預習閱讀測驗十

姓名：_____ 系級：_____ 學號：_____ 分數：_____

閱讀第九章第一節(pages 195-199)並回答下列問題

1. 四郎擁有一份文件m_4，三毛同意在上面簽名。可如下進行

   (a) 準備工作：三毛選取兩個大質數p_3, q_3並計算其乘積$n_3 = p_3q_3$。她同時又選取與$\varphi(n_3) = (p_3 - 1)(q_3 - 1)$互質的加密次冪$e_3$，並計算在模$\varphi(n_3)$之下$e_3$的乘法反元素$d_3$。三毛將_____公開，但_____則保持私密。

   (b) 三毛簽名：三毛計算簽署文爲$s_3 \equiv$_____，並將明文及簽署文(m_4, s_3)公開之。

   (c) 四郎驗證：四郎或任何其他第三者皆可驗證簽署文s_3的確是三毛所簽名過的文件，先下載或查出三毛的公開鑰匙_____，並計算$z_4 \equiv$_____。若是_____，則四郎接受此簽名爲有效的，否則爲無效。

2. 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_4,那麼四郎和三毛可如下進行：

   - 三毛選取RSA演算法中的模$n_3 = p_3q_3$及加密次冪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，簽完名後即可將此三數從電腦的記憶體中刪除。
   - 四郎選隨機整數$k_4 \pmod{n_3}$並計算$t_4 \equiv$_____ $\pmod{n_3}$然後將t_4傳送給三毛。
   - 三毛簽署t_4爲$s_3 \equiv$_____ $\pmod{n_3}$，然後將s_3回傳給四郎。
   - 四郎算出_____ $\pmod{n_3}$，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，請參閱課本第199頁的表格。