Report

0616098黃秉茂

Cryptographic primitive的選擇：

1 symmetric cipher with 3 mode of operations：AES-256-CBC, AES-256-CFB, AES-256-CTR

1 asymmetric cipher：RSA-2048

2 stream cipher：ARC4, Salsa20

2 hash function：SHA-256, SHA-512

2 MAC：HMAC(with SHA-256), CMAC(with AES)

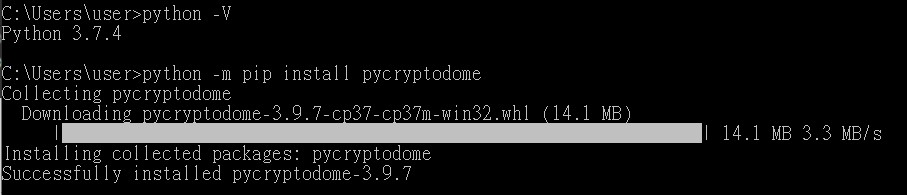
Library的選擇：pycryptodome

pycryptodome與pycrypto差不多，但因為pycrypto沒有向上支援到python3.7，因此我選擇安裝pycryptodome

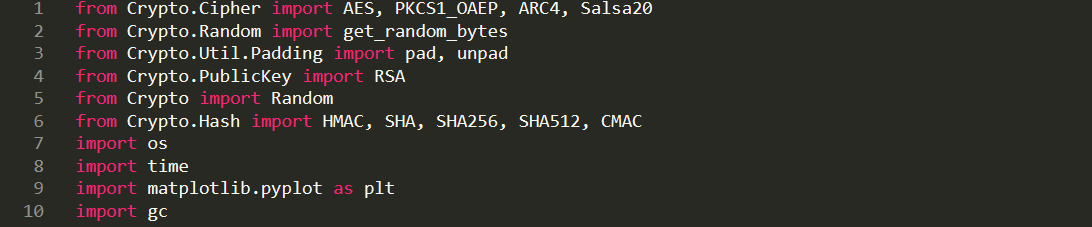
安裝pycryptodome：

先進入cmd

輸入”python -m pip install pycryptodome”



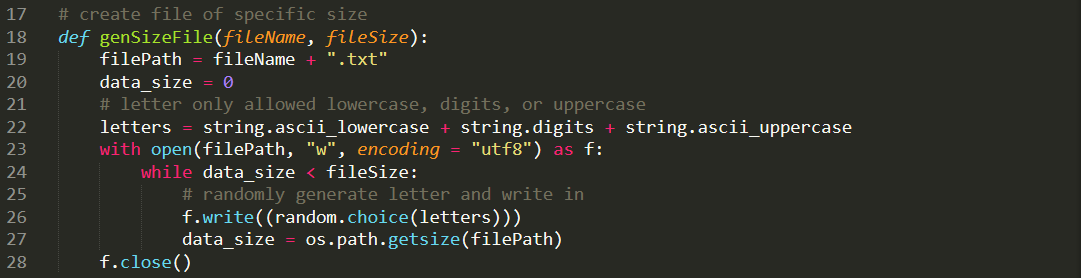
Code：



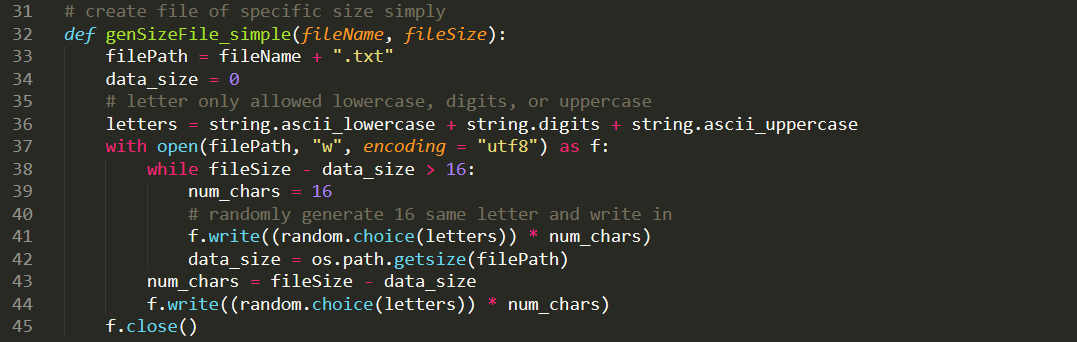
Import Crypto.Cipher(密碼學相關)、Crypto.Rando(變數產生)、Crypto.Util.Padding (padding相關)、Crypto.Hash (hash function相關)、os(os、路徑、讀檔相關)、time(time相關)、matplotlib(plot、畫圖相關)和gc(釋放記憶體相關)



