



عملي أمن المعلومات

جلسة العملي الثانية

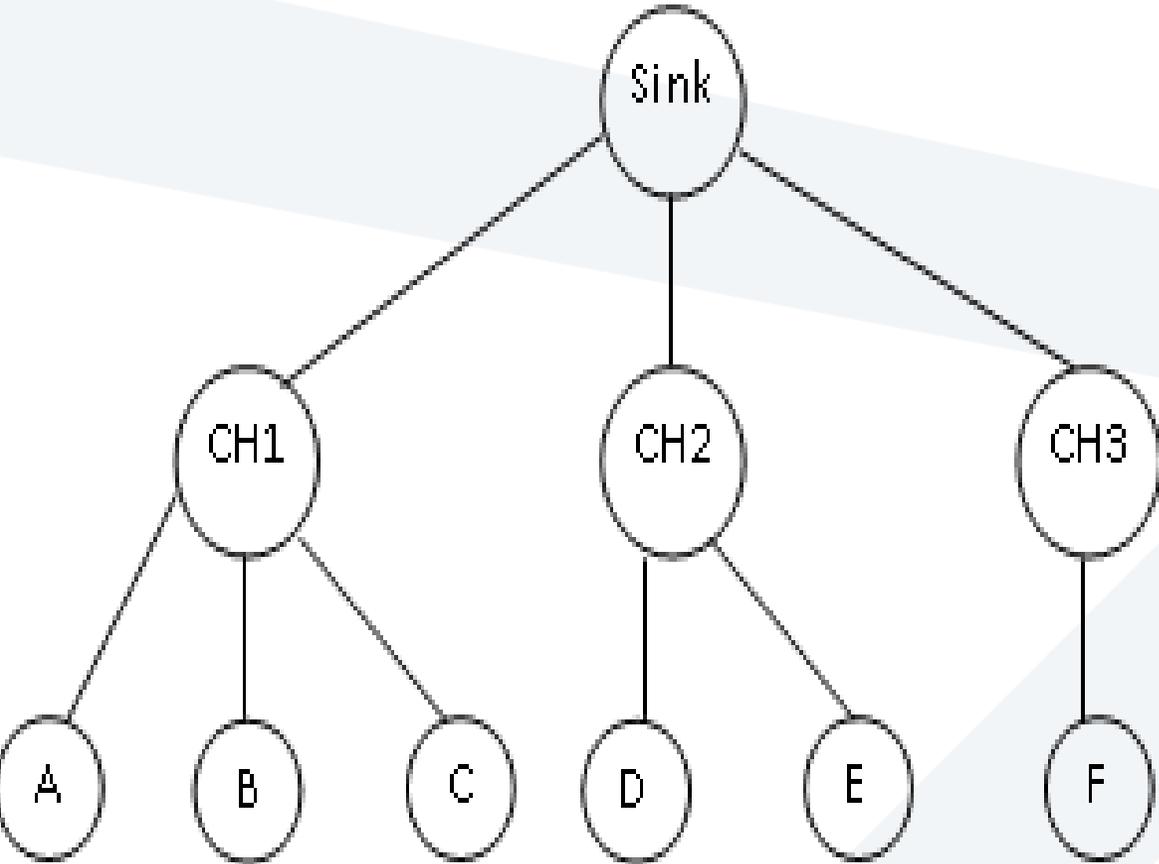
مدرسة المقرر

د. بشرى علي معلا



محاضرة مسائل

المسألة الأولى:



بفرض لدينا الشبكة الآتية:
حيث يمثل SINK مركز الشبكة ،
قادة العناقيد CH1,CH2,CH3

A,B,C,D,E,F هي العقد ضمن هذه العناقيد. و المطلوب:

1. 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.

2. في حال طبق نظام تشفير هجين كالآتي :

- نظام تشفير متناظر ثنائي بين ال 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:

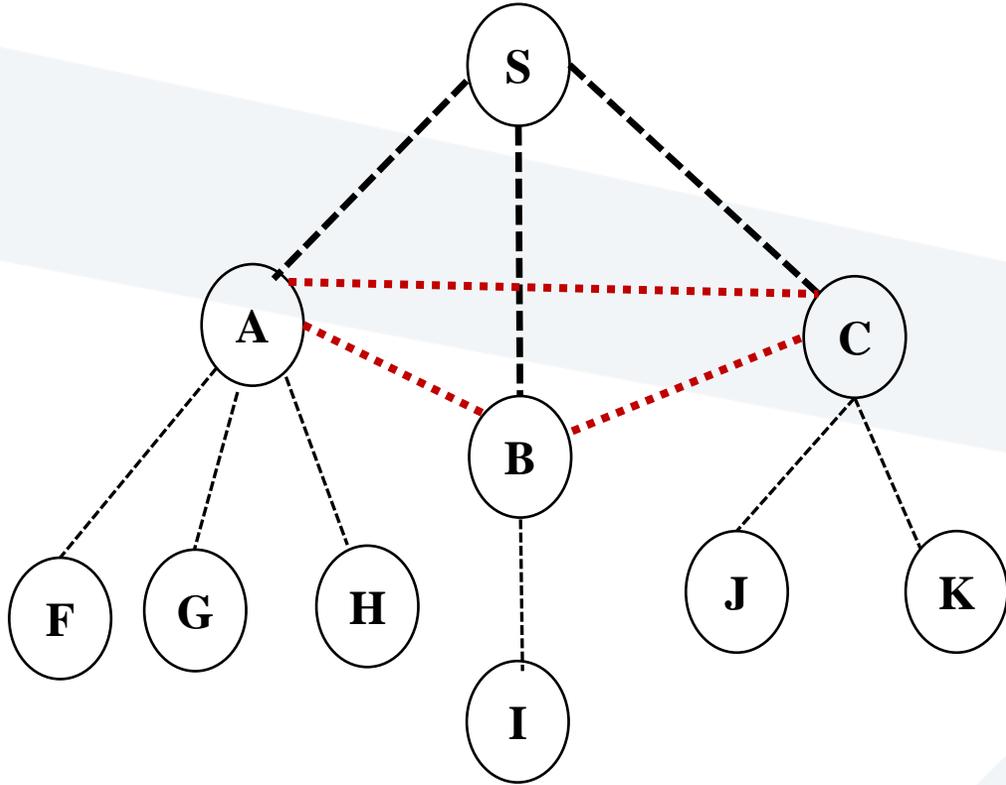
العقدة	عدد المفاتيح	التعليق
SINK	5	مفتاح عام و خاص لـ SINK ، المفتاح عام لكل من CH1,CH2,CH3
CH1	6	المفتاح العام و الخاص لـ CH1 ، المفتاح العام لكل من A,B,C والمفتاح العام لـ sink
CH2	5	المفتاح العام و الخاص لـ CH2 ، المفتاح العام لكل من D,E والمفتاح العام لـ sink
CH3	4	المفتاح العام و الخاص لـ CH1 ،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

الطلب الثاني:

العقدة	عدد المفاتيح	التعليق
SINK	3	مفتاح ثنائي مع كل قائد عنقود
CH1	6	مفتاح مع الـ sink و المفتاح العام والخاص لـ CH1 و المفتاح 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

جامعة
المنارة
MANARA UNIVERSITY



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 المنقطعة.
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.



جامعة
المنصورة

تابع المسألة الثانية

3. في حال طبق نظام التشفير الهجين الآتي:

✓ تشفير متناظر تقليدي فيما بين المركز و قادة العناقيد

✓ تشفير غير متناظر فيما بين قادة العناقيد

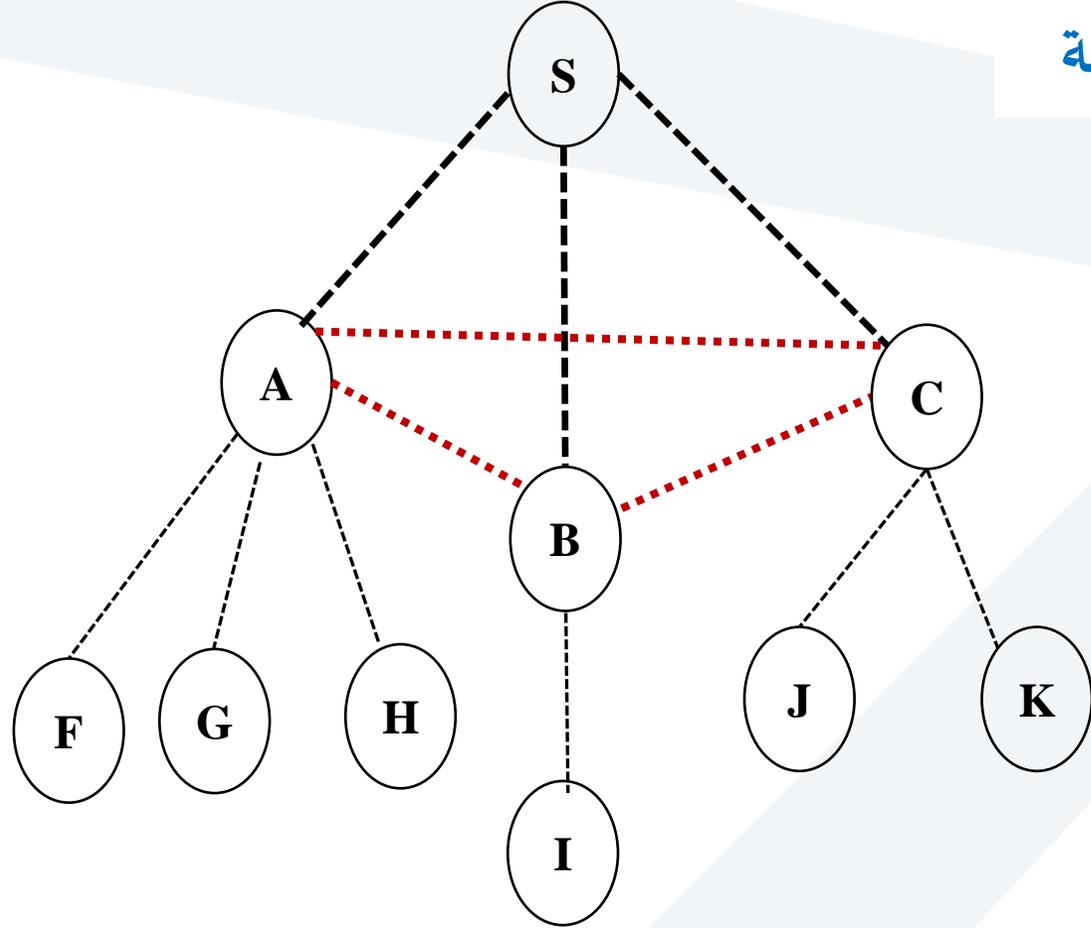
✓ نظام تشفير ثنائي فيما بين العقد وقائد العنقود

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؟

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

تابع المسألة الثانية



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 العقد K (نظم إجابتك في جدول)

ب. احسب عدد المفاتيح المخزن على مستوى الشبكة؟



جامعة
المنارة

حل المسألة الثانية

الطلب الأول:

نظام تشفير متناظر ثنائي

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

الطلب الثاني:

نظام تشفير متناظر تقليدي

التعليق: تخزن كل عقدة مفتاح واحد فقط .

العقدة	عدد المفاتيح	التعليق
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

$$\text{عدد المفاتيح المخزنة} = 1 + 8 + 6 + 7 + (1 \times 6) = 28 \text{ مفاتيح}$$



جامعة
منارة
MANARA UNIVERSITY

ج. 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 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 = $(1 \times 6) + 1 + 5 + 3 + 4 = 19$ مفتاح

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 ا
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

$$\text{عدد المفاتيح المخزنة} = 5 + 8 + 7 + 6 + (3 \times 6) = 44 \text{ مفاتيح}$$

المسألة الثالثة

إذا كان لدينا نظام حقيبة الظهر المستخدم يعتمد على إحدى المجموعتين :

$$b'=[1,2,4,5,9] , b=[2,7,11,21,42]$$

بفرض أن $n \in [80,85]$ وهي عدد فردي ، و أن $r \in]3,6[$ وبفرض أن التدوير المفروض هو: $[4,2,1,5,3]$ و المطلوب:

1. أوجد المفتاحين العام و الخاص
2. شفر النص الصريح $X=01010$
3. فك تشفير النص $S=52$ بفرض أن معكوس r ينتمي إلى المجال $[63,65]$

الطلب الأول: أوجد المفتاحين العام والخاص

1. يجب أن نختار إحدى المجموعتين المتزايدتين $b=[2,7,11,21,42]$, $b'=[1,2,4,5,9]$

1. نلاحظ في المجموعة أن الشرط غير محقق $b' = [1,2,4,5,9]$

$$b_i \geq b_1 + b_2 + \cdots + b_{i-1}$$

$$5 \geq b_1 + b_2 + b_3 = 1 + 2 + 4 = 7 \text{ غير محقق}$$

بالنتيجة ليست مجموعة متزايدة.

