أمن نظم المعلومات

جلسة العملي الثانية

مدرسة المقرر

د. بشرى علي معلا

QUIZ1

<u>السؤال الأول :</u> أجب بـ صح أو خطأ مع التعليل لكتا الإجابتين: (6 درجات)

1. إن استخدام كاشفات الحركة يندرج تحت فئة التحكم الإداري بأمن المعلومات.
2. يهدد هجوم الاعتراض متطلب التوافرية.
3. يعد هجوم الاحتيال على البريد الالكتروني هجوماً فعالاً.

<u>السؤال الثاني:</u>

لدينا السيناريو الآتي: (4 درجات)

موظف في شركة مسؤول عن جدولة رواتب الموظفين و تثبيت قيم المكافآت الشهرية باستخدام برنامج محاسبة.بينما كان يعمل، أحس بالتعب، فقرر أن يذهب لتناول القهوة، وترك جهازه في حالة عمل، و باب مكتبه مفتوحاً. فدخل أحد الموظفين و قام بالعبث بجداول المكافآت وتغيير بعض القيم فيه زيادة و أخرى نقصاناً. برأيك:

1. ما نوع التحكم بأمن المعلومات الذي أهمل في هذا السيناريو؟ مع التعليل.
2. ما اسم الهجوم الذي حدث في السيناريو؟ وما نوعه؟ وما هو المتطلب الأمني الذي انتهك مع التعليل؟

الحل

السؤال الأول :

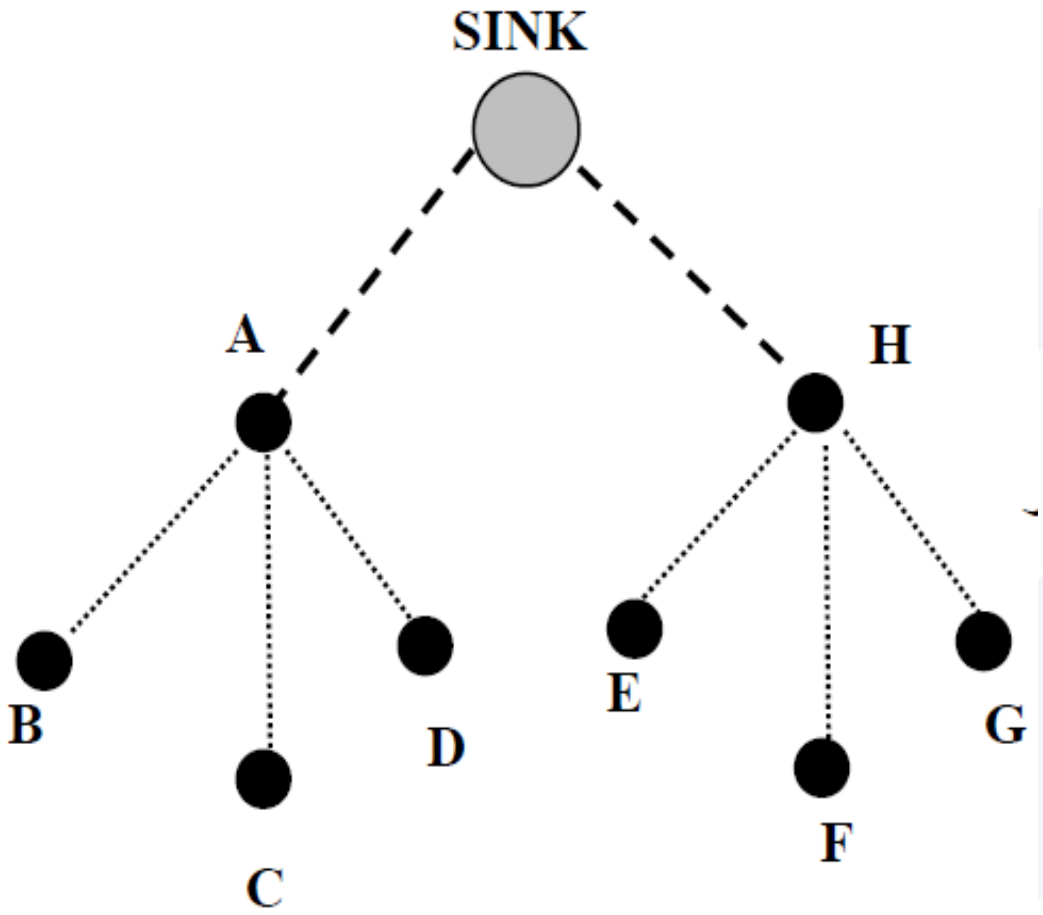
1. خطأ. إن كاشفات الحركة هي من فئة التحكم الفيزيائي فهي تجهيزات ولا علاقة لها بسلوك الأفراد .
2. خطأ. هجوم الاعتراض لا يتسبب في قطع الاتصال أو قطع الخدمة لذا لا يهدد متطلب الوافرية.
3. صح. لأنه يسمح للمهاجم بإرسال رسائل مزيفة قد تلحق الأذى بالأشخاص الواصلة إليهم.

