

資訊安全作業 Assignment1

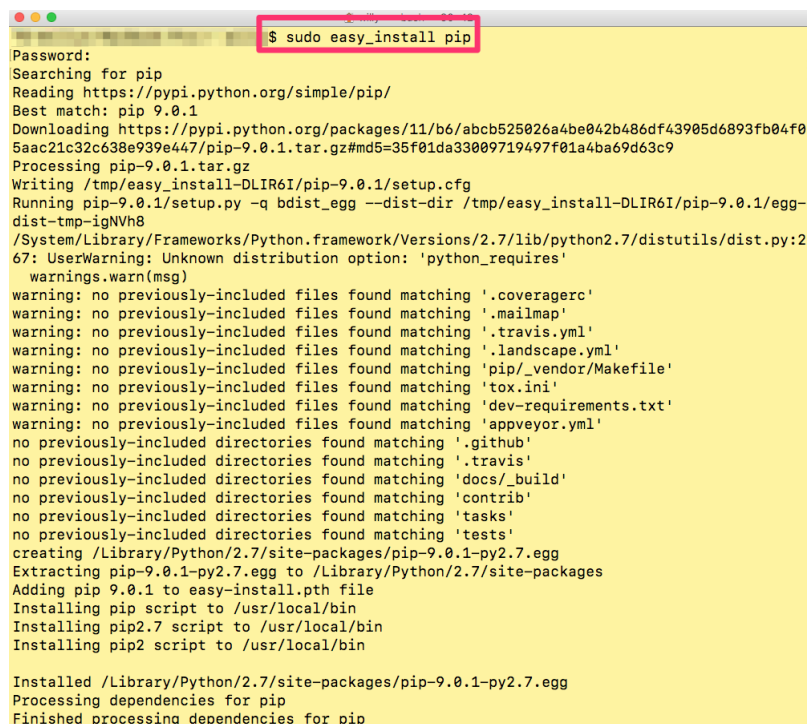
吳嘉偉 5105056013

2017/03/26

1 安裝 Python Packages

1.1 使用終端機安裝 pip

打開 terminal 後，先輸入指令安裝 pip
`sudo easy_install pip`

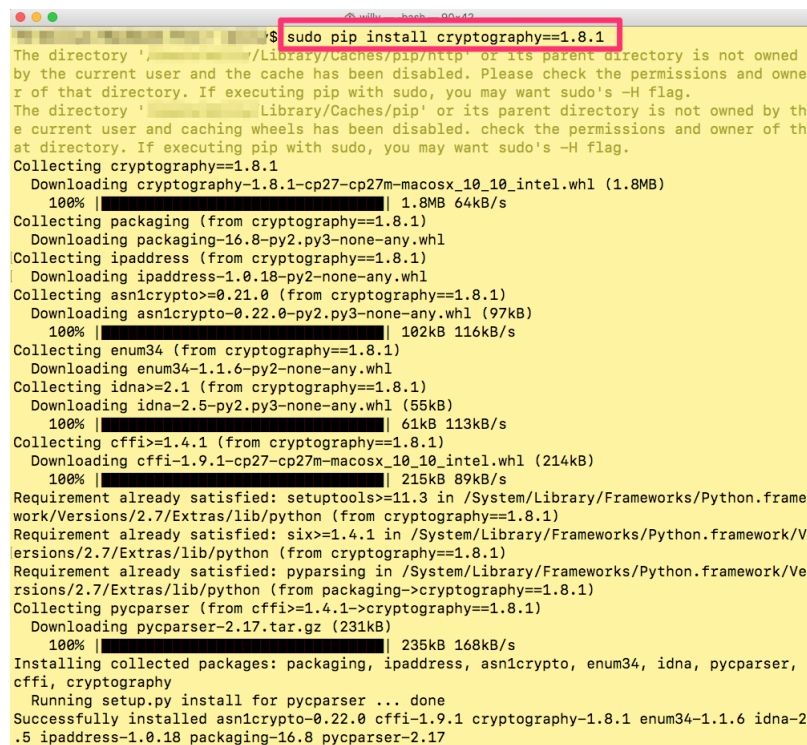
A terminal window screenshot showing the command '\$ sudo easy_install pip' being executed. The command is highlighted with a red box. The output shows the process of searching for pip, downloading it from PyPI, and installing it. It includes several warnings about previously included files and directories, and finally shows the successful installation of pip-9.0.1-py2.7.egg to the site-packages directory, along with the installation of the pip script to the local bin directory.

```
$ sudo easy_install pip
Password:
Searching for pip
Reading https://pypi.python.org/simple/pip/
Best match: pip 9.0.1
Downloading https://pypi.python.org/packages/11/b6/abcb525026a4be042b486df43905d6893fb04f0
5aac21c32c638e939e447/pip-9.0.1.tar.gz#md5=35f01da33009719497f01a4ba69d63c9
Processing pip-9.0.1.tar.gz
Writing /tmp/easy_install-DLIR6I/pip-9.0.1/setup.cfg
Running pip-9.0.1/setup.py -q bdist_egg --dist-dir /tmp/easy_install-DLIR6I/pip-9.0.1/egg-
dist-tmp-igNVh8
/System/Library/Frameworks/Python.framework/Versions/2.7/lib/python2.7/distutils/dist.py:2
67: UserWarning: Unknown distribution option: 'python_requires'
  warnings.warn(msg)
warning: no previously-included files found matching '.coveragerc'
