جامعة المنارة
كلية الهندسة
قسم المعلوماتية

Information System Security
أمن نظم المعلومات

مدرسة المقرر

د. بشرى علي معلا

الجلسة السابعة

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

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

المطلوب:

1. فك تشفير النص ED
2. إنشاء التوقيع الرقمي للنص GO
3. 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:

١. احسب n : n=p.q=3.11=33

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

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

$\Rightarrow e=3$

٤. نحسب d :

$$d \times e \equiv 1 mod \emptyset(n) \Rightarrow d \equiv e^{-1} mod \emptyset(n)$$

$$d \equiv 3^{-1} mod 20 \Rightarrow d = 7$$

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 (3,33} =KPUB للمفتاح الخاص فق العلاقة فيكون :

$$M = S^e mod(n)$$

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 لدينا خوارزمية RSA، 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 الصريح على شكل كتل عددية المقابل للنص المشفر **GNIH** إذا علمت أن p=23، q=17 ، **e=235** (علماً أنه يحقق الشروط المطلوبة). علماً ان الخانة الأقل أهمية هي أول خانة على اليمين.

2. أوجد النص الصريح بالطلب السابق إلى كتل محرفية وفق الخوارزمية:

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

3.احسب قيمة التوقيع الرقمي للرسالة BE وكيف سترسل؟

حل المسألة الثانية

الطلب الأول:

١. نرمز النص المشفر المعطى:

يقسم النص المشفر إلى كتل طول كل منها 2 محرفين: **GN IH**

$$\left.\begin{aligned} C1=GN &= 6\times 26^1 + 13\times 26^0 = 169 \\ C2=IH &= 8\times 26^1 + 7\times 26^0 = 215 \end{aligned}\right\} \quad C=(169,215)$$

الطلب الأول:

٢. إيجاد المفتاح الخاص :

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

$$\emptyset(n) = (p-1)\times(q-1) = 352$$

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

$$d \equiv 235^{-1} mod 352 \Longrightarrow d = 3$$

فيكون المفتاح الخاص : kpri={d,n}={3,391}

تابع الطلب الأول:

٣. عملية فك التشفير:

$M=m^d mod\ n$

$M1=169^3 mod\ 391 = 305$

$M2=215^3 mod\ 391 = 328$

النص الصريح على شكل كتل عددية $M=(305,328)$

2 . الطلب الثاني:

$M1= 305$

$305 \div 26^1 = 11\ rem\ 19$

$\Longrightarrow ch1 = L$

$19 \div 26^0 = 19\ rem\ 0$

$\Longrightarrow ch2 = \mathrm{T}$

$M1= LT$

$M2 = 328$

$328 \div 26^1 = 12\ rem\ 16$

$\Longrightarrow ch1 = M$

$16 \div 26^0 = 16\ rem\ 0$

$\Longrightarrow ch2 = \mathrm{Q}$ $C2= MQ$

نرمز النص الصريح المعطى :

فيكون النص الصريح على شكل محارف $\Rightarrow M=LTMQ$

الطلب الثالث:

1. نرمز النص الصريح المعطى: نلاحظ أن النص الصريح يمثل كتلة واحدة فقط (طولها 2) : **BE**

$$C=1 \times 26^1 + 4 \times 26^0 = 30$$

2. نوجد التوقيع الرقمي بشكل عددي أولاً $S=m^d mod\ n=30^3 mod\ 391 = 21$

3. نوجد التوقيع الرقمي بشكل محرفي ثانياً

$$21 \div 26^1 = 21\ rem\ 0 \Longrightarrow ch1 = V$$
$$0 \div 26^0 = 0\ rem\ 0 \Longrightarrow ch2 = A$$
$$\Rightarrow S = VA$$

3. سترسل الرسالة الموقعة كالآتي:

$$BE \parallel VA$$

نهاية الجلسة