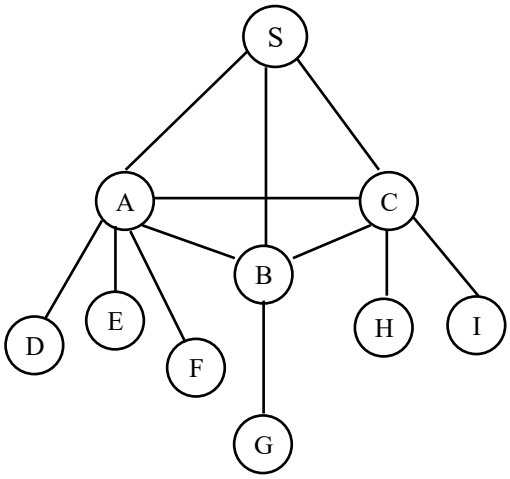
تمارين إضافية



السؤال الأول : بفرض لدينا الشبكة الآتية:

حيث يمثل S مركز الشبكة، A,B,C قادة العناقيد ، D,E,F,G,H,I هي العقد ضمن هذه العناقيد. بفرض أن المركزS هي عقدة محمية ضد الهجمات

بفرض طبق نظام تشفير هجين كالآتي :

بين المركز و قادة العناقيد : نظام تشفير متناظر تقليدي.

بين قادة العناقيد : نظام تشفير متناظر ثنائي

بين قائد كل عنقود والعقد التابعة له: نظام تشفير غير متناظر

احسب عدد المفاتيح المخزنة في كل من S,A,B,C,G مع التعليل لكل منها

الحل :

العقدة	عدد المفاتيح	التعليل
S	1	K (مفتاح لكل الوصلات مع قادة العناقيد)
A	8	$K, K_{AB}, K_{AC}, K_{PUBA}, K_{PRIA}, K_{PUBD}, K_{PUBE}, K_{PUBF}$
B	6	$K, K_{AB}, K_{BC}, K_{PUBB}, K_{PRIB}, K_{PUBG}$
C	7	$K, K_{CB}, K_{AC}, K_{PUBC}, K_{PRIC}, K_{PUBH}, K_{PUBI}$
G	3	$K_{PUBG}, K_{PRIG}, K_{PUBB}$

السؤال الثاني :

بفرض استخدمت المجموعة b=[3,7,12,25,50] المتزايدة في نظام حقيبة الظهر يعتمد على n يقبل القسمة على 3 و بحيث $n \in [100 - 95]$ و $r \in [4 - 2]$. بفرض أن التدوير المستخدم هو: [5,1,4,3,2]

١. احسب المفتاح العام والمفتاح الخاص.

٢. شفر النص X=11001 .

٣. بفرض S= 30 احسب النص الصريح X الموافق له، علماً أن معكوس $r \in [51 - 49]$

الحل:

١.احسب المفتاح العام والمفتاح الخاص.

حساب n :

$$n > b_1 + b_2 + b_3 + b_4 + b_5$$
$$n > 3 + 7 + 12 + 25 + 50$$
$$n > 97$$

حسب شرط n=99 .

حساب r : r أولي مع n و حسب شرط المسألة r=2 .

حساب المصفوفة t :

$$t_i = (b_i \times r) mod n$$
$$t_1 = (3 \times 2) mod 99 = 6$$
$$t_2 = (7 \times 2) mod 99 = 14$$
$$t_3 = (12 \times 2) mod 99 = 24$$
$$t_4 = (25 \times 2) mod 99 = 50$$
$$t_5 = (50 \times 2) mod 99 = 1$$

t=[6,14,24,50,1]

بتطبيق التدوير المفروض:[1,6,50,24,14]=a (المفتاح العام)

المفتاح الخاص: r,n,b, التدوير

2.شفر النص X=11001 .