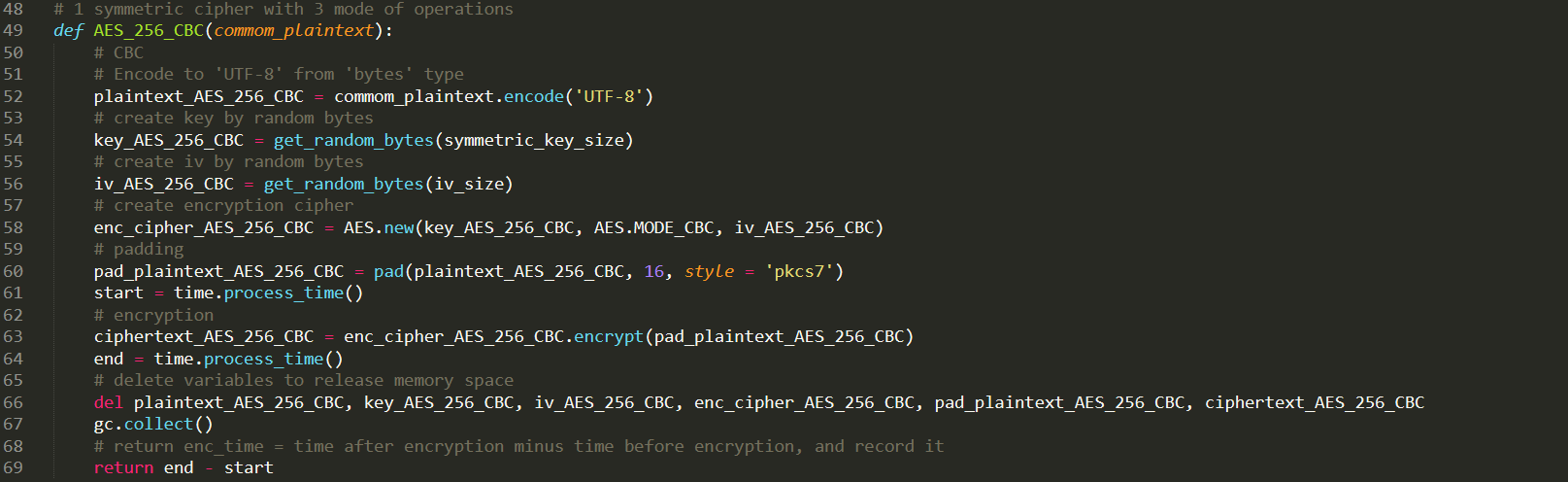
定義key size和 iv size



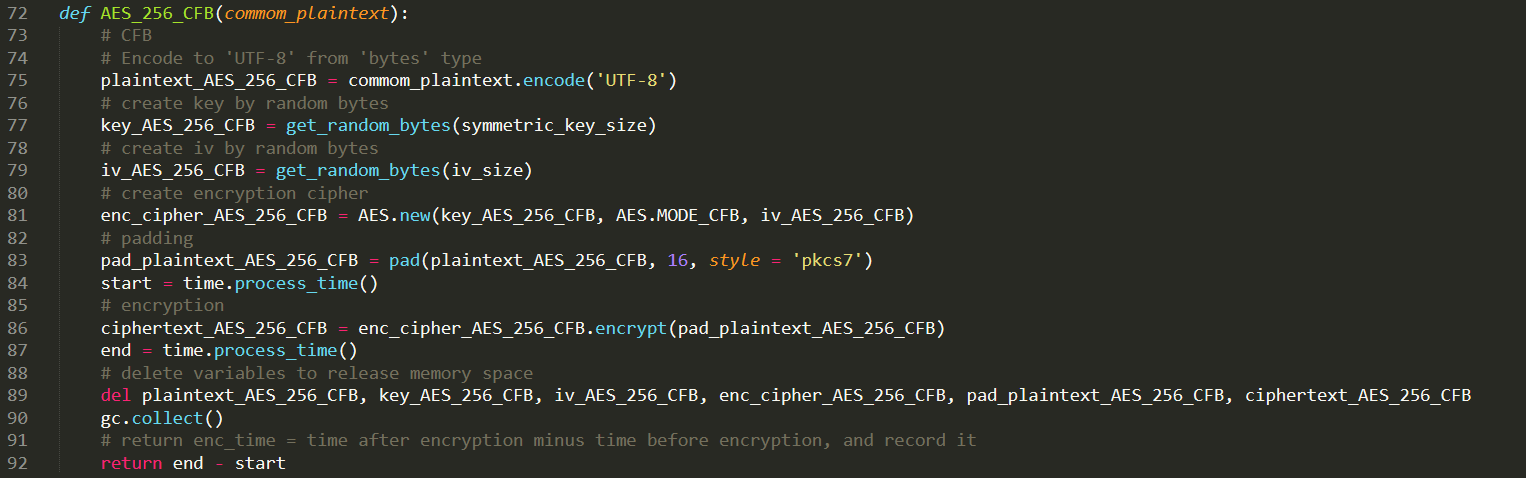