warning: no previously-included files found matching '.mailmap'
warning: no previously-included files found matching '.travis.yml'
warning: no previously-included files found matching '.landscape.yml'
warning: no previously-included files found matching 'pip/_vendor/Makefile'
warning: no previously-included files found matching 'tox.ini'
warning: no previously-included files found matching 'dev-requirements.txt'
warning: no previously-included files found matching 'appveyor.yml'
no previously-included directories found matching '.github'
no previously-included directories found matching '.travis'
no previously-included directories found matching 'docs/_build'
no previously-included directories found matching 'contrib'
no previously-included directories found matching 'tasks'
no previously-included directories found matching 'tests'
creating /Library/Python/2.7/site-packages/pip-9.0.1-py2.7.egg
Extracting pip-9.0.1-py2.7.egg to /Library/Python/2.7/site-packages
Adding pip 9.0.1 to easy-install.pth file
Installing pip script to /usr/local/bin
Installing pip2.7 script to /usr/local/bin
Installing pip2 script to /usr/local/bin

Installed /Library/Python/2.7/site-packages/pip-9.0.1-py2.7.egg
Processing dependencies for pip
Finished processing dependencies for pip
```

Figure 1: 安裝 pip

接著輸入下圖指令，安裝需要的 package
這邊是安裝 cryptography，版本為 1.8.1
sudo pip install packagename==version
packagename：要安裝的 package 名稱
version：要安裝的版本號碼

