證明解決一個就可以解決其他

**1和2能互換**

因為α2 = α\*α，把2轉成gα\*gα，用1的方法就能算出gαα

**3和4能互換**

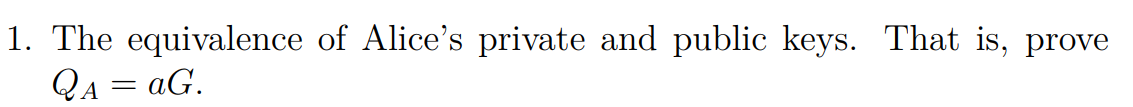
因為可以用4的方法算g1, gα得到3要的g1/α

**1和4能互換**

因為可以用3把gβ轉成g1/β

所以能解決一個就可以解決其他的





Alice 的私鑰a是由QA=γ’+QCA得出，其中 γ’=Decode(Cert)

根據證書請求協議，Cert是由γ和IDA編碼而成的，而γ=αG+kG

證明QA=aG：

aG=(e’α+s)G

s=ek+c

aG=(e’α+ek+c)G

因為e’=H(Cert)且e=H(Cert)，因此e‘=e

aG=(eα+ek+c)G

aG=eαG+ekG+cG

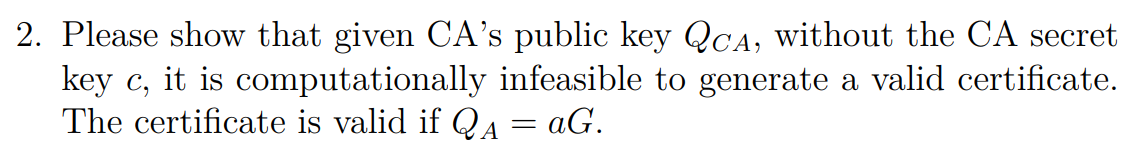
由於γ=αG+kG

aG=eγ+QCA

由於QA=γ+QCA且e=H(Cert)：

QA=eγ+QCA

因此，證明了QA=aG



假設有人試圖偽造一個有效證書，他需要滿足：

1. 計算出γ，使得QA=γ+QCA成立。

2. 根據證書請求協議，γ=αG+kG，且Cert=Encode(γ,IDA)

要達到這一點需要：

1. 生成Cert並計算e=H(Cert)：

Cert=Encode(γ,IDA)

2.計算s：

s=ek+c

但c是CA的秘鑰，只有CA知道。因此如果沒有c，計算s是不可行的

證明：

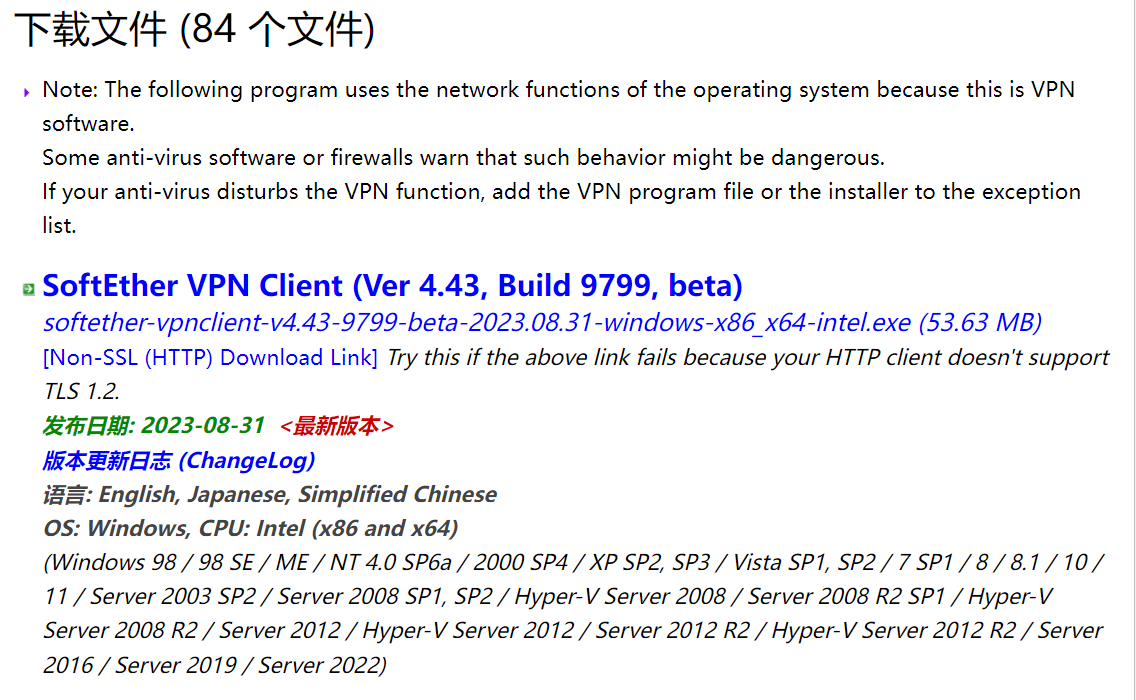
根據s=ek+c，如果不知道c，則無法計算s

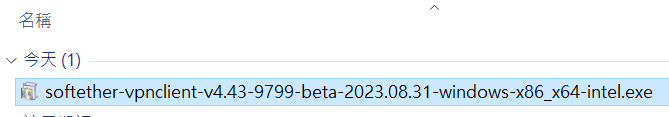
沒有s，Alice 無法計算她的私鑰a=e’α+s，因此也無法計算出對應的公鑰QA=aG

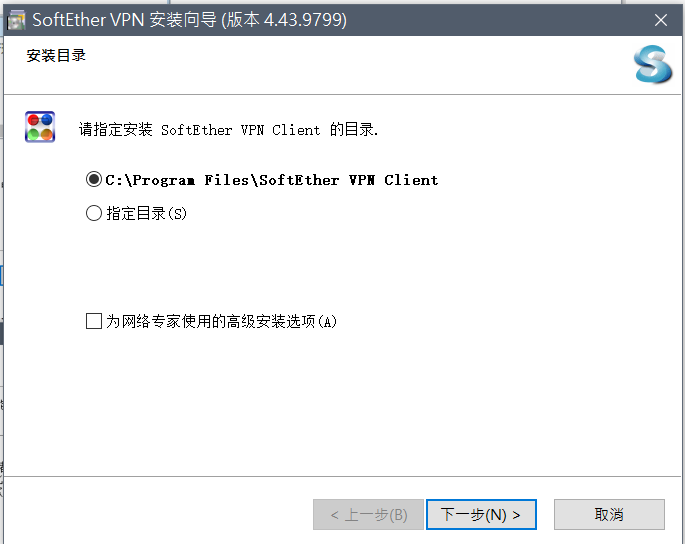
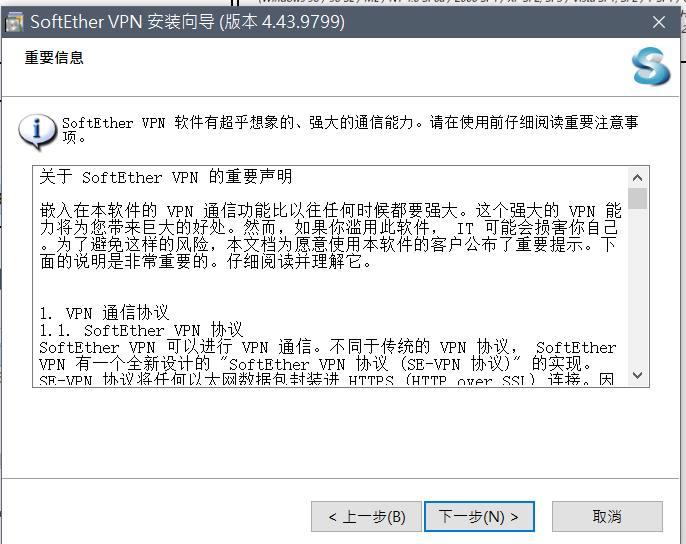
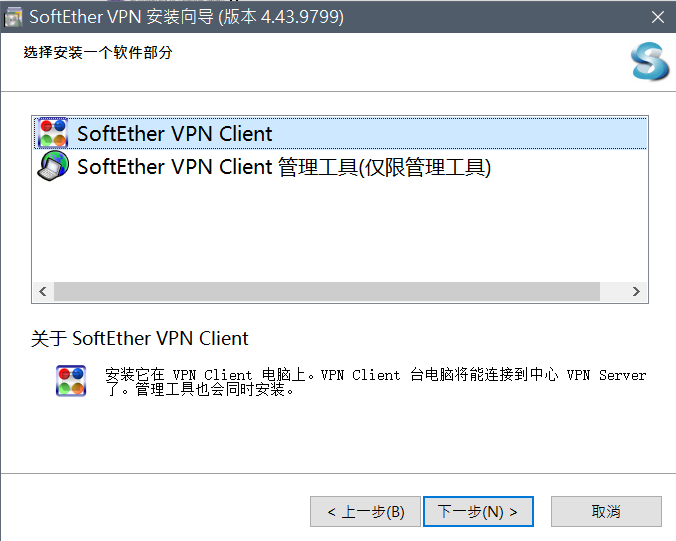
因此，給定CA的公鑰QCA而沒有CA的秘鑰c，生成一個有效證書（滿足QA=aG）在計算上是不可行的

