python crypto安装_关于python安装pip及crypto库

weixin_39635648 于 2020-12-08 22:46:55 发布 595 收藏
文章标签： python crypto安装

Capture The Flag (CTF) 常用到的crypto库，有很多技术人员不知道怎么安装。而crypto库已经有三五年没有团队维护更新，网络上很多旧版安装方法不可用。本篇记录了作者安装pip及PyCryptodome库的过程。最新安装测试于2020.7，新版适用。Linux系统，Windows系统均有记录。

判断系统是否已安装pip：

pip --version

下载并安装pip，linux和windows系统的操作方法详见代码：

curl https://bootstrap.pypa.io/get-pip.py -o get-pip.py #下载安装脚本//Linux/Windows

运行安装脚本(此处pip关联的是python3)：

sudo python3 get-pip.py #运行安装脚本//Linux

get-pip.py //Windows

升级pip至最新版：

sudo apt-get install python-pip //Linux

pip install -U pip//Linux

sudo easy_install --upgrade pip//Linux

python -m pip install --upgrade pip //Windows

安装PyCryptodome：

pip install PyCryptodome

测试：

```
from Crypto.Cipher import AES

import base64

aes_instance = AES.new(b'密钥, AES.MODE_ECB)

cipher = base64.b64decode('密文')

plaintext = aes_instance.decrypt(cipher)

print(plaintext)

//输出明文
```

Ps：

pip常用 命令

pip --version #显示版本和路径

pip --help #获取帮助

安装包

pip install name #最新版本

pip install 'name==1.0.4' #指定版本

pip install 'mane>=1.0.4' #最小版本

升级包

pip install --upgrade name

卸载包

pip uninstall name

搜索包

pip search name

显示包信息

pip show

显示指定包信息

pip show -f name

查看已安装包

pip list -o

pip升级

pip install --upgrade pip//Linux

python -m pip install -U pip//Windows

对于包，使用==, >=, <=, >, < 以指定版本号。

PyCryptodome是PyCrypto的一个分支。基于PyCrypto2.6.1，多了以下特性：

Authenticated encryption modes (GCM, CCM, EAX, SIV)

Accelerated AES on Intel platforms via AES-NI

First class support for PyPy

SHA-3 hash algorithm

Salsa20 stream cipher

scrypt and HKDF

Deterministic DSA

Password-protected PKCS#8 key containers

Shamir’s Secret Sharing scheme

Random numbers get sourced directly from the OS (and not from a CSPRNG in userspace)

Simplified install process, including better support for Windows

Cleaner RSA and DSA key generation (largely based on FIPS 186-4)

Major clean ups and simplification of the code base