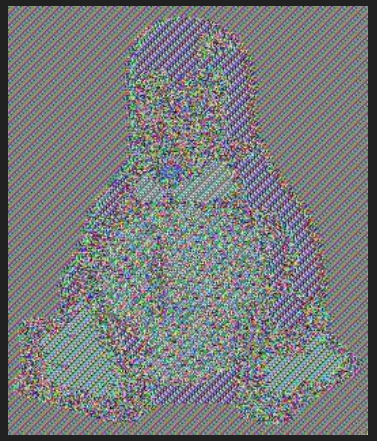
HW3

2021/05/11

Problem

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


Programing Language

- C
- Python
- C++

作業繳交

- 以 [Student ID]_HW3.zip 包含以下檔案
  - README.pdf: 說明文件
  - 以 python 寫作的內容如下
    - enc.py / dec.py: 加密/解密程式碼
  - 以 C/C++ 寫作的內容如下
    - enc.[c / cpp] / dec.[c / cpp]: 加密/解密程式碼
    - enc / dec: 加密/解密執行檔
  - Makefile: 請見後面投影片敘述
  - img 目錄
    - ECB.jpeg : 以 ECB 加密過後的圖片
    - CTR.jpeg : 以 CTR 加密過後的圖片
    - Custom.jpeg : 以自訂方式加密過後的圖片
- 每個人都須 moodle 上傳
- 圖片使用 linux.jpeg

評分標準

- 說明文件 (40%)
- 程式 (30%)
- 輸出 image (30%)

- 助教會於 Ubuntu 20.04 上進行測試

套件使用規則

- 本次作業期望讓大家熟悉各種 Block Cipher Operation
- 因此開放使用套件，但只能使用套件一次加密一個 Block

說明文件

- 每個人單獨寫一份
- 文件中需要說明
  - 分工
  - 建置環境/依賴套件
  - 操作方式
  - 程式碼解說
  - 自行設計的 Block Cipher Operation 的架構圖
  - 遇到困難與心得

Makefile

- 執行 make install 後
  - 安裝依賴的套件
- 執行 make enc 後
  - 創造一個 test_enc 目錄
  - 將三種模式加密過後的圖片存放於 test_enc 目錄
  - 圖片名稱分別為
    - ECB.jpeg
    - CTR.jpeg
    - Custom.jpeg
- 執行 make dec 後
  - 創造一個 test_dec 目錄
  - 將三種模式解密過後的圖片存放於 test_dec 目錄
  - 圖片名稱如上

Input & Output

- 沒有限定格式 (請在說明文件中的操作方式敘述)
- e.g.
  - ./enc.py linux.jpeg -o EBC.jpeg -m EBC
  - ./enc -f linux.jpeg --mode EBC

Padding method

- 不限定
- 將所使用的 padding 紀錄在說明文件中

Hint

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

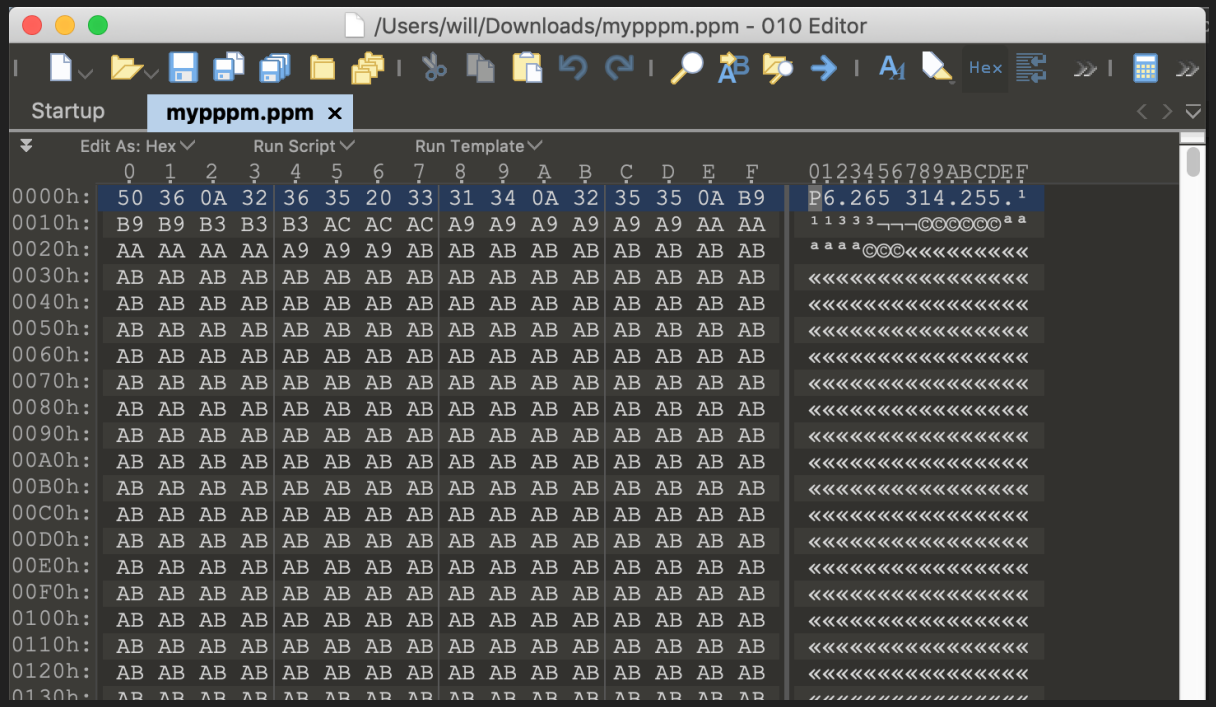
- PPM 用在彩色的像素圖
- 用三個 bytes 代表一個像素
- 三個 bytes 對應的就是 RGB 三原色