產生固定大小的隨機txt檔案的function，但時間複雜度很高



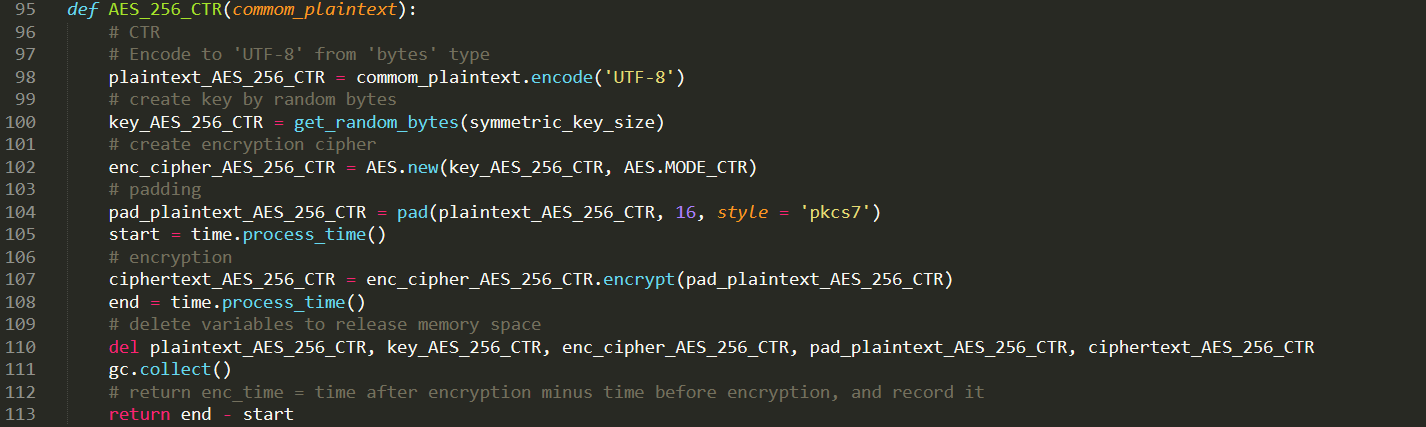
較簡單產生固定大小的隨機txt檔案的function，但亂度不夠高