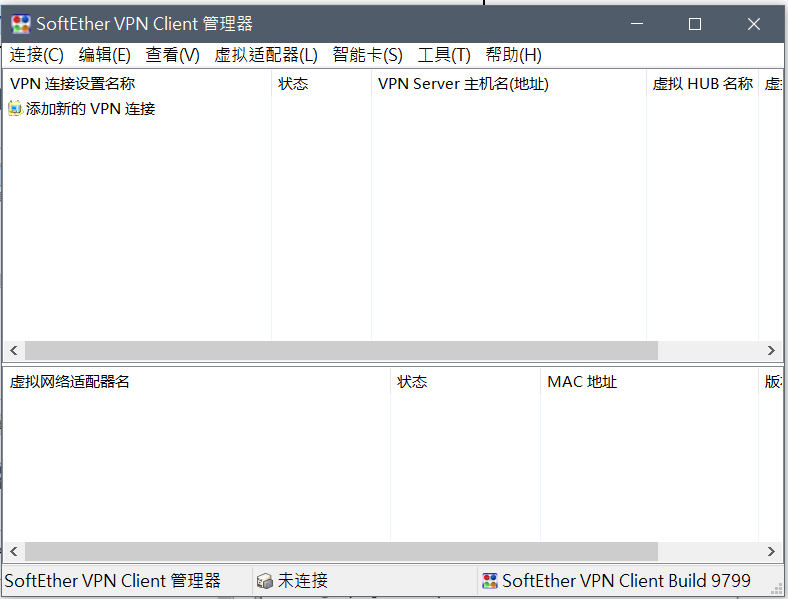


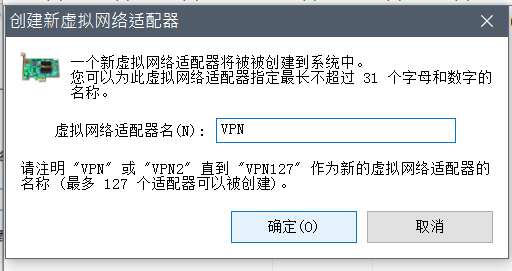
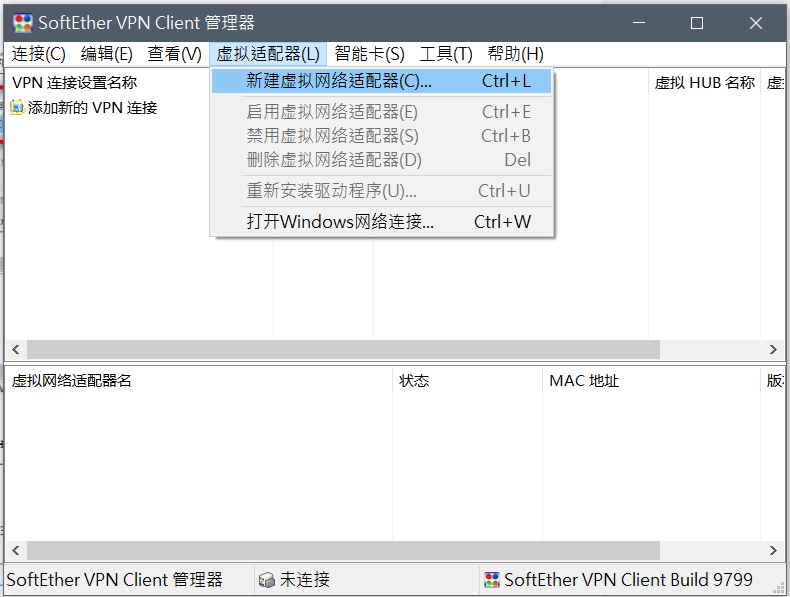
進入官網點選下載

