لا تنتظر وقتاً إضافياً ..... لا تؤجل عمل اليوم إلى الغد ..... اجعل هدفك ليس النجاح فقط بل التفوق والتميز

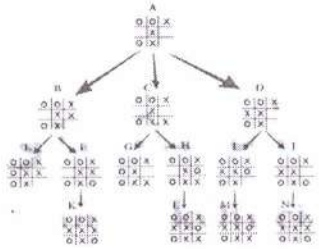
إهداء إلى روح والداي
غفر الله لهما وجعلهما
من أهل الجنة

علوم الحاسوب العلامة الكاملة

لكافة الفروع الأكاديمية

الوحدة الرابعة

أمن المعلومات والتشفير



إعداد الأستاذ

عبد الغفار الشيخ

0796692579

0786502073

اللهم إني وكلتك أمري فكن لي خير وكيل ودبر لي أمري فإني لا أحسن التدبير

الوحدة الرابعة

أمن المعلومات والتشفير

أذكر أسباب الاهتمام بأمن المعلومات ؟

1 – التطور الهائل في مجال الانترنت

2 – سهولة الوصول على المعلومات

3 – وجود المخترقين والمتطفلين

ما المقصود بمفهوم 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 ويبقى على إبقائها متاحة للأفراد المصرح لهم باستخدامها

اذكر الخصائص الأساسية لأمن المعلومات ؟

1 – السرية

2 – السلامة

3 – توافر المعلومات

اشرح (وضح) الخصائص الأساسية لأمن المعلومات :

أ – السرية : تعني أن الشخص المخول هو الوحيد القادر على الوصول إلى المعلومات والاطلاع عليها

مصطلح السرية مرادف لمفهومان ما هما ؟

المفهومان هما الأمن والخصوصية

ب – السلامة : تعني حماية الرسائل أو المعلومات التي تم تداولها والتأكد بأنها لم تتعرض لأي عملية تعديل سواء

ما المقصود بعملية التعديل في مفهوم السلامة ؟

الإضافة أو الاستبدال أو الحذف

أذكر مثالا على سلامة المعلومات ؟

نتائج الثانوية العامة يجب الحفاظ على سلامة هذه النتائج من أي تعديل

جـ - توافر المعلومات : أن تكون المعلومات متاحة للأشخاص المصرح لهم بالتعامل معها والوصول إليها في أقصر وقت

ما الوسائل التي يقوم بها المخترقون ؟

جعل المعلومات غير متاحة إما بحذفها أو الاعتداء على الأجهزة التي تخزن فيها هذه المعلومات

ما المخاطر التي تهدد أمن المعلومات ؟

التهديدات ، الثغرات

أ – التهديدات : يحدث التهديد للأسباب (ما أسباب حدوث التهديد)

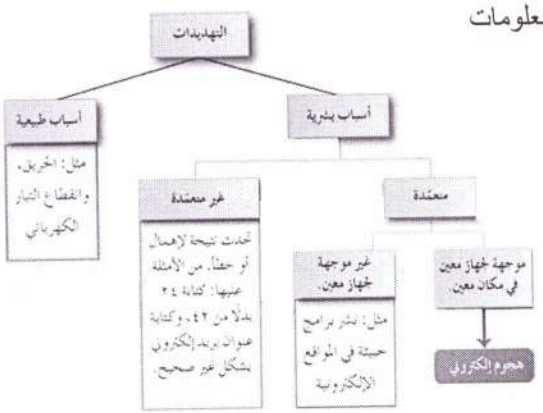
1 – أسباب طبيعية مثل حدوث حريق أو انقطاع للتيار الكهربائي مما يؤدي إلى فقدان المعلومات

2 – أسباب بشرية : نتيجة الإهمال أو الخطأ مثل كتابة عنوان بريد الكتروني بشكل غير صحيح

3 – متعمدة : تقسم إلى

* غير موجهة لجهاز معين مثل نشر فيروس

* موجهة لجهاز معين ويسمى هذا الهجوم بالهجوم الالكتروني (الاعتداء الالكتروني) مثل 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



ما هو اخطر أنواع الاعتداءات ؟ الاعتداء الالكتروني

ما العوامل الرئيسية التي يعتمد نجاح الاعتداء الالكتروني ؟
(ما العوامل الرئيسية التي تؤخذ بالحسبان لتقييم التهديد)
1 – الدافع
2 – الطريقة
3 – فرصة النجاح

ما الذي يدفع الأفراد لتنفيذ الهجوم الالكتروني ؟
1 – الرغبة في الحصول على المال
2 – محاولة لإثبات القدرات التقنية بقصد الإضرار بالآخرين

ما المهارات (الطريقة) اللازم توافرها في الفرد المعتدي ؟
1 - قدرته على توفير المعدات والبرمجيات الحاسوبية اللازمة
2 – معرفته بتصميم وآلية عمل الجهاز
3 – معرفة نظام القوة والضعف لهذا النظام

على ماذا تعتمد فرصة نجاح الهجوم الالكتروني ؟
1 - تحديد الوقت المناسب للتنفيذ
2 - كيفية الوصول إلى الأجهزة

حدد العامل الرئيسي الذي يؤخذ بالحسبان لتقييم التهديد ؟
أ - الرغبة في إثبات القدرات : دافع
ب – معرفة نقاط القوة والضعف للنظام : الطريقة
جـ - تحديد الوقت المناسب لتنفيذ الهجوم : فرصة نجاح
د - الإضرار بالآخرين : دافع
هـ - الرغبة في الحصول على المال : دافع
و – القدرة على توفير المعدات والبرمجيات : الطريقة

أذكر أربعة أنواع من الاعتداءات الالكترونية التي تتعرض لها المعلومات؟
1 - التنصت على المعلومات
2 - التعديل على المحتوى
3 – الإيقاف
4 – الهجوم المزور أو المفبرك