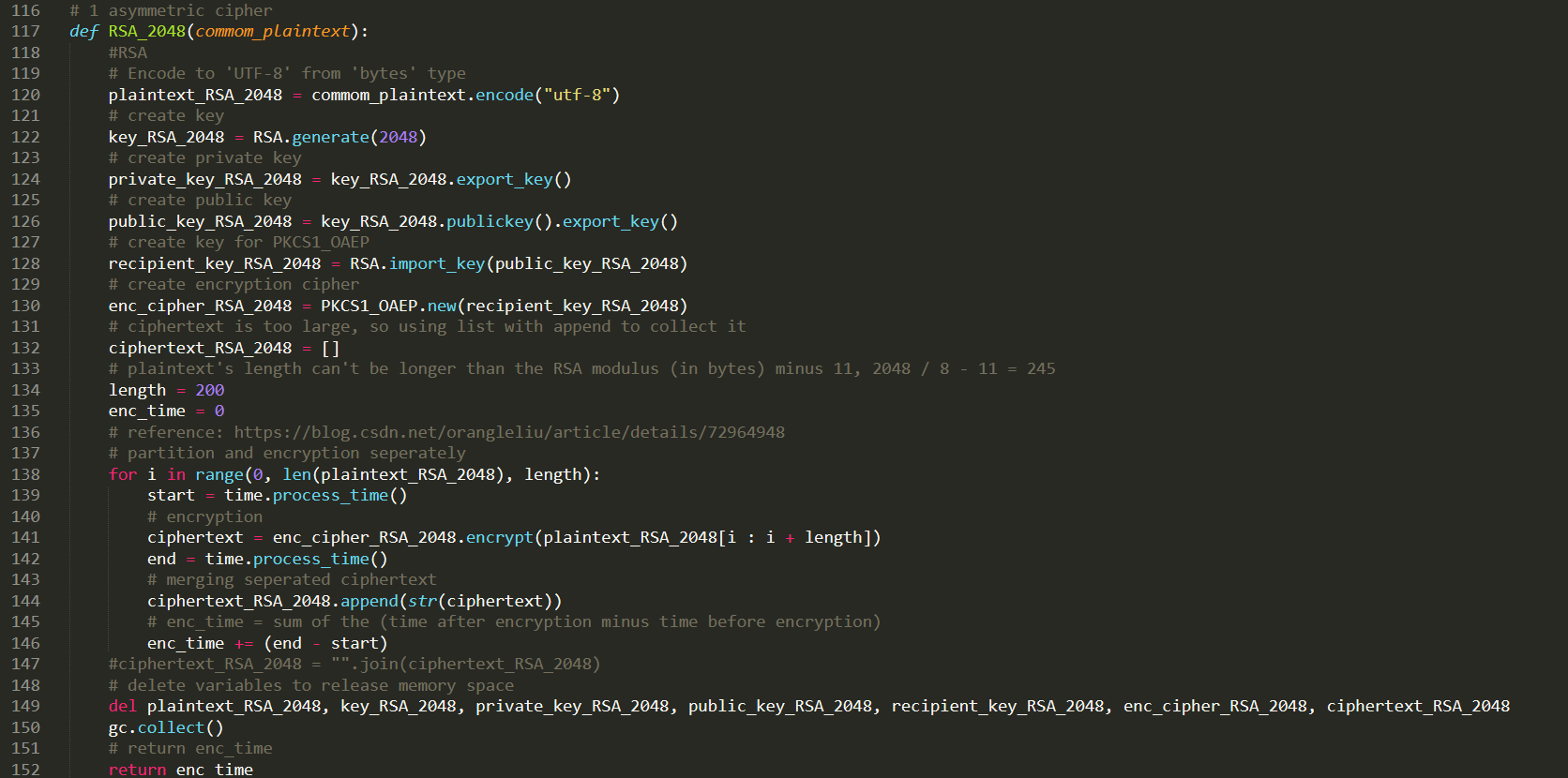
AES\_256\_CBC的encryption function，會return它的encryption time



