1. pycryptodome

pycryptodome
说明:
pycryptodome是一个强大的第三方工具，可以实现多种复杂的加密和解密，你可以使用pycryptodome来满足你日常的加密和解密需求。

2.安装方法

```
# 使用pip命令进行安装
# 示例
pip install pycryptodome 或 pip3 install pycryptodome
# 可指定安装源
pip install pycryptodome -i https://mirrors.aliyun.com/pypi/simple/
```

3.主要功能

pycryptodome 可实现常见的加密和解密功能，包括AES加密/解密。

4. 使用方法及相关函数

```
class new(key, mode, *args, **kwargs):
    '''创建一个AES工具，用于加密和解密。
    :参数 key:
        加密过程中使用的密钥。
        它必须是16、24或32字节长度
    :参数 mode:
        用于加密或解密的模式，常用的模式如AES.MODE_ECB;AES.MODE_CBC;AES.MODE_CFB;
    :参数 *args, **kwargs 在ECB模式中该参数无需传入(*表示以元祖形式接受参数)
    :参数 **kwargs 在ECB模式中该参数无需传入(**表示以字典形式接受参数)
    :返回值: 返回一个用于加密的AES工具。
    '''

#示例代码
# 导入模块
from Crypto.Cipher import AES
# 指定AES模式
model = AES.MODE_ECB
# 创建秘钥(一般情况下，秘钥为16个字节，你也可以使用24或者32字节)
# get_random_bytes函数可以随机生成一个指定长度的字节数据，16表示16字节
key_A = get_random_bytes(16)
# 用户指定一个长度为16字节的秘钥，b表示字节数据
key_B = b"0123456789123456"
# 创建一个AES工具用于加密和解密操作，你可以使用创建好的aes调用对应的加密和解密函数实现加密或解密功能。
```

```
ase = AES.new(key,model)
```

```
 def encrypt(plaintext):
    '''加密函数。
    :参数 plaintext:
         需要加密的明文；
         传入的参数必须是字节类型的数据；
         它必须是16字节长度的整数倍。
    :返回值: 返回一个加密完成的字节型数据。
    '''
# 示例代码
from Crypto.Cipher import AES
model = AES.MODE_ECB
# 用户指定秘钥长度为16字节
key = b"0123456789123456"
# 创建AES工具
ase = AES.new(key,model)
# 指定需要加密的明文，需要注意的是，这里必须是字节类型，字节长度必须是16字节长度的整数倍
plaintext = b"abcdefghijklmnop"
# 使用aes执行加密操作
encrypt_text = ase.encrypt(plaintext)
print("加密后的数据为:" ,encrypt_text)
# 输出: 加密后的数据为: b'\x98\xeb\x8fg1\xc8\x13\x9d\x99Z\x88\x9aS\xec\xfa\xb4'
```

```
def decrypt(ciphertext):
    '''解密函数。
    :参数 ciphertext:
         需要解密的数据
         传入的参数必须是需要是字节数据
         它必须是16字节长度的整数倍。
    :返回值: 返回一个解密完成的字节型数据。
    '''
# 示例代码
from Crypto.Cipher import AES
model = AES.MODE_ECB
key = b"0123456789123456"
# 创建AES工具
ase = AES.new(key,model)
# 指定需要解密的密文，需要注意的是，这里必须是字节类型
ciphertext = b'\x98\xeb\x8fg1\xc8\x13\x9d\x99Z\x88\x9aS\xec\xfa\xb4'
# # 使用aes执行解密操作
decrypt_text = ase.decrypt(ciphertext)
print("解密后的数据为:",decrypt_text)
# 输出: 解密后的数据为: b"abcdefghijklmnop"
```