اشرح أنواع الاعتداءات الالكترونية على المعلومات ؟
1 – التنصت على المعلومات : الهدف 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 الوصول إلى المستقبل وفي هذه الحالة تصبح المعلومات غير متوافرة
4 – الهجوم المزور أو المفبرك : حيث يرسل المعتدي الالكتروني رسالة إلى أحد الأشخاص على الشبكة يخبره فيها بأنه صديقه ويحتاج إلى معلومات أو كلمات سرية خاصة تتأثر بهذه الطريقة سرية المعلومات وقد تتأثر سلامتها

ب – الثغرات يقصد بها نقطة الضعف في النظام سواء أكانت في الإجراءات المتبعة مثل تحديد صلاحيات الوصول إلى المعلومات أو مشكلة في تصميم النظام أو عدم كفاية الحماية المادية للأجهزة والمعلومات (تسبب في فقدان المعلومات أو هدم النظام أو تجعله عرضة للاعتداء الالكتروني)

علل : استخدام بعض الضوابط في نظام المعلومات
لتقليل المخاطر التي تتعرض لها المعلومات والحد منها

يرى المختصون في مجال أمن المعلومات بأن الحفاظ على المعلومات وأمنها ينبع من التوازن بين ؟
تكلفة الحماية وفعالية الرقابة واحتمالية الخطر

ما هي الضوابط التي تقلل من المخاطر التي تتعرض لها المعلومات ؟
أ – الضوابط المادية : مراقبة بيئة العمل وحمايتها من الكوارث الطبيعية وغيرها باستخدام الجدران والأسوار والأقفال وحراس الأمن وغيرها من أجهزة إطفاء الحريق
ب – الضوابط الإدارية : تستخدم مجموعة من الأوامر والإجراءات المتفق عليها مثل : القوانين واللوائح والسياسات والإجراءات التوجيهية وحقوق النشر وبراءات الاختراع والعقود والاتفاقيات
جـ - الضوابط التقنية : وهي الحماية التي تعتمد على التقنيات المستخدمة سواء أكانت معدات أو برمجيات وتتضمن كلمات المرور ومنح صلاحيات الوصول وبروتوكولات الشبكة والجدر النارية وتنظيم تدفق المعلومات في الشبكة

الهندسة الاجتماعية

ما المقصود بالهندسة 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 المعلومات ؟

بسبب قلة اهتمام المختصين في مجال أمن المعلومات وعدم وعي مستخدمي الحاسوب بالمخاطر المترتبة عليها

أذكر مجالات الهندسة الاجتماعية ؟

البيئة المحيطة والجانب النفسي

ما مكونات بالبيئة المحيطة في الهندسة الاجتماعية ؟

1 – مكان العمل : مثل كتابة كلمة المرور على ورقة ملصقة على جهاز الحاسوب وعند دخول شخص غير مخول (عامل النظافة ، زبون) فانه يدخل إلى النظام بسهولة ليحصل على المعلومات التي يريدها

2 – الهاتف : يتصل الشخص غير المخول بمركز الدعم الفني هاتفيا ويطلب إليه بعض المعلومات الفنية ويستدرجه للحصول على كلمة المرور وغيرها من المعلومات ليستخدمها فيما بعد

3 – النفايات الورقية : يدخل الشخص غير المخول إلى مكان العمل ويجمعون النفايات التي قد تحتوي على كلمات مرور ومعلومات تخص الموظفين وأرقام هواتفهم وبياناتهم الشخصية التي يمكن استغلالها في تتبع أعمال الموظفين أو الحصول على المعلومات المرغوبة

4 – الانترنت : من الخطأ استخدام كلمة مرور واحدة للتطبيقات جميعها حيث ينشئ المعتدي الالكتروني موقعا على الشبكة يقدم خدمات معينة ويشترط التسجيل فيه للحصول على هذه الخدمات وذلك بإدخال اسم المستخدم وكلمة المرور وبهذه الطريقة يتمكن المعتدي الالكتروني من الحصول عليها

يستخدم المعتدي الالكتروني الجانب النفسي لكسب ثقة مستخدم الحاسوب ما هي الأساليب التي يستخدمها لذلك ؟

1 – الإقناع : يستطيع المعتدي إقناع الموظف أو مستخدم الحاسوب بطريقة مباشرة بحيث يقدم 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 مثل كأن يظهر كصاحب سلطة ، أو إغراء المستخدم بامتلاك خدمة نادرة ، حيث يقدم له عرضا معينا من خلال موقعه الالكتروني لمدة محدودة يمكنه من الحصول على كلمة المرور

2 – انتحال الشخصية والمداهنة : حيث يتقمص شخص شخصية آخر وهذا الشخص قد يكون حقيقيا أو وهميا فقد ينتحل شخصية فني صيانة معدات الحاسوب أو عامل النظافة أو المدير أو السكرتير وغالبا ما تكون الشخصية المنتحلة ذات سلطة عندها يبدي أغلب الموظفين خدماتهم ولن يترددوا بتقديم أي معلومات لهذا الشخص المسؤول

3 – مسايرة الركب : مثلا إذا حضر المعتدي مقدما نفسه على أنه من فريق الدعم الفني فإذا سمح له أحد الموظفين بعمل التحديثات فسيقوم باقي زملاءه غالبا بطلب عمل التحديثات اللازمة من المعتدي

أسئلة الفصل

1 – وضح المقصود بكل من : أمن المعلومات ، الثغرات

2 – يهدف أمن المعلومات للحفاظ على ثلاث خصائص أساسية هي (سرية الملومات وسلامة المعلومات وتوافر المعلومات) حدد إلى أي هذه الخصائص يتبع كل مما يأتي :

أ – التأكد من عدم حدوث أي تعديل على المعلومات .....

ب – الشخص المخول هو الوحيد القادر على الوصول إلى المعلومات والاطلاع عليها .....

جـ - الوصول إلى المعلومات يحتاج إلى وقت كبير .....

د - مصطلح مرادف لمفهومي الأمن والخصوصية .....

