學號：F74036467
系級：資訊107級
姓名：李至青

開發環境：Eclipse 4.5.1
執行環境：OSX 10.11.2, JRE 8

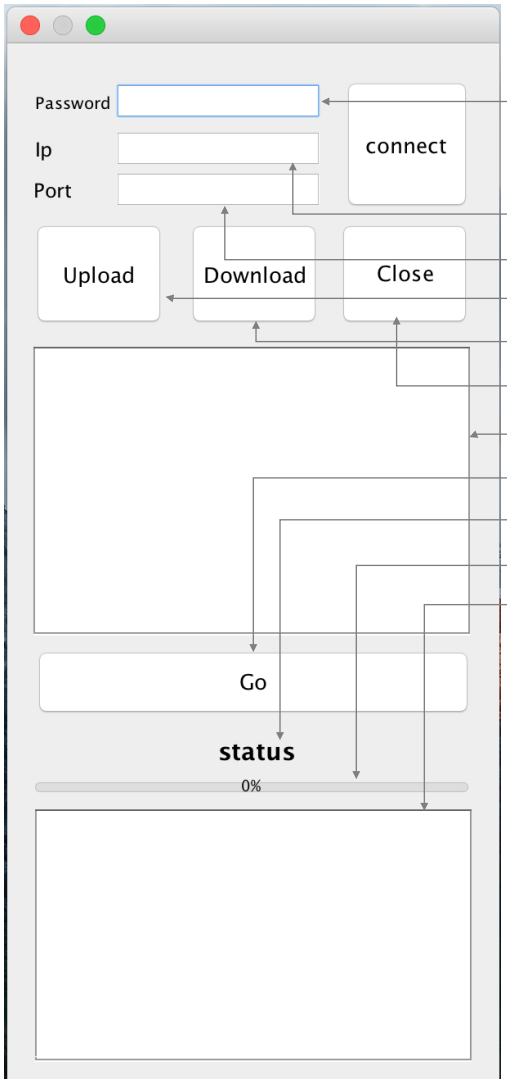
目錄：程式特色｜程式截圖｜操作說明｜檔案說明｜詳細實作方法

程式特色：

1. 使用MAKA驗證雙方身份
2. 使用EZprivacy實作的上傳以及下載檔案功能
3. GUI

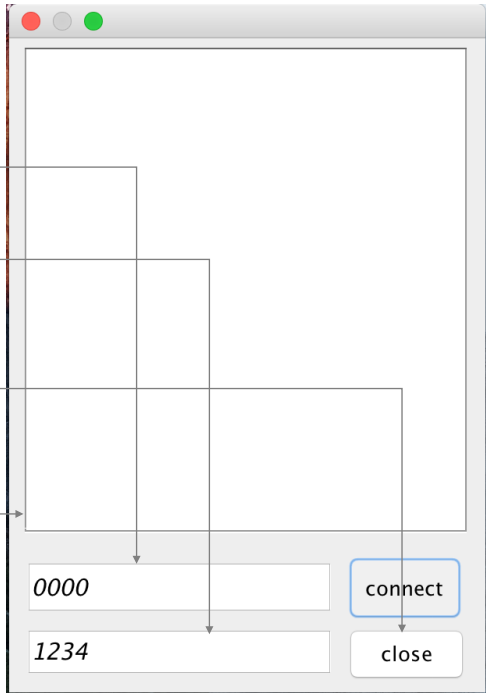
程式截圖：（註：在windows執行會跑版，還請助教調整一下邊界即可正常顯示）

▼ client端

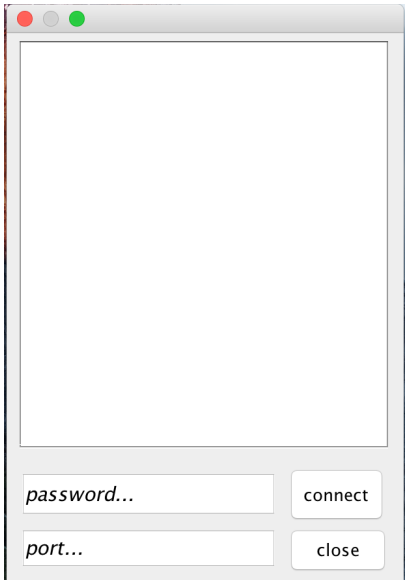


