Introduction

- Objective

  Objective of this exercise is to provide a general overview of common cryptography related Python libraries and packages.

  Setting up a baseline platform (Ubuntu) to facilitate the cryptography practical exercises with Python.

- Learning Outcome
  - Understand the setup procedures of the Python and required cryptography packages.
  - Able to test and verify the setup using Python Shell.

Cryptography related libraries

- "Python 3 doesn’t have very much in its standard library that deals with encryption. Instead, you get hashing libraries."
  - Quoted from:
    - https://www.blog.pythonlibrary.org/2016/05/18/python-3-an-intro-to-encryption/
- 3rd party packages:
  - PyCrypto
  - cryptography."

hashlib

- A standard Python module that provides mainly hashing functions :
  - md5, SHA1, SHA256 ... crc32.

- Sample Usage at Python Shell:
  - Hashing a 'byte' string using MD5 algorithm.

```
>>> import hashlib
>>> h = hashlib.new("MD5")
>>> h.update(b"Hello World")
>>> h.hexdigest()
'b10a8db164e0754105b7a99be72e3fe5'
>>>
```

Crypto (or Cryptodome)

- pyCrypto
  - One of the most popuplar 3rd party packages.
  - It has been stopped since 2012.
  - module name
    - Crypto
- pyCryptodome
  - A fork from the original pyCrypto.
  - Can be used as a replacement or add on of pyCrypto.
  - Module name
    - Cryptodome

Installation options of pyCryptodome

- Option 1
  - Add on to Crypto
  - Usage
    - from Cryptodome import DES
      - This is used in the case the installation allows both Crypto and Cryptodome packages.
- Option 2
  - 1 to 1 replacement
  - Usage
    - from Crypto import DES
      - This is used in the case the installation uses Cryptodome package to replace the Crypto package.
      - May be confused.

Features and sample

- Features
  - PyCryptodome is a self-contained Python package of low-level cryptographic primitives.
    - Symmetric ciphers, Asymmetric ciphers, hashes, mode of operation, common utility functions …. Etc.
  - Complete feature list https://pycryptodome.readthedocs.io/en/latest/src/features.html
- Sample Usage at Python Shell
-

```
>>> from Cryptodome.Hash import MD5
>>> h = MD5.new()
>>> h.update(b"Hello World")
>>> h.hexdigest()
'b10a8db164e0754105b7a99be72e3fe5'
>>>
```

cryptography package

- cryptography
  - Another popular 3rd party Python package
  - Consider to be easier to use.
  - Many features are overlapping with hashlib and Cryptodome.
- Features
  - includes both high level recipes and low level interfaces to common cryptographic algorithms such as symmetric ciphers, message digests, and key derivation functions.

Sample usage at the Python Shell

```
>>> from cryptography.hazmat.backends import default_backend
>>> from cryptography.hazmat.primitives import hashes
>>> h = hashes.Hash(hashes.MD5(),backend=default_backend())
>>> h.update(b"Hello World")
>>> digest = h.finalize()
>>> for b in digest:
        print("{0:02x}".format(b),end="")


b10a8db164e0754105b7a99be72e3fe5
>>>
```

References

- hashlib
  - https://docs.python.org/3/library/crypto.html
- pycryptodome
  - https://pycryptodome.readthedocs.io/en/latest/src/introduction.html
- cryptography
  - https://cryptography.io/en/latest/