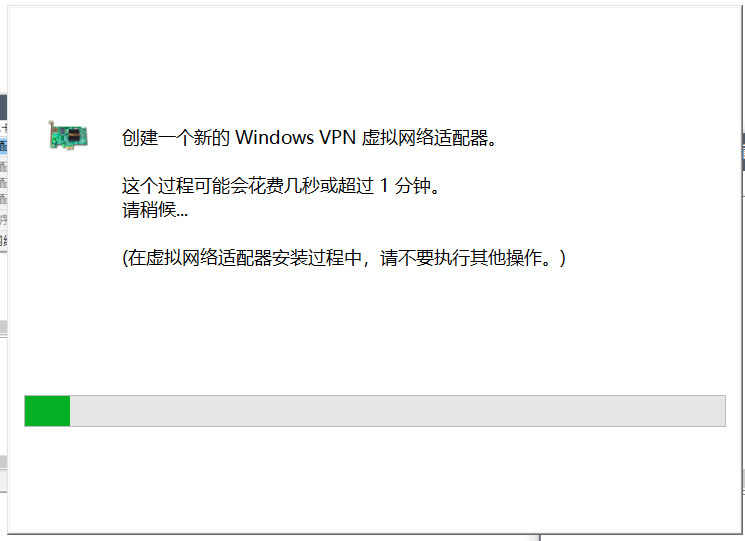
下載最新版本

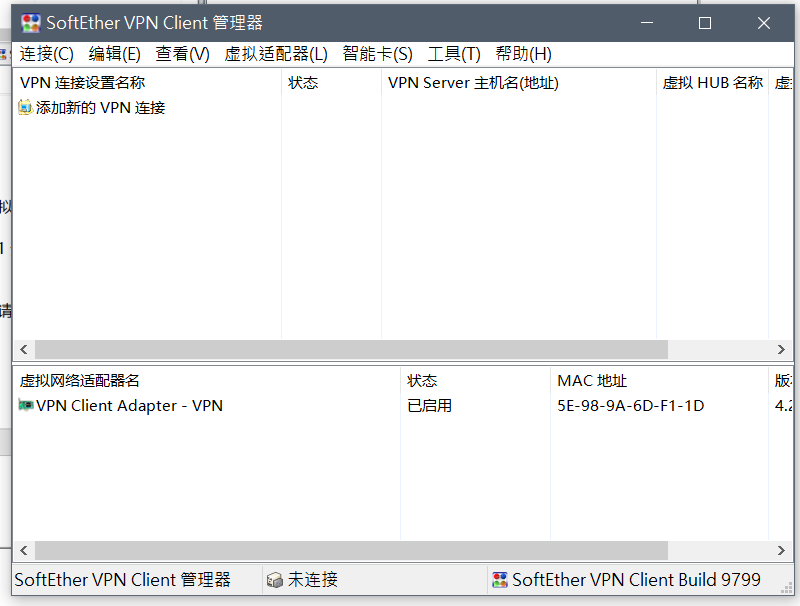
 點擊安裝

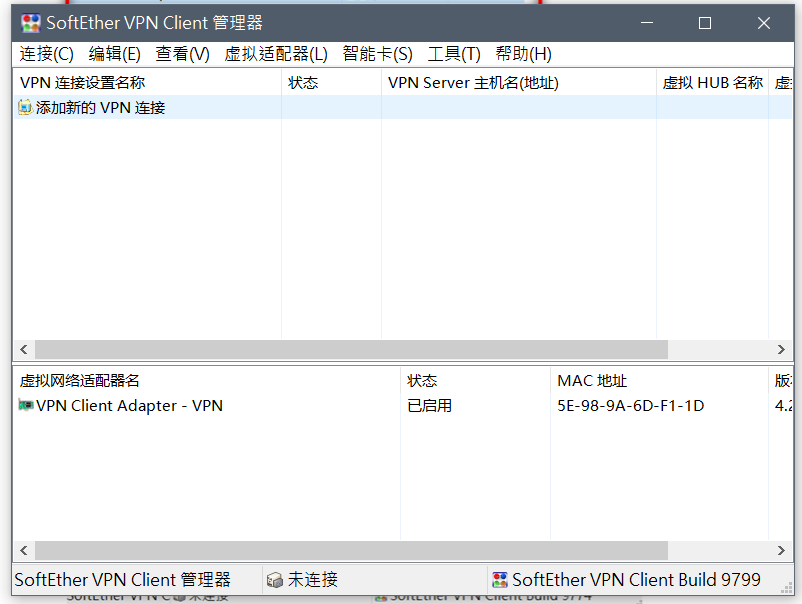
進行安裝設定

 安裝完成，進入軟體

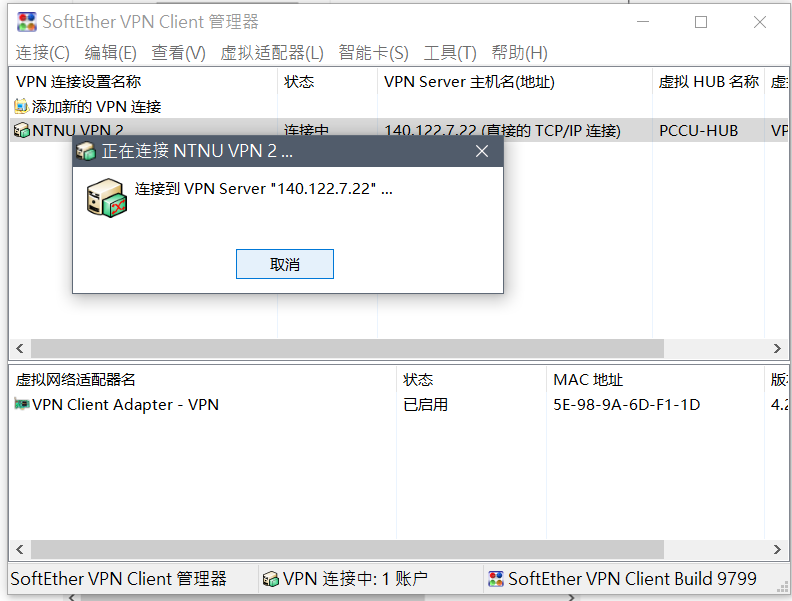


 創建新的虛擬網路適配器

建立完畢

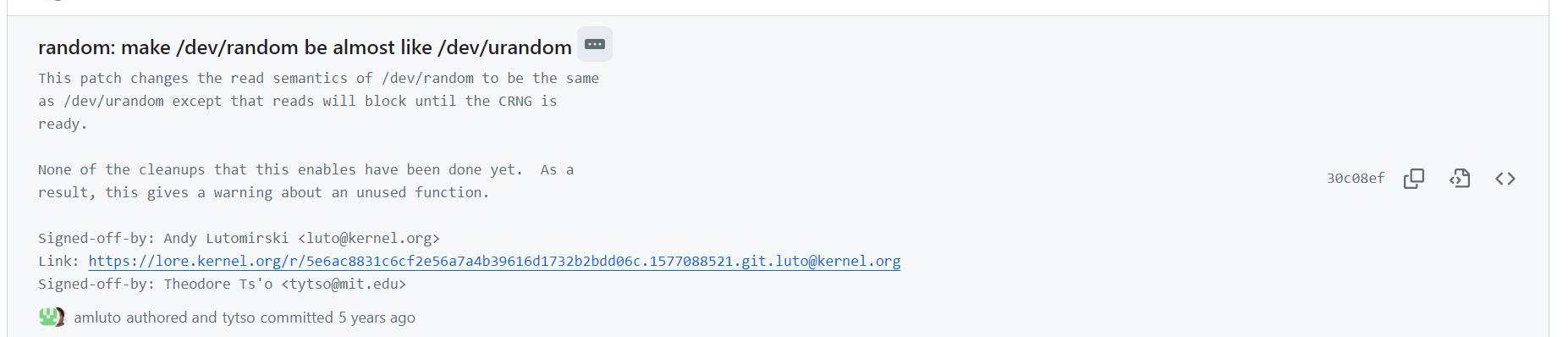
添加新的VPN連線

輸入資訊

雙擊進行連接

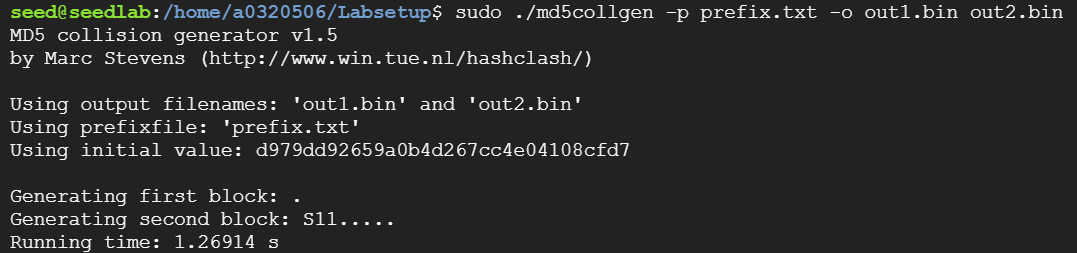


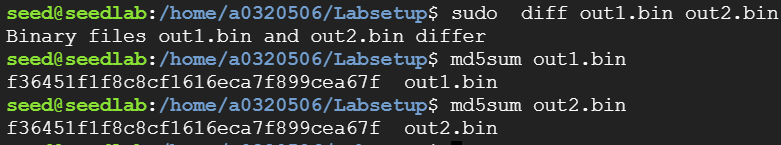
Commit在這裡<https://github.com/torvalds/linux/commit/30c08efec8884fb106b8e57094baa51bb4c44e32>





