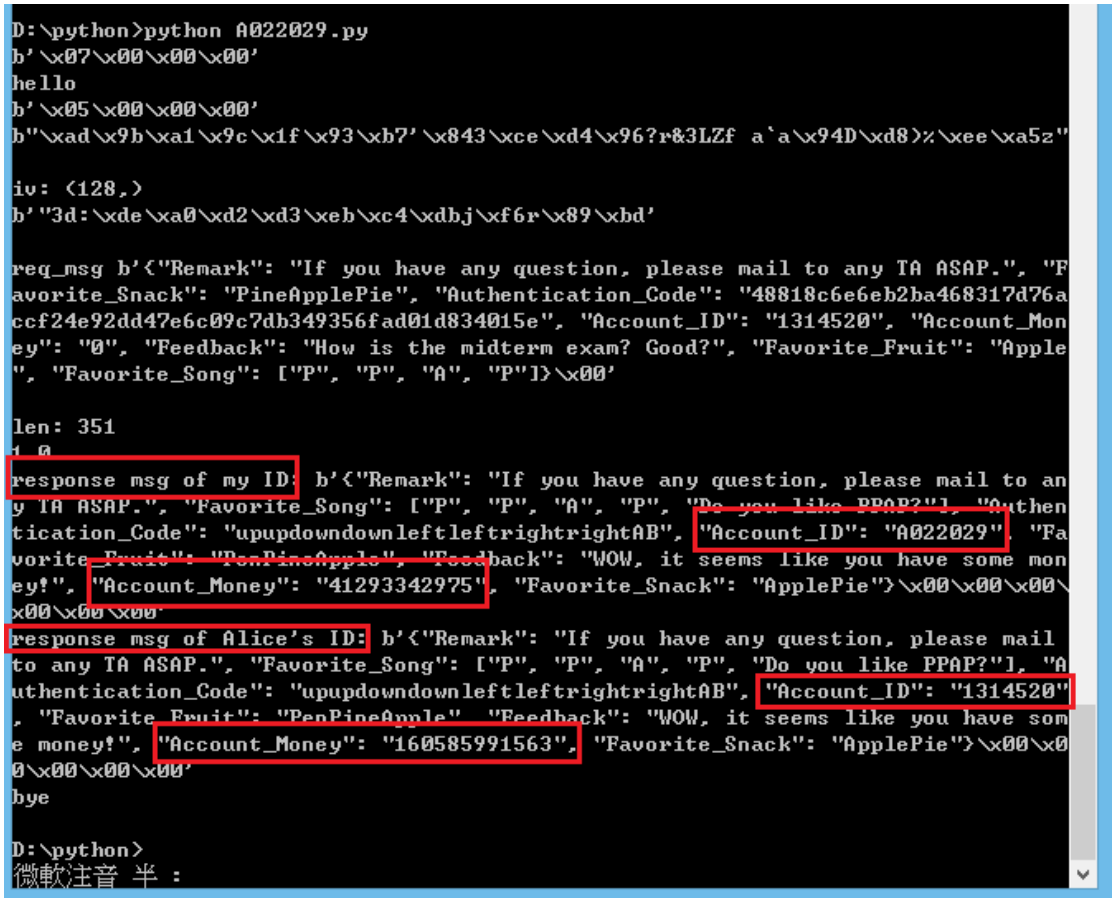

Alice's Money : 160585991563

My Money: 41293342975

ARP Spoofing:

是一種網路攻擊的技術。藉由偽造 ARP Reply，讓網路上的某些機器錯誤地把 ARP table 裡特定的 IP 位址對應的 MAC address 換成攻擊者的 MAC address，藉此讓攻擊者能夠截獲某些原本不應該導向它的流量。具體流程如下：

1. 攻擊者首先聆聽區域網路上的 ARP Request。當它收到兩台機器 A B 的 Flood 過來的 ARP Request 就可以開始攻擊。
2. 攻擊者傳送一個偽造的 ARP Reply 給 B，裏頭的 Sender IP 是 A，而 Sender MAC 卻是攻擊者的 MAC Address
3. B 更新自己的 ARP Table
4. B 之後要傳送給 A 的封包在送到交換器的地方時會被轉送給攻擊者

(以上簡單假設三者都在同一個 LAN 內)

ARP 欺騙亦有正當用途。其一是在一個需要登入的網路中，讓未登入的電腦將其瀏覽網頁強制轉向到登入頁面，以便登入後才可使用網路。

The way to generate authentication code:

首先先在不更改 authentication code 的狀況下直接把 request message 傳給 Bob，得到 Response 後確認裏頭的 Feedback。猜測應該是使用 SHA-256。於是使用下面這段 CODE 來產生我要傳給 Bob 來要取我的 Money 資訊的 Message

```
mstr = str(req_msg,"utf-8")
strlen = len(mstr)
while mstr[strlen-1]=='\0':
    strlen = strlen-1

json_str = mstr[0:strlen]
print()
#print("json:L",json_str)
json_data = json.loads(json_str)
#print("jsondata:",json_data)
json_data['Account_ID'] = "A022029"
digest = hashes.Hash(hashes.SHA256(), backend=default_backend())
digest.update(b"A022029")
code = digest.finalize()
json_data['Authentication_Code'] = str(binascii.hexlify(code),"utf=8")

final_obj = json.dumps(json_data)
```

req_msg 是解密後的 Alice 的 request message。首先把後面的 padding 拿掉，接著轉換成 json 格式，更改 Account_ID 成自己的學號，用 python cryptography library 裡的 hashes.Hash，指定雜湊函式為 SHA-256 接著產生雜湊值。不過這邊我必須先用 binascii.hexlify 把產生出來的雜湊值用 16 進為字串表示再放入 json 裡的 Authentication_code 欄位中，再傳給 Bob。

Compile 的方法：

在可以執行 python 的環境下執行 python A022029.py 就可以了。(要先確認環境中有 python 的 cryptography 函式庫可以 import)