

預習測驗十

姓名：_____ 系級：_____ 學號 (序號)：_____ 分數：_____

閱讀第九章第一節(第179頁)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。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 公開, 但 則保持私密。
- 三毛的簽名為 , 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 。
- 若 , 則四郎接受此簽名為有效的, 否則為無效。

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：

- 三毛選取一個 RSA 演算法中的模 $n_3 = p_3q_3$ 。一個加密次幂 e_3 , 並計算解密次幂 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 , 然後將 t 傳送給三毛。
- 三毛簽署 t 為 $s \equiv$, 然後將 s 回傳給四郎。
- 四郎算出 , 這就是簽署文 $m_4^{d_3}$ 。

因為 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為 , 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。