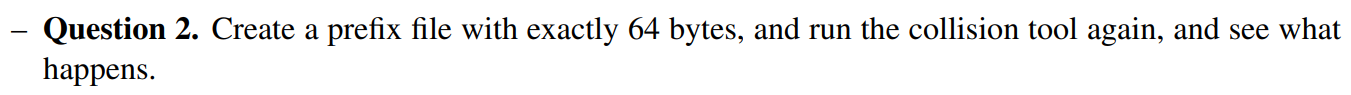


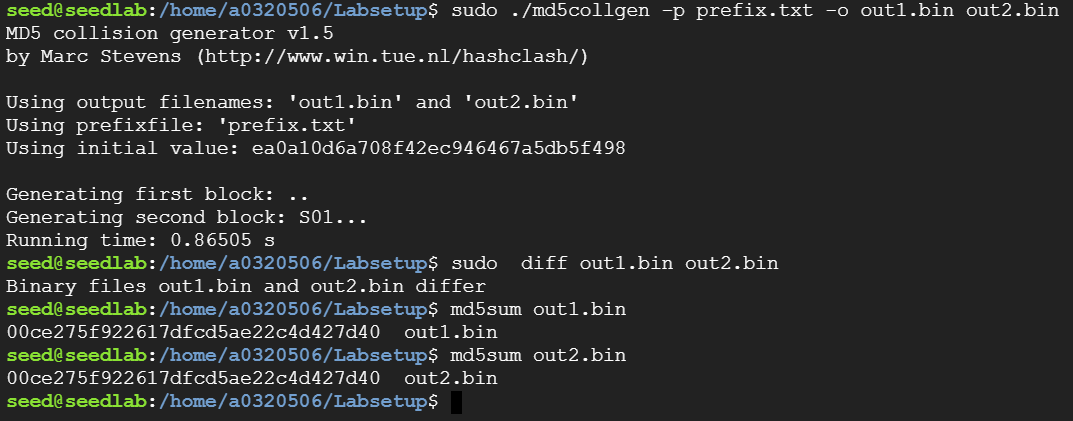


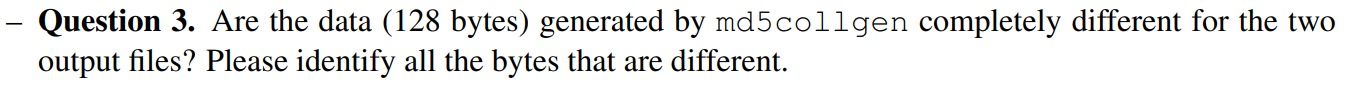


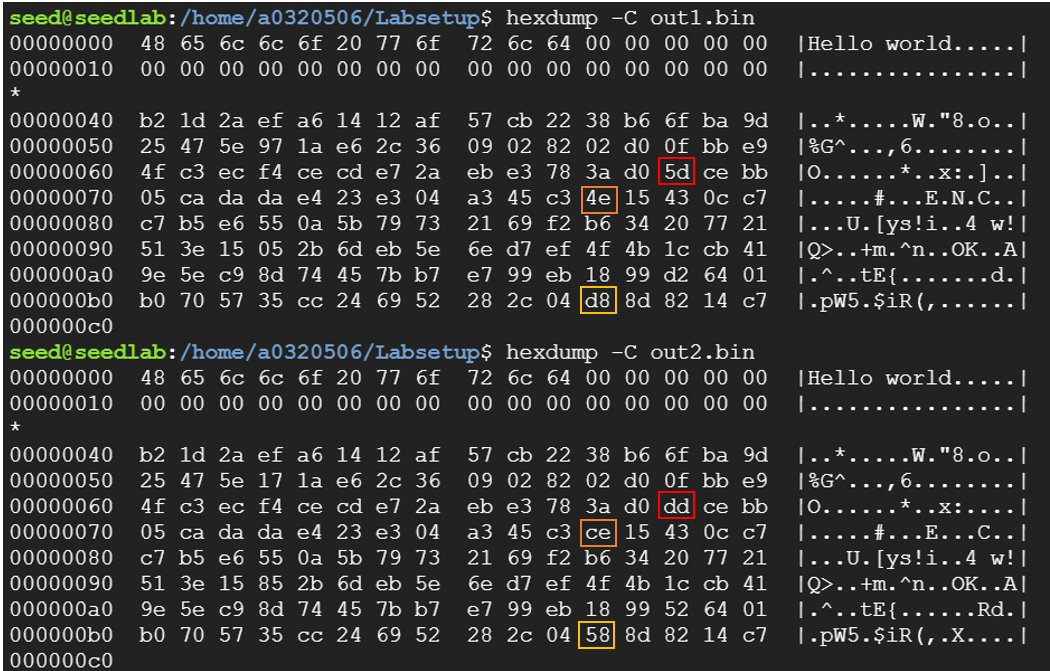


如果prefix file不是64的倍數，md5collgen用0填充

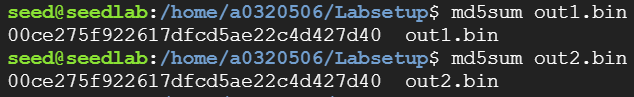




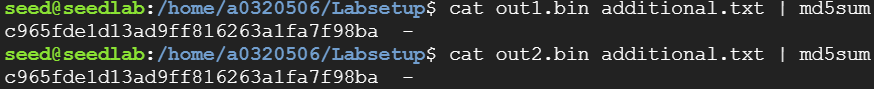










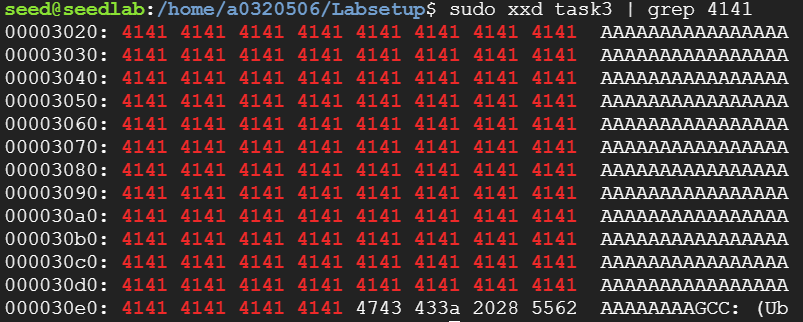




**識別前綴**



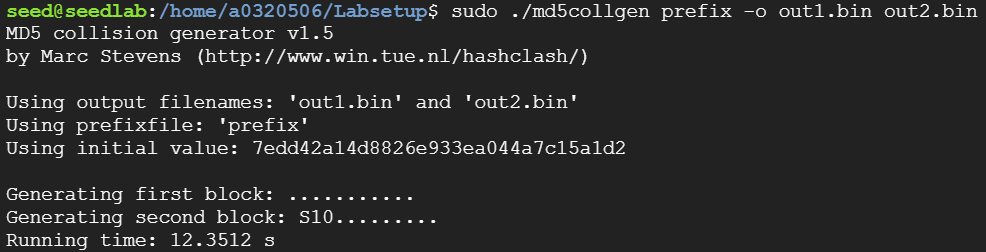


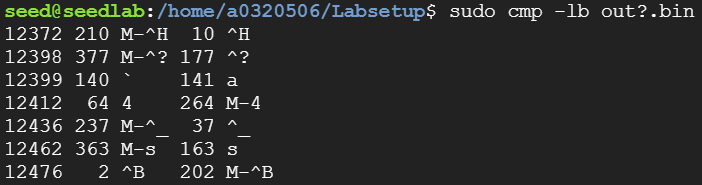


0x3020 = 12320

**提取前綴**





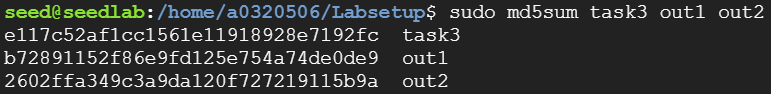


