

一、凱薩密碼加密解密

Main function :

先判別要執行哪項功能(加密、解密、離開)，再輸入字串

```
while(1){
    cout << "請選擇要加密還是解密(加密請按1, 解密請按2, 離開請按其他數字) : ";
    cin >> com;

    //判別加密、解密、離開
    if(com == 1){ //加密
        cout << "請輸入key(為數字) : ";
        cin >> key;

        cin.get(); //清除cin剩餘的字

        cout << "請輸入所要加密的字串 : ";
        getline(cin, str);

        encode(key, str);
    }
    else if(com == 2){ //解密
        cout << "請輸入key(為數字) : ";
        cin >> key;

        cin.get(); //清除cin剩餘的字

        cout << "請輸入所要解密的字串 : ";
        getline(cin, str);

        decode(key, str);
    }
    else{ //離開
        break;
    }
}
```

Encode function :

加密方程式，將字串加密並印出 output

```
void encode(int key, string str){
    int ascii;
    int number;
    //依序編碼
    for(int i = 0; i < str.length(); i++){
        if(str[i] >= 'A' && str[i] <= 'Z'){
            ascii = str[i] - 'A';
            number = mod(1, key, ascii);
            str[i] = number + 'A';
        }
        else if(str[i] >= 'a' && str[i] <= 'z'){
            ascii = str[i] - 'a';
            number = mod(1, key, ascii);
            str[i] = number + 'a';
        }
    }
    cout << "output : " << str << endl << endl;
}
```

Decode function :

解密方程式，將字串解密並印出 output

```
void decode(int key, string str){
    int ascii;
    int number;
    //依序編碼
    for(int i = 0; i < str.length(); i++){
        if(str[i] >= 'A' && str[i] <= 'Z'){
            ascii = str[i] - 'A';
            number = mod(2, key, ascii);
            str[i] = number + 'A';
        }
        else if(str[i] >= 'a' && str[i] <= 'z'){
            ascii = str[i] - 'a';
            number = mod(2, key, ascii);
            str[i] = number + 'a';
        }
    }
    cout << "output : " << str << endl << endl;
}
```

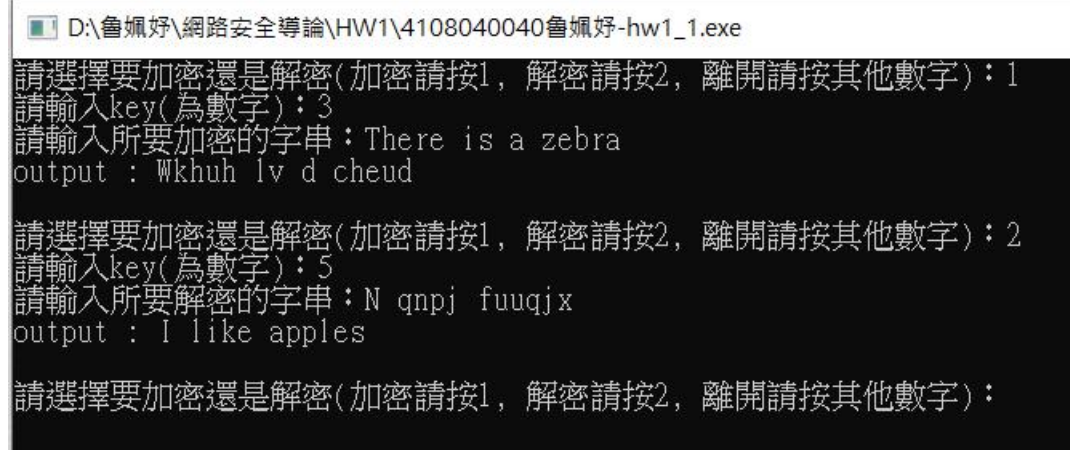
Mod function :

加密：將字元的 ascii code 加上 key 並 mod 26

解密：將字元的 ascii code 減掉 key 並 mod 26

```
int mod(int code, int key, int ascii){
    int number;
    int asciiNum;
    if(code == 1){
        asciiNum = ascii + key;
        while(asciiNum < 0){
            asciiNum = asciiNum + 26;
        }
        number = asciiNum % 26;
    }
    else if(code == 2){
        asciiNum = ascii - key;
        while(asciiNum < 0){
            asciiNum = asciiNum + 26;
        }
        number = asciiNum % 26;
    }
    return number;
}
```

Output result :



```
D:\魯佩好\網路安全導論\HW1\4108040040魯佩好-hw1_1.exe
請選擇要加密還是解密(加密請按1, 解密請按2, 離開請按其他數字): 1
請輸入key(為數字): 3
請輸入所要加密的字串: There is a zebra
output: Wkhuh lv d cheud

請選擇要加密還是解密(加密請按1, 解密請按2, 離開請按其他數字): 2
請輸入key(為數字): 5
請輸入所要解密的字串: N qnpj fuuqjx
output: I like apples

請選擇要加密還是解密(加密請按1, 解密請按2, 離開請按其他數字):
```

二、使用暴力法破解不知道 key 的密文

Main function :

輸入字串並用 for 去跑 1~25 的 key

```
string str;

while(1){
    cout << "請輸入字串(輸入exit為離開) : ";
    getline(cin, str);

    if(str.compare("exit") == 0){
        break;
    }

    for(int i = 1; i < 26; i++){
        decode(str, i);
    }

    cout << endl;
}

system("pause");
return 0;
```

Decode function :