تابع الطلب الأول: أوجد المفتاحين العام والخاص

2. نختبر فيما إذا كانت المجموعة $b = [2, 7, 11, 21, 42]$ تحقق الشرط $b_i \geq b_1 + b_2 + \dots + b_{i-1}$

$$7 \geq b_1 = 2 \text{ محقق}$$

$$11 \geq b_1 + b_2 = 2 + 7 = 9 \text{ محقق}$$

$$21 \geq b_1 + b_2 + b_3 = 2 + 7 + 11 = 20 \text{ محقق}$$

وهي تحقق الشرط و هي المجموعة المتزايدة التي سنختارها

تابع الطلب الأول: أوجد المفتاحين العام والخاص

2. نختار n بحيث هي تحقق الشرط $n > b_1 + b_2 + b_3 + b_4 + b_5$

$$n > 2 + 7 + 11 + 21 + 42 = 83$$

وحسب فرض المسألة $n \in [80, 85]$ و هي عدد فردي فتكون $n=85$

3. نختار $r=4$ فتكون أولية مع n و حسب فرض المسألة $r \in]3, 6[$

4. نحسب بعدها المصفوفة t باستخدام العلاقة: $t_i = (b_i \times r) \bmod(n)$

$$t_1 = (2 \times 4) \bmod(85) = 8$$

$$t_2 = (7 \times 4) \bmod(85) = 28$$

$$t_3 = (11 \times 4) \bmod(85) = 44$$

$$t_4 = (21 \times 4) \bmod(85) = 84$$

$$t_5 = (42 \times 4) \bmod(85) = 83$$

فتكون المصفوفة $t=[8, 28, 44, 84, 83]$

تابع الطلب الأول: أوجد المفاتيح العام والخاص

5. بفرض أن التدوير هو: $[4,2,1,5,3]$ بعد تدوير t ينتج المفتاح العام: $a=[84, 28,8,83,44]$

6. ويكون المفتاح الخاص هو: $n=85$ $r=4$ $b = [2,7,11,21,42]$ التدوير: $[4,2,1,5,3]$

الطلب الثاني: تشفير النص $X=01010$

من أجل عملية التشفير نستخدم المفتاح العام: $a=[84, 28,8,83,44]$

$$S = X_1 a_1 + X_2 a_2 + X_3 a_3 + X_4 a_4 + X_5 a_5$$

$$S = 0.84 + 1.28 + 0.8 + 1.83 + 0.44 = 111$$

الطلب الثالث: فك تشفير $S=52$

1. معكوس $r=4$ بالنسبة لـ $\text{mod}(85)$

$$4^{-1} \text{mod}(85) \equiv 64$$

$$4 \times 64 \text{mod}(85) = 256 \text{mod}(85) = 1 \quad \text{بحيث:}$$

2. نحسب $s' = (r^{-1} \times s) \text{mod}(n) = (64 \times 52) \text{mod}85 = 3328 \text{mod}85 = 13$

3. لدينا $b=[2,7,11,21,42]$ فيكون $s' = X'_1 b_1 + X'_2 b_2 + X'_3 b_3 + X'_4 b_4 + X'_5 b_5$

$$13 = 1 \times 2 + 0 \times 7 + 1 \times 11 + 0 \times 21 + 0 \times 42$$

فتكون قيم $X' = 10100$

4. ندور قيم X' وفق التدوير المفروض $[4,2,1,5,3]$ فنحصل على $X=00101$

المسألة الرابعة

إذا كان لدينا نظام حقية الظهر المستخدم يعتمد على المجموعة : $b=[1,2,4,10,20,40]$
بفرض أن $n=110$ و أن $r \in [30,32]$ وبفرض أن التدوير المفروض هو : $[1,2,4,3,6,5]$

و المطلوب:

1. ما هي قيمة K ؟
2. أوجد المفتاحين العام و الخاص
3. شفر النص الصريح 100100111100101110
4. فك تشفير النص $S=45\ 121$ بفرض أن معكوس r ينتهي إلى المجال $[70,73]$

الطلب الأول:

قيمة $K=6$ لأنها مساوية لعدد عناصر المجموعة b

الطلب الثاني:

1. نختبر فيما إذا كانت المجموعة المتزايدة $b=[1,2,4,10,20,40]$ تحقق الشرط $b_i \geq b_1 + b_2 + \dots + b_{i-1}$

$$2 \geq b_1 = 1 \text{ محقق}$$

$$4 \geq b_1 + b_2 = 1 + 2 = 3 \text{ محقق}$$

$$10 \geq b_1 + b_2 + b_3 = 1 + 2 + 4 = 7 \text{ محقق}$$

$$20 \geq b_1 + b_2 + b_3 + b_4 = 1 + 2 + 4 + 10 = 17 \text{ محقق}$$

$$40 \geq b_1 + b_2 + b_3 + b_4 + b_5 = 1 + 2 + 4 + 10 + 20 = 37 \text{ محقق}$$

وهي تحقق الشرط

الطلب الثاني :

