Homework 4

Programming exercise class

題目：通訊資料傳遞與加解密

Introduction

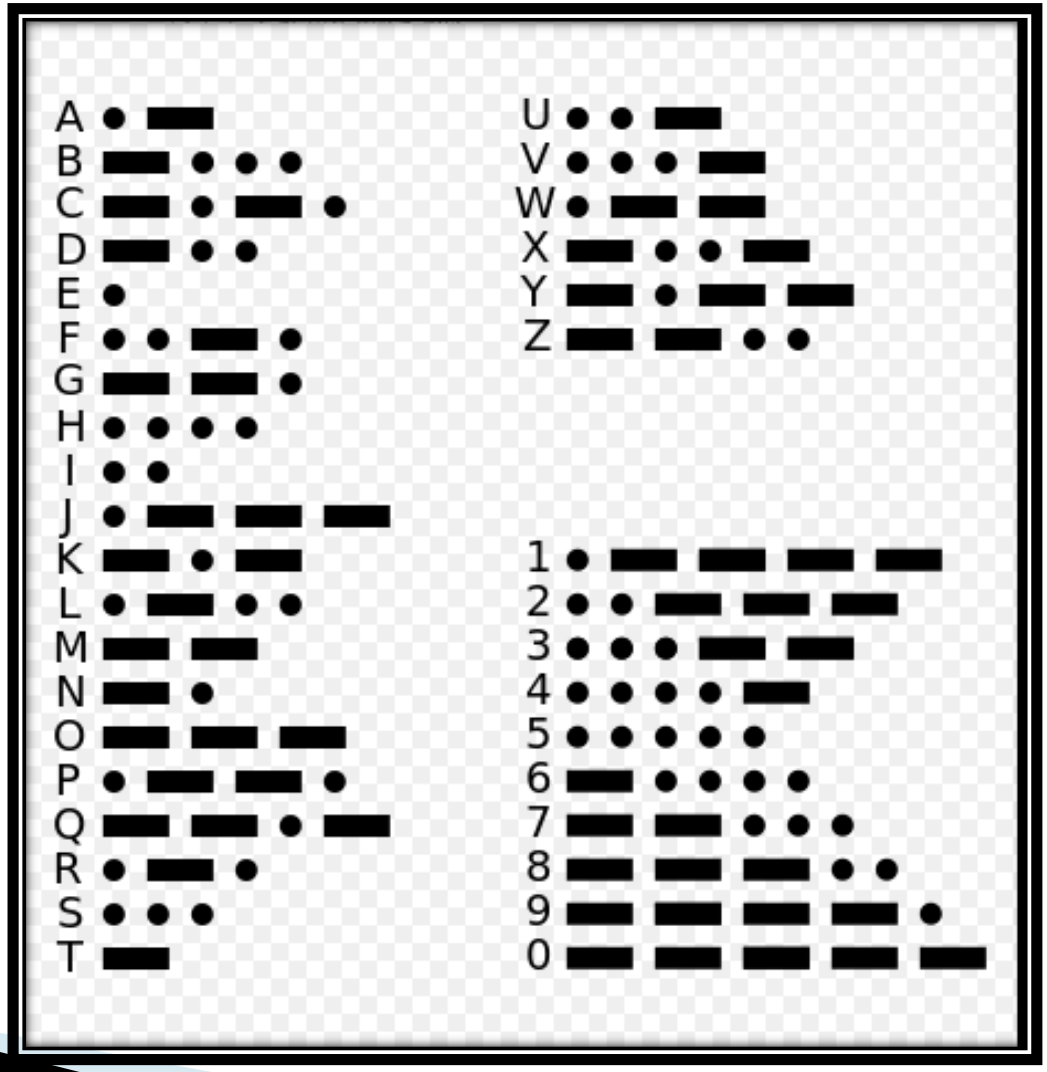
- 自從人們知道如何**“傳遞訊息”**後，既使人們之間隔上一段距離，我們仍然能互相分享、聊天、傳送資訊給對方。