AES\_256\_CFB的encryption function，會return它的encryption time



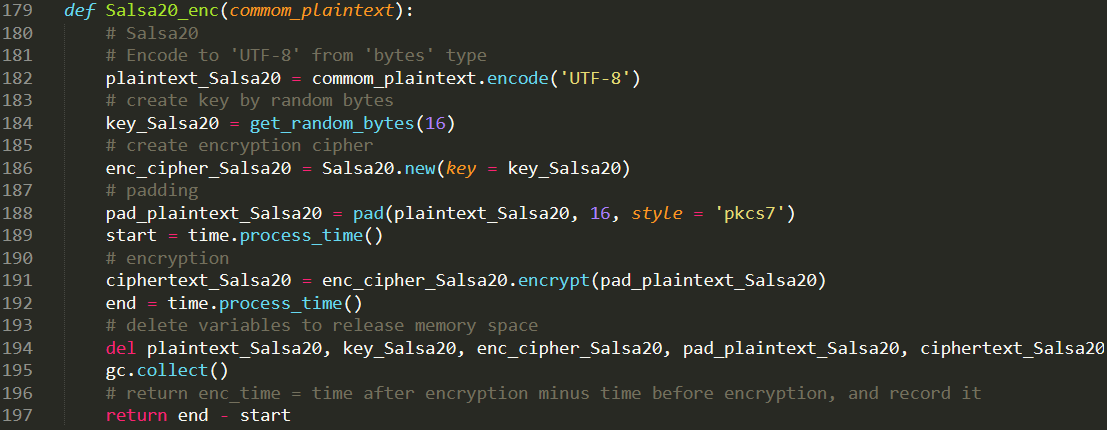
AES\_256\_CTR的encryption function，會return它的encryption time



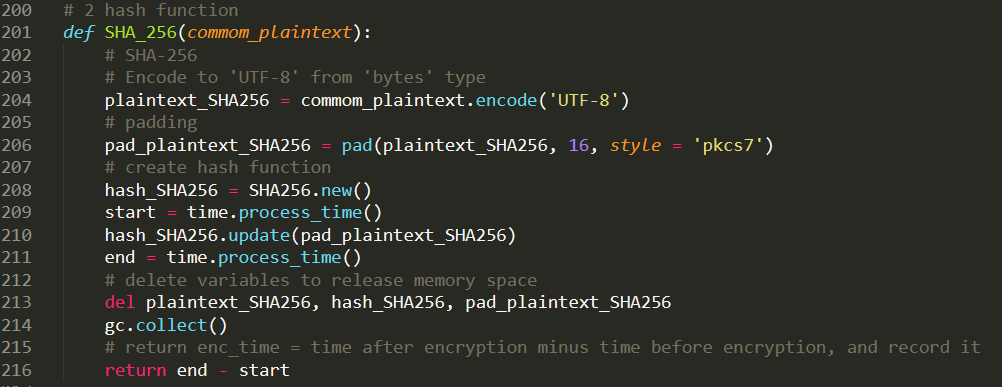
RSA-2048的encryption function，會return它的encryption time



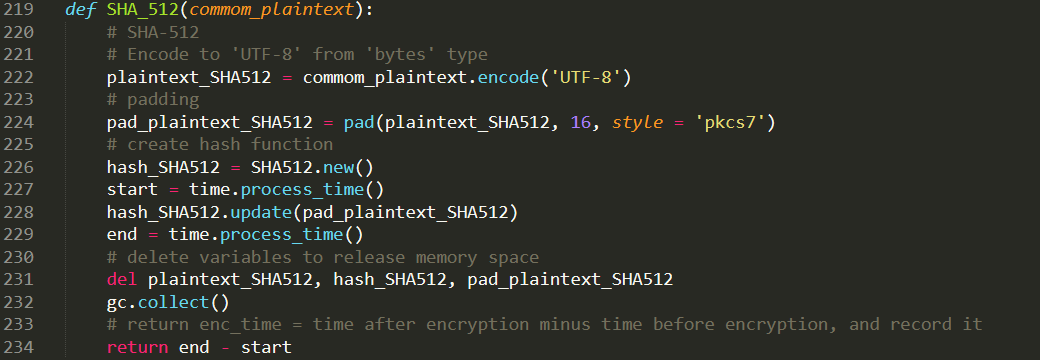
ACR4的encryption function，會return它的encryption time