$$S = x_1 \times a_1 + x_2 \times a_2 + x_3 \times a_3 + x_4 \times a_4 + x_5 \times a_5 =$$

$$S = 1 \times 1 + 1 \times 6 + 0 \times 50 + 0 \times 24 + 1 \times 14 = 21$$

3. بفرض S= 30 احسب النص الصريح X المو افق له، علماً أن معكوس $r \in [49 - 51]$

$$r \times r^{-1} \equiv 1 mod n$$

$$2 \times 50 \equiv 1 mod 99 \Rightarrow r^{-1} = 50$$

$$\acute{S} = (S \times r^{-1}) mod n \Rightarrow \acute{S} = (30 \times 50) mod 99 = 15$$

$$S` = \grave{x_1} \times b_1 + \grave{x_2} \times b_2 + \grave{x_3} \times b_3 + \grave{x_4} \times b_4 + \grave{x_5} \times b_5$$

$$15 = 1 \times 3 + 0 \times 7 + 1 \times 12 + 0 \times 25 + 0 \times 50 \Longrightarrow \grave{X} = 10100$$

$$X = 01010$$

السؤال الثالث :

من أجل خوارزمية RSA ذات القيم p=3,q=11 و المطلوب:

شفر النص الصريح: CORONA ، بفرض أن هذا النص تم ترميزه اعتماداً على تمثيل الأحرف الأبجدية بأعداد صحيحة كالآتي:

A=2,B=3,C=4.....Z=27,&=28,%=29,@=30,#=31,!=32. علماً $e \in [1-5]$

الحل:

ترميز النص المطلوب : (4,16,19,16,15,2)

١. احسب n : n=p.q=3.11=33

٢. نحسب $\phi(n)$: $\phi(n) = (p-1)\times(q-1) = 20$

٣. نختار e ضمن المجال المعطى بحيث تحقق الشروط :

$\gcd(\phi(n), e) = 1; \quad 1 < e < \phi(n) \Rightarrow e = 3$

المفتاح العام : $K_{Pub} = \{e, n\} = \{3,\ 33\}$

٤.نقوم بالتشفير : نلاحظ أن جميع النصوص تحقق شرط إمكانية التشفير m<n

$$C = M^{e} \bmod(n)$$

$C1=(4)^3 \bmod 33=31 \rightarrow \#$

$C2=(16)^3 \bmod 33=4 \rightarrow C$

$C3=(19)^3 \bmod 33=28 \rightarrow \&$

$C4=(16)^3 \bmod 33=4 \rightarrow C$

$C5=(15)^3 \bmod 33=9 \rightarrow H$

$C6=(2)^3 \bmod 33=8 \rightarrow G$

فيكون : C=(31,4,28,4,9,8) ، فيكون النص المشفر هو: C=#C&CHG

السؤال الرابع:

بفرض أن المرسل A و المستقبل B يستخدمان خوارزمية ديفي هيلمان (DH) . المطلوب:

طبق هذه الخوارزمية بين الطرفين A, B مبيناً خطوات الخوارزمية بالتفصيل.

بفرض أن: العددين الأوليين المستخدمين في الخوارزمية هما : 17و 5

و أن القيمتين العشوائيتين اللتين يختارهما B,A هما 3 ، 2 على الترتيب.

يتفق الطرفان على القيم P=17,g=5

A	B
1-يختار A عدداً عشوائياً XA=3	١-يختار B عدداً عشوائياً XB=2
2-يحسب A مفتاحه العام :	2-يحسب B مفتاحه العام :
$YA = g^{XA} mod p$ $= (5)^3 mod 17 = 6$	$YB = g^{XB} mod p$ $= (5)^2 mod 17$ $= 8$
- يولد B المفتاح السري المشترك وفق العلاقة:	٣- يولد B المفتاح السري المشترك وفق العلاقة:
$K = YB^{XA} mod p$ $= 8^3 mod 17$ $= 2$	$K = YA^{XB} mod p = 6^2 mod 17$ $= 2$

==========نهاية الملف بالتوفيق للجميع==========