HW3

2019/11/14

Github 專案整理

- 在同一個專案下建立新資料夾 HW3 存放作業三

Programing Language

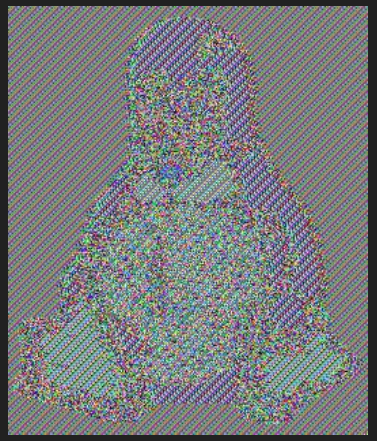
- C
- Python
- C++

作業繳交

- 程式碼部分 - github
- 說明文件部分 - moodle

Problem

- Use AES to encrypt/decrypt a Picture
  - ECB mode
  - CBC mode
  - Find a cool mode or design your own block cipher mode


作業注意事項

- 由於要讓 ECB 加密完能夠看出是隻企鵝，所以我們必須要將圖片轉成 ppm 格式再進行加密
- 看懂 ppm 這個格式是怎麼儲存圖片的，這樣你才會知道哪些要加密哪些不能加密（像是紀錄長寬之類的地方）
- 加密部分可以使用 library 但是每次能放入加解密函式的 plaintext 只能是一個block，block 與 block 間的運作要由自己處理，不能整段plaintext 一次丟進加解密函式執行
- 由於這個作業蠻簡單的，所以第三小題希望大家能花點心思跟組員討論

Ppm format introduction

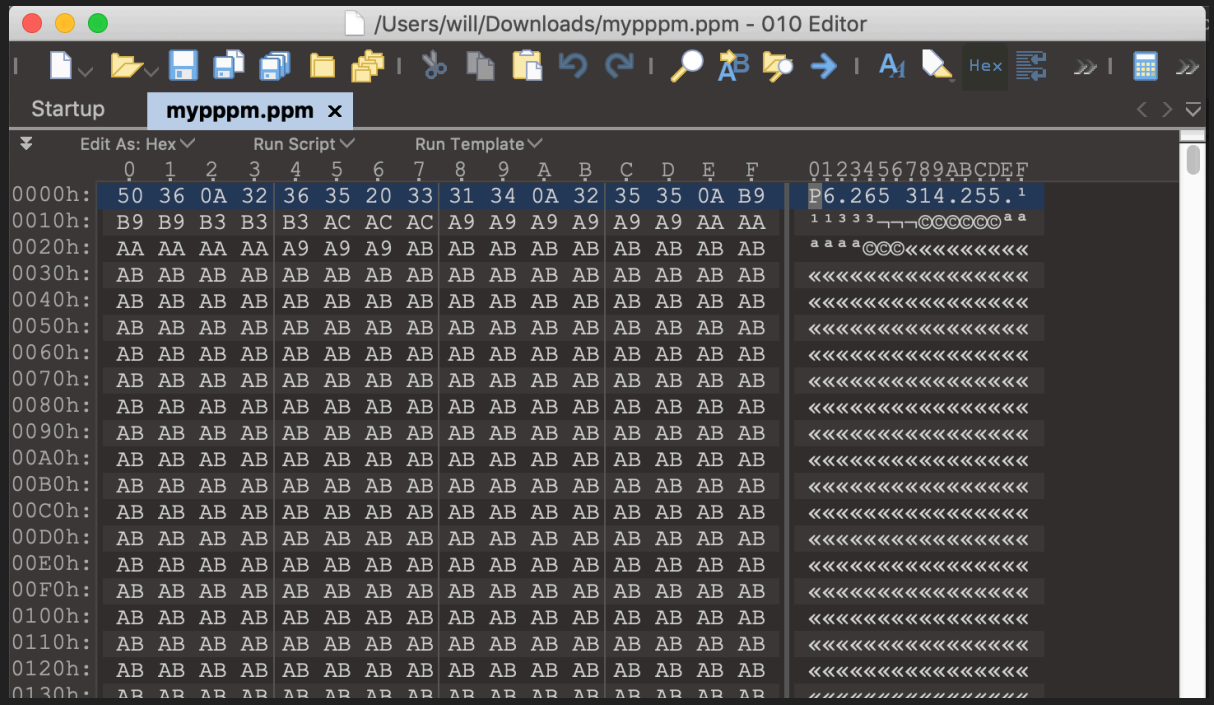
- PPM 用在彩色的像素圖
- 用三個 bytes 代表一個像素
- 三個 bytes 對應的就是 RGB 三原色

