

1. 請加入引入檔於程式中，

例(Ex): `#include "TCPIP_Sync.cpp"`
`#include "MD5.c"`

2. 使用 TCP(Port=6000)連線伺服器 140.113.144.227。

例(Ex): `Start_TCP_Client(...)`

3. 請使用下列格式送出註冊指令(REGISTER/姓名/學號)。

範例: `strcpy_s(S1, "REGISTER/王大明/1090123");`
`send(Sock, S1, strlen(S1), 0);`

4. 您將收到 “註冊成功/16-Bytes Hash” 之訊息

範例: “註冊成功/3df5e3812619a480202795efbedc693a”

此 16-Bytes Hash 是由介於[0~32767]整數經過 200 次 MD5 攪亂(Hash)之結果
以 “16146” 為例，遞迴將輸出再帶進輸入跑 200 次:

```
1st: MD5_Encoder( "16146" , Resp); //Resp= "b996f9609f0750e3bbdf52445a22cfc1"
2nd: MD5_Encoder( "b996f9609f0750e3bbdf52445a22cfc1" , Resp); //Resp= "890a752b53cdbbddd7828c143b2ecd41"
3rd: MD5_Encoder( "890a752b53cdbbddd7828c143b2ecd41" , Resp); //Resp= "2dcbb3071e04a985896022f96f05cc41"
4th: MD5_Encoder( "2dcbb3071e04a985896022f96f05cc41" , Resp); //Resp= "b781c41ec0f4c54b1717d912983d2f0d"
...
200th: MD5_Encoder( "99e10ad82c7ac65a5b7e0605bd3b01e7" , Resp); //Resp= "3df5e3812619a480202795efbedc693a"
```

註 1: 也就是說 “16146” 做 MD5 演算法 200 次，可以得到 “3df5e3812619a480202795efbedc693a” ，
 $MD5^{200}(\text{“16146”}) = \text{“3df5e3812619a480202795efbedc693a”}$

註 2: 而 MD5 是一個不可逆的雜湊函式，若獲得 $Resp = \text{“3df5e3812619a480202795efbedc693a”}$ ，想要逆向推出 “16146” 是不可能的，只能用暴力破解法將 0~32767 間之值一個個帶入遞迴算 200 次，看誰的產出符合 Resp

5. 您在第 4 步收到的 16-Bytes Hash 是由一個介於[0~32767]之數字(Key)經過 200 次 MD5_Encoder 所產生的 Hash，因此您必須在第 4 步收到 16-Bytes Hash 後，利用暴力攻擊法找出介於[0~32767]之 Key。(註:暴力攻擊需要十餘秒時間計算出 Key)
6. 使用下列指令格式將找出的 Key 傳給伺服器
例: “ANSWER/姓名/學號/Key”
範例: `sprintf_s(S1, "ANSWER/王大明/1090123/%d", Key);`
`send(Sock, S1, strlen(S1), 0);`
7. 請接收伺服器回傳之作答結果