السؤال الثاني:

1. نوعه: التحكم الإداري بأمن المعلومات. **التعليل**: لأنه يتعلق بسلوك غير صحيح للموظف .
2. اسم الهجوم: هجوم التعديل، نوعه: فعال، المتطلب:التكاملية ، **التعليل:** لأن المهاجم قام بتعديل على معلومات لا يحق له العبث فيها.

المسألة الأولى:

بفرض لدينا الشبكة اللاسلكية المبينة في الشكل المجاور:



تتكون الشبكة من عنقودين لكل عنقود قائد عنقود يتصل مع المركز الرئيسي Sink .

الاتصالات الممكنة بين العقد هي الاتصالات المبينة في الشكل حصراً.

المطلوب: أيها أفضل للتطبيق على هذه الشبكة :

- خوارزمية التشفير المتناظر التقليدية
- خوارزمية التشفير المتناظر الثنائي
- خوارزمية التشفير غير المتناظر

اعتمد في إجابتك على المقارنة على أساس معيارين هما:

1. عدد المفاتيح المخزنة في كل من المركز و قائد العنقود و العقدة ضمن العنقود (مع التعليل) (نظم إجابتك في جدول)
2. المستوى الأمني (مع التعليل)

حل المسألة الأولى:

1. عدد المفاتيح المخزنة في كل من المركز و قائد العنقود و العقدة ضمن العنقود (مع التعليل) (نظم إجابتك في جدول)

خوارزمية التشفير غير المتناظر		خوارزمية التشفير المتناظر الثنائي		خوارزمية التشفير المتناظر التقليدية		الخوارزمية
التعليل	العدد	التعليل	العدد	التعليل	العدد	عدد المفاتيح المخزنة
المفتاح العام و الخاص للمركز نفسه و المفتاح العام لقائدي العنقودين	4	مفتاح ثنائي لكل اتصال	2	مفتاح واحد لكل العقد	1	المركز
المفتاح العام والخاص للقائد ، المفتاح العام لكل من المركز وكل عقدة من عقد العنقود	6	مفتاح ثنائي لكل اتصال	4	مفتاح واحد لكل العقد	1	قائد العنقود
المفتاح العام والخاص للعقدة ، و المفتاح العام لقائد العنقود التابعة له	3	مفتاح ثنائي للاتصال مع قائد العنقود	1	مفتاح واحد لكل العقد	1	العقدة في العنقود

من الجدول السابق نلاحظ أن :

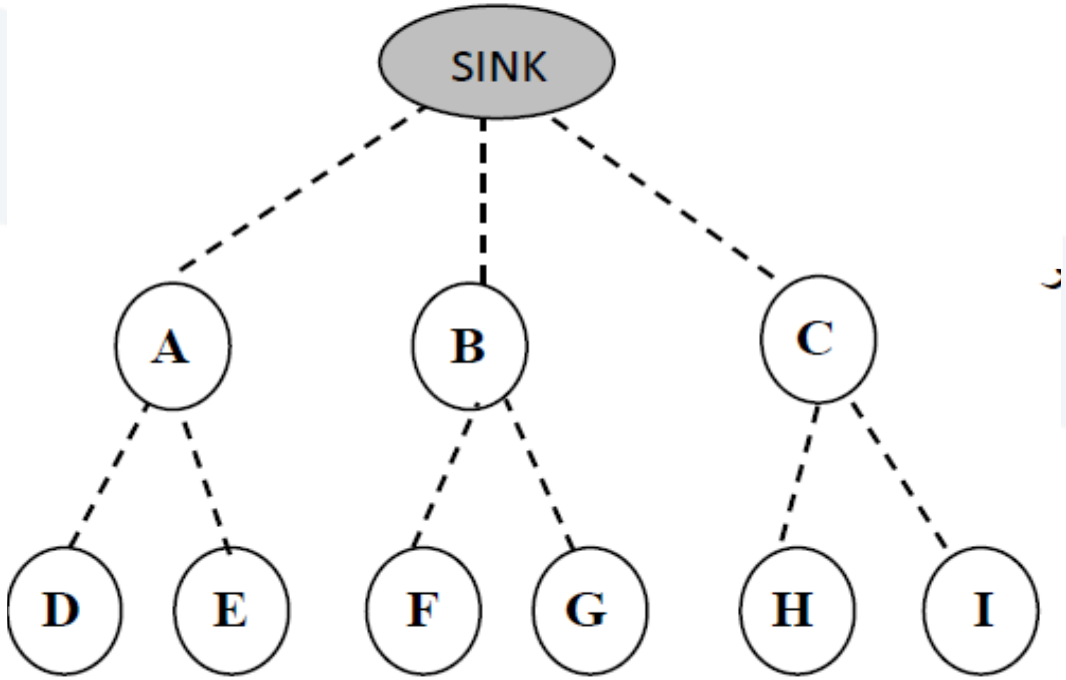
خوارزمية التشفير المتناظر التقليدية تتطلب أقل عدد مفاتيح فهي الأفضل من حيث عدد المفاتيح المطلوب تخزينها، تليها خوارزمية التشفير المتناظر الثنائي و من ثم المتناظر التقليدية.