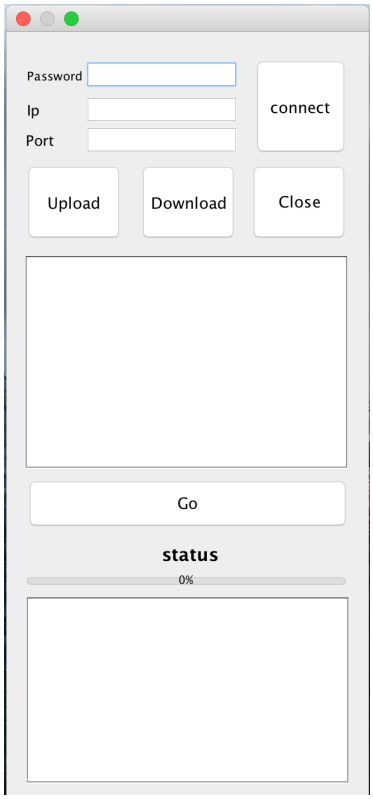
輸入EZcard密碼
輸入欲連接的IP
輸入port
上傳模式
下載模式
關閉連線
檔案清單
上傳/下載
狀態列
進度條
狀態文字

▼ server端

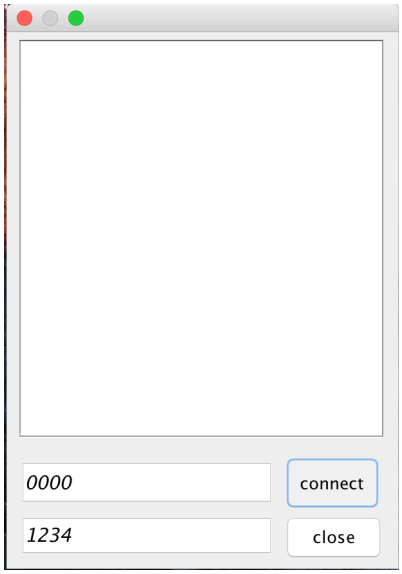


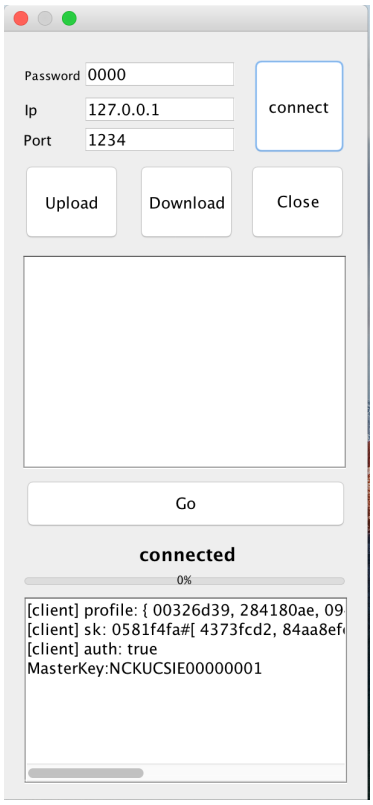
操作說明：
(0)預備環境：server.card與client.card放置於同一目錄，並將ms.k(masterKey)放置於client資料夾內
註：交上的壓縮內有附上ms.k : NCKUCSIE00000000
(1)連接
1. 打開server及client程式





