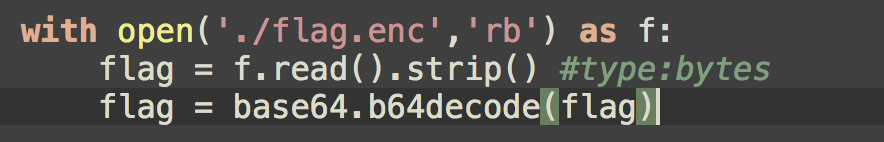
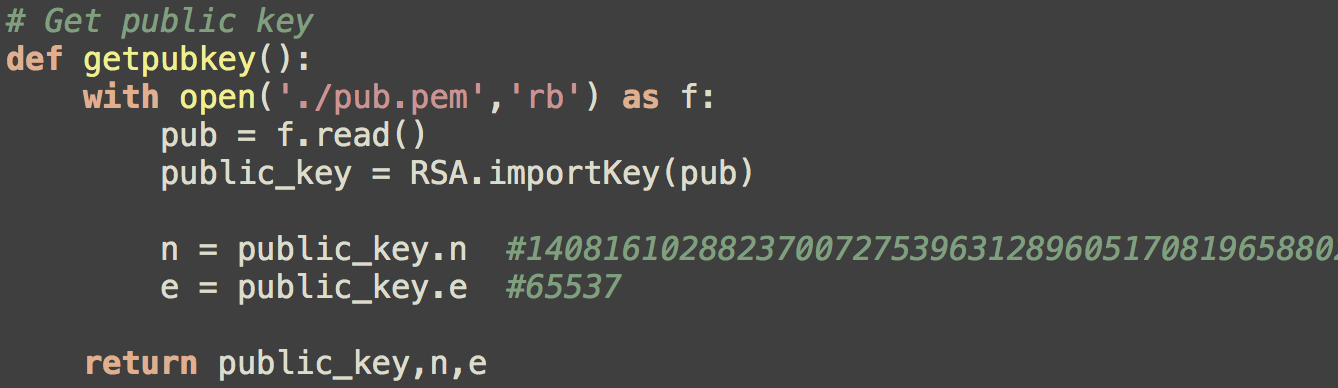
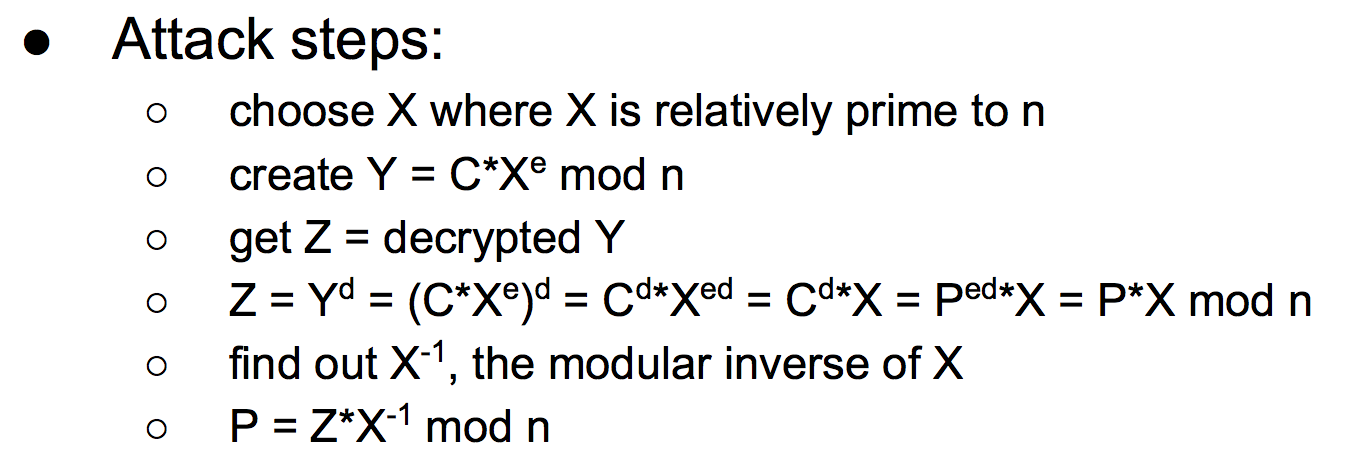
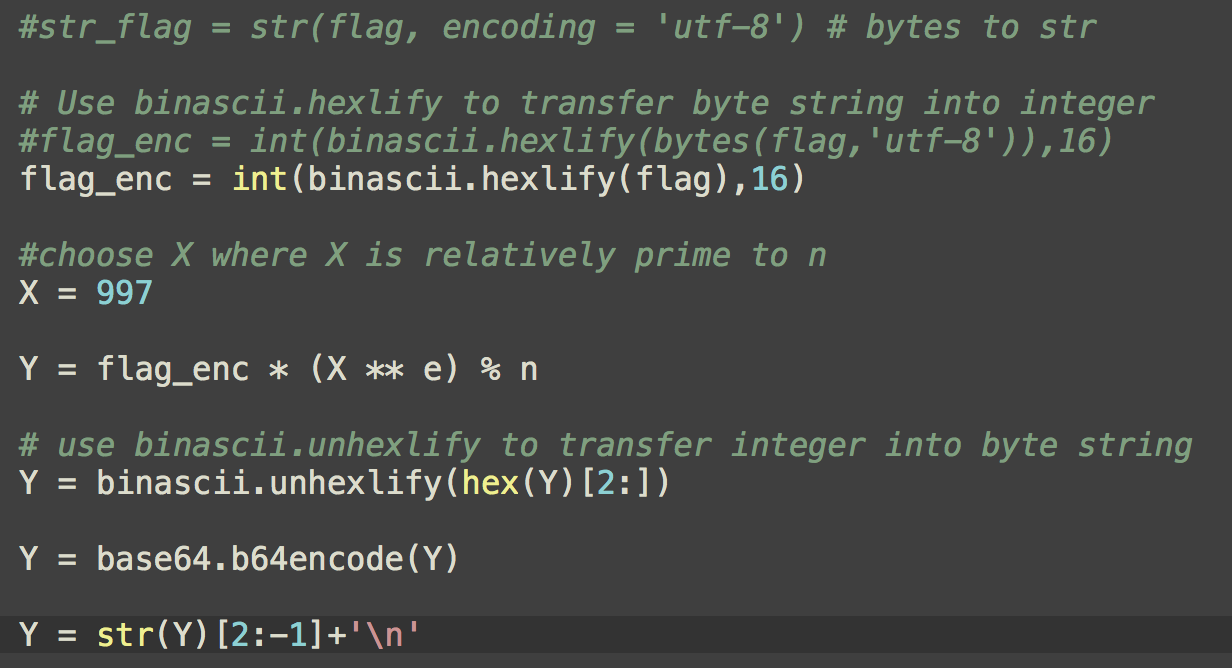
Course：Network Security