هـ - المعلومات العسكرية .....

3 – توجد ثلاثة عوامل رئيسية تؤخذ في الحسبان لتقييم التهديد ز بناء على دراستك الوحدة ، حدد العامل الذي يندرج تحته كل مما يأتي :

أ – الرغبة في إثبات القدرات .....

ب _ معرفة نقاط القوة والضعف للنظام .....

جـ - تحديد الوقت المناسب لتنفيذ الهجوم الالكتروني .....

د – الإضرار بالآخرين .....

هـ - الرغبة في الحصول على المال .....

و – القدرة على توفير المعدات والبرمجيات الحاسوبية .....

4 – عدد أربعة من أنواع الاعتداءات الإلكترونية التي تتعرض لها المعلومات

5 – علل ما يأتي :

أ – استخدام بعض الضوابط في نظام المعلومات

ب – تعد الهندسة الاجتماعية من أنجح الوسائل وأسهلها للحصول على المعلومات

6 – قارن بين الضوابط المادية والضوابط الاجتماعية في كل مجال من المجالات الآتية :

وجه المقارنة	الضوابط المادية	الضوابط الإدارية
المقصود بها		
أمثلة عليها		

7 – وضح آلية عمل الهندسة الاجتماعية في كل مجال من المجالات الآتية :

المجال	
مكان العمل	
الهاتف	
انتحال الشخصية	
الإقناع	

أمن الإنترنت

الاعتداءات الالكترونية على الويب

أذكر أمثلة على الاعتداءات الالكترونية على الويب ؟

الاعتداء على متصفح الانترنت Browsers Attack

الاعتداء على البريد الالكتروني E – mail Attack

ما المقصود بمتصفح الانترنت ؟

برنامج ينقل المستخدم إلى صفحة (الويب) التي يريدها بمجرد كتابة العنوان والضغط على زر الذهاب ، ويمكنه من مشاهدة المعلومات على الموقع

ما طرق الاعتداءات الالكترونية على متصفحات الانترنت؟

أ - الاعتداء عن طريق (كود) بسيط ، يمكن إضافته إلى المتصفح وباستطاعته القراءة والنسخ وإعادة إرسال أي شيء يتم إدخاله من قبل المستخدم ويتمثل التهديد بالقدرة على الوصول إلى الحسابات المالية والبيانات الحساسة الأخرى

ب – توجيه المستخدم إلى صفحة أخرى غير التي يريدها

ما المقصود بالاعتداءات الالكترونية على البريد الالكتروني؟

بعض الرسائل الالكترونية مزيفة ، بعضها يسهل اكتشافها ، بعضها استخدم بطريقة احترافية

المستهدف هو المستخدم قليل الخبرة برسائل مثلا إذا أردت أن تصبح ثريا اتبع الرابط الآتي .

ما المقصود بتقنية تحويل العناوين الرقمية ؟

هي التقنية التي تعمل على إخفاء العنوان الرقمي للجهاز في الشبكة الداخلية ليتوافق مع العنوان الرقمي المعطى للشبكة وعليه يكون الجهاز الداخلي غير معرف للجهات الخارجية وهذا يسهم في حمايته من أي هجوم

ما هي مراحل تطور العناوين الالكترونية ؟

العناوين الرقمية الالكترونية IP Address

كل جهاز له عنوان رقمي خاص به يميزه عن غيره (IP Address) يتكون من 32 خانة ثنائية تتوزع على أربعة مقاطع يفصل بينها نقاط وهذا يسمى IP4 وكل مقطع من هذه المقاطع يتضمن رقم من (0) إلى (255) مثل

168.001.002.170

علل : التطور الهائل في أعداد مستخدمي الانترنت أدت إلى تطور IP4 إلى ما يسمى IPv6 ثم إلى ما يسمى NAT

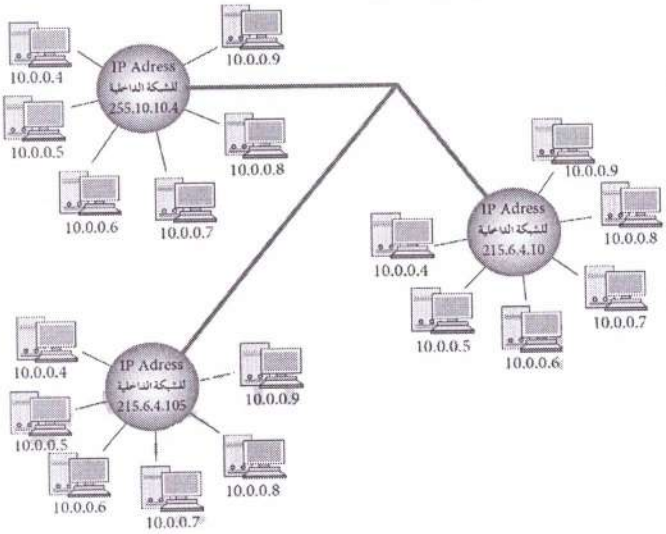
ما اسم الجهة المانحة للأرقام الالكترونية ؟

تعتبر IANA السلطة المسؤولة عن منح أرقام الانترنت المخصصة لإعطاء العناوين الرقمية للأجهزة على الانترنت

ما المقصود بتقنية تحويل العناوين الرقمية NAT :

إعطاء الشبكة الداخلية عنوانا واحدا (و مجموعة عناوين) ويكون معرفا لها عند التعامل في شبكة الانترنت

مثال :



