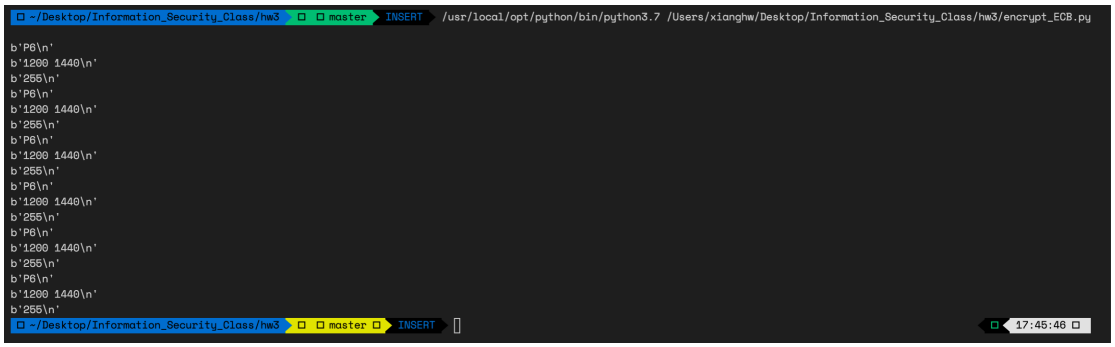
B10615056 黃暉翔

分工：加密

建置環境：　python VScode
執行結果截圖：



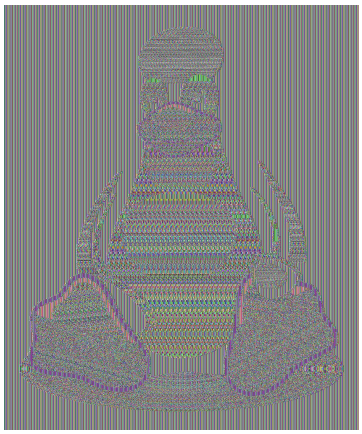
操作方式：

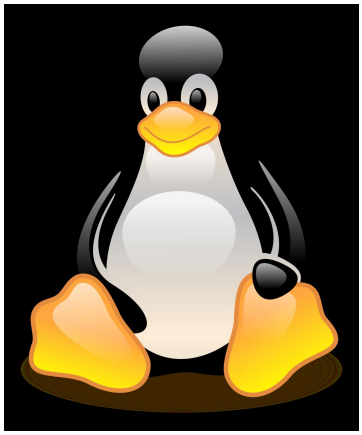
　　程式會開啟在同目錄下的photo.png，產生ppm檔，再經過三種MODE的加解密後產生相對應的ppm跟jpg檔。

執行結果圖：

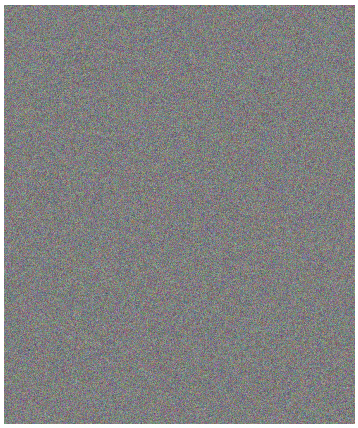
原圖：

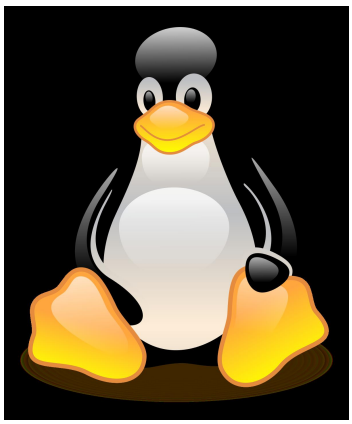
EBC：



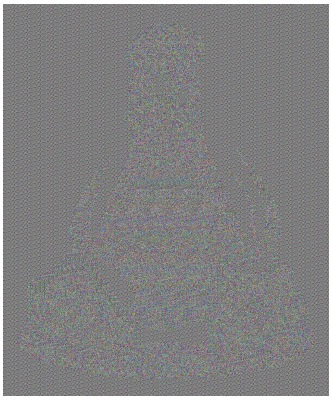


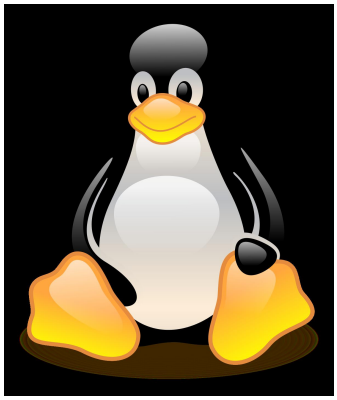
CBC：





COOL：





程式碼解說：

三種模式都先開PPM檔

```
f = open('EBC_encrypt.ppm','rb')
output = open('EBC_decrypt.ppm','wb')
```

開啟block

```
cipher_block = AES.new(key,AES.MODE_ECB)
```

讀取輸出前三行PPM的格式

```
for i in range(3):
    data = f.readline()
    output.write(data)
    print(data)
```

持續讀取PPM檔直到EOF，每次讀取16bytes = 128bits = 1 block

```
data = f.read(16)
while data:
```

避免最後一個block不夠16bytes，後續補0直到16bytes

```
    if len(data) < 16:
        pd = 16 - len(data)
        for i in range (pd):
            data += bytes([0])
```

Cool：先說明我們第三個mode的作法，是將CBC中的IV向右roll 1 bit

跟CBC一樣先進行跟IV XOR在加密

```
temp = []
for d,i in zip(data ,iv):
        temp.append((d ^ i) % 256)
data = bytes(temp)
cipher = cipher_block.encrypt(data)
```

```
output.write(cipher)
```

接著將IV向右roll 1 bit，並讀取下個block

```
temp = iv[15:16]
temp += iv[:15]
iv = bytes(temp)
data = f.read(16)
```

在每個mode最後，關檔並且將加解密後的ppm另存jpg以便檢視

```
f.close()
output.close()
jpgPicture = 'Cool_encrypt.jpg'
im = Image.open('Cool_encrypt.ppm')
im.save(jpgPicture)
```

遇到困難與心得：

python 在裝cypryto的時候花了一些時間，再來只要知道ppm的格式然後再按照相應的架構圖實作就沒什麼問題了。