載入套件

from Crypto.PublicKey import RSA

from Crypto.Random import get\_random\_bytes

from Crypto.Cipher import AES, PKCS1\_OAEP

輸入公鑰

public\_key = b'-----BEGIN RSA PUBLIC KEY-----\nMIGJAoGBAJUYCLRfdeaqBBcr9FXXA5d58v7jSd2hdWB/ODnmZ/EBaIY7QfF/azxP\njweOssBlVhyK6gFLq9B5NHBM6twwbrKFznHCrSOHAYxrE7AYx8l4bVwssEveyGcC\n7LivblQjkijZ+M3rMhC+ytXFpjXxMzNYULx0X1mR3QqYIZ4GwQP9AgMBAAE=\n-----END RSA PUBLIC KEY-----\n'

輸出到receiver.pem文件

file\_out = open("receiver.pem", "wb")

輸出公鑰

file\_out.write(public\_key)

關閉輸出

file\_out.close()

讀取recipient\_key，從receiver.pem文件

recipient\_key = RSA.import\_key(open("receiver.pem").read())

輸入AES金鑰

session\_key = b'isu10503301a9862'

將recipient\_key輸出到顯示器

print(recipient\_key)

用老師的RSA公鑰加密我的AES金鑰

cipher\_rsa = PKCS1\_OAEP.new(recipient\_key)

enc\_session\_key = cipher\_rsa.encrypt(session\_key)

將enc\_session\_key輸出到顯示器

print(enc\_session\_key)

b"\t$s\x14\*;\x12Q\xdfA[S\xa5\xda\xd9V\xa3\xfc\xe9 \x92\xa0\xbe\xadM\xfb\xa9W\xae\xa1\x0f\xb3\xd8\xe4\x08-6\xe9\xe0Z\xb0\xd1\x1c\x97\xf3^\x05\xcaa\x1f0\xfcx\xf8\xb2,\xc2\x98\x041KB\xc1\xdc\xd6\x92\xb35$\x18H\xcb\xe8\xca\x93\xaa\xd6\x8c'A\xb3\x1bP\xd1\xe6/W\xf5\_ta\xd1\_d8\xe5\xd6\xbd\xc6\xd6a\x82j\xa4\x1d\x94u8hg\xc7\xde\x95\xf7s\xf6\xf7Te\xa3\x1d\x9eG\xfa\xd9\x00\x87&"

將中文祝福字符寫入

cong = '祝各位前程似錦。'

data1 = bytearray(cong,'utf-8')

tcong = str(data1,'utf-8')

print(tcong)

用aes金鑰加密我的祝福話語

cipher\_aes = AES.new(session\_key, AES.MODE\_EAX)

ciphertext, tag = cipher\_aes.encrypt\_and\_digest(data1)

輸出到encrypted\_data.bin

file\_out = open("encrypted\_data.bin", "wb")

輸出以下資料

[ file\_out.write(x) for x in (enc\_session\_key, cipher\_aes.nonce, tag, ciphertext) ]

關閉輸出

file\_out.close()

print(ciphertext)

print(tag)

將加密後的aes金鑰轉換為16進制數字

myaes=int.from\_bytes(enc\_session\_key,byteorder='big')

顯示myaes

print(hex(myaes))

讀取encrypted\_data.bin

file\_in = open("encrypted\_data.bin", "rb")

讀取以下資料

enc\_session\_key, nonce, tag, ciphertext = \

[ file\_in.read(x) for x in (128, 16, 16, -1) ]

讀取加密後的祝福話語然後解密

cipher\_aes = AES.new(session\_key, AES.MODE\_EAX, nonce)

data = cipher\_aes.decrypt\_and\_verify(ciphertext, tag)

用utf8來顯示已解密完的data

print(data.decode("utf-8"))

祝各位前程似錦。

將被aes金鑰加密後的祝福話語轉換16進制然後輸出

myciphertext=int.from\_bytes(ciphertext,byteorder='big')

mytag=int.from\_bytes(tag,byteorder='big')

print(hex(myciphertext))

0x4555b518679e7c86571ab4042a38723cc7107d976173d063

print(hex(mytag))

0xcedba41ec3ee6a306a7bc9e93dfb9522

以上作業參考老師與<https://pycryptodome.readthedocs.io/en/latest/src/examples.html>

的資料實作。

   