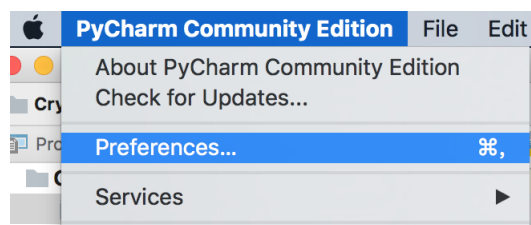


```
$ sudo pip install cryptography==1.8.1
The directory '/Library/Caches/pip/http' or its parent directory is not owned
by the current user and the cache has been disabled. Please check the permissions and own
er of that directory. If executing pip with sudo, you may want sudo's -H flag.
The directory '/Library/Caches/pip' or its parent directory is not owned by th
e current user and caching wheels has been disabled. check the permissions and owner of th
at directory. If executing pip with sudo, you may want sudo's -H flag.
Collecting cryptography==1.8.1
  Downloading cryptography-1.8.1-cp27-cp27m-macosx_10_10_intel.whl (1.8MB)
    100% |#####| 1.8MB 64kB/s
Collecting packaging (from cryptography==1.8.1)
  Downloading packaging-16.8-py2.py3-none-any.whl
Collecting ipaddress (from cryptography==1.8.1)
  Downloading ipaddress-1.0.18-py2-none-any.whl
Collecting asn1crypto>=0.21.0 (from cryptography==1.8.1)
  Downloading asn1crypto-0.22.0-py2.py3-none-any.whl (97kB)
    100% |#####| 102kB 116kB/s
Collecting enum34 (from cryptography==1.8.1)
  Downloading enum34-1.1.6-py2-none-any.whl
Collecting idna>=2.1 (from cryptography==1.8.1)
  Downloading idna-2.5-py2.py3-none-any.whl (55kB)
    100% |#####| 61kB 113kB/s
Collecting cffi>=1.4.1 (from cryptography==1.8.1)
  Downloading cffi-1.9.1-cp27-cp27m-macosx_10_10_intel.whl (214kB)
    100% |#####| 215kB 89kB/s
Requirement already satisfied: setuptools>=11.3 in /System/Library/Frameworks/Python.frame
work/Versions/2.7/Extras/lib/python (from cryptography==1.8.1)
Requirement already satisfied: six>=1.4.1 in /System/Library/Frameworks/Python.framework/V
ersions/2.7/Extras/lib/python (from cryptography==1.8.1)
Requirement already satisfied: pyparsing in /System/Library/Frameworks/Python.framework/Ve
rsions/2.7/Extras/lib/python (from packaging->cryptography==1.8.1)
Collecting pycparser (from cffi>=1.4.1->cryptography==1.8.1)
  Downloading pycparser-2.17.tar.gz (231kB)
    100% |#####| 235kB 168kB/s
Installing collected packages: packaging, ipaddress, asn1crypto, enum34, idna, pycparser,
cffi, cryptography
  Running setup.py install for pycparser ... done
Successfully installed asn1crypto-0.22.0 cffi-1.9.1 cryptography-1.8.1 enum34-1.1.6 idna-2
.5 ipaddress-1.0.18 packaging-16.8 pycparser-2.17
```