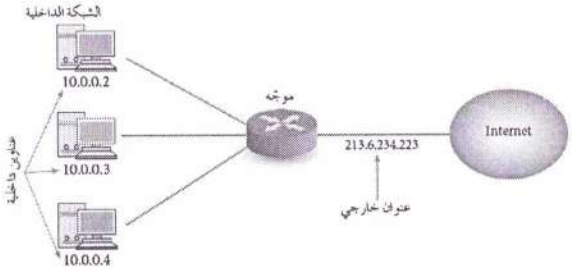
الشكل يبين 3 شبكات داخلية كل شبكة منحت عنوانا خاصا بها على الانترنت وهذا العنوان لا يمكن أن يمنح لشبكة أخرى تعطي الشبكة الداخلية كل جهاز داخل الشبكة عنوانا رقميا لغرض الاستخدام فقط ، ولا يعترف بهذا العنوان خارج الشبكة (يمكن أن يتكرر العنوان الرقمي للجهاز في أكثر من شبكة داخلية)

(لا يمكن أن يتكرر العنوان الرقمي للشبكة الداخلية)

وعند رغبة أحد الأجهزة بالتواصل مع جهاز خارج الشبكة الداخلية يعدل العنوان الرقمي الخاص به باستخدام تقنية تحويل العناوين الرقمية (NAT) وذلك يتم باستخدام جهاز بسيط يكون غالبا موجه أو جدارا ناريا (وظيفته) يحول العنوان الرقمي الداخلي إلى عنوان رقمي خارجي ويسجل ذلك في سجل خاص للمتابعة

يتم التواصل مع الجهاز الهدف في الشبكة الأخرى عن طريق هذا 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 إلى الجهاز المرسل

مثال



ما هي طريقة (آلية) بتقنية تحويل العناوين الرقمية ؟

أ – النمط الثابت للتحويل : حيث يتم تخصيص عنوان رقمي خارجي لكل جهاز داخلي وهذا العنوان الرقمي ثابت لا يتغير

ب – النمط المتغير للتحويل : حيث يكون لدى الجهاز الوسيط عدد من العناوين الرقمية الخارجية ولكنها غير كافية لعدد الأجهزة في الشبكة ، هذه العناوين تبقى متاحة لجميع الأجهزة على الشبكة وعند رغبة أحد الأجهزة بالتراسل خارجيا فإنه يتواصل مع الجهاز الوسيط الذي يعطيه عنوانا خارجيا مؤقتا يستخدمه لحين انتهاء عملية التراسل ، يفقد الجهاز الداخلي هذا العنوان ويصبح العنوان متاحا للتراسل مرة أخرى ، ليس من الضروري أن يستخدم الجهاز نفس العنوان في كل مرة

أسئلة الفصل

1 – ما أسباب إيجاد وسائل تقنية لحماية الانترنت ؟

2 – ما أشهر الاعتداءات على (الويب)

3 – حدد نوع الاعتداء في كل مما يأتي :

أ – توجيه المستخدم إلى صفحة أخرى غير الصفحة التي تريدها

ب – كود بسيط يمكن إضافته إلى المتصفح وباستطاعته القراءة والنسخ وإعادة الإرسال لأي شيء يتم إدخاله من قبل المستخدم

جـ - يتضمن عروضا وهمية ومضللة ويحتوي رابطا يتم الضغط عليه للحصول على معلومات إضافية

4 – وضح ما يأتي :

أ – تحدث اعتداءات على (الويب) من خلال البريد الالكتروني

ب – تحافظ تقنية تحويل العناوين الرقمية على أمن المعلومات في (الويب)

5 – ما الفرق بين العناوين الرقمية IP4 , IPv6

6 – من السلطة المسؤولة عن منح أرقام الانترنت المخصصة لإعطاء العناوين الرقمية ؟

7 – ما وظيفة الجهاز الوسيط ؟

8 – قارن ين طريقتي العمل لكل من :

النمط الثابت لتحويل العناوين الرقمية والنمط المتغير لتحويل العناوين الرقمية

مفهوم علم التشفير والهدف منه

ما المقصود بمفهوم بالتشفير ؟

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

ما هدف التشفير ؟

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

ما المقصود بالخوارزمية : مجموعة الخطوات المتسلسلة منطقيا ورياضيا لحل مشكلة ما

عدد عناصر عملية التشفير ؟

أ – خوارزمية التشفير : مجموعة الخطوات المستخدمة لتحويل الرسالة الأصلية إلى رسالة مشفرة

ب – مفتاح التشفير (Key) وهو سلسلة الرموز المستخدمة في خوارزمية التشفير وتعتمد قوة التشفير على قوة هذا المفتاح

جـ - النص الأصلي (Plain Text) محتوى الرسالة الأصلية قبل التشفير وبعد عملية فك التشفير

د – نص الشيفرة (Cipher Text) الرسالة بعد عملية التشفير

بخوارزميات التشفير

ما المعايير التي تصنف خوارزميات التشفير ؟

استخدام المفتاح : خوارزميات المفتاح الخاص

خوارزميات المفتاح العام

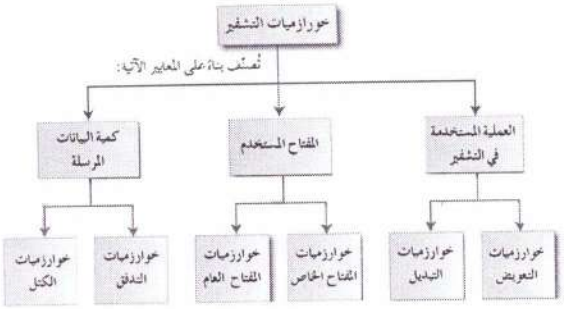
كمية المعلومات المرسلة : خوارزميات التدفق

خوارزميات الكتل

العملية المستخدمة في عملية التشفير:

خوارزميات التعويض

خوارزميات التبديل



ما طرق التشفير المعتمد على نوع عملية التشفير ؟

طريقة التعويض ، طريقة التبديل

ما المقصود بطريقة التعويض في عملية التشفير ؟

تعني استبدال حرف مكان حرف أو مقطع مكان مقطع مثل شيفرة الإزاحة

ما المقصود بطريقة التبديل في عملية التشفير ؟

ويتم فيها تبديل أماكن الأحرف وذلك عن طريق ترتيب أحرف الكلمة ، بشرط استخدام الأحرف نفسها دون إجراء أي تغيير عليها ، فعند تنفيذ عملية التبديل يختفي معنى النص الحقيقي وهذا يشكل عملية التشفير، شريطة أن تكون قادرا على استرجاع النص الأصلي وهذا يسمى عملية فك التشفير