2. المستوى الأمني (مع التعليل)

خوارزمية التشفير غير المتناظر	خوارزمية التشفير المتناظر الثنائي	خوارزمية التشفير المتناظر التقليدية	الخوارزمية
المتوسط	الأفضل	الأسوء	المستوى الأمني
1. السيطرة على قائد العنقود تسبب السيطرة على هذا العنقود و جميع الوصلات التي تستخدم المفتاح العام للمركز أيضاً. 2. السيطرة على عقدة في العنقود تسبب السيطرة على جميع الوصلات في العنقود لأنها تخزن المفتاح العام لقائد العنقود.	1. السيطرة على قائد العنقود تسبب السيطرة على هذا العنقود. 2. السيطرة على عقدة في العنقود تسبب السيطرة على وصلة هذه العقدة فقط.	السيطرة على عقدة واحدة في الشبكة تتسبب في كشف المفتاح بالنتيجة السيطرة على كل وصلات الشبكة	التعليل

المسألة الثانية:

بفرض لدينا الشبكة اللاسلكية المبينة في الشكل المجاور:



تتكون الشبكة من 3 عناقيد، قادة العناقيد هي A,B,C حيث:

A هو قائد للعنقود D,E

B هو قائد للعنقود F,G

C هو قائد للعنقود H,I

الوصلات في الشبكة تمثل بالخطوط المنقطة.

إذا كان نظام التشفير المستخدم هو نظام تشفير هجين كالآتي:

- يستخدم خوارزمية التشفير المتناظر الثنائي بين قادة العناقيد و المركز
- يستخدم خوارزمية التشفير غير المتناظر فيما بين كل قائد عنقود و العقد التابعة له.

و المطلوب :

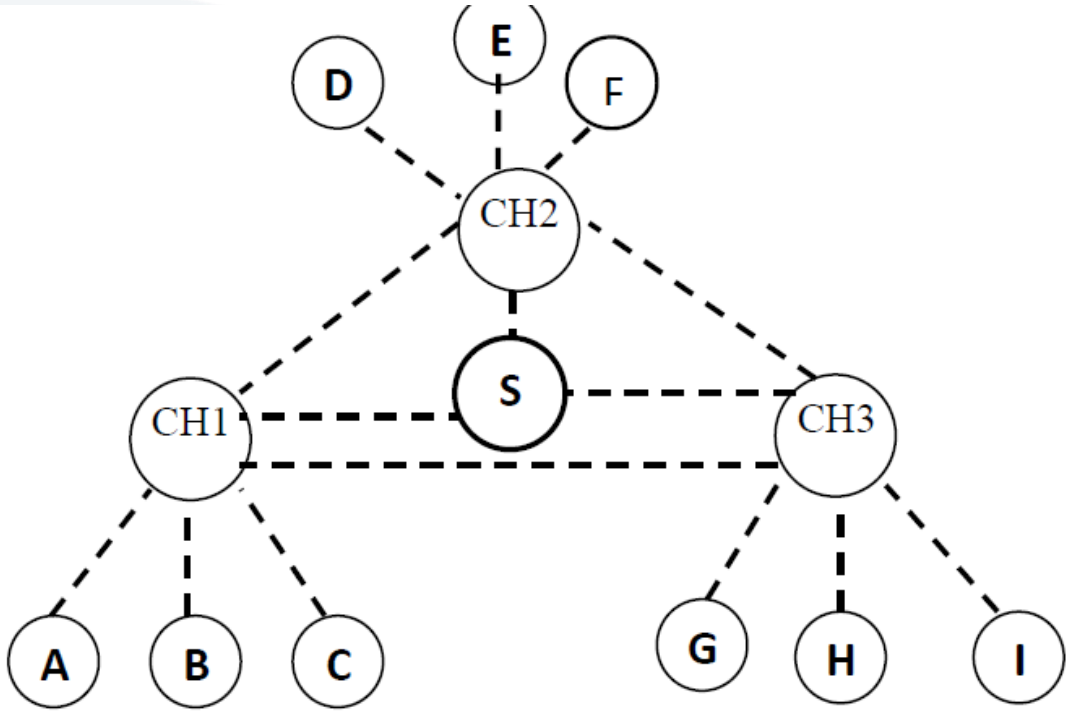
حدد مع التعليل عدد المفاتيح المخزنة في كل من : المركز ،القادة A,B,C ، العقدة D مع التعليل (نظم إجابتك في جدول)