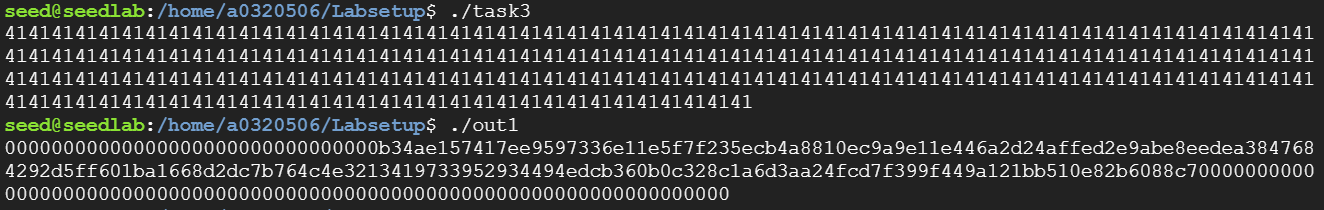
**使用dd取代數據**

12320+128 = 12448

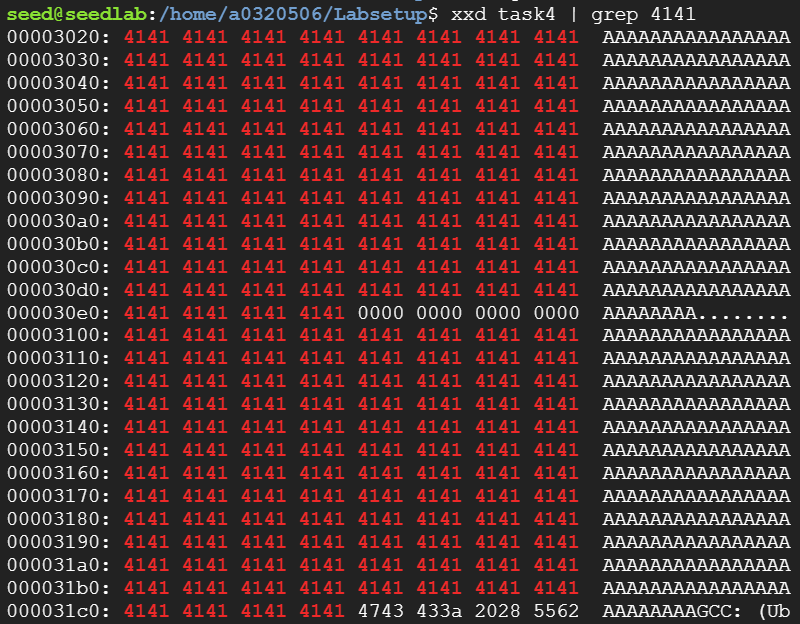


驗證並執行修改後的二進位文件



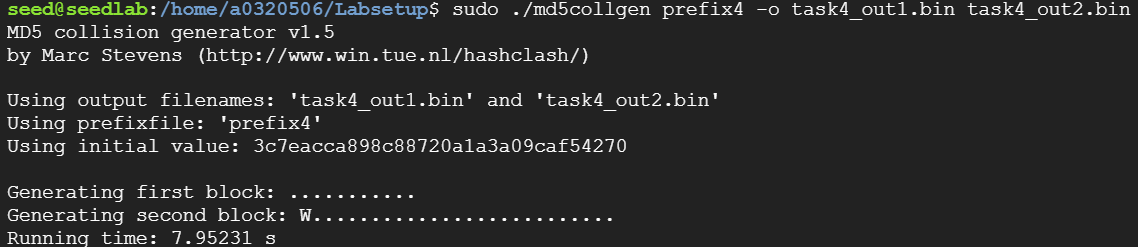


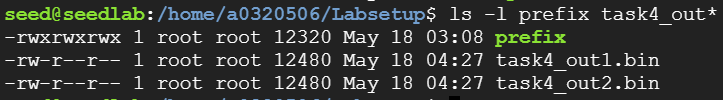


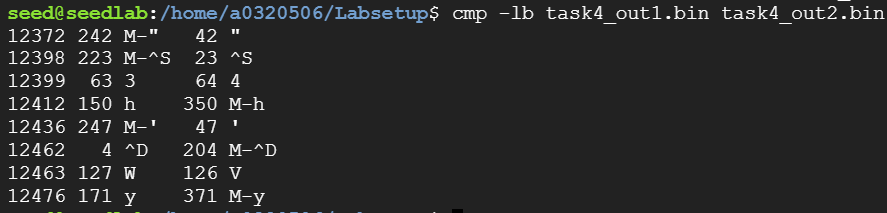


0x3020 = 12320

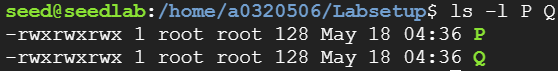


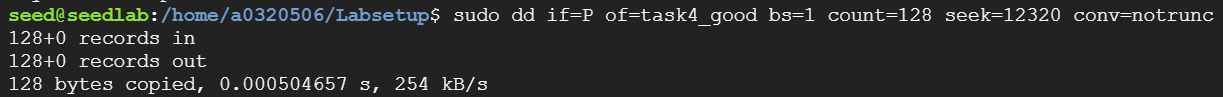


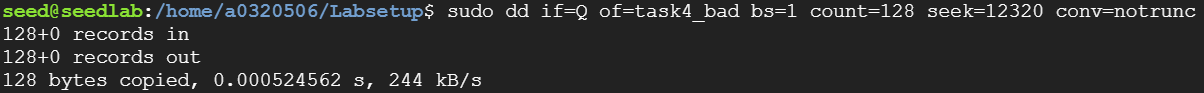


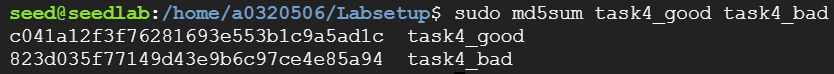










