Information System Security

أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

الأربعاء 14/6/2023

جامعة المنارة

كلية الهندسة

هندسة الميكاترونيكس

جلسة العملي الثامنة
أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

المسألة الأولى

بفرض خوارزمية RSA ذات القيم p=3,q=11 ، وعلماً أن $e \in [1-5]$ 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

الطلب الأول: فك تشفير النص ED

الطلب الثاني :إنشاء التوقيع الرقمي للنص GO

الطلب الثالث وصلت الرسالة الموقعة الآتية : YT%LT || START المطلوب تحقق من صحة التوقيع الرقمي

حل المسألة الأولى (1/4)

الطلب الأول:

من أجل فك تشفير النص نحتاج نحسب المفتاح الخاص:

1. احسب n : n=p.q=3.11=33

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

3. نختار e ضمن المجال المعطى حيث تحقق الشروط : $1<e<\phi(n)\Rightarrow e=3 \quad ;\gcd(\phi(n),e)=1$

4. نحسب d : $d\times e\equiv 1 mod\emptyset(n)\Longrightarrow d\equiv e^{-1}mod\emptyset(n)$

$$d\equiv 3^{-1}mod20\Longrightarrow d=7$$

فيكون المفتاح الخاص : kpri={d,n}={7,33}

حل المسألة الأولى (2/4)

تابع للطلب الأول:

نرمز النص المشفر المراد فك تشفير فيكون :C=(6,5)

لفك التشفير نستخدم العلاقة: $M=C^d \bmod n$

$M1=(6)^7 \bmod(33)=30 \rightarrow @$

$M2=(5)^7 \bmod(33)=14 \rightarrow M$

فيكون النص الصريح : @M

حل المسألة الأولى (3/4)

الطلب الثاني:

نرمز النص الصريح المراد توقيعه فيكون :M=(8,16)

من أجل التوقيع نستخدم المفتاح الخاص وفق العلاقة فيكون : $S = m^d mod(n)$

$$S1 = 8^7 mod(33) = 2 \Longrightarrow A$$
$$S2 = 16^7 mod(33) = 25 \Longrightarrow X$$

فيكون التوقيع : S=AX

حل المسألة الأولى (4/4)

الطلب الثالث :

من أجل للتأكد من صحة التوقيع الرقمي نستخدم المفتاح العام المقابل KPUB= {3,33} للمفتاح الخاص فق العلاقة فيكون :

$$\mathrm{M} = S^{e} mod(n)$$

نرمز النص الصريح المراد التأكد من صحة توقيعه فيكون : M=(20,21,2,19,21)

نرمز التوقيع الرقمي فيكون : S=(26,21,29,13,21)

$$M1 = 26^{3} mod(33) = 20 \Longrightarrow S$$

$$M2 = 21^{3} mod(33) = 21 \Longrightarrow T$$

$$M3 = 29^{3} mod(33) = 2 \Longrightarrow A$$

$$M4 = 13^{3} mod(33) = 19 \Longrightarrow R$$

$$M5 = 21^{3} mod(33) = 21 \Longrightarrow T$$

بالمقارنة نلاحظ أن التوقيع صحيح .

المسألة الثانية

بفرض أن دخل خوارزمية RSAهو **HELP**، يتم التعامل مع هذا النص على شكل كتل طول كل كتلة 2 محارف بفرض أن هذا النص تم ترميزه اعتماداً على نظام للأساس 26 حيث A=0,B=1,.....,Z=25. المطلوب :

1. أوجد النص المشفر على شكل كتل عددية المقابل للنص الصريح المعطى إذا علمت أن p=23، q=17 ، **e**=3 (علماً أنه يحقق الشروط المطلوبة). علماً ان الخانة الأقل أهمية هي أول خانة على اليمين.
2. أوجد النص المشفر بالطلب السابق إلى كتل محرفية وفق الخوارزمية:

$$m \div 26^{T-1} = Ch_1 \text{ rem } m_1$$
$$m_1 \div 26^{T-2} = Ch_2 \text{ rem } m_2$$
$$\vdots$$
$$m_i \div 26^{0} = Ch_T rem\ 0$$