حل المسألة الثانية:

العقدة	عدد المفاتيح	التعليل
المركز	3	مفتاح ثنائي للاتصال مع كل قائد عنقود
قادة العناقيد	5	مفتاح ثنائي مع المركز و المفتاحان العام و الخاص له و المفتاح العام للعقدتين المكونتين للعنقود
العقدة D	3	المفتاح الخاص و العام للعقدة ، و المفتاح العام لقائد العنقود.

المسألة الثالثة:

بفرض لدينا الشبكة اللاسلكية المبينة في الشكل المجاور:



تتكون الشبكة من 3 عناقيد، قادة العناقيد هي CH1,CH2,CH3 حيث:

CH1 هو قائد للعنقود A,B,C

CH2 هو قائد للعنقود D,E,F

CH3 هو قائد للعنقود G,H,I

الوصلات في الشبكة تمثل بالخطوط المنقطة.

و المطلوب :

1. إذا كان طبق نظام التشفير **متناظرثنائي** على الشبكة كاملة :

أ. ما عدد المفاتيح المخزنة في كل من : المركز و القادة الثلاثة و العقدة D مع التعليل (نظم إجابتك في جدول)

ب. ما تأثير سيطرة مهاجم على قائد العنقود CH3 ؟

تابع المسألة الثالثة:

2. إذا طبق نظام التشفير هجين على الشبكة كالآتي:

- خوارزمية التشفير المتناظر التقليدية ضمن العنقود الواحد
- خوارزمية التشفير المتناظر الثنائي فيما بين قادة العناقيد و المركز
- خوارزمية التشفير غير المتناظر فيما بين العناقيد

أ. ما عدد المفاتيح المخزنة في كل من : المركز و القادةالثلاثة و العقدة D مع التعليل (نظم إجابتك في جدول)

ب. ما تأثير سيطرة مهاجم على العقدة A ؟

حل المسألة الثالثة:

الطلب الأول:

أ. عدد المفاتيح المخزنة :

التعليل	عدد المفاتيح	العقدة
مفتاح ثنائي للاتصال مع كل قائد عنقود	3	المركز
مفتاح ثنائي مع المركز و مفتاح ثنائي مع كل قائد عنقود آخر و مفتاح ثنائي مع كل عقدة ضمن العنقود	6	قادة العناقيد
مفتاح ثنائي للاتصال مع قائد العنقود	1	العقدة D

ب. سيحصل المهاجم على المفاتيح التي يختزنها قائد العنقود CH3 و بالنتيجة سيسطر على جميع وصلاته ضمن العنقود نفسه و بينه و بين المركز فقط . لكن لن يؤثر على الوصلات الأخرى في الشبكة.

حل المسألة الثالثة:

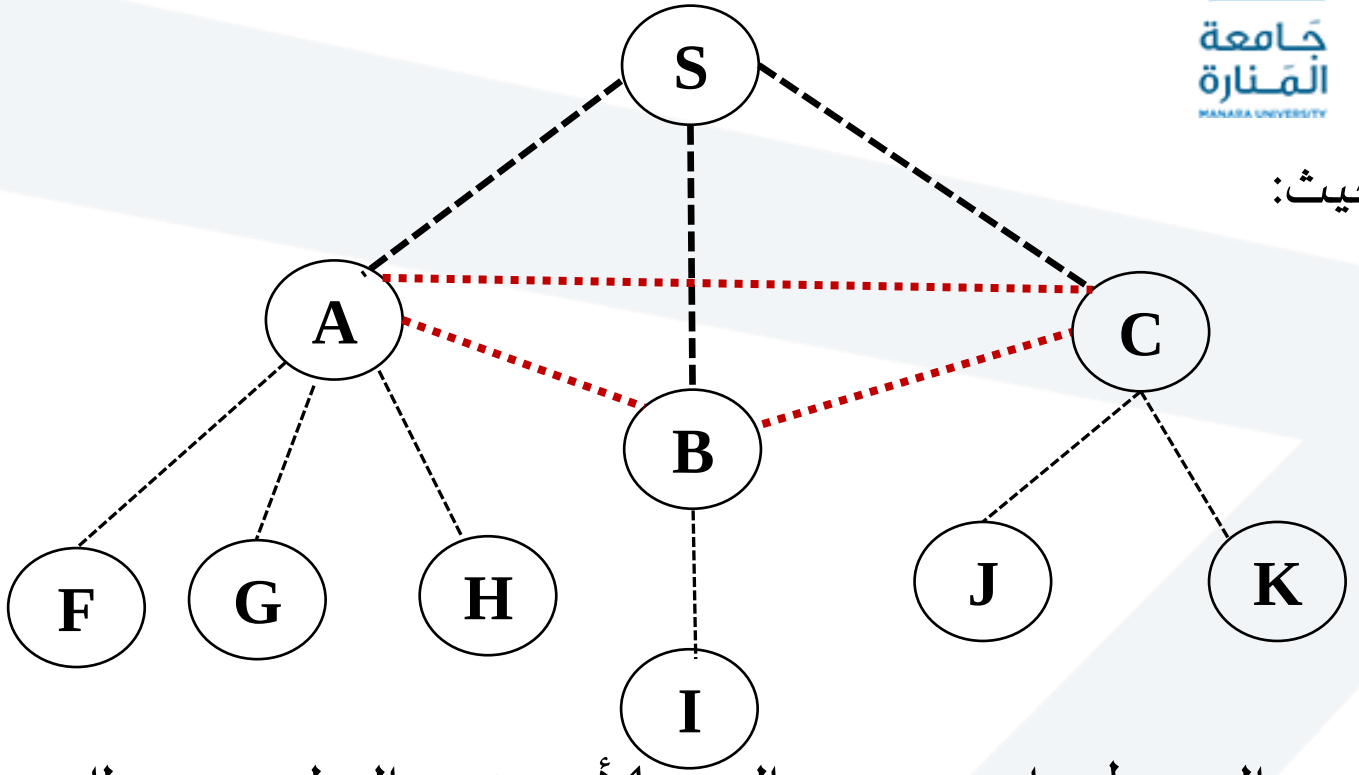
الطلب الثاني :

أ. عدد المفاتيح المخزنة

العقدة	عدد المفاتيح	التعليل
المركز	3	مفتاح ثنائي للاتصال مع كل قائد عنقود
قادة العناقيد	6	مفتاح ثنائي مع المركز و المفتاح العام و الخاص للقائد العنقود نفسه و المفتاح العام لكل قائد عنقود آخر و مفتاح للاتصال مع العقد التابعة له
العقدة D	1	مفتاح واحد للاتصال مع قائد العنقود

ب. سيحصل المهاجم على المفتاح المخزن فيها وسيتسبب بسيطرة المهاجم على جميع الوصلات في هذا العنقود لأنه المفتاح المستخدم لتأمين جميع الاتصالات ما بين العقد و قائد العنقود CH1.

المسألة الرابعة



بفرض لدينا الشبكة اللاسلكية المبينة في الشكل المجاور:

تتكون الشبكة من ثلاث عناقيد ، قادة العناقيد هي A,B,C حيث:

A هو قائد للعنقود F,G,H

B هو قائد للعنقود I

C هو قائد للعنقود J,K

الوصلات في الشبكة تمثل بالخطوط المنقطة.