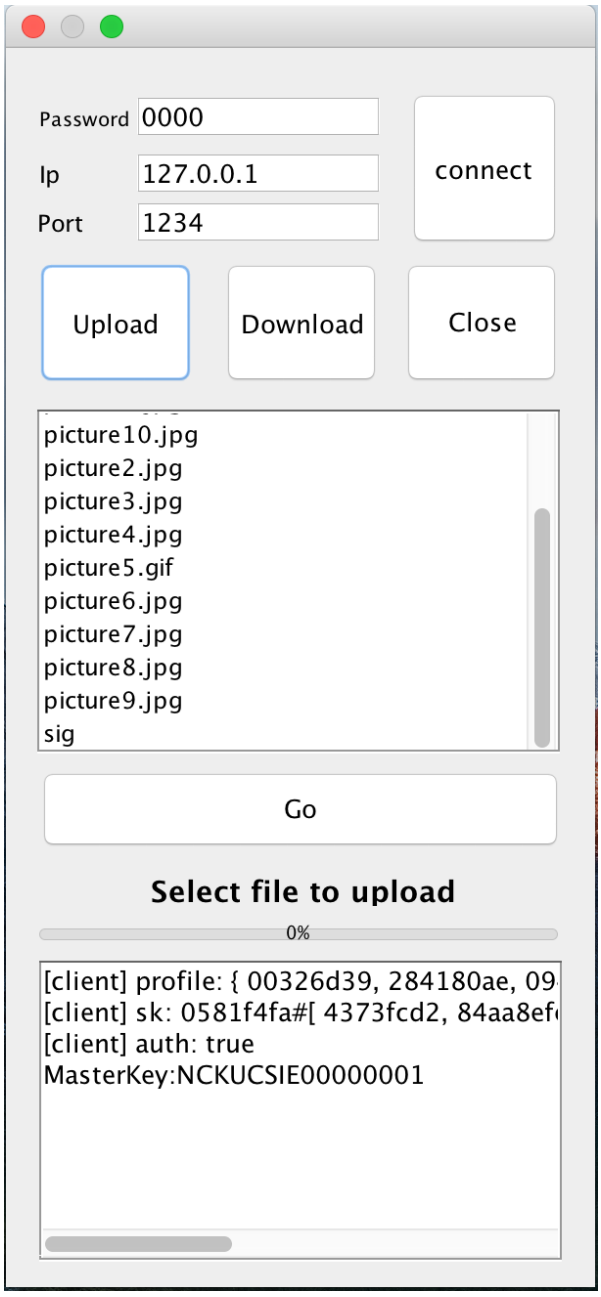
2. 在server端輸入EZcard的密碼以及port，點擊connect。然後再client輸入EZcard的密碼，以及server的ip以及port，點擊connect。
（註：EZcard必須放置與程式同一個目錄，並且命名為server.card/client.card）