أذكر خوارزمية تستخدم في عملية التبديل في عملية التشفير ؟

خوارزمية الخط المتعرج :

ما ميزات خوارزمية الخط المتعرج ؟

بأنها خوارزمية سهلة وسريعة

يمكن تنفيذها يدويا باستخدام الورقة والقلم

ملاحظة : عدد الأعمدة يتفق عليها المرسل والمستقبل

المثلث المقلوب يعني فراغ ▽

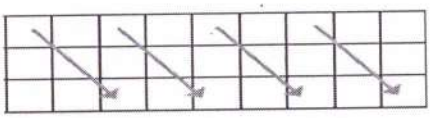
وضح خطوات خوارزمية الخط المتعرج المستخدمة في التشفير ؟ (خطوات التشفير)

1 – حدد عدد الأسطر التي ستستخدم لتشفير النص (علل) حيث أن عدد الأسطر مفتاح التشفير ولا يلزم معرفة عدد الأعمدة

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 السهم)



5 – ضع المثلث المقلوب ▽ في الفراغ الأخير (علل) كي تكون الأطوال متساوية

6 – اكتب النص المشفر سطرا سطراً

مثال : شفر النص التالي علما بأن مفتاح التشفير سطران ؟

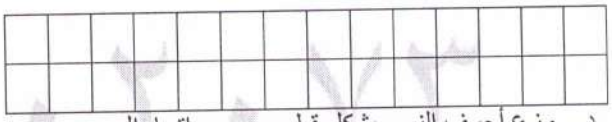
I LOVE MY COUNTRY

أ - مفتاح التشفير سطران

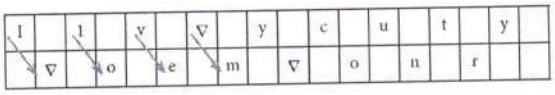
ب - املأ الفراغ في النص الأصلي بمثلث مقلوب

I ▽LOVE ▽MY ▽COUNTR

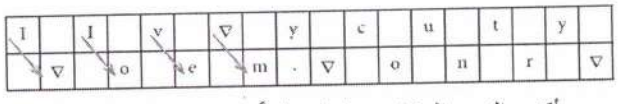
جـ – أنشئ جدولا علما بأن عدد الصفوف = 2



د – وزع أحرف النص بشكل قطري حسب اتجاه السهم



هـ - ضع مثلثا مقلوبا ▽ في الفراغ الأخير وذلك لكي تصبح الأطوال متساوية



و – أكتب النص المشفر سطرا سطراً

النص الأصلي : I LOVE MY COUNTRY

النص المشفر : ILV▽ YCUTY ▽OEM ▽ONR

ILV YCUTY OEM ONR

مثال : أوجد النص المشفر للنص الأصلي علماً بأن مفتاح التشفير هو خمسة أسطر

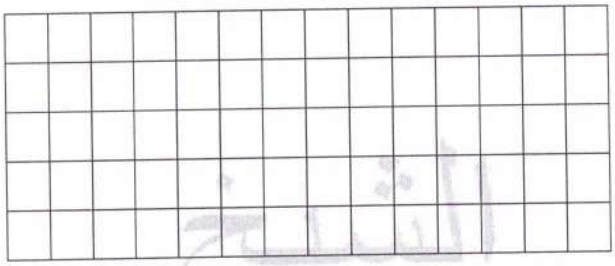
Stay positive this year makes you happy all life

أ – حدد مفتاح التشفير وهو خمسة أسطر

ب - املأ الفراغ في النص الأصلي بمثلث مقلوب▽

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

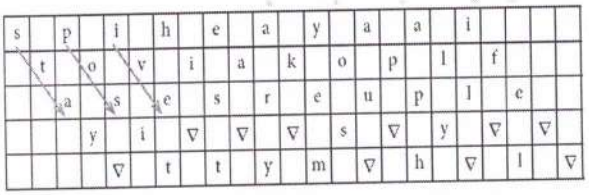
جـ – أنشئ جدولا علما بأن عدد الصفوف = 5



د – وزع أحرف النص بشكل قطري حسب اتجاه السهم

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

هـ - ضع مثلثا مقلوبا ▽ في الفراغ الأخير وذلك لكي تصبح الأطوال متساوية



و – أكتب النص المشفر سطرا سطراً

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

استخدم خوارزمية الخط المتعرج في تشفير الجل الآتية ؟

Stop thinking about your past mistakes

مفتاح التشفير أربعة أسطر

Never give up on your goals

مفتاح التشفير ثلاثة أسطر

خطوات عملية فك التشفير :

1 – املأ الفراغات بمثلث مقلوب▽

2 – قسم النص المشفر إلى أجزاء اعتمادا على عدد الأسطر (مفتاح التشفير) أي أن عدد الأجزاء يساوي عدد الأسطر لتحديد عدد الأحرف في كل جزء ننفذ المعادلة الآتية :

مجموع أحرف النص المشفر ÷ عدد الأجزاء

3 – أكتب الحرف الأول من كل جزء ثم الحرف الثاني ثم الحرف الثالث وهكذا

أوجد النص الأصلي للنص المشفر الآتي علما بأن مفتاح التشفير سطران ILV YCUTY OEM ONR

1 – املأ الفراغات بمثلث مقلوب▽

ILV ▽YCUTY ▽OEM ▽ONR

2 – قسم النص المشفر إلى جزأين لأن مفتاح التشفير سطران عدد الأحرف مع الفراغات ونحسب المعادلة (إذا كان ناتج القسمة عدداً كسريًا نقربه إلى أقرب عدد صحيح أكبر منه)

