جامعة المنارة

كلية الهندسة

الهندسة المعلوماتية

عملي أمن المعلومات

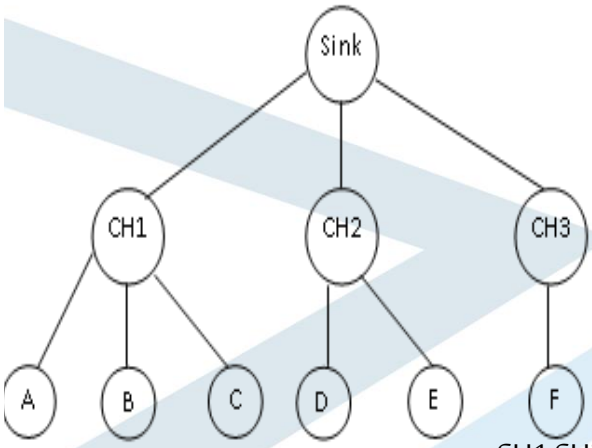
مدرسة المقرر

د. بشرى علي معلا

جلسة العملي الأولى

MU-EPP-FM-005 Issue date 17November2025 issue no:1 https://manara.edu.sy

مسألة الكويز ١



بفرض لدينا الشبكة الآتية:
حيث يمثل SINK مركز الشبكة ،
CH1,CH2,CH3 قادة العناقيد
A,B,C,D,E,F هي العقد ضمن هذه العناقيد. و المطلوب:

١.في حال طبق نظام تشفير غير متناظر على الشبكة كلها،
احسب عدد المفاتيح المخزن في كل من SINK, CH1,CH2,CH3,D
مع التعليل لكل منها.

٢. في حال طبق نظام تشفير هجين كالآتي :

- نظام تشفير متناظر ثنائي بين الـ SINK قادة العناقيد CH1,CH2,CH3
- نظام تشفير غير متناظر بين كل قائد عنقود و العقد التابعة له.

احسب عدد المفاتيح المخزنة في كل من SINK,CH1,CH2,CH3,A مع التعليل لكل منها.

حل المسألة الأولى

الطلب الأول:

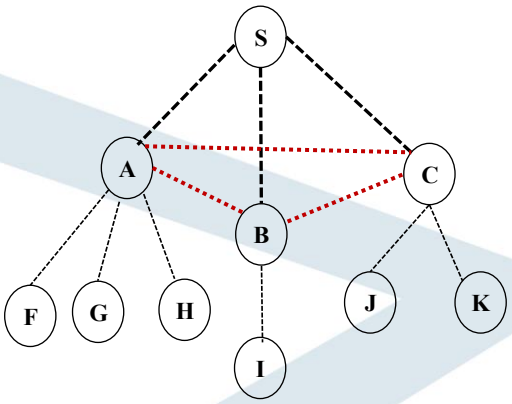
العقدة	عدد المفاتيح	التعليل
SINK	5	مفتاح عام و خاص لـ SINK ، المفتاح عام لكل من CH1,CH2,CH3
CH1	6	المفتاح العام و الخاص لـ CH1، المفتاح العام لكل من A,B,C والمفتاح العام لـ sink
CH2	5	المفتاح العام و الخاص لـ CH2، المفتاح العام لكل من D,Eوالمفتاح العام لـ sink
CH3	4	المفتاح العام و الخاص لـ CH1، المفتاح العام لكل من Fوالمفتاح العام لـ sink
D	3	المفتاح العام و الخاص لـ D، المفتاح العام لـ CH2

الطلب الثاني:

العقدة	عدد المفاتيح	التعليل
SINK	3	مفتاح ثنائي مع كل قائد عنقود
CH1	6	مفتاح مع الـ sink و المفتاح العام والخاص لـ CH1 والمفتاح العام لكل من A,B,C
CH2	5	مفتاح مع الـ sink و المفتاح العام والخاص لـ CH2 و المفتاح العام لكل من D,E
CH3	4	مفتاح مع الـ sink و المفتاح العام والخاص لـ CH3 و المفتاح العام لـ F
A	3	المفتاح العام والخاص لـ A و المفتاح العام لقائد العنقود CH1

المسألة الثانية

بفرض لدينا الشبكة اللاسلكية المبينة في الشكل المجاور:



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

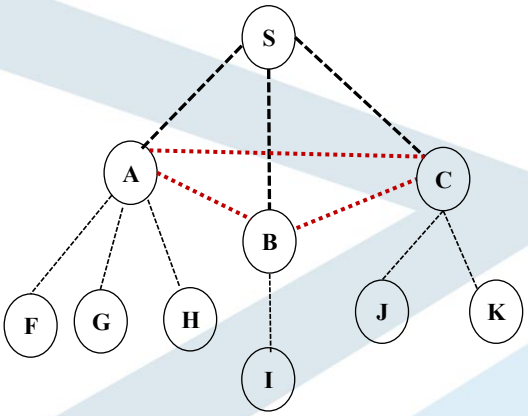
A هو قائد للعنقود F,G,H
B هو قائد للعنقود I
C هو قائد للعنقود J,K

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.

٢ . 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 الثانية



٣. في حال طبق نظام التشفير الهجين الآتي:

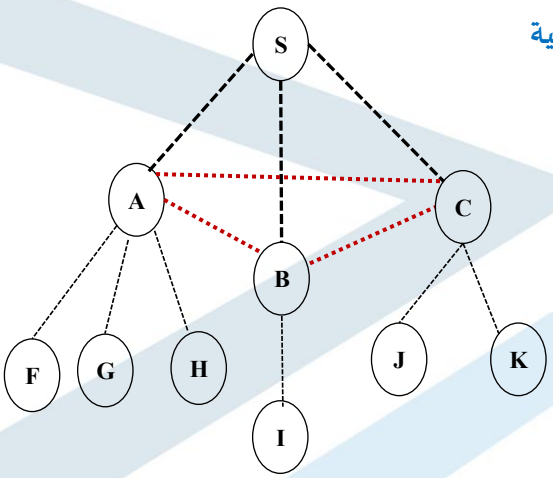
- ✓ تشفير متناظر تقليدي فيما بين المركز و قادة العناقيد
- ✓ تشفير غير متناظر فيما بين قادة العناقيد
- ✓ نظام تشفير ثنائي فيما بين العقد وقائد العنقود

أ. ما هو عدد المفاتيح المخزن في كل من : S وA,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 الثانية



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

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

ب. احسب عدد المفاتيح المخزن على مستوى الشبكة؟

حل المسألة الثانية

الطلب الأول:

نظام تشفير متناظر ثنائي

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

الطلب الثاني:

نظام تشفير متناظر تقليدي

التعليل: تخزن كل عقدة مفتاح واحد فقط .

الطلب الثالث: أ.

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 والمفتاحان العامان 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 والمفتاحان العامان 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 والمفتاحان العامان للقائدين الآخرين و مفتاح ثنائي واحد للاتصال مع كل عقدة ضمن العنقود
K	1	مفتاح ثنائي واحد للاتصال مع قائد العنقود

ب. 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 نستبدل نظام التشفير غير متناظر فيما بين قادة العناقيد الى 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 العنقودين الآخرين و مفتاح ثنائي لكل عقدة ضمن العنقود
B	3	مفتاح مع المركز و مفتاح ثنائي للاتصال مع قائدي العنقودين الآخرين و مفتاح ثنائي مع العقدة ضمن العنقود
C	4	مفتاح مع المركز و مفتاح للاتصال مع قائدي العنقودين الآخرين و مفتاح ثنائي لكل عقدة ضمن العنقود
K	1	مفتاح ثنائي واحد للاتصال مع قائد العنقود

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

الطلب الرابع:

أ.

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 المفتاحان العامان للقائدين الآخرين و المفاتيح العامة الثلاثة للعقد المكونة للعنقود
B	6	المفتاح العام للمركز و المفتاح العام و الخاص للعقدة نفسها و المفتاحان العامان للقائدين الآخرين و المفتاح العام للعقدة I
C	7	المفتاح العام للمركز و المفتاح العام و الخاص للعقدة نفسها و المفتاحان العامان للقائدين الآخرين و المفتاحين العامين للعقدتين المكونتين للعنقود
K	3	المفتاح العام و الخاص للعقدة نفسها و المفتاح العام لقائد العنقود

ب. 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

جَـامعة
المَـنارة
MANARA UNIVERSITY

نهاية الجلسة الأولى