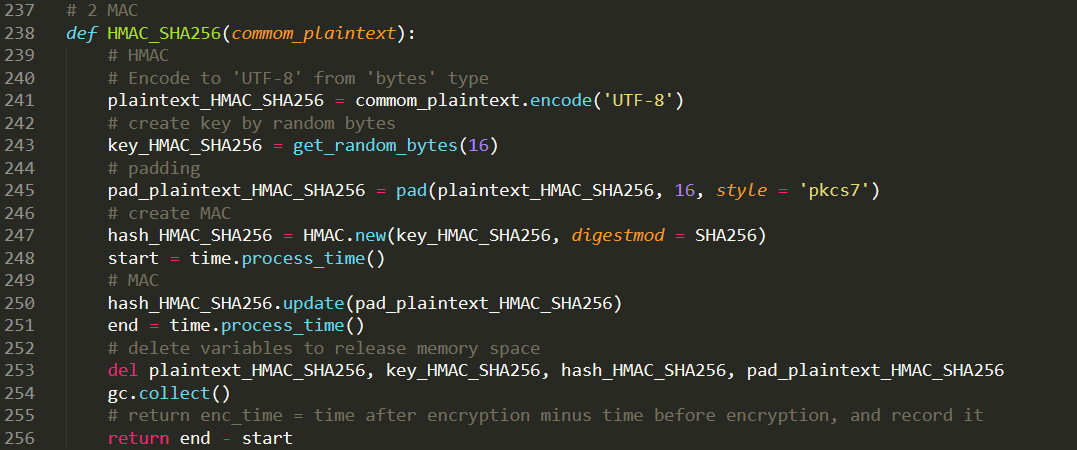
Salsa20的encryption function，會return它的encryption time



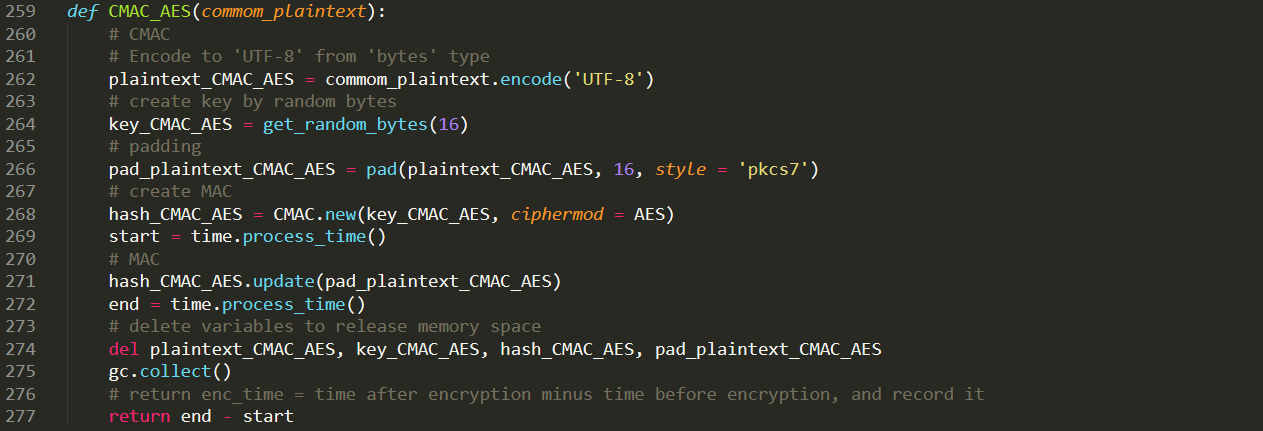
SHA-256的hash function，會return它的hash time



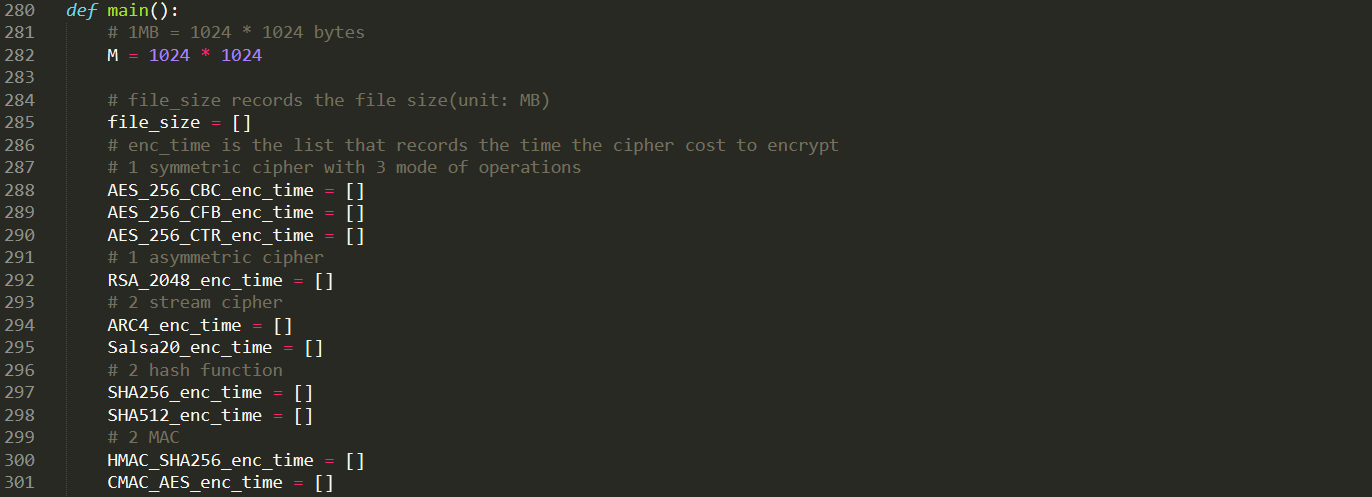
SHA-512的hash function，會return它的hash time