حل المسألة الثانية (1/3)

الطلب الأول:

1. نرمز النص الصريح المعطى:

يقسم النص الصريح إلى كتل طول كل منها 2 محرفين: **HE LP**

$$m1 = HE = 7 \times 26^1 + 4 \times 26^0 = 186$$

$$m2 = LP = 11 \times 26^1 + 15 \times 26^0 = 301$$

$$m = (186, 301)$$

2. إيجاد المفتاح العام:

$$n = p \times q = 23 \times 17 = 391$$

$$k_{pub} = \{e, n\} = \{3, 391\}$$

حل المسألة الثانية (2/3)

تابع الطلب الأول:

3. عملية التشفير:

نتحقق من شرط التشفير M <n نلاحظ أنه محقق لأن186,301 <391

$$C=m^e mod\ n$$

$$\left.\begin{aligned} C1=186^3 mod\ 391 = 169 \\ C2=301^3 mod\ 391 = 215 \end{aligned}\right\} \quad C=(169,215)$$

حل المسألة الثانية (3/3)

الطلب الثاني:

C1= 169

$169 \div 26^1 = 6\ rem\ 13 \Longrightarrow ch1 = G$

$13 \div 26^0 = 13\ rem\ 0 \Longrightarrow ch2 = \mathrm{N}$

C1= GN

C2= 215

$215 \div 26^1 = 8\ rem\ 7 \Longrightarrow ch1 = I$

$7 \div 26^0 = 7\ rem\ 0 \Longrightarrow ch2 = \mathrm{H}$

C1= IH

⇒C=GNIH

فيكون النص المشفر على شكل محارف

المسألة الثالثة

إذا كان لدينا نظام حقيبة الظهر المستخدم يعتمد على المجموعة :b=[2,6,13,25] ، و بفرض أن n=110 و أن $r \in [32,34]$ ، وبفرض أن التدوير المفروض هو [2,4,1,3] .

1.أوجد المفتاحين العام و الخاص

2. شفر النص الصريح 10000011.

حل المسألة الثالثة (1/)

1. نختبر فيما إذا كانت المجموعة المتزايدة b=[2,6,13,25] تحقق الشرط $b_i \geq b_1 + b_2 + \cdots + b_{i-1}$

$b_2 = 6 \geq b_1 = 2$ محقق

$b_3 = 10 \geq b_1 + b_2 = 2 + 6 = 8$ محقق

$b_4 = 25 \geq b_1 + b_2 + b_3 = 2 + 6 + 13 = 21$ محقق

وهي تحقق الشرط

2 . لدينا من فرض المسألة n=110 لذا نختار r=33 فتكون أولية مع n و ضمن المجال $r \in [32,34]$

حل المسألة الثالثة (2/)

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

$$t_1 = (2 \times 33) mod 110 = 66$$

$$t_2 = (6 \times 33) mod 110 = 88$$

$$t_3 = (13 \times 33) mod 110 = 99$$

$$t_4 = (25 \times 33) mod 110 = 55$$

فتكون المصفوفة t=[66,88,99,55]

4. بفرض أن التدوير هو : [2,4,1,3] بعد تدوير t ينتج المفتاح العام : a=[66, 88,99,55]

5.ويكون المفتاح الخاص هو: n=110 r=33 b=[2,6,13,25] التدوير : [2,4,1,3]

حل المسألة الثالثة (3/2)

الطلب الثاني:

نلاحظ ان طول النص المطلوب تشفير أكبر عدد الأغراض من k=4 لذا نقسم النص الصريح إلى سلاسل طول كل منها مساوٍ k=4

فيكون : x1= 1000

X2= 0011

من أجل عملية التشفير نستخدم المفتاح العام:

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

$$S1 = 1.66 + 0.88 + 0.99 + 0.55 = 88$$

$$S2 = 0.66 + 0.88 + 1.99 + 1.55 = 165$$

$$S = S1 \quad s2$$

$$S = 88\ 165$$

جَامعة
المَنارة
MANARA UNIVERSITY

نهاية الجلسة الثامنة