

安裝套件： Python Cryptography Toolkit (pycrypto)

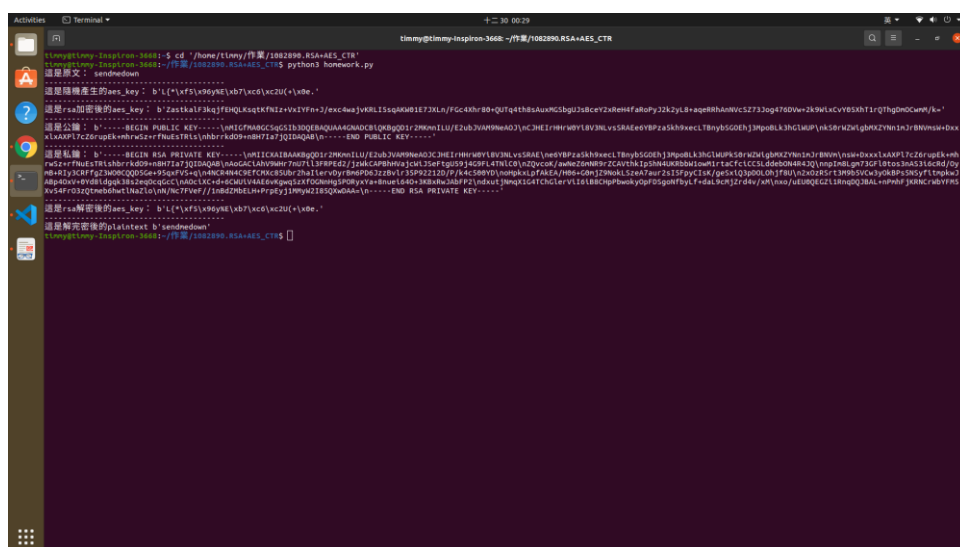
作業系統：ubuntu20.04

透過指令：pip install pycrypto

執行程式檔的命令：python3 homework.py

執行程式後會看見輸出 7 個結果

分別是：原文，隨機產生的 AES\_key，加密後的 AES\_key，RSA\_公鑰，RSA\_私鑰，解密後的 AES\_key，解密後的明文



```
timmy@timmy-aspiron-3668: ~/作業/1082890_RSA+AES_CTR
timmy@timmy-aspiron-3668:~$ cd ~/home/timmy/作業/1082890_RSA+AES_CTR
timmy@timmy-aspiron-3668:~/作業/1082890_RSA+AES_CTR$ python3 homework.py
這是原文: b'sendndown'
這是隨機產生的aes_key: b'l('vfrs\969NE\ab7LkcD\kczU(+\abe.'
這是rsa加密後的aes_key: b'Zaske43h3j7fHQLAgqKfzi+vcYfn+2/escdwaJvKRLIsq00b1E73Lh/Fc48hrB9+qU7qetth8AuqG5bgJ3BceY2aRenffatUpY23k2yl+aqB8HauMvC5273op47609w+3k9elAcv8Isht1rQThgDhCueW/b-'
這是公鑰: b'-----BEGIN PUBLIC KEY-----\nMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBgQQUEgQZA4TBggpILU/E2ubJvAPWwAG3\ncHEIrrMYWYrBV3NLvsSRAeYBPzaS8hveclT8yb5GDEhJ3mpuDLk3nCLuUP\k58rMZWigbKXZYmInJrB8Vms+Dax\nAAPI7C26rpgk+mh+ecrPhu5T8L5\mhbr+809+mh717JQ10qM8\n-----END PUBLIC KEY-----'
這是私鑰: b'-----BEGIN RSA PRIVATE KEY-----\nMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBgQQUEgQZA4TBggpILU/E2ubJvAPWwAG3\ncHEIrrMYWYrBV3NLvsSRAeYBPzaS8hveclT8yb5GDEhJ3mpuDLk3nCLuUP\k58rMZWigbKXZYmInJrB8Vms+Dax\nAAPI7C26rpgk+mh+ecrPhu5T8L5\mhbr+809+mh717JQ10qM8\n-----END RSA PRIVATE KEY-----'
這是rsa解密後的aes_key: b'l('vfrs\969NE\ab7LkcD\kczU(+\abe.'
這是解密完密後的plaintext: b'sendndown'
```

而執行過程中會產生 4 個檔案分別是公鑰 私鑰 aes 密文 加密後的 aes\_key