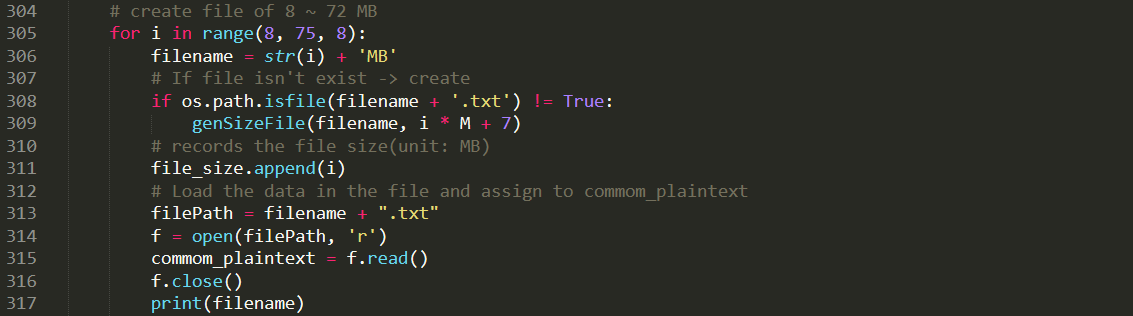
HMAC\_SHA256的MAC function，會return它的MAC time



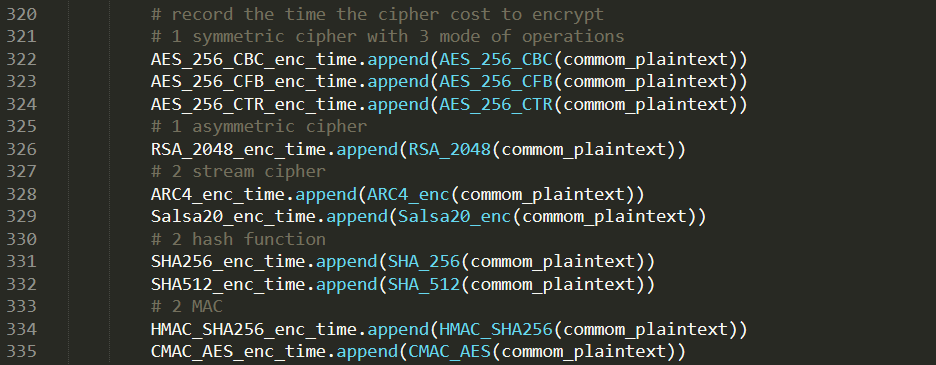
CMAC\_AES的MAC function，會return它的MAC time