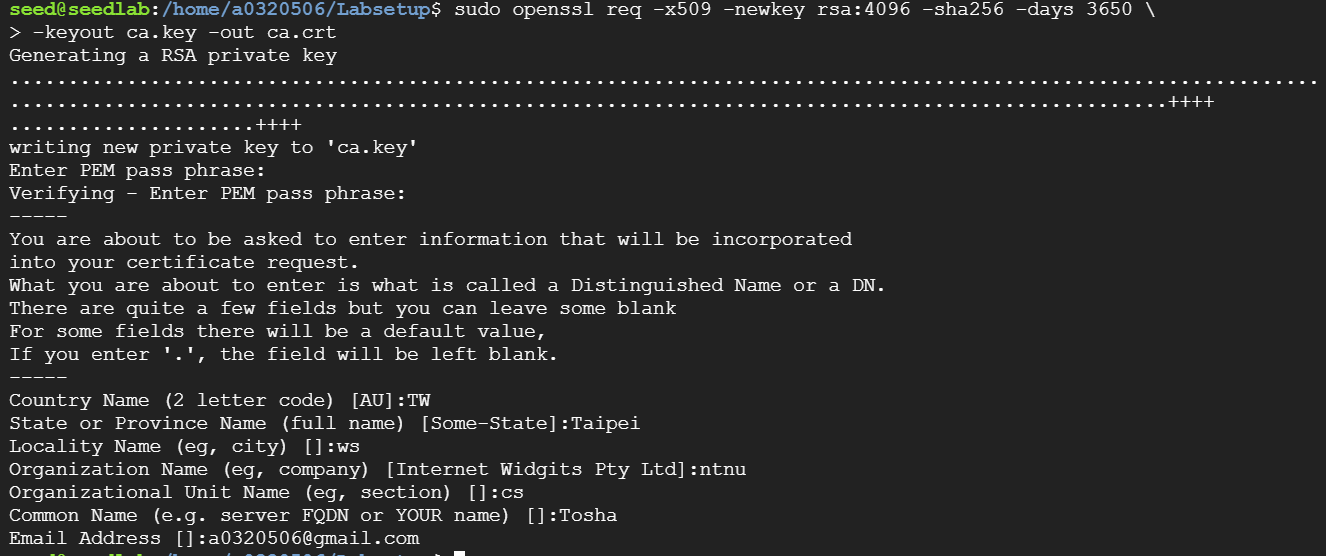




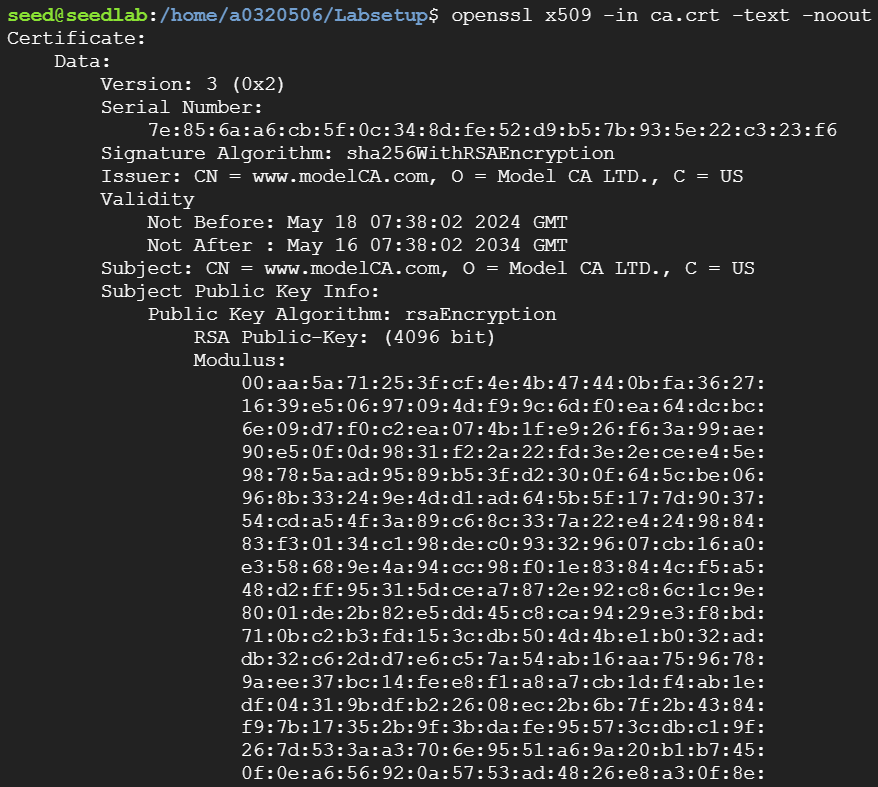
dcup -d 跑在背景

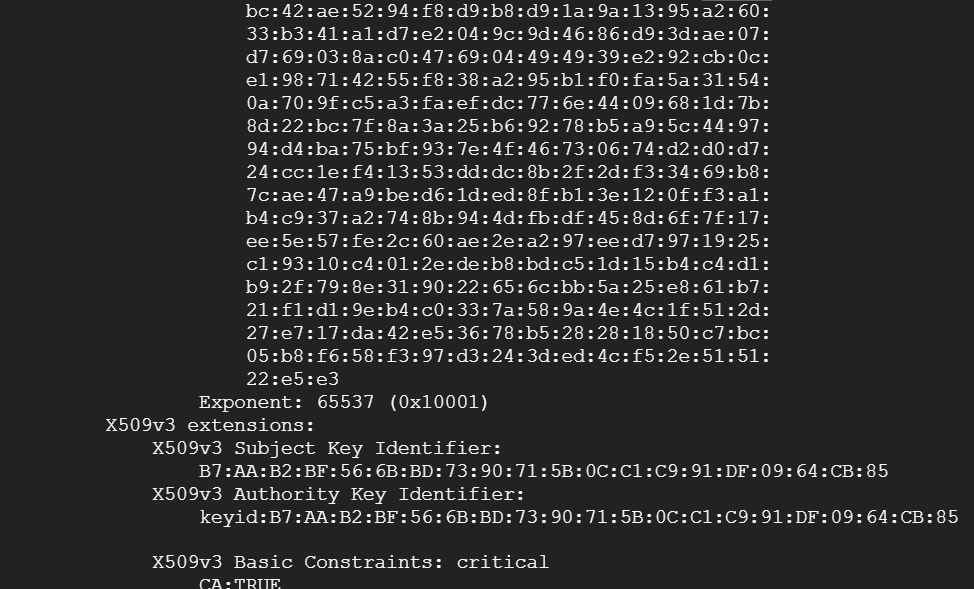


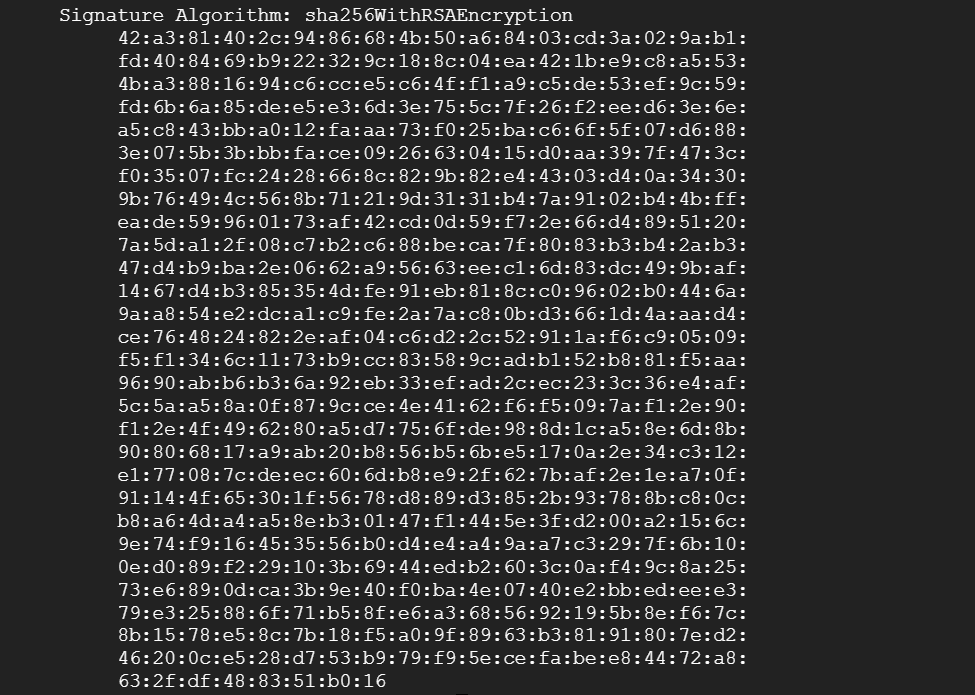
密碼0000



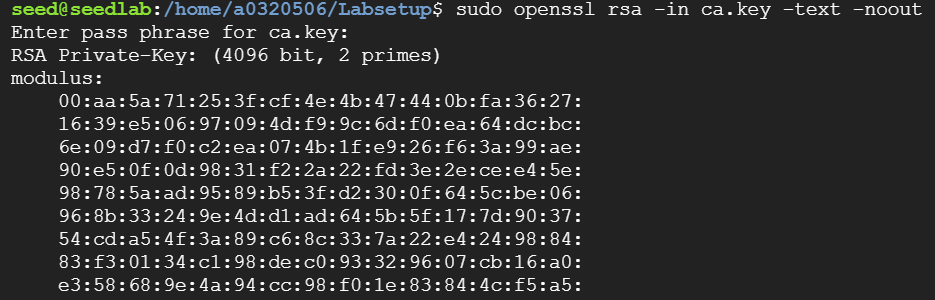


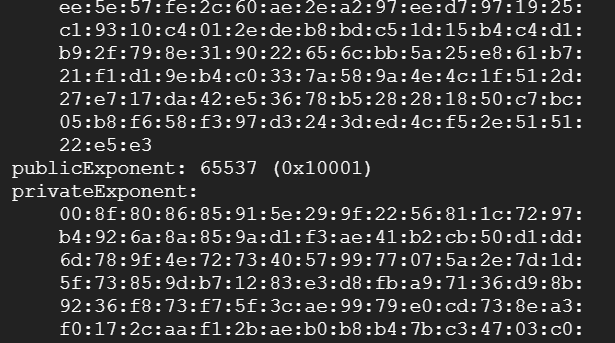


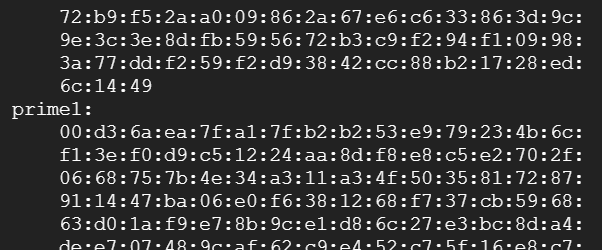


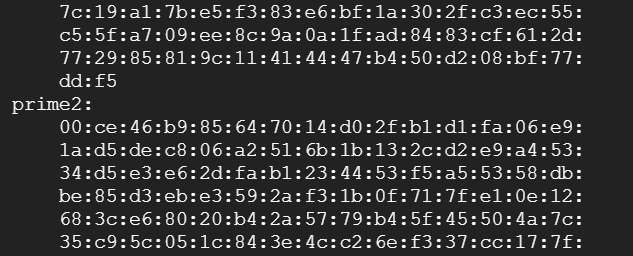


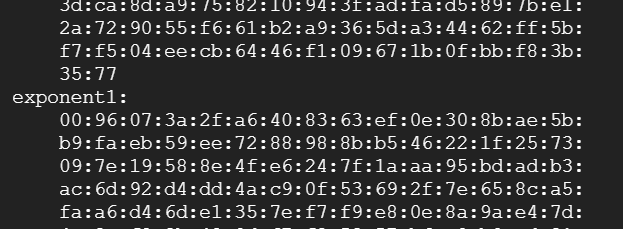
密碼dees

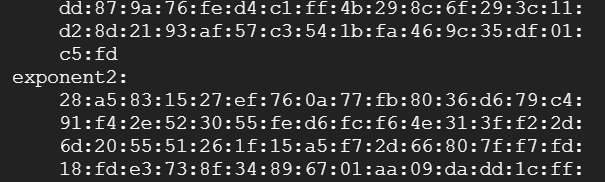


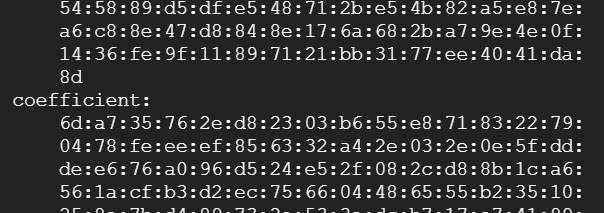