مجموع أحرف النص المشفر ÷ عدد الأجزاء

17 ÷ 2 = 8.5 نقربه إلى العدد 9 وعليه يكون الجزء الأول مكون من 9 رموز

الجزء الأول	Ilv ▽ ycuty
الجزء الثاني	▽ oem ▽ onr

3 – نأخذ الحرف الأول من كل جزء بشكل عمودي (حرف I من الجزء الأول O من الجزء الثاني) ثم الحرف الثاني ثم الحرف الثالث وهكذا

I▽LOVE ▽MY ▽COUNTR

I LOVE MY COUNTRY

أوجد النص الأصلي للنص المشفر الآتي باستخدام خوارزمية الخط المتعرج علما بأن مفتاح التشفير هو خمسة أسطر

النص المشفر

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

1 – قسم النص المشفر إلى أجزاء اعتماداً على عدد الأسطر (مفتاح التشفير) مفتاح التشفير = عدد الأسطر = 5

2 - ننفذ المعادلة الآتية :

مجموع أحرف النص المشفر ÷ عدد الأجزاء

50 ÷ 5 = 10

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

3 – نأخذ الحرف الأول من كل جزء بشكل عمودي حرف s ثم t ثم a ثم y ثم فراغ ثم p وهكذا

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

النص الأصلي

Stay positive this year makes you happy all life

فك التشفير باستخدام خوارزمية الخط المتعرج ؟

Bieno▽itsee▽▽uali▽lviyrbie ▽

علماً بأن مفتاح التشفير ثلاثة أسطر

فك التشفير باستخدام خوارزمية الخط المتعرج ؟

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

مفتاح التشفير سبعة أسطر

خوارزمية التشفير المعتمد على المفتاح

يعتمد هذا النوع على سرية المفتاح وليس على تفاصيل الخوارزمية (علل) لأنه يصنف من الخوارزميات التي تعتمد على عدد المفاتيح المستخدمة في عملية التشفير

ما أقسام خوارزمية التشفير المعتمد على المفتاح ؟

أ – خوارزميات المفتاح الخاص

ب - خوارزميات المفتاح العام

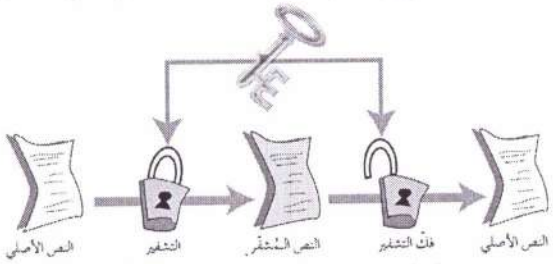
ماذا يطلق على خوارزميات المفتاح الخاص ؟

أ - الخوارزميات التناظرية

ب – خوارزميات المفتاح السري

وضح المقصود خوارزميات المفتاح الخاص ؟

يستخدم المفتاح نفسه لعمليتي التشفير وفك التشفير حيث يتم الاتفاق عليه قبل بدء عملية التراسل بين المرسل والمستقبل



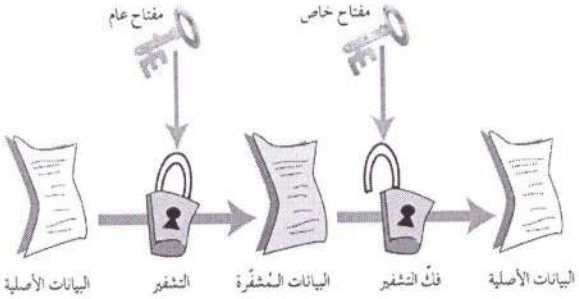
ماذا يطلق على خوارزميات المفتاح العام ؟

الخوارزميات اللاتناظرية

وضح المقصود خوارزميات المفتاح العام ؟

تستخدم هذه الخوارزميات مفتاحين أحدهما يستخدم لتشفير الرسالة ويكون معروفا للمرسل والمستقبل ويسمى المفتاح العام والآخر يكون معروفاً لدى المستقبل فقط ويستخدم لفك التشفير ويسمى المفتاح الخاص يتم إنتاج المفتاحين من خلال عمليات رياضية

لا يمكن معرفة المفتاح الخاص من خلال معرفة المفتاح العام



ما أنواع التشفير المعتمد على كمية المعلومات المرسلة :

خوارزميات (شيفرات) التدفق

خوارزميات (شيفرات) الكتل

ما المقصود بشيفرات التدفق ؟

يعمل هذا النوع على تقسيم الرسالة إلى مجموعة من أجزاء ويشفر كل منها على حدة ومن ثم يرسله

ما المقصود بشيفرات الكتل ؟

يعمل هذا النوع على تقسيم الرسالة إلى مجموعة من أجزاء ولكن بحجم أكبر من حجم الأجزاء في شيفرات التدفق ويشفر أو يفك تشفير كل كتلة على حده ، هنا حجم المعلومات أكبر لذا فهي أبطأ

أسئلة الفصل

1 – وضح المقصود بكل من التشفير وفك التشفير

2 – فسر ما يأتي :

يعد التشفير من أفضل الوسائل المستخدمة للحفاظ على أمن المعلومات

3 – إلام يهدف علم التشفير ، وما عناصره ؟

4 – حدد إلى أي من عناصر التشفير يتبع كل مما يأتي :

أ – مجموعة من الخطوات المستخدمة لتحويل الرسالة الأصلية إلى رسالة مشفرة .....

ب - الرسالة بعد عملية التشفير .....

جـ - سلسلة من الرموز التي تستخدم من خلال خوارزمية التشفير .....

د – الرسالة قبل عملية التشفير .....

