Information Security HW3

B10630436 林玉庭
B10632026 吳苡瑄

開發環境

Windows10 Python3

操作說明

- 直接輸入 `python AES.py`
  - 使用linux企鵝圖片
  - 使用hellomynameiskey作為key
- 指定加解密圖片 `python AES.py kabo.py`
  - 參數為圖片名稱
  - 使用預設key
- 指定加解密圖片及key `python AES.py hellomynameiskey`
  - 參數輸入圖片名稱及欲使用之key

程式流程

- key長度
  - 若非使用default key，會調整長度到16 bytes
  - 過長，取前16 bytes
  - 過短，補上'x'
- 照順序進行ECB、CBC、OFB三種加解密並show出結果圖片
- 先進行padding
  - 使用 `np.zeros()` 補上到16的整數
- reshape成16 bytes一組的nparray
- 進到各自的加解密function
- show出加密及解密的圖片

加解密

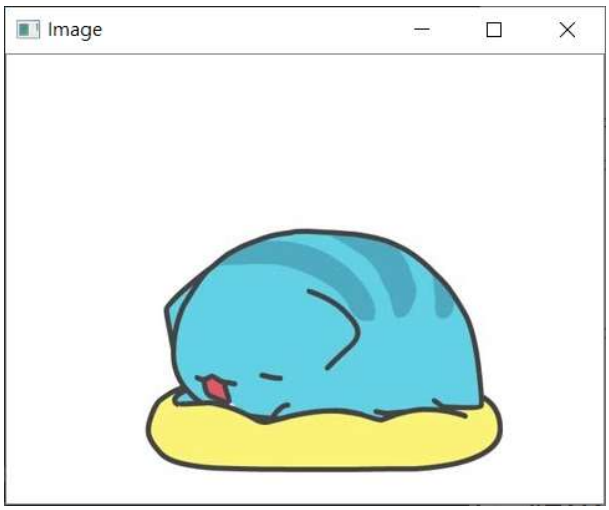
- ECB
  - 直接使用 `AES.new(key, AES.MODE_ECB)` 即可
- CBC

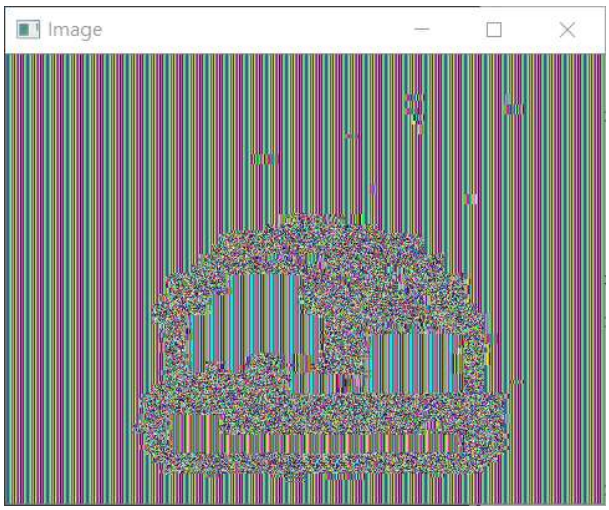
    - 加密
        - 先將plaintext及iv做xor
        - 使用 `AES.new(key, AES.MODE_ECB)` 加密
        - 每輪結束更新iv成當輪密文
    - 解密
        - 先decrypt
        - 再跟iv做xor
        - 把當輪密文作為下一輪的新iv
- OFB
    - 加密
        - 先將iv和key加密
        - 再跟明文做xor
        - iv和key加密的結果為下一輪的iv
    - 解密
        - 和加密基本上一樣
        - 除了做xor的從明文換成跟密文

結果

```
python AES.py kabo.jpg kabokabo
```

- plain、ECB、CBC、OFB






Image


Image