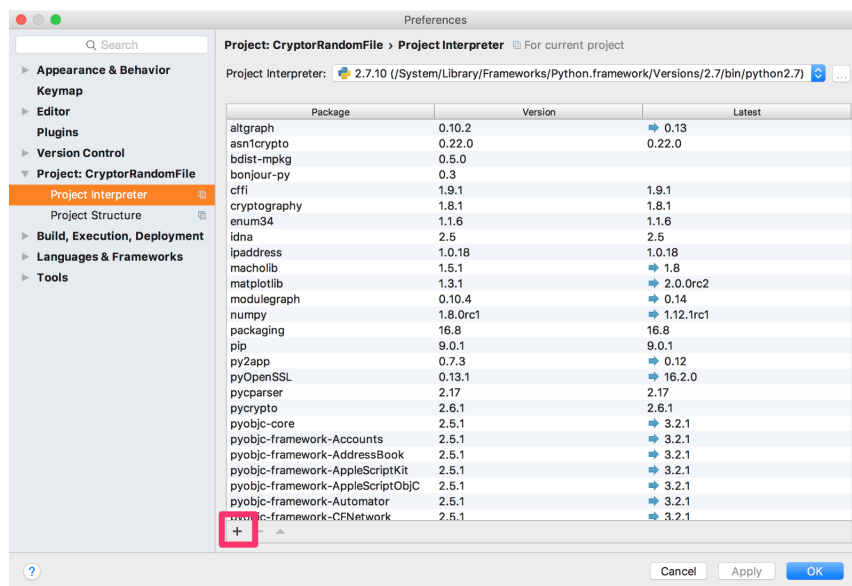
Figure 2: 安裝 package

1.2 使用 PyCharm

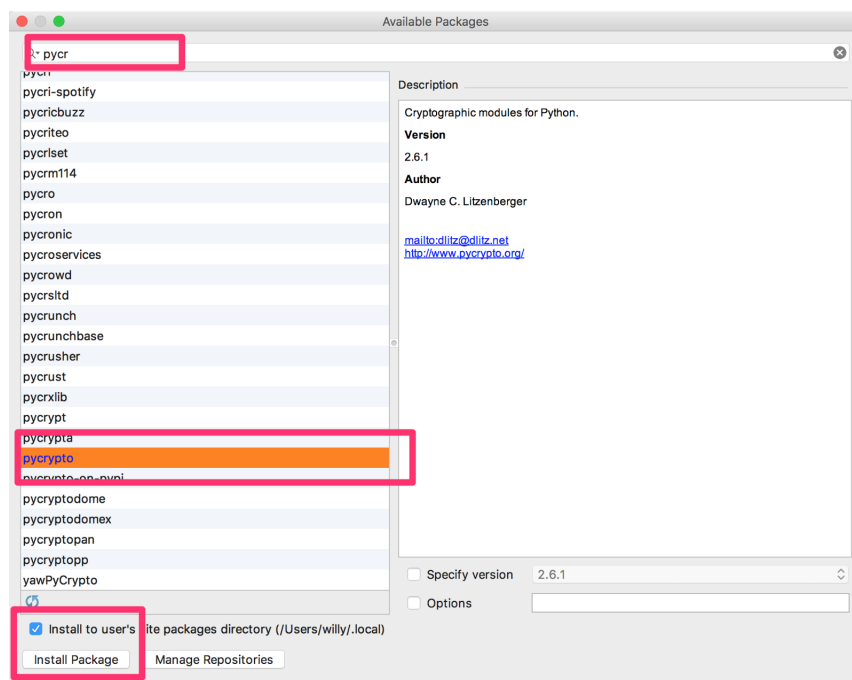
打開 PyCharmCE，先點選 Preferences...



選擇 Project: ProjectName » Project Interpreter » +



輸入要加入的 package name



2 PyCrypto

2.1 PyCrypto AES-256 ECB

```
# -*- coding: utf-8 -*-

from __future__ import absolute_import, division, unicode_literals

import os
from Crypto.Cipher import AES

_KEY = os.urandom(32)          # 設定Key
_BlockSize = AES.block_size    # Block Size

#padding
_Pad = lambda s: s + (_BlockSize - len(s) % _BlockSize) * chr(_BlockSize - len(s) % _BlockSize)
_Unpad = lambda s : s[0:-ord(s[-1])]

# 使用ECB加密
def aes_encrypt(data):
    cryptor = AES.new(_KEY, AES.MODE_ECB)
    return cryptor.encrypt(_Pad(data))

# 使用ECB解密
def aes_decrypt(data):
    cryptor = AES.new(_KEY, AES.MODE_ECB)
    return _Unpad(cryptor.decrypt(data))
```

2.2 PyCrypto AES-256 CBC

```
# -*- coding: utf-8 -*-

from __future__ import absolute_import, division, unicode_literals

import os
from Crypto.Cipher import AES

_IV = os.urandom(16)          # 產生隨機亂數IV
```

```

_KEY = os.urandom(32)          # 設定Key
_BlockSize = AES.block_size    # Block Size

#padding
_Pad = lambda s: s + (_BlockSize - len(s) % _BlockSize) * chr(_BlockSize)
_Unpad = lambda s : s[0:-ord(s[-1])]

# 使用CBC加密
def aes_encrypt(data):
    cryptor = AES.new(_KEY, AES.MODE_CBC, _IV)
    return cryptor.encrypt(_Pad(data))

# 使用CBC解密
def aes_decrypt(data):
    cryptor = AES.new(_KEY, AES.MODE_CBC, _IV)
    return _Unpad(cryptor.decrypt(data))

```

2.3 PyCrypto AES-256 CTR

```

# -*- coding: utf-8 -*-

from __future__ import absolute_import, division, unicode_literals

import os
from Crypto.Cipher import AES

_IV = os.urandom(16)          # 產生隨機亂數IV
_KEY = os.urandom(32)          # 設定Key
_COUNTER = os.urandom(16)
_BlockSize = AES.block_size    # Block Size

#padding
_Pad = lambda s: s + (_BlockSize - len(s) % _BlockSize) * chr(_BlockSize)
_Unpad = lambda s : s[0:-ord(s[-1])]

# 使用CTR加密
def aes_encrypt(data):
    cryptor = AES.new(_KEY, AES.MODE_CTR, counter=lambda: _COUNTER)
    return cryptor.encrypt(_Pad(data))