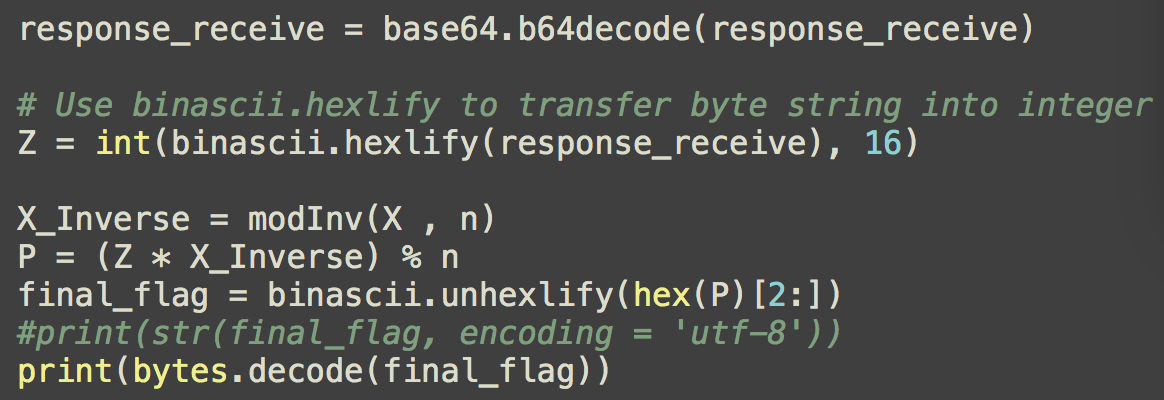
Homework 1

Name：0653422 林容伊

Explanation：

1. 首先，我們每個人都有flag.enc，先把他讀進來之後用base64解密。  
   
2. 然後我們每個人身上都會有一把public key 先從公鑰裡面求得n和e  
   
3. 再接著使用chosen cyphertext attack的步驟一步步算出加密後的Y  
     
   
4. 算好加密後的Y之後再send 進 server去解密



1. 解密後的message再去算Ｚ和P(照著上面attack的步驟)解出最後真正的flag  
   
2. 最後FLAG{S0\_y0u\_d0\_know\_th3\_cho5en\_c1ph3r\_4ttack!}