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

如何觀察檔案的 hex

- 下載 101 editor (或其他的 hex editor)
  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

AES Crypto Library

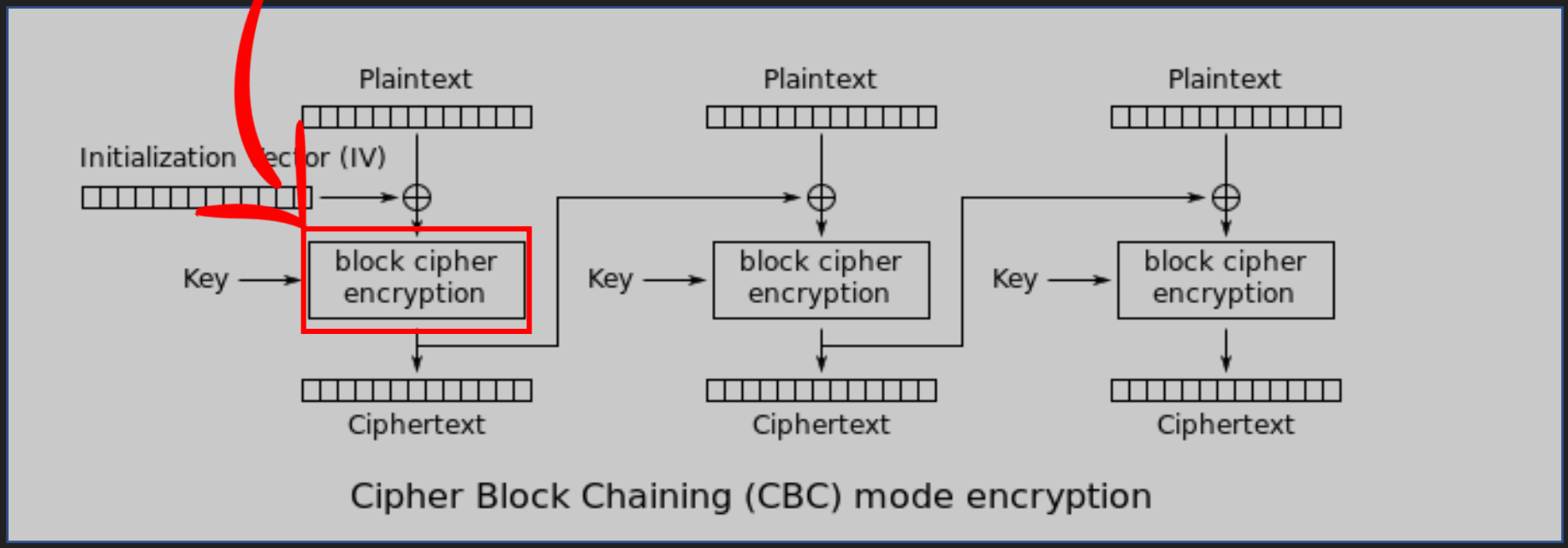
- 安裝: pip install pycryptodome (windows ok)

```
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