```

```
# 使用CTR解密
def aes_decrypt(data):
    cryptor = AES.new(_KEY, AES.MODE_CTR, counter=lambda: _COUNTER)
    return _Unpad(cryptor.decrypt(data))
```

2.4 PyCrypto RSA-2048

2.5 PyCrypto SHA-512

```
# -*- coding: utf-8 -*-
from __future__ import absolute_import, division, unicode_literals

from Crypto.Hash import SHA512

def hashSHA512(data):
    hash = SHA512.new()
    hash.update(data)
    return hash.hexdigest()
```

3 Cryptography

3.1 Cryptography AES-256 ECB

```
import os
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes
from cryptography.hazmat.backends import default_backend

backend = default_backend()
_KEY = os.urandom(32)    # 設定Key
_BlockSize = 16          # Block Size

#padding
_Pad = lambda s: s + (_BlockSize - len(s) % _BlockSize) * chr(_BlockSize - len(s) % _BlockSize)
_Unpad = lambda s: s[:ord(s[-1])]

# 使用ECB加密
def aes_encrypt(data):
    cipher = Cipher(algorithms.AES(_KEY), modes.ECB(), backend=backend)
    encryptor = cipher.encryptor()
    ciphertext = encryptor.update(_Pad(data))
    return ciphertext

# 使用ECB解密
def aes_decrypt(data):
    cipher = Cipher(algorithms.AES(_KEY), modes.ECB(), backend=backend)
    decryptor = cipher.decryptor()
    plaintext = _Unpad(decryptor.update(data)) # + decryptor.finalize()
    return plaintext
```

3.2 Cryptography AES-256 CBC

```
import os
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes
from cryptography.hazmat.backends import default_backend

backend = default_backend()
_IV = os.urandom(16)    # 產生隨機亂數IV
```

```

_KEY = os.urandom(32)    # 設定Key
_BlockSize = 16          # Block Size

#padding
_Pad = lambda s: s + (_BlockSize - len(s) % _BlockSize) * chr(_BlockSize)
_Unpad = lambda s : s[0:-ord(s[-1])]

# 使用CBC加密
def aes_encrypt(data):
    cipher = Cipher(algorithms.AES(_KEY), modes.CBC(_IV), backend=backend)
    encryptor = cipher.encryptor()
    ciphertext = encryptor.update(_Pad(data))
    return ciphertext

# 使用CBC解密
def aes_decrypt(data):
    cipher = Cipher(algorithms.AES(_KEY), modes.CBC(_IV), backend=backend)
    decryptor = cipher.decryptor()
    plaintext = _Unpad(decryptor.update(data))
    return plaintext

```

3.3 Cryptography AES-256 CTR

```

import os
from cryptography.hazmat.primitives.ciphers import Cipher, algorithms, modes
from cryptography.hazmat.backends import default_backend

backend = default_backend()
_IV = os.urandom(16)    # 產生隨機亂數IV
_KEY = os.urandom(32)   # 設定Key
_BlockSize = 16         # Block Size

#padding
_Pad = lambda s: s + (_BlockSize - len(s) % _BlockSize) * chr(_BlockSize)
_Unpad = lambda s : s[0:-ord(s[-1])]

# 使用CTR加密
def aes_encrypt(data):
    cipher = Cipher(algorithms.AES(_KEY), modes.CTR(_IV), backend=backend)

```



```

    encryptor = cipher.encryptor()
    ciphertext = encryptor.update(_Pad(data))
    return ciphertext

# 使用CTR解密
def aes_decrypt(data):
    cipher = Cipher(algorithms.AES(_KEY), modes.CTR(_IV), backend=backend)
    decryptor = cipher.decryptor()
    plaintext = _Unpad(decryptor.update(data))
    return plaintext