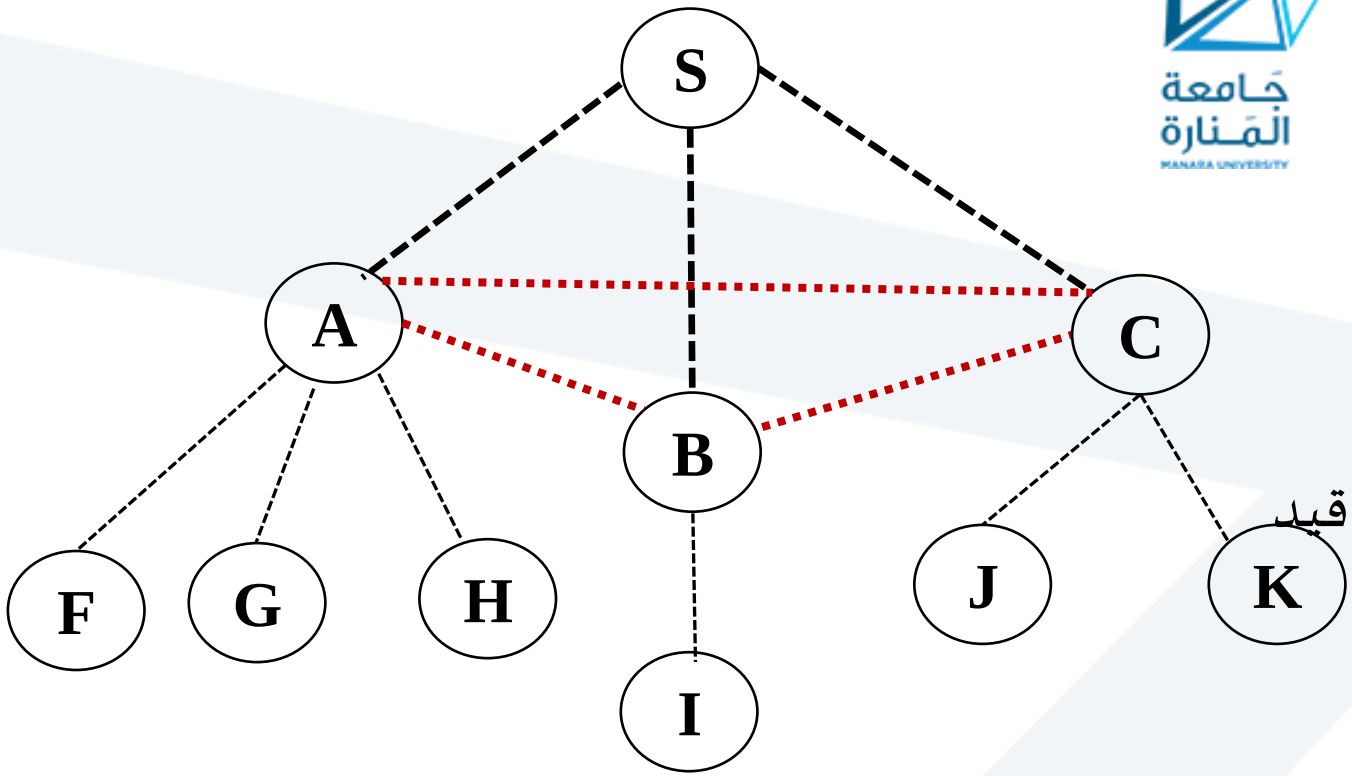
و المطلوب :

1 . إذا كانت الغاية الأساسية من نظام التشفير المستخدم هي الحصول على مستوى عال من الأمن بغض النظر عن متطلب التخزين. ما هو نظام التشفير الذي تقترح استخدامه في هذه الشبكة . وضح إجابتك.

2. إذا كانت الغاية الأساسية من نظام التشفير المستخدم هي الحصول على تأمين الوصلات ضمن الشبكة لكن مع مراعاة متطلب التخزين بالدرجة الأولى. ما هو نظام التشفير الذي تقترح استخدامه في هذه الشبكة . وضح إجابتك.

تابع المسألة الرابعة

3. في حال طبق نظام التشفير الهجين الآتي:



- ✓ تشفير متناظر تقليدي فيما بين المركز و قادة العناقيد
- ✓ تشفير غير متناظر فيما بين قادة العناقيد
- ✓ نظام تشفير ثنائي فيما بين العقد وقائد العنقود