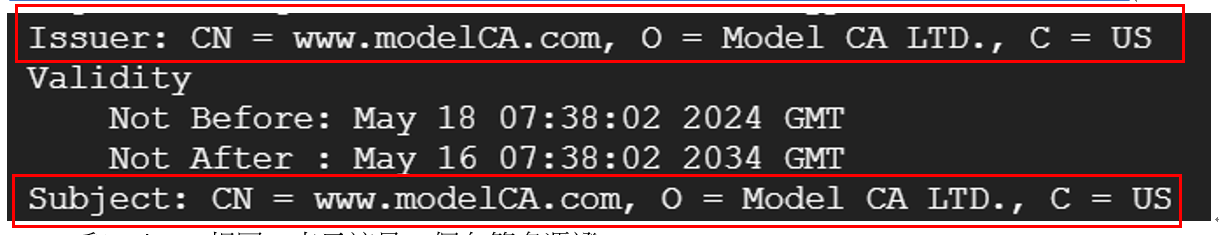




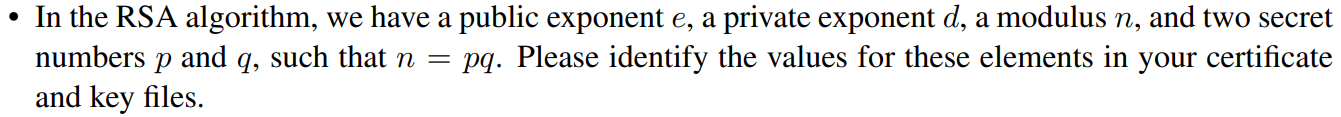




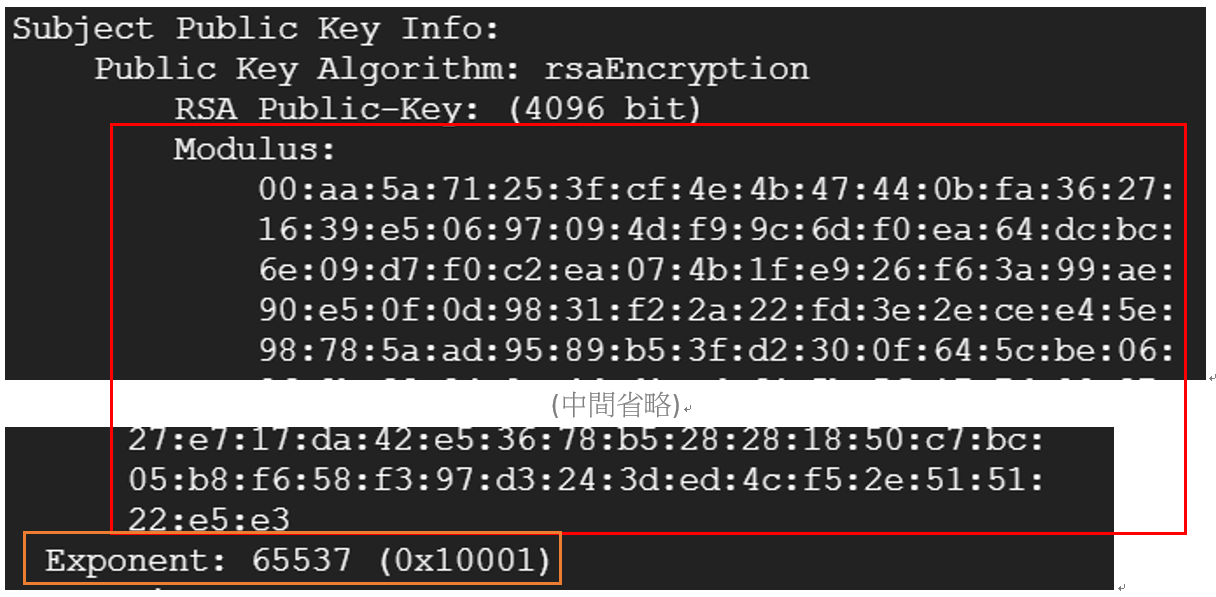




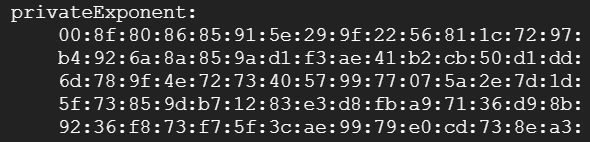
Issuer和Subject相同，表示這是一個自簽名憑證

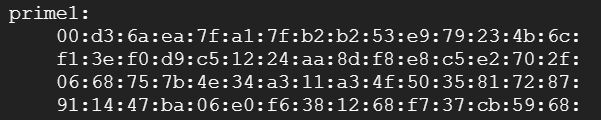


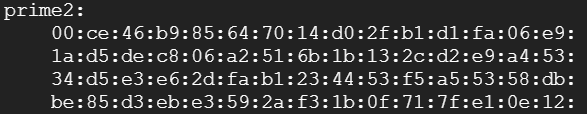
在憑證檔案中，公有指數(**e**)和模數(**n**)是公鑰的一部分，可以在Subject Public Key Info找到



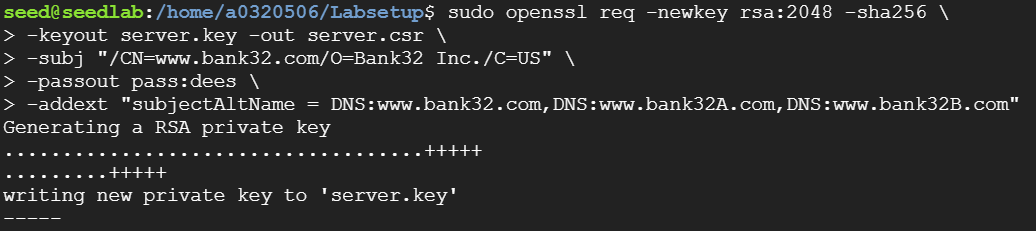
私有指數 (d)、秘密數 (p和q) 通常在私鑰檔案中

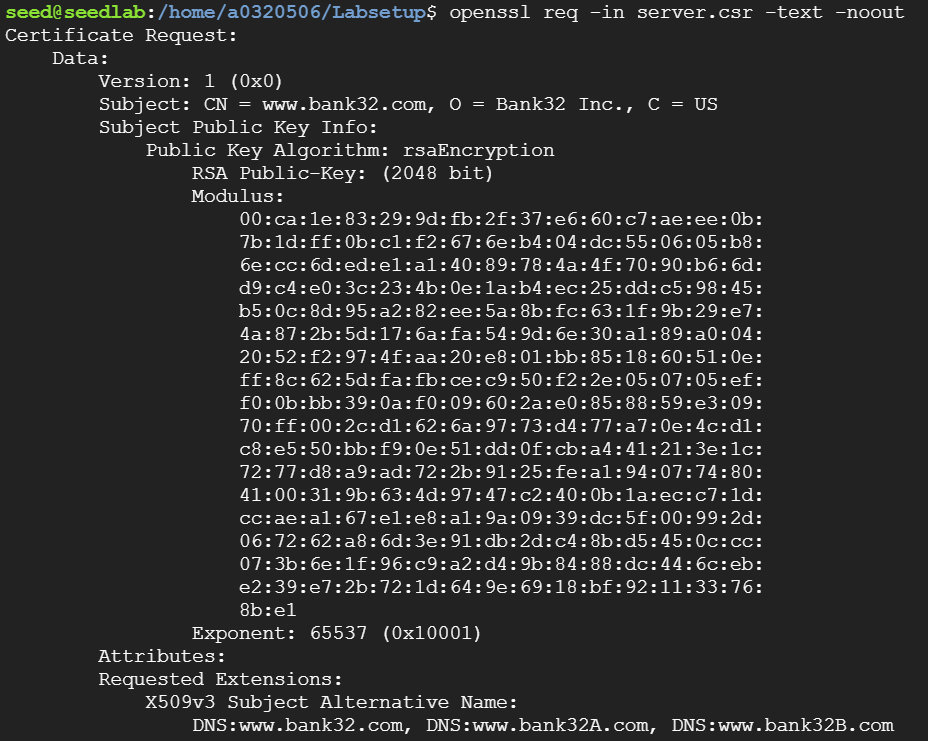
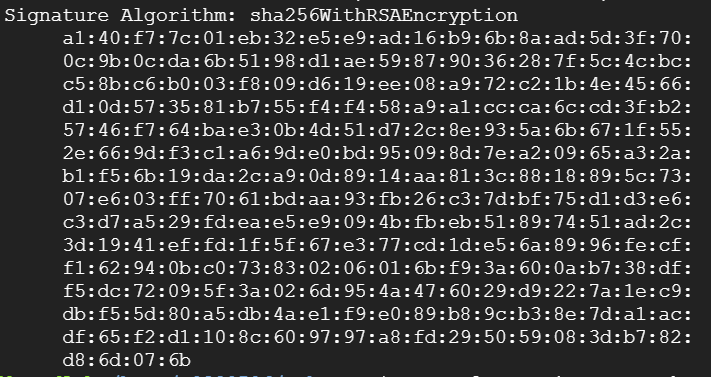
d 