```

3.4 Cryptography RSA-2048

3.5 Cryptography SHA-512

```

from cryptography.hazmat.primitives import hashes
from cryptography.hazmat.backends import default_backend

backend = default_backend()

def hashSHA512(data):
    digest = hashes.Hash(hashes.SHA512(), backend=default_backend())
    digest.update(data)
    return digest.finalize()

```

4 PyCrypto 與 Cryptography 速度的比較

利用 Python 隨機產生一個大小為 512+7byte 的字串檔案並且丟到每一個加解密演算法計算時間

4.1 隨機產生字串檔案

```
# -*- coding: utf-8 -*-
import random, string

# 隨機產生大小為 size 的字串檔案
def generateStringFile(size):
    text = ''.join(random.choice(string.ascii_letters + string.digits) for _ in range(size))
    file = open('RandomString.txt', 'wb')
    file.write(text)
```

4.2 AES-256 ECB

```
# PyCrypto_AES_256_ECB
print ('PyCrypto_AES_256_ECB')
start = time.time()
encrypt = PyCrypto_AES_256_ECB.aes_encrypt(plaintext)
end = time.time()
elapsed = end - start
print ('Time taken: ' + str(elapsed) + 'seconds.')
```

```
# Cryptography_AES_256_ECB
print ('Cryptography_AES_256_ECB')
start = time.time()
encrypt = Cryptography_AES_256_ECB.aes_encrypt(plaintext)
end = time.time()
elapsed = end - start
print ('Time taken: ' + str(elapsed) + 'seconds.')
```

輸出的結果為

PyCrypto AES256 ECB Time taken: 8.11543488503seconds.

Cryptography AES256 ECB Time taken: 2.48533296585seconds.

4.3 AES-256 CBC

```
# PyCrypto_AES_256_CBC
print ( 'PyCrypto_AES_256_CBC' )
start = time.time()
encrypt = PyCrypto_AES_256_CBC.aes_encrypt(plaintext)
end = time.time()
elapsed = end - start
print ( 'Time taken: ' + str(elapsed) + 'seconds.' )

# Cryptography_AES_256_CBC
print ( 'Cryptography_AES_256_CBC' )
start = time.time()
encrypt = Cryptography_AES_256_CBC.aes_encrypt(plaintext)
end = time.time()
elapsed = end - start
print ( 'Time taken: ' + str(elapsed) + 'seconds.' )
```

輸出的結果為

PyCrypto AES256 CBC Time taken: 6.45398807526seconds.

Cryptography AES256 CBC Time taken: 3.81276679039seconds.

4.4 AES-256 CTR

```
# PyCrypto_AES_256_CTR
print ( 'PyCrypto_AES_256_CTR' )
start = time.time()
encrypt = PyCrypto_AES_256_CTR.aes_encrypt(plaintext)
end = time.time()
elapsed = end - start
print ( 'Time taken: ' + str(elapsed) + 'seconds.' )

# Cryptography_AES_256_CTR
print ( 'Cryptography_AES_256_CTR' )
start = time.time()
```

```

encrypt = Cryptography_AES_256_CTR.aes_encrypt(plaintext)
end = time.time()
elapsed = end - start
print ( 'Time taken: ' + str(elapsed) + 'seconds.')

```

輸出的結果為

PyCrypto AES256 CTR Time taken: 21.1867408752seconds.

Cryptography AES256 CTR Time taken: 2.08338999748seconds.

4.5 RSA-2048

輸出的結果為

4.6 SHA-512

```

# PyCryo_SHA_512
print ( 'PyCryo_SHA_512 ')
start = time.time()
hash = PyCryo_SHA_512.hashSHA512(plaintext)
end = time.time()
elapsed = end - start
print ( 'Time taken: ' + str(elapsed) + 'seconds.')

```

```

# Cryptography_SHA_512
print ( 'Cryptography_SHA_512 ')
start = time.time()
hash = Cryptography_SHA_512.hashSHA512(plaintext)
end = time.time()
elapsed = end - start
print ( 'Time taken: ' + str(elapsed) + 'seconds.')

```

輸出的結果為

PyCrypto SHA512 Time taken: 2.17035508156seconds.

Cryptography SHA512 Time taken: 1.27641797066seconds.