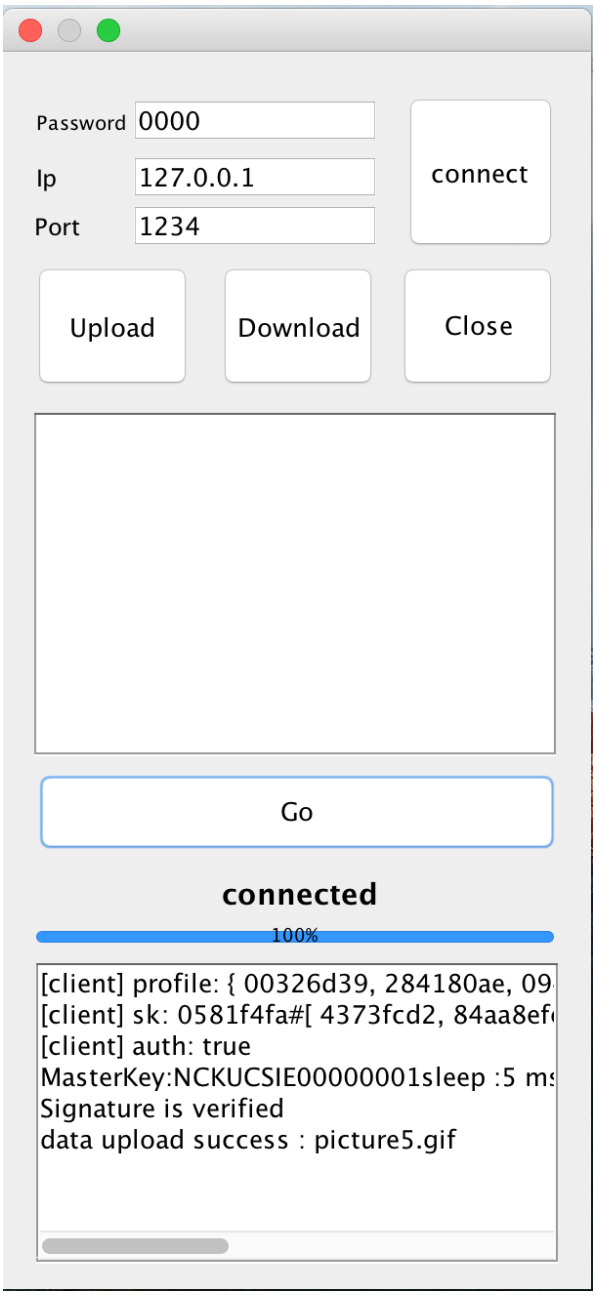




(2)client上傳檔案

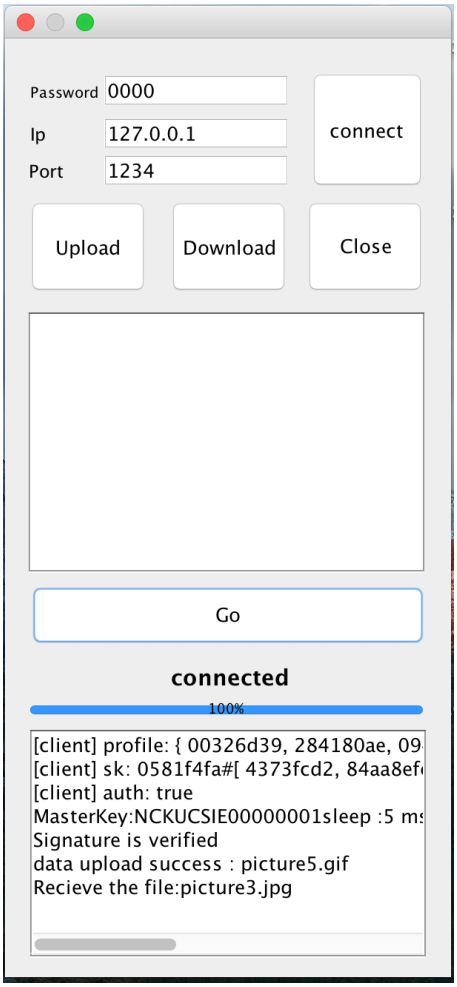
建立連線後，client點擊upload，即會顯示放置於client資料夾下的檔案清單，選取後，在點擊GO，即開始上傳。





(3)client檔案下載

建立連線後，client點擊download，即會顯示server的檔案清單，選取後，在點擊GO，即開始下載。



(4) 會造成當機的狀況

在選了Upload/Download模式後，沒有輸出/下載檔案，再選了另外一個模式。

(5) 當機處理

請將程式雙雙關閉，重新連線。

檔案說明：

(1)server
-> server.card

-> server (資料夾) -> 檔案密文（含IND）

(2)client
-> client.card

-> client (資料夾) -> 待上傳的檔案
-> ms.k (MasterKey明文)
-> fk (資料夾) -> <filename>.fk (以MasterKey加密後的金鑰)
-> sig (資料夾) -> <filename>.sig (收到的簽章)

詳細實作方法：

(1) 金鑰管理

Session Key : 用來進行MAC的金鑰。由MAKA產生，Client與Server共有，其餘金鑰僅有Client有。
Master Key： 是用來加密FileKey的金鑰。由client端自行準備，以明文儲存在client資料夾內，並更名為ms.k。
File Key：檔案加密使用的金鑰。隨機產生，以Master Key加密後，以<filename>.fk儲存在cilent / fk資料夾內。

(2) 檔案上傳

1. MAKA
雙方認證身份，取得Session key。

2. Client加密
Client隨機產生檔案金鑰，以檔案金鑰使用EZprivacy的 authEncrypt 加密檔案。
(在下載後 authDecrypt解密，確保檔案完整性。)

3. Client傳輸
Client將 2 所得的檔案密文，再以 Session Key 作 authEncrypt。然後Client傳輸Session Key加密後的檔案密文與檔名明文給Server。
（此時是將以檔案金鑰加密過後的密文與IND，一同再以Session Key作auth加密，傳輸給Server驗證作為Mac。）

4. Server儲存
Server收到檔案後，將檔案密文以Session Key做解密，驗證成功後，得到以File Key加密的密文。儲存資料並回傳簽章。

5. Client儲存
Client驗證簽章後，將簽章儲存，並用Master Key加密檔案金鑰，儲存檔案金鑰的密文。

(3) 檔案下載

1. MAKD

雙方認證身份，取得session key。

2. Client要求檔案

Client將檔案名稱明文傳送給Server。

3. Server傳輸

Server找到要傳輸的檔案密文，再以Session Key做authEncrypt (MAC) ，然後傳送給Client。

4. Client驗證

Client接收檔案，然後將檔案密文以Session Key解密驗證通道完整性，再以Master Key解開對應的File Key，然後用 File Key 對檔案密文authDecrypt，驗證檔案完整性，同時得到檔案明文，輸出檔案。