2. لدينا من فرض المسألة $n=110$ لذا نختار $r=31$ فتكون أولية مع n و ضمن المجال $r \in [30,32]$

3. نحسب بعدها المصفوفة t باستخدام العلاقة : $t_i = (b_i \times r) \bmod(n)$

$$t_1 = (1 \times 31) \bmod 110 = 31$$

$$t_4 = (10 \times 31) \bmod 110 = 90$$

$$t_2 = (2 \times 31) \bmod 110 = 62$$

$$t_5 = (20 \times 31) \bmod 110 = 70$$

$$t_3 = (4 \times 31) \bmod 110 = 14$$

$$t_6 = (40 \times 31) \bmod 110 = 30$$

فتكون المصفوفة $t = [31,62,14,90,70,30]$

4. بفرض أن التدوير هو: $[1,2,4,3,6,5]$ بعد تدوير t ينتج المفتاح العام: $a=[31, 62,90,14,30,70]$

5. ويكون المفتاح الخاص هو: $n=110$ $r=31$ $b=[1,2,4,10,20,40]$ التدوير: $[1,2,4,3,6,5]$

الطلب الثالث: شفر النص الصريح 100100111100101110

نلاحظ ان طول النص المطلوب تشفير أكبر عدد الأغراض من $k=6$ لذا نقسم النص الصريح إلى سلاسل طول كل منها مساوٍ

$k=6$ فيكون: $x_1= 100100, x_2= 111100, x_3= 101110$

من أجل عملية التشفير نستخدم المفتاح العام: $a=[31, 62,90,14,30,70]$

$$S = X_1 a_1 + X_2 a_2 + X_3 a_3 + X_4 a_4 + X_5 a_5 + X_6 a_6$$

$$S_1 = 1.31 + 0.62 + 0.90 + 1.14 + 0.30 + 0.70 = 45$$

$$S_2 = 1.31 + 1.62 + 1.90 + 1.14 + 0.30 + 0.70 = 197$$

$$S_3 = 1.31 + 0.62 + 1.90 + 1.14 + 1.30 + 0.70 = 165$$

$$S = s_1 \quad s_2 \quad s_3$$

$$S = 45 \quad 197 \quad 165$$

الطلب الرابع: فك تشفير 121 S=45

1. من أجل عملية فك التشفير يلزمنا حساب معكوس r بالنسبة لـ $\text{mod}(n)$:

نختبر القيم الموجودة ضمن المجال المفروض فنجد أن قيمة المعكوس هي 71 لأن

$$31^{-1} \text{mod}(110) \equiv 71 \quad \text{معكوس } r=31 \text{ بالنسبة لـ } \text{mod}(110)$$

$$31 \times 71 \text{mod}(110) = 2201 \text{mod}(110) = 1 \quad \text{بحيث:}$$

نلاحظ أن لدينا S_2 و $S_1=45$ حيث: $S=S_1 S_2$ و $S_2=121$

الطلب الرابع: فك تشفير $S=45$ 121

2. لفك تشفير $S1=45$

$$s1' = (r^{-1} \times s1) \bmod(n) = (71 \times 45) \bmod 110 = 3195 \bmod 110 = 5$$

$$s1' = X'_1 b_1 + X'_2 b_2 + X'_3 b_3 + X'_4 b_4 + X'_5 b_5 + X'_6 b_6$$

• نحسب:

$$11 = 1 \times 1 + 0 \times 1 + 1 \times 4 + 0 \times 10 + 0 \times 20 + 0 \times 40$$

• لدينا:

$$X'_1 = 101000 \text{ ومنه:}$$

• ندور $X1'$ وفق التدوير المفروض $[1,2,4,3,6,5]$ فنحصل على $X1=100100$

3. فك تشفير $S_2=121$

• نحسب: $s_2' = (r^{-1} \times s_2) \bmod(n) = (71 \times 121) \bmod 110 = 8591 \bmod 110 = 11$

• لدينا: $s' = X'_1 b_1 + X'_2 b_2 + X'_3 b_3 + X'_4 b_4 + X'_5 b_5 + X'_6 b_6$

$$11 = 1 \times 1 + 0 \times 1 + 0 \times 4 + 1 \times 10 + 0 \times 20 + 0 \times 40$$