初始化設定



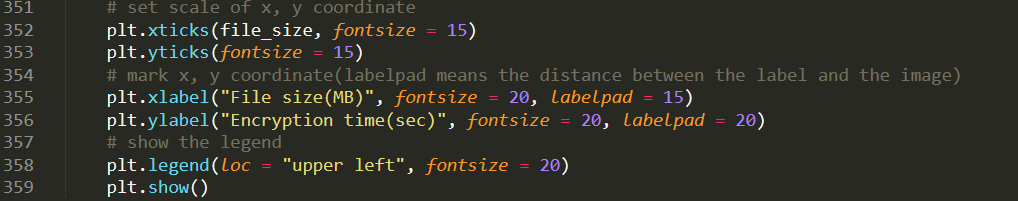
生成8 ~ 56MB的隨機txt檔案



呼叫原先定義好的便屬=數，append進list裡，以記錄各個cipher的encryption time



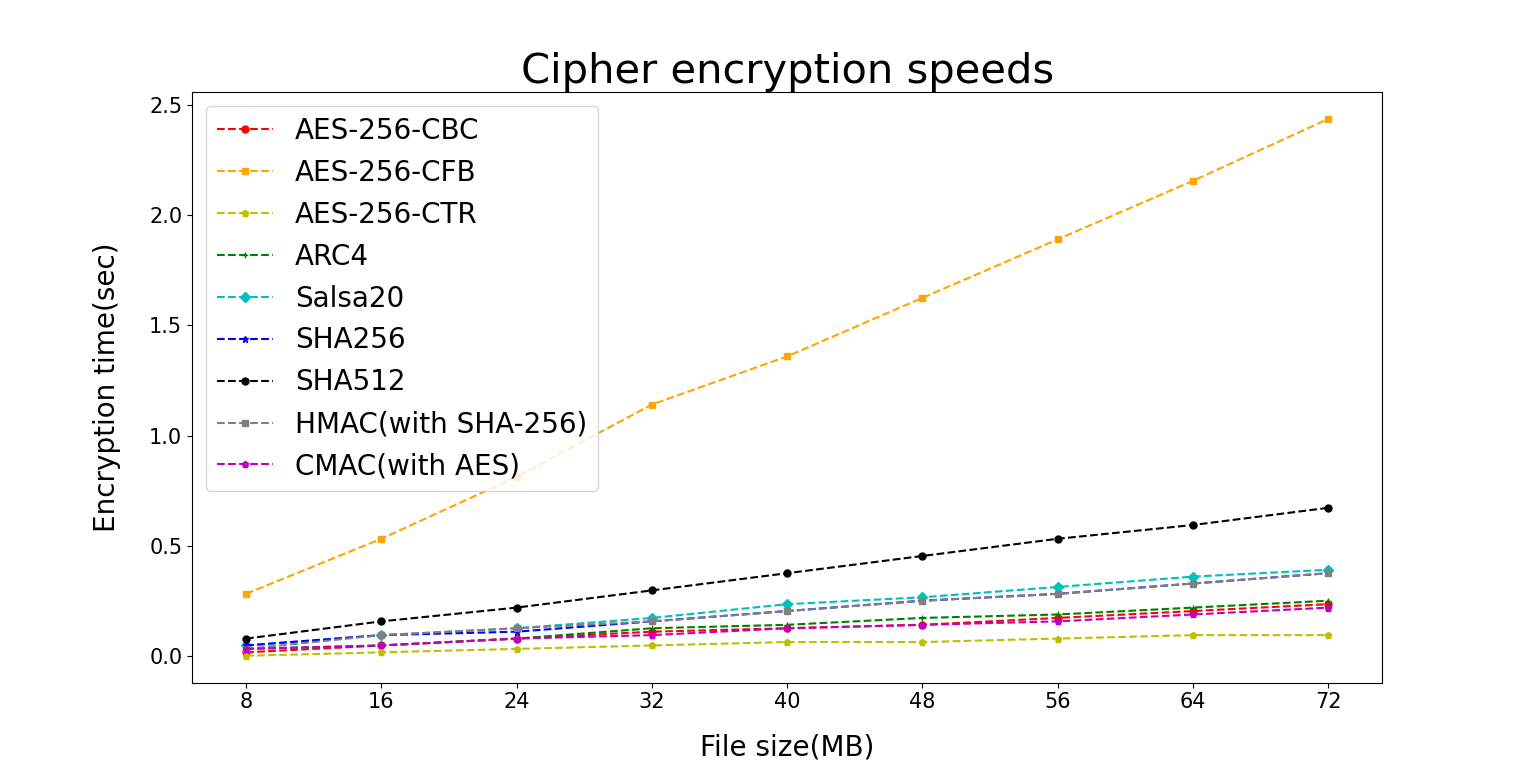
畫出時間比較圖



設定圖片的座標、圖例等

Result：

Without RSA-2048：



With RSA-2048：