- Reference: https://zh.wikipedia.org/wiki/PBM格式

如何觀察檔案的 hex

- 下載 101 editor (網路上有很多種 請搜尋：hex viewer)
  https://www.sweetscape.com/download/010editor/
- 安裝完後把你要的檔案丟進去
- 就可以觀察檔案的每一個byte的資訊了

（圖例為ppm格式的檔案）



ppm 與 其他圖片格式 轉換

- Python 有套件可讓 png 和 jpg 轉為 ppm 格式
- 安裝：pip install Pillow

```
ppmPicture = "./mypppm.ppm”)
im = Image.open('./restart.jpg’ )
im.save(ppmPicture)
```

JPEG -> PPM

```
ppmPicture = "./restartppm.ppm”
im = Image.open(ppmPicture)
im.save('./restart.png', 'png')
```

PPM -> JPEG

Padding method

- 不限定
- 將所使用的 padding 紀錄在文件中

AES Crypto Library

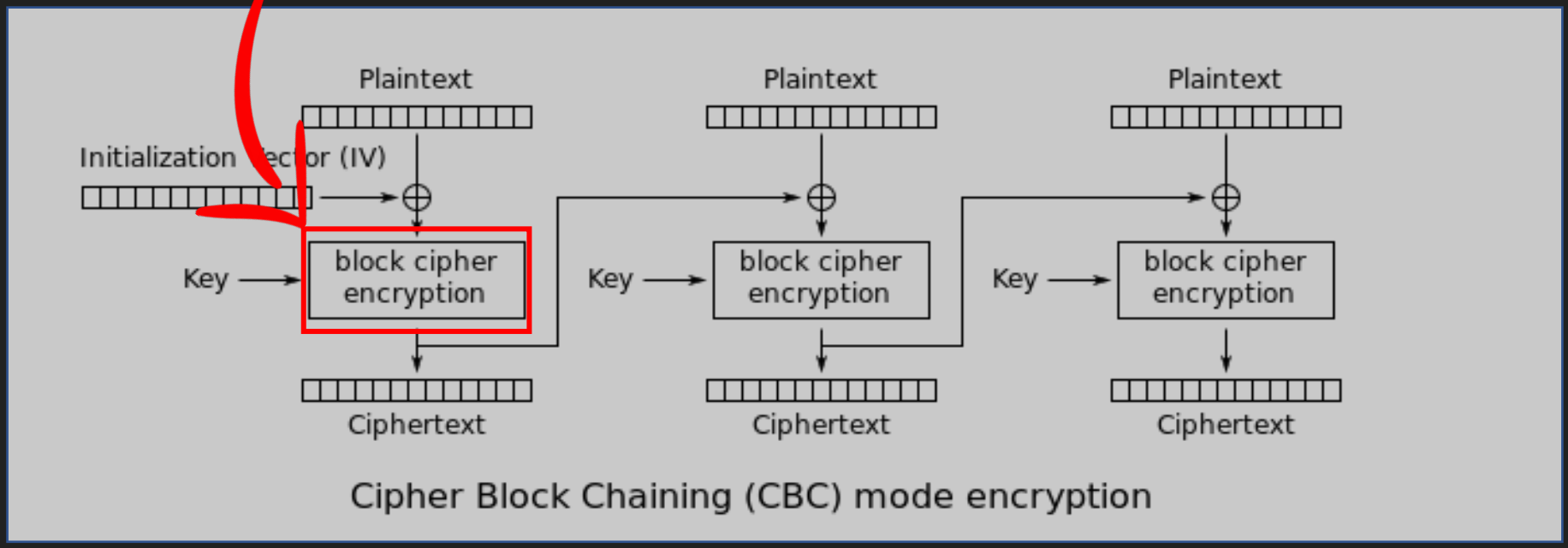
- 安裝: pip install pycryptodome (windows ok)

```
import Crypto.Cipher import AES

cipher = AES.new(key, AES.MODE_ECB)

ciphertext = cipher.encrypt(one_block_text)
```

- Reference: https://blog.csdn.net/five3/article/details/86160683?fbclid=IwAR0hNwGrJsXzT1vqvnfFl5IRmqx-2Scxq_ZFa5twnYeRpHyLlZfsDBnk7FY