5 – عدد المعايير التي تصنف خوارزميات التشفير بناءً عليها

6 – ما الفرق بين طريقتي التشفير باستخدام عملية التبديل وعملية التعويض

7 – لماذا سميت خوارزميات المفتاح الخاص بهذا الاسم

8 – أوجد النص المشفر لكل نص مما يأتي باستخدام خوارزمية الخط المتعرج

أ - Let us keep our home safe and united

علما بأن مفتاح التشفير ثلاثة أسطر

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

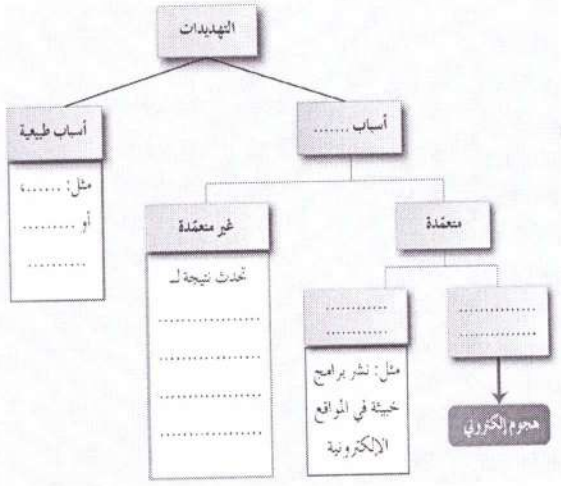
علما بأن مفتاح التشفير ثمانية أسطر

9 – فك تشفير النص الآتي مستخدما خوارزمية الخط المتعرج علما بأن مفتاح التشفير عشرة أسطر

Tnr ▽▽o▽eie▽t▽ ndbhwvureeeci▽▽ sagfmtthuu ▽ ittsioeutnn

أسئلة الوحدة

1 – بناء على دراستك أنواع التهديدات أكمل الشكل الآتي :



2 – وضح المقصود بالمفاهيم الآتية :

الهندسة الاجتماعية

السلامة

مفتاح التشفير

3 – عند تعرض المعلومات للهجمات الالكترونية يتأثر واحد أو أكثر من عناصر أمن المعلومات فيما يأتي بعض الاعتراضات للبيانات حدد عناصر أمن المعلومات التي تتأثر بها ؟

أ – اعتراض الرسالة والتغيير على محتواها .....

ب – الهجوم المزور أو المفبرك .....

جـ - التصنت على الرسائل .....

د – إدعاء شخص بأنه صديق ويحتاج إلى معلومات

هـ - قطع قناة الاتصال .....

4 – فسر اختلاف IP address للجهاز عند تراسله أكثر من مرة ؟

5 – من المخاطر التي تهدد الشبكات وجود الثغرات ، أذكر ثلاثة أمثلة عليها ؟

6 – ما الوسائل التي يستخدمها المعتدي الالكتروني للتأثير في الجانب النفسي للشخص المستهدف؟

7 – تعد الثغرات من المخاطر التي تهدد أمن المعلومات وضح ذلك ؟

8 – أوجد النص المشفر لكل نص مما يأتي مستخدما خوارزمية الخط المتعرج ؟

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

علما بأن مفتاح التشفير أربعة أسطر

ب – school is the place where great people and ideas are formed

علما بأن مفتاح التشفير ستة أسطر

9 - فك التشفير باستخدام خوارزمية الخط المتعرج

Hwote ▽▽eoem▽ esp▽ meeupwl▽ et▽ s▽

ee▽▽ l▽ iea▽ shektts▽

$8 = 6 \div 48$

10 – حدد أنواع خوارزميات التشفير إذا قسمت بناء على المعايير الآتية :

أ – المفتاح المستخدم

ب – كمية المعلومات المرسلة

جـ - العملية المستخدمة في التشفير

عبد الغفار الشيخ ٠٧٨٦٥٠٢٠٧٣

وزارة 2018 شتوي

قم بإجراء عمليات التحويل المناسبة لكل من الأعداد الآتية :

1	$(83)_{10}$	( )$_2$	4	$(10110)_2$	( )$_8$
2	$(215)_{10}$	( )$_8$	5	$(111110000)_2$	( )$_{16}$
3	$(1000111)_2$	( )$_{10}$	6	$(DC3)_{16}$	( )$_2$

ما ناتج القيام بالعمليات الحسابية الآتية من الأعداد الممثلة بالنظام الثنائي :

1 0 1 0 1 1 1 1 1 0 1 1 +	1 0 1 0 0 0 0 0 1 0 0 1 -
1 1 1 1 1 1 ×	1 0 0 0 1 ×

علل كل مما يأتي :

1. يعد النظام العشري أحد أنظمة العد الموضعية
2. يختلف العنوان الرقمي (IP Address) للجهاز نفسه عند تراسل أكثر من مرة في النمط المتغير للتحويل .
3. تسمية الجبر البولي بهذا الاسم

أدرس العبارة المنطقية الآتية ثم أجب عن الأسئلة التي تليها :

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

1- كم عدد البوابات المنطقية في العبارة المنطقية

2- جد ناتج العبارة المنطقية إذا علمت أن

A = 0 , B = 1 , C = 1 , D = 0

3- حول العبارة المنطقية إلى عبارة جبرية منطقية

يتكون الروبوت من عدة أجزاء ، اكتب الجزء من الروبوت الذي تعبر عنه كلاً من الجمل الآتية :

1 . يستقبل البيانات ثم يعالجها ويعطي الاوامر اللازمة للاستجابة لها وهو يهتبر بمثابة الدماغ للروبوت .....

2 . تحتوي على مفاصل صناعية لتسهيل حركتها عند تنفيذ الأوامر الصادرة إليها وتشبه ذراع الإنسان.....

3. مسؤولة عن جمع البيانات من البيئة المحيطة وتشبه وظيفتها الحواس الخمس عند الانسان ....

4 . مسؤول عن حركة الروبوت وهو بمثابة عضلات الروبوت ....

