陳奕嘉 E94115011 資訊 115

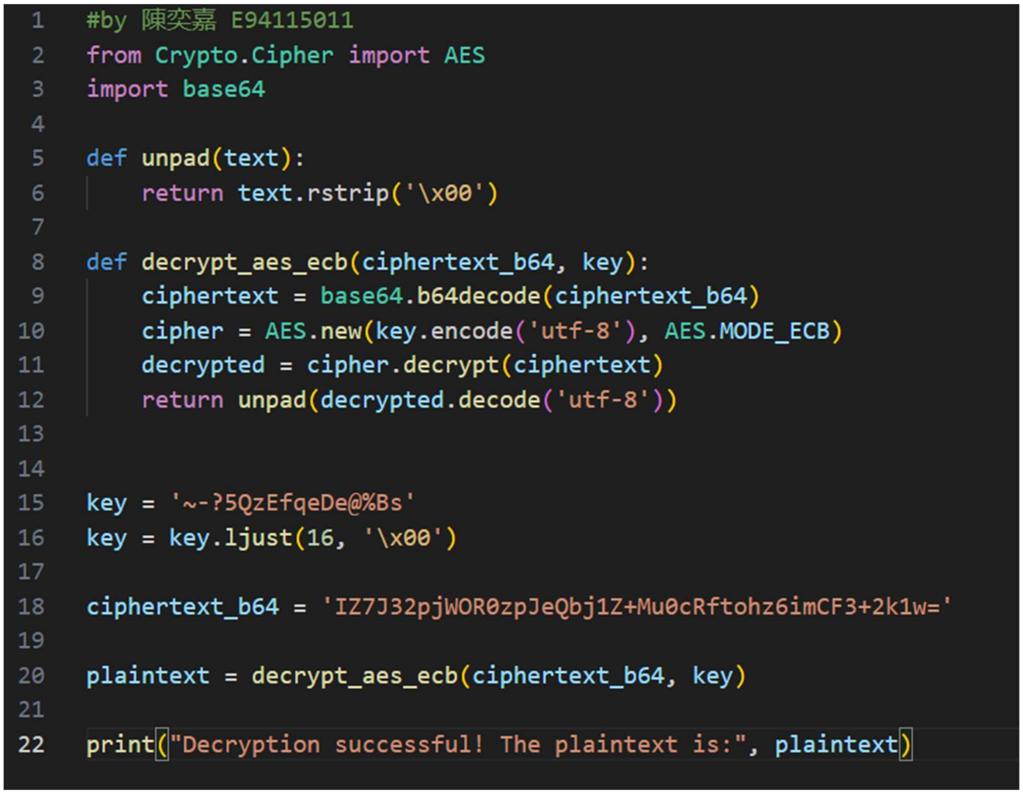
資訊安全 HW4

本人學號為 E94115011，所以解 X=1 的金鑰和明文

正確密鑰：~-?5QzEfqeDe@%Bs

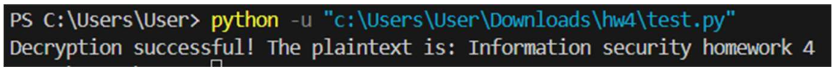
解出明文：Information security homework 4

程式碼：（自己有一份把四個空位作排列組合的程式碼，但輸出被我刪掉了，而且不想再跑多一次 ww，所以這裏只放了輸出能看得懂的明文和使用的金鑰）



```python
#by 陳奕嘉 E94115011
from Crypto.Cipher import AES
import base64

def unpad(text):
    return text.rstrip('\x00')

def decrypt_aes_ecb(ciphertext_b64, key):
    ciphertext = base64.b64decode(ciphertext_b64)
    cipher = AES.new(key.encode('utf-8'), AES.MODE_ECB)
    decrypted = cipher.decrypt(ciphertext)
    return unpad(decrypted.decode('utf-8'))


key = '~-?5QzEfqeDe@%Bs'
key = key.ljust(16, '\x00')

ciphertext_b64 = 'IZ7J32pjWOR0zpJeQbj1Z+Mu0cRftohz6imCF3+2k1w='

plaintext = decrypt_aes_ecb(ciphertext_b64, key)

print("Decryption successful! The plaintext is:", plaintext)
```

解出畫面：



```
PS C:\Users\User> python -u "c:\Users\User\Downloads\hw4\test.py"
Decryption successful! The plaintext is: Information security homework 4
```