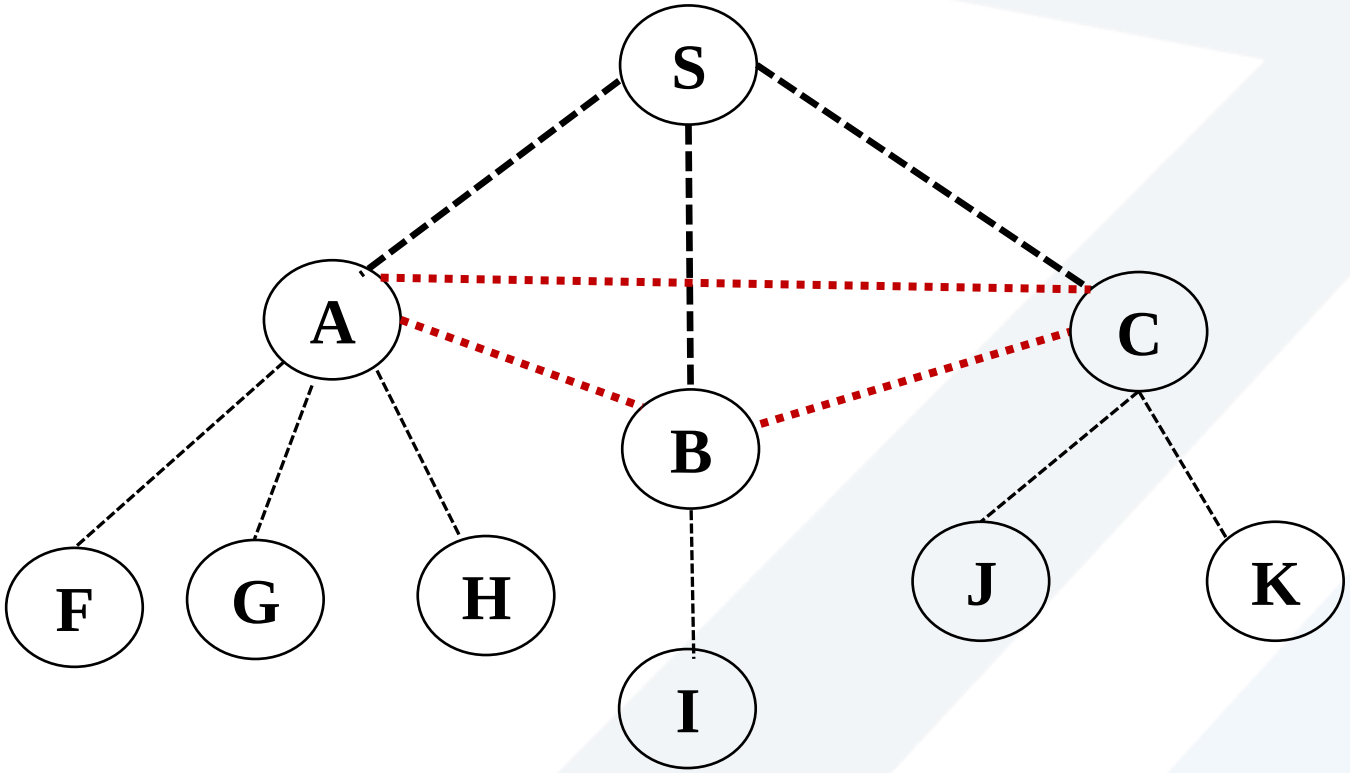
أ. ما هو عدد المفاتيح المخزن في كل من : S و A,B,C العقدة K (نظم إجابتك في جدول)

ب. احسب عدد المفاتيح المخزن على مستوى الشبكة؟

جـ. اقترح تعديلاً واحداً فقط يمكن إجراؤه على نظام التشفير الهجين ينتج عنه تخفيض في عدد المفاتيح المخزنة على مستوى الشبكة.

تابع المسألة الرابعة

4. في حال طبق نظام التشفير غير المتناظر على كامل الشبكة :



أ. ما هو عدد المفاتيح المخزن في كل من : S و A,B,C العقدة K (نظم إجابتك في جدول)

ب. احسب عدد المفاتيح المخزن على مستوى الشبكة؟

حل المسألة الرابعة

1 . إذا كانت الغاية الأساسية من نظام التشفير المستخدم هي الحصول على مستوى عال من الأمن بغض النظر عن متطلب التخزين. ما هو نظام التشفير الذي تقترح استخدامه في هذه الشبكة . وضح إجابتك.

نظام تشفير متناظر ثنائي

التعليل: يستخدم مفتاح مختلف لكل وصلة ، سيطرة المهاجم على أية عقدة يؤثر فقط على وصلات هذه العقدة.

2. إذا كانت الغاية الأساسية من نظام التشفير المستخدم هي الحصول على تأمين الوصلات ضمن الشبكة لكن مع مراعاة متطلب التخزين بالدرجة الأولى. ما هو نظام التشفير الذي تقترح استخدامه في هذه الشبكة . وضح إجابتك.

نظام تشفير متناظر تقليدي

التعليل: تخزن كل عقدة مفتاح واحد فقط .