نشأت فكرة الروبوت منذ عدة قرون ، في الجدول الآتي وفق بين كل من العمود الأول الذي يحتوي على الفترات الزمنية لنشأة الروبوت مع ما يناسبه من العمود الثاني الذي يحتوي على التطورات التي حصلت على الروبوت وانقل الاجابة الى دفتر اجابتك :

الرقم	الفترات الزمنية		الرمز	التطورات التي حصلت على الروبوت
1	منذ عام 2000		أ	ظهر مصطلح الذكاء الاصطناعي وصمم أول نظام خبير لحل مشكلات رياضية صعبة كما صمم أول ذراع روبوت في الصناعة
2	القرن التاسع عشر		ب	قام العالم المسلم الملقب ب (الجزري)بتصميم ساعة مائية وآلات أخرى وإنتاجها مثل آلة لغسل اليدين تقدم الصابون والمناشف آليا لمستخدميها
3	القرن الثاني عشر والثالث عشر		جـ	تم ابتكار دمى آلية في اليابان قادرة على تقديم الشاي أو اطلاق السهام أو الطلاء
			د	ظهر الجيل الجديد من الروبوتات التي تشبه في تصميمها جسم الإنسان وأطلق عليها اسم الإنسان الآلي استخدمت في أبحاث الفضاء من قبل وكالة ناسا

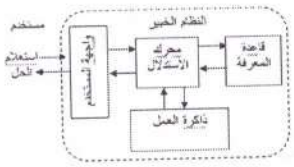
تأمل الشكل ، ثم أجب عن الأسئلة التي الآتية :

1- عن ماذا يعبر هذا الشكل

2- وضح لماذا تتصف قاعدة المعرفة بالمرونة

3- ما هي فائدة واجهة المستخدم

4- أذكر ثلاثاً من مزايا النظم الخبيرة



ادرس العبارة الجبرية المنطقية الاتية ثم أجب عن الأسئلة التي تليها

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

1- جد ناتج العبارة الجبرية المنطقية إذا علمت أن :

A = 0 , B = 0 , C = 1 , D = 0

2- حول العبارة الجبرية إلى عبارة منطقية

3- مثل العبارة الجبرية باستخدام البوابات المنطقية

للحد من مخاطر أمن المعلومات هناك عدد من الضوابط ، صنف الجدول الموضح أدناه كلاً مما يأتي إلى أحد الضوابط

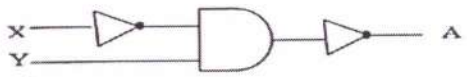
(المادية ، الإدارية ، التقنية)

(استخدام الأقفال ، حقوق النشر ، التشفير ، استخدام أجهزة الحريق ، الجدر النارية ، براءة الاختراع ، حراس الأمن ، بروتوكولات الشبكات)

ادرس البوابات المنطقية ثم أجب عن الأسئلة الآتية :

1- أكتب العبارة المنطقية التي تمثلها البوابات المنطقية

2- أكتب عبارة الجبر المنطقي التي تمثلها البوابات المنطقية



التهديدات والثغرات تعتبر من أنواع المخاطر التي تهدد أمن المعلومات ، صنف الجمل الآتية إلى تهديدات أو ثغرات :

1- عدم كفاية الحماية المادية للأجهزة والمعلومات

2- حريق أدى إلى فقدان المعلومات

3- لم يتم تحديد صلاحيات الوصول إلى المعلومات

4- كتابة عنوان بريد الكتروني خاطئ

أكتب المكافئ في النظام العشري لكل رمز من رموز النظام السادس عشر المبينة في الجدول الآتي :

النظام السادس عشر	النظام العشري
B	
D	
F	
C	

وضح المقصود بكل مما يأتي :

1- النظام العددي

2- الذكاء الاصطناعي

3- الهندسة الاجتماعية

أدرس العبارة المنطقية الآتية ثم أجب عن الأسئلة التي تليها :

NOT (A NAND NOT B) NAND C

1- مثل العبارة المنطقية باستخدام البوابات المنطقية

2- جد ناتج العبارة المنطقية علما أن :

A = 1 , B = 1 , C = 1

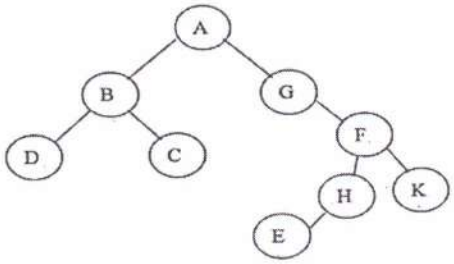
ادرس الشكل الآتي ثم أجب عن الأسئلة التي تليه :

1- كم عدد حالات فضاء البحث في الشجرة

2- ما جذر الشجرة

3- كم عدد النقاط الميتة في الشجرة

4- استخدم خوارزمية البحث في العمق أولا لإيجاد مسار البحث عن الحالة الهدف (E)



من خلال دراستك لوحدة أمن المعلومات والتشفير أجب عن الأسئلة الآتية:

1- شفر النص الآتي مستخدما خوارزمية الخط المتعرج علما بأن مفتاح التشفير سطران

I LOST MY CHARGER

2- فك تشفير النص الآتي مستخدما خوارزمية الخط المتعرج علما بأن مفتاح التشفير أربعة أسطر

T ∇UOOPSAATUWL ∇LB∇RNA ∇KOY ∇∇ N

أجب ب (نعم) أو (لا) على كل عبارة من العبارات الآتية :

1- تتمتع إيانا (IANA) بالسلطة المسؤولة عن منح أرقام الإنترنت المخصصة لإعطاء العناوين الرقمية للأجهزة على الإنترنت

2- تصنف خوارزميات التشفير بناء على معيار المفتاح المستخدم وكمية المعلومات المرسلة فقط

3- تتميز خوارزمية الخط المتعرج بأنها خوارزمية معقدة وطويلة

4- من آليات عمل تقنية تحويل العناوين الرقمية النمط الثابت للتحويل والنمط المتغير للتحويل

5- وظيفة الجهاز الوسيط هي تحويل العنوان الرقمي الداخلي إلى عنوان رقمي خارجي

مع تمنياتي للجميع

بالتوفيق والنجاح

عبد الغفار الشيخ