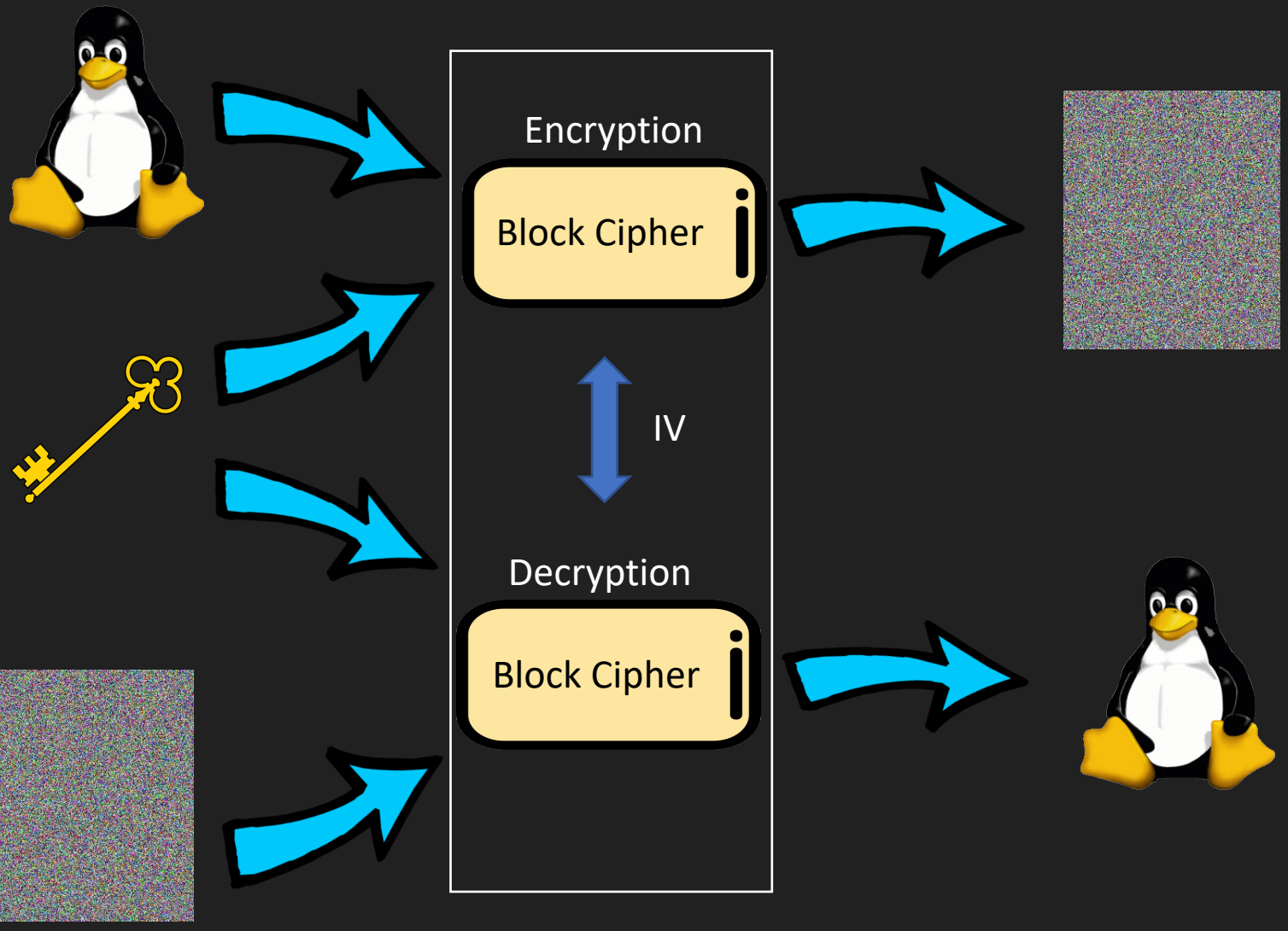
AES Library 使用限制

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

ciphertext = cipher.encrypt(one_block_text)
```



每一個 block 的 cipher encryption 可以用 library 來做但其他機制請自己做

Example



Input & Output

- 沒有限定格式 (請在文件中說明如何使用)
- Input output 的圖片可以是任何常見格式 (擇一即可)
  - GIF JPEG BMP

說明文件部分

- 每個人單獨寫一份

- 請在文件中說明
  - 分工
  - 建置環境
  - 操作方式
  - 執行結果圖
  - 程式碼解說
  - 遇到困難與心得

注意事項

- 請寫 c 或 c++ 的同學要記得編譯出可執行檔，我會依據你的說明文件所提供的開發環境進行測試
- 如果想再補交請寄信通知我
- 上傳說明文件時請把檔名改成 [Student ID]_HW3_report.pdf

評分標準

- 說明文件 (70%)
- 程式 (30%)