Reading Quiz #09

姓名：_____ 系級：_____學號：_____ 分數：_____

閱讀第9章第1節(第179頁)並回答下列問題

1. RSA密碼系統中，加解密的演算法如下：(三毛要傳遞信息x給四郎)

   (a) 四郎選取二相異大質數p_4和q_4,並將此二數相乘得$n_4 = p_4q_4$。

   (b) 然後選取加密次冪e_4使得$\gcd(e_4, (p_4-1)(q_4-1)) = 1$,將$(n_4, e_4)$經由公開的頻道告知三毛，但$p_4$和$q_4$則保密。

   (c) 三毛將所要傳送的信息轉換成一個數m_3 (假設$m_3 < n_4$)。

   (d) 計算密文$c_3 \equiv m_3^{e_4} \pmod{n_4}$,然後將密文$c_3$傳送給四郎。

   (e) 因爲只有四郎知道p_4和q_4,所以他可以算出$\varphi(n_4) = (p_4-1)(q_4-1)$。

   (f) 再透過延伸輾轉相除法求得解密鑰匙d_4,滿足$d_4e_4 \equiv 1 \pmod{\varphi(n_4)}$。

   (g) 最後四郎將密文c_3取d_4次冪，如此即可還原成明文並讀取此信息：

   $$m_3 \equiv c_3^{d_4} \pmod{n_4}。$$

2. 四郎擁有一份文件m_4,三毛同意在上面簽名。他們可如下進行：

   - 三毛選取二個大質數p_3, q_3並計算其乘積$n_3 = p_3q_3$。她同時又選取一介於1與$\phi(n_3) = (p_3-1)(q_3-1)$之間與$\phi(n_3)$互質的整數$e_3$,並計算在模$\phi(n_3)$之下$e_3$的乘法反元素$d_3$。三毛將$(n_3, e_3)$公開，但$d_3, p_3, q_3$則保持私密。
   - 三毛的簽名爲$y \equiv$ _____,可將數對(m_4, y)公開之。

   四郎可驗證信息的確是三毛所簽名過的，步驟如下：

   - 下載或查出三毛的公開鑰匙_____,並計算$z \equiv$ _____。
   - 若 _____,則四郎接受此簽名爲有效的，否則爲無效。

3. 若將上述整個程序步驟做一個小小的變動，那麼就能提供給三毛一個機會，在不知文件內容之下去做簽署的動作。假設四郎有一個非常重要的發現。他要當眾記錄下他所作的東西(所以當時機來臨時他將擁有優先權可以獲得諾貝爾獎),但他不要任何其他的人知道細節(所以他可以從他自己的發明當中獲取巨利)。如果所要簽署的文件是m_3,那麼四郎和三毛可如下進行：

   - 三毛選取一個RSA演算法中的模$n_3 = p_3q_3$。一個加密次冪e_3,並計算解密次冪d_3。她將(n_3, e_3)公開，但d_3, p_3, q_3則保持私密。實際上，當她簽完名後即可將此三數從電腦的記憶體中刪除。
   - 四郎選取一隨機整數$k_4 \pmod{n_3}$並計算$t \equiv$ _____,然後將t傳送給三毛。
   - 三毛簽署t爲$s \equiv$ _____,然後將s回傳給四郎。
   - 四郎算出 _____,這就是簽署文$m_4^{d_3}$。

   因爲k_4的選擇是隨機的，所以$k_4^{e_3} \pmod{n_3}$乃是RSA演算法中，對一隨機整數的加密，還是隨機的。因此$k_4^{e_3}m_4$在本質上並沒有提供我們有關m_4的任何蛛絲馬跡(雖然這無法掩藏像$m_4 = 0$的信息)。從這個角度來看，三毛對自己所簽署的文件內容是一無所知的。一旦簽署的步驟完成，四郎所擁有的簽署文件就如同用標準的簽署步驟所得到的一樣。

   此處存在著若干潛在的危機。例如，四郎可能設計三毛簽下一個要給付他百萬元應許的文件。所以需要有配套的防護措施來防止這一類的問題，我們在此不予討論。

   上述的簽署方法稱之爲_____,乃是由_____所發展出來的並且拿到好幾個這方面的專利，請參閱下表。

美國專利號碼	日期	標　　題
4,795,063	07/19/88	Blind Signature Systems
4,795,064	07/19/88	Blind Unanticipated Signature Systems
4,914,698	03/03/90	One-Show Blind Signature Systems
4,949,380	08/14/90	Returned-Value Blind Signature Systems
4,991,210	02/05/91	Unpredictable Blind Signature Systems