• فتكون $X' = 100100$

ندور X' وفق التدوير المفروض $[1,2,4,3,6,5]$ فنحصل على $X=101000$

المسألة الخامسة

في خوارزمية حقيبة الظهر بفرض لدينا المجموعة $b = [1,2,6,12]$ وبفرض أن $n \in [23,26]$ ومن مضاعفات العدد 6 و بفرض أن $r \in [3,6]$ و أن التدوير المفروض هو $[4,1,2,3]$

المطلوب:

1. أثبت أن المجموعة b هي مجموعة متزايدة
2. أوجد المفتاح العام و المفتاح الخاص لهذه الخوارزمية.
3. شفر النص $x=1101$.
4. فك تشفير النص $s=102$ ، إذا علمت أن معكوس r هي ضمن المجال $[3,6]$.

الطلب الأول:

1. إذا كانت المجموعة المتزايدة $b = [1,2,6,12]$ يجب أن تحقق الشرط

$$b_i \geq b_1 + b_2 + \dots + b_{i-1}$$

$$2 \geq b_1 = 1 \text{ محقق}$$

$$6 \geq b_1 + b_2 = 1 + 2 = 3 \text{ محقق}$$

$$12 \geq b_1 + b_2 + b_3 = 1 + 2 + 6 = 9 \text{ محقق}$$

وهي تحقق الشرط

الطلب الثاني:

1. نختار n بحيث تحقق الشرط $n > b_1 + b_2 + b_3 + b_4$

$$n > 1 + 2 + 6 + 12$$

$$n > 21$$

لدينا من نص المسألة أن n مضاعفات العدد 6 و $n \in [23, 26]$ وبالنتيجة $n=24$

2. نختار r بحيث أولية مع n و حسب فرض المسألة $r \in]3, 6[$ فتكون $r=5$

3. نحسب بعدها المصفوفة t باستخدام العلاقة: $t_i = (b_i \times r) \bmod(n)$

$$t_1 = (1 \times 5) \bmod 24 = 5$$

$$t_3 = (6 \times 5) \bmod 24 = 6$$

$$t_2 = (2 \times 5) \bmod 24 = 10$$

$$t_4 = (12 \times 5) \bmod 24 = 12$$

فتكون المصفوفة $t = [5, 10, 6, 12]$

تابع الطلب الثاني:

4. بفرض أن التدوير هو: $[4,1,2,3]$ بعد تدوير t ينتج المفتاح العام: $a=[12, 5,10,6]$

5. ويكون المفتاح الخاص هو: $n=24$ $r=5$ $b = [1,2,6,12]$ التدوير: $[4,1,2,3]$

الطلب الثالث: شفر النص $x=1101$.

طول النص الصريح مساوٍ لعدد الأغراض $k=4$

من أجل عملية التشفير نستخدم المفتاح العام: $a=[12, 5,10,6]$

$$S = X_1 a_1 + X_2 a_2 + X_3 a_3 + X_4 a_4$$

$$S = 1.12 + 1.5 + 0.10 + 1.6 = 33$$

الطلب الرابع: فك تشفير النص $s=102$ ، إذا علمت أن معكوس r هي ضمن المجال $[3,6]$

1. من أجل عملية فك التشفير يلزمنا حساب معكوس r بالنسبة لـ $\text{mod}(n)$:

نختبر القيم الموجودة ضمن المجال المفروض فنجد أن قيمة المعكوس هي 5 لأن

$$5^{-1} \text{mod}(24) \equiv 5$$

معكوس $r=5$ بالنسبة لـ $\text{mod}(24)$

$$5 \times 5 \text{mod}(24) = 25 \text{mod}(24) = 1$$

بحيث:

$$s' = (r^{-1} \times s) \text{mod}(n) = (5 \times 102) \text{mod} 24 = 510 \text{mod} 24 = 6 \quad \text{2. نحسب}$$

تابع الطلب الرابع:

3. لدينا فيكون $s' = X'_1 b_1 + X'_2 b_2 + X'_3 b_3 + X'_4 b_4$

$$6 = 0 \times 1 + 0 \times 2 + 1 \times 6 + 0 \times 12$$

فتكون قيم $X'_1 = 0010$:

4. ندور قيم X' وفق التدوير المفروض $[4,1,2,3]$ فنحصل على $X=0001$

نهاية المحاضرة الثانية عملي