حل المسألة الرابعة

3. في حال طبق نظام التشفير الهجين الآتي:

أ. ما هو عدد المفاتيح المخزن في كل من : S و A,B,C العقدة K (نظم إجابتك في جدول)

العقدة	عدد المفاتيح	التعليل
S	1	مفتاح واحد للاتصال مع قادة العناقيد
A	8	مفتاح مع المركز و المفتاح العام و الخاص للقائد العنقود نفسه والمفتاحين العاميين للقائدين الآخرين و مفتاح ثنائي واحد للاتصال مع كل عقدة ضمن العنقود
B	6	مفتاح مع المركز و المفتاح العام و الخاص للقائد العنقود نفسه والمفتاحين العاميين للقائدين الآخرين و مفتاح ثنائي واحد للاتصال مع كل عقدة ضمن العنقود
C	7	مفتاح مع المركز و المفتاح العام و الخاص للقائد العنقود نفسه والمفتاحين العاميين للقائدين الآخرين و مفتاح ثنائي واحد للاتصال مع كل عقدة ضمن العنقود
K	1	مفتاح ثنائي واحد للاتصال مع قائد العنقود

حل المسألة الرابعة:

3. في حال طبق نظام التشفير الهجين الآتي:

ب. احسب عدد المفاتيح المخزنة على مستوى الشبكة؟

عدد المفاتيح المخزنة= المفاتيح المخزنة في المركز + المفاتيح المخزنة في قادة العناقيد + المفاتيح المخزنة في العقد F,G,H,I,J,K

عدد المفاتيح المخزنة=(1X6)+7+6+8+1 = 28مفتاح

جـ. اقترح تعديلاً واحداً فقط يمكن إجراؤه على نظام التشفير الهجين ينتج عنه تخفيض في عدد المفاتيح المخزنة .

نستبدل نظام التشفير غير متناظر فيما بين قادة العناقيد إلى نظام تشفير متناظر تقليدي

العقدة	عدد المفاتيح	التعليل
S	1	مفتاح واحد للاتصال قادة العناقيد
A	5	مفتاح مع المركز و مفتاح واحد للاتصال مع قائدي العناقيد الأخرى ع مفتاح ثنائي لكل عقدة ضمن العنقود
B	3	مفتاح مع المركز و مفتاح ثنائي للاتصال مع كل قائد عنقود و مفتاح ثنائي مع العقدة ضمن العنقود
C	4	مفتاح مع المركز و مفتاح للاتصال مع قائدي العناقيد الأخرى و مفتاح ثنائي لكل عقدة ضمن العنقود
K	1	مفتاح ثنائي واحد للاتصال مع قائد العنقود

حل المسألة الرابعة:

عدد المفاتيح المخزنة= المفاتيح المخزنة في المركز + المفاتيح المخزنة في قادة العناقيد + المفاتيح المخزنة في العقد F,G,H,I,J,K

عدد المفاتيح المخزنة=(1X6)+4+3+5+1 = 19مفتاح

حل المسألة الرابعة:

4. في حال طبق نظام التشفير غير المتناظر على كامل الشبكة :

أ. ما هو عدد المفاتيح المخزن في كل من : S و A,B,C العقدة K (نظم إجابتك في جدول)

العقدة	عدد المفاتيح	التعليل
S	5	المفتاح العام و الخاص للمركز و المفاتيح العامة للقادة الثلاثة
A	8	المفتاح العام للمركز و المفتاح العام و الخاص للعقدة نفسها و المفتاحين العامين للقائدين الآخرين و المفاتيح العامة الثلاثة للعقد المكونة للعنقود
B	6	المفتاح العام للمركز و المفتاح العام و الخاص للعقدة نفسها و المفتاحين العامين للقائدين الآخرين و المفتاح العام للعقدة I
C	7	المفتاح العام للمركز و المفتاح العام و الخاص للعقدة نفسها و المفتاحين العامين للقائدين الآخرين و المفتاحين العامين للعقدتين المكونتين للعنقود
K	3	المفتاح العام و الخاص للعقدة نفسها و المفتاح العام لقائد العنقود

حل المسألة الرابعة:

ب. احسب عدد المفاتيح المخزن على مستوى الشبكة؟

عدد المفاتيح المخزنة= المفاتيح المخزنة في المركز + المفاتيح المخزنة في قادة العناقيد + المفاتيح المخزنة في العقد F,G,H,I,J,K

عدد المفاتيح المخزنة=(3X6)+6+7+8+5 = 44مفتاح

نهاية الجلسة الثانية