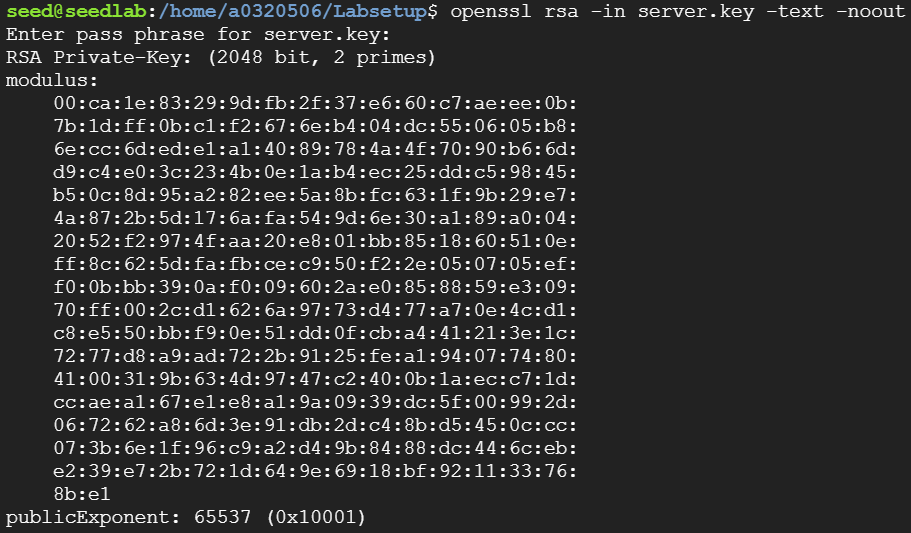
p 

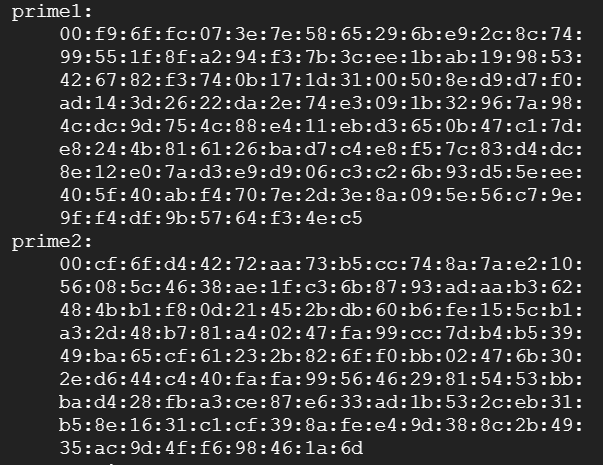
q 

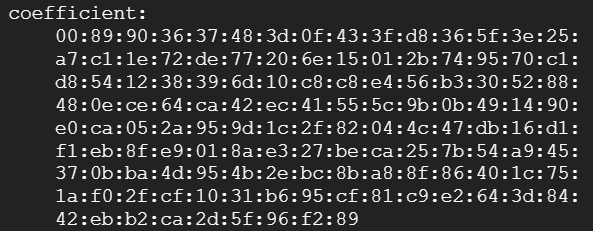




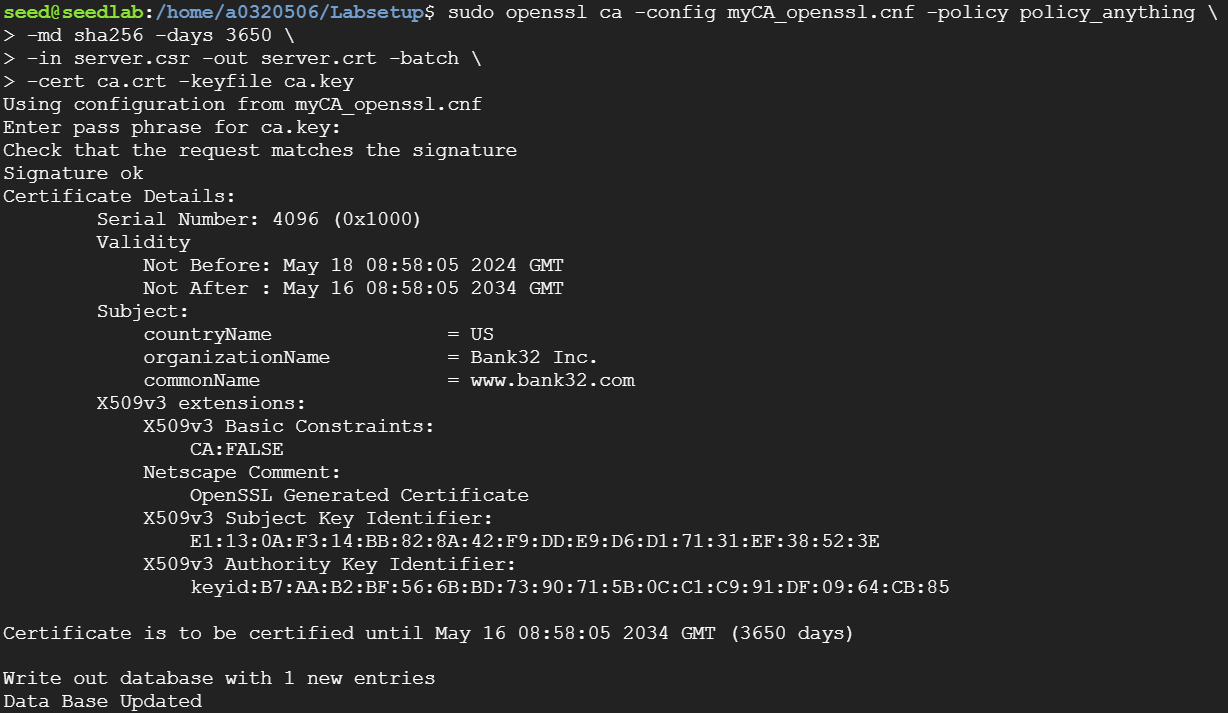
 

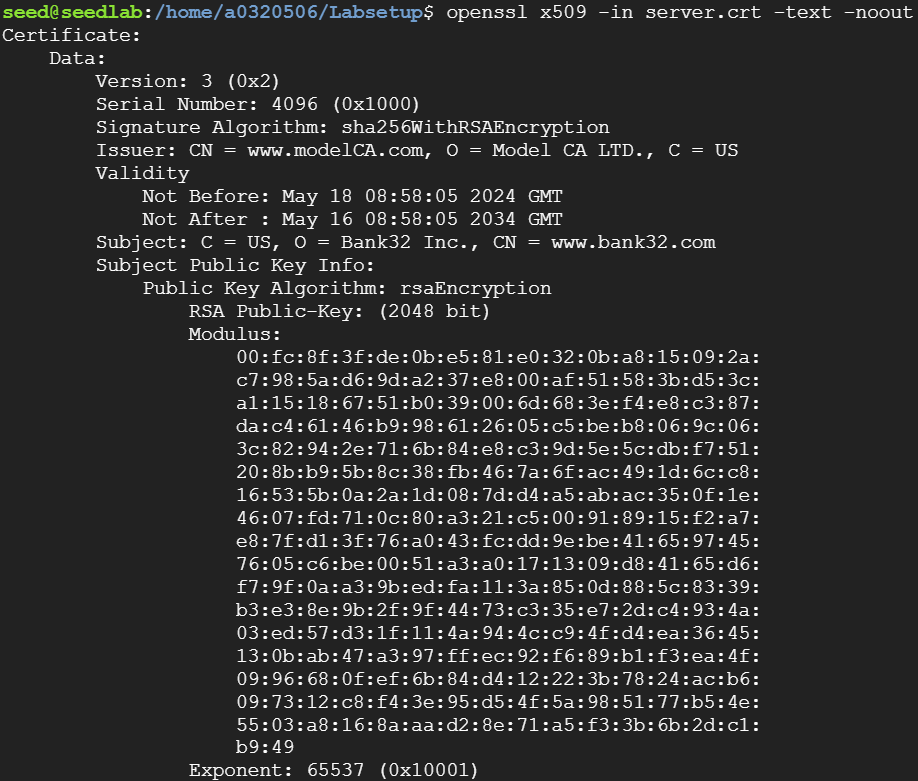
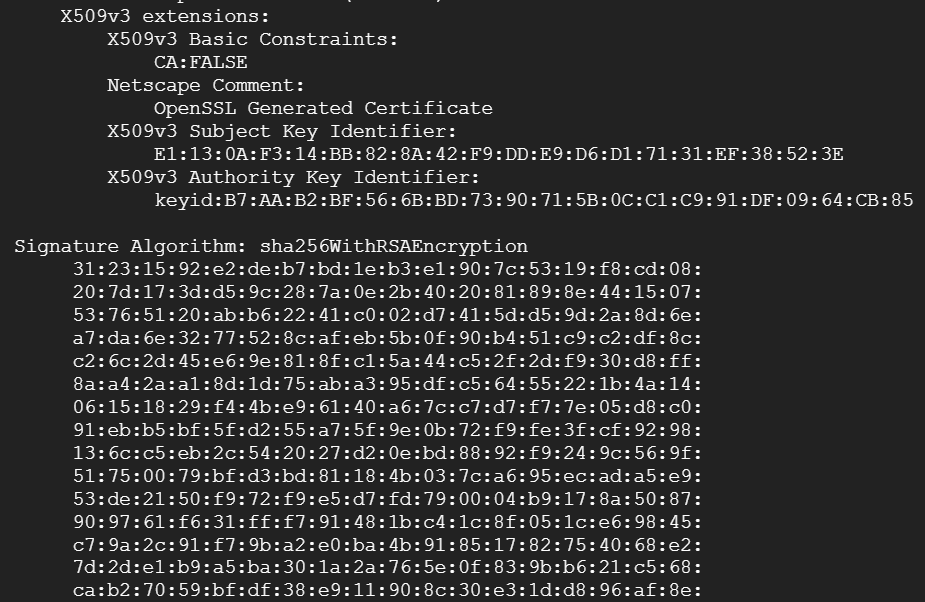
 



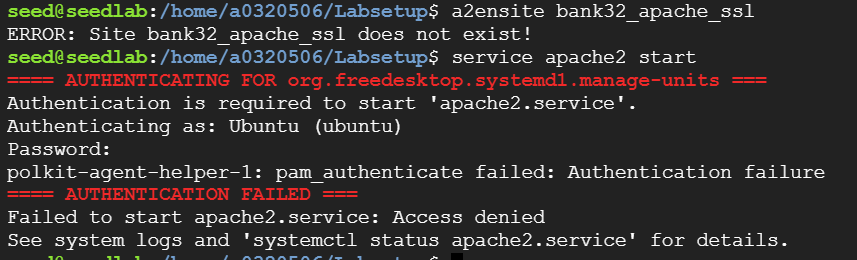










網頁無法開啟