً بين المرسل والمستقبل ويسمى المفتاح العام ، والآخر يكون معروفاً لدى المستقبل فقط ، ويستخدم لفك التشفير ويسمى المفتاح الخاص ،يتم إنتاج المفتاحين خلال عمليات رياضية ، ولا بمكن معرفة المفتاح الخاص من خلال معرفة المفتاح العام



- عرف المفتاح العام : هو مفتاح الرسالة ويكون معروفاً لكل من المُرسل والمُستقبل
- عرف المفتاح الخاص: هو مفتاح فك التشفير ويكون معروفاً فقط للمستقبل

2-التشفير المعتمد على كمية المعلومات المرسلة

- يقسم التشفير المعتمد على كمية المعلومات المرسلة إلى قسمين ، إذكرهما ؟
  1. شيفرات الكتل
  2. شيفرات التدفق
- ما هي آلية أو مبدأ عمل شيفرات التدفق ؟
  - يعمل هذا النوع من الخوارزميات على تقسيم الرسالة إلى مجموعة أجزاء ،ويشفر كل جزء منها على حدة ، ومن ثم يرسله .
- ماهي آلية عمل شيفرات الكتل ؟
  - تقسم أيضا إلى أجزاء ولكن بحجم أكبر من حجم الأجزاء في شيفرات التدفق ،ويشفر أو يفك تشفير كل كتلة على حدة . ويختلف عن شيفرات التدفق ،بأن حجم المعلومات أكبر ؛ لذا ،فإنها أبطأ
- علل ركز) شيفرات الكتل أبطأ من شيفرات التدفق ؟
  - لأن حجم المعلومات أكبر لذا فأنها ابطأ
- وضح الفرق بين شيفرات التدفق وشيفرات الكتل ؟
  - الفرق حجم الأجزاء أكبر من الأجزاء في شيفرات التدفق ، وحجم البيانات فيها أكبر من حجم المعلومات في شيفرات التدفق ، وهي أبطأ من شيفرات التدفق .

اللهم لك الحمد الحمد : احتاج منك الدعاء
اللهم وفق جميع الطلبة : الى 150 ناوين

☒ بعض حلول اسئلة الفصل واسئلة الوحدة :

8–أوجد النص المُشفر لكل نص مما يأتي باستخدام خوارزمية الخط المتعرج Zig Zag:

أ- Let us keep our home safe and united

علمًا بأن **مفتاح التشفير**: ثلاثة أسطر.

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

L▽▽ eo▽msenuteukpuhea▽dnetse▽ ro▽ fa▽ id ▽

ب- Investing in people is more important than investing in things

علمًا بأن **مفتاح التشفير**: ثمانية أسطر.

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		▽		▽			

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

9- فك تشفير النص الآتي مستخدمًا خوارزمية الخط المتعرج Zig Zag علمًا بأن مفتاح التشفير عشرة أسطر.

أ- النص المُشفر:

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

8- أوجد النص المُشفر لكل نص مما يأتي مستخدمًا خوارزمية الخط المتعرج Zig Zag:

أ- Youth is the future and the spirit of our home

علمًا بأن **مفتاح التشفير** أربعة أسطر.

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

النص المشفر:

Yh▽▽ uasifrmd▽tfrnpt▽▽ euihuedi▽oh▽tset▽▽ rouo▽

ب- School is the place where great people and ideas are formed

علمًا بأن مفتاح التشفير ستة أسطر.

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		▽	

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

9- فك تشفير كل نص من النصوص الآتية مستخدمًا خوارزمية الخط المتعرج Zig Zag علمًا بأن مفتاح التشفير ستة أسطر.

النص المُشفر:

Hwote ▽▽eoem▽ esp▽meeupwl▽et ▽s ▽ee▽▽▽l▽iea▽shektts▽

عدد أحرف النص 48 حرف

48 ÷ 6 = 8 أحرف بكل سطر

H w o t e ▽ ▽ e	الجزء الأول
o e m ▽ e s p ▽	الجزء الثاني
m e e u p w l ▽	الجزء الثالث
e t ▽ s ▽ e e ▽	الجزء الرابع
▽ ▽ l ▽ i e a ▽	الجزء الخامس
s h e K t t s ▽	الجزء السادس

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

10- حدد أنواع خوارزميات التشفير إذا تم تقسيمها بناءً على المعايير الآتية:

أ- المفتاح المستخدم :**خوارزميات التشفير باستخدام المفتاح الخاص ، وخوارزميات التشفير باستخدام المفتاح العام.**

ب- كمية المعلومات المُرسلة :**شيفرات التدفق وشيفرات الكتل.**

ج- العملية المستخدمة للتشفير :**التشفير بالتعويض أو التشفير بالتبديل.**