解碼方程式，使用傳入的 key 和 string 來解密並印出 output

```
void decode(string str, int key){
    int ascii;
    int number;
    // 依序解碼
    for(int i = 0; i < str.length(); i++){
        if(str[i] >= 'A' && str[i] <= 'Z'){
            ascii = str[i] - 'A';
            number = mod(key, ascii);
            str[i] = number + 'A';
        }
        else if(str[i] >= 'a' && str[i] <= 'z'){
            ascii = str[i] - 'a';
            number = mod(key, ascii);
            str[i] = number + 'a';
        }
    }
    cout << "key = " << key << " : " << str << endl;
}
```

Mod function :

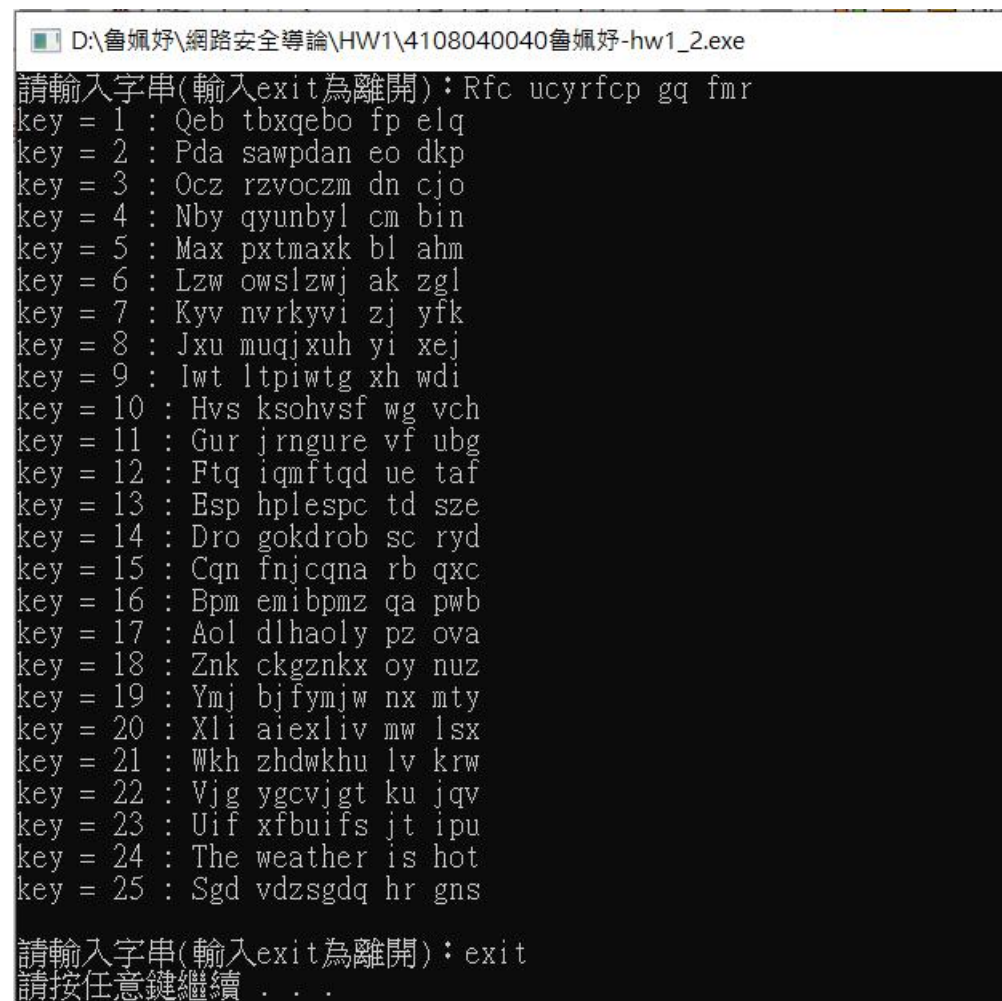
利用字元的 ascii 去減掉 key 並 return ascii 給 decode function

```
int mod(int key, int ascii){
    int number;
    int asciiNum;

    asciiNum = ascii - key;
    while(asciiNum < 0){
        asciiNum = asciiNum + 26;
    }
    number = asciiNum % 26;

    return number;
}
```

Output result :



```
D:\魯佩好\網路安全導論\HW1\4108040040魯佩好-hw1_2.exe
請輸入字串(輸入exit為離開):Rfc ucyrfcg qg fmr
key = 1 : Qeb tbxqebo fp elq
key = 2 : Pda sawpdan eo dkp
key = 3 : Ocz rzvoczm dn cjo
key = 4 : Nby qyunbyl cm bin
key = 5 : Max pxtmaxk bl ahm
key = 6 : Lzw owslzwj ak zgl
key = 7 : Kyv nvrkyvi zj yfk
key = 8 : Jxu muqjxuh yi xej
key = 9 : lwt ltpiwtg xh wdi
key = 10 : Hvs ksohvsf wg vch
key = 11 : Gur jrngure vf ubg
key = 12 : Ftq iqmftqd ue taf
key = 13 : Esp hplespc td sze
key = 14 : Dro gokdrob sc ryd
key = 15 : Cqn fnjcqna rb qxc
key = 16 : Bpm emibpmz qa pwb
key = 17 : Aol dlhaoly pz ova
key = 18 : Znk ckgznkx oy nuz
key = 19 : Ymj bjfymjw nx mty
key = 20 : Xli aiexliv mw lsx
key = 21 : Wkh zhdwkhu lv krw
key = 22 : Vjg ygcvjgt ku jqv
key = 23 : Uif xfbuifs jt ipu
key = 24 : The weather is hot
key = 25 : Sgd vdzsgdq hr gns
請輸入字串(輸入exit為離開):exit
請按任意鍵繼續 . . .
```