- **傳遞訊息**有許多不同的方式，除了紅燕捎書、馬拉松捷報等，這類傳統而費時費力的方式外，人們發明了更聰明的方法 **– 電報機**、現代的網路通訊等。而最經典的傳遞方式就是電報機以及電報機常用也為人所知的**“摩斯密碼”**。

- 然而我們會因為某些因素而不希望我們傳出去的內容被其他人看見。所以聰明的人類就想出了一種保護資料的方法 **– 加密** 。

- 加密**(encode)**，是指對資料或文件中的內容經由重新排列、單字的兌換等，產生出新的加密文件以達到保護文件的一種方法。加密在商業機密、軍事通訊等用途上是非常常見的。而最著名的一種加密方式就是 **- 維吉尼亞表格加密法**。

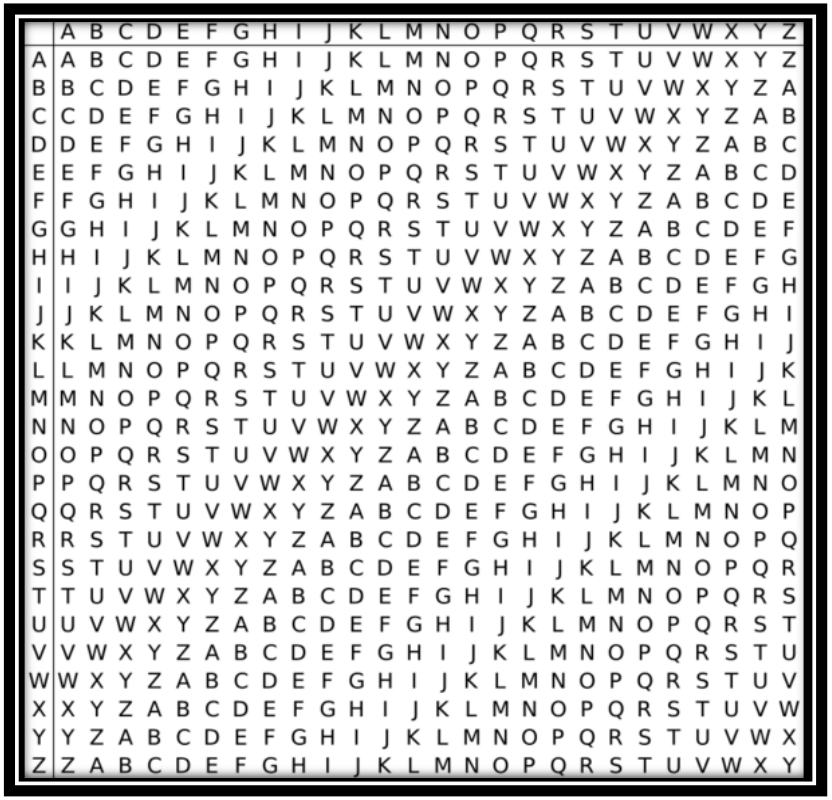
摩斯密碼表



維吉尼亞密碼使用方式：

- 使用一個關鍵字來加密。關鍵字用完就再次重複。假設關鍵字是「CAT」，則內容的第一個字由「C」加密，第二個字由「A」加密，第三個則由「T」加密，然後再回到C加密，一直重複。
  - 先選取一個關鍵字(假設：cat)，和欲加密的內容(假設：ball)。
  - 利用上述的方式會得到：
  - b用c加密 … 所以對照表格座標(c,b)為D。
  - a用a加密 … 所以對照表格座標(a,a)為A
  - l用t加密 … 所以對照表格座標(t,l)為E
  - l用c加密 … 所以對照表格座標(c,l)為N
- 得加密結果為：DAEN

- 當然也能利用敘述1.的方式進行解密：如內容為DAEN、關鍵字為CAT則，D在座標(c,$)上時可得 $ =B。以此類推A在 (a,$)上得 $ = A、E對應t得到L … 所以解密後結果為BALL 。



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

情境~

- 有一天，**Mike**老師在中正大學的噴水池裡撿到了一台電報機。這台電報機看起來雖舊但功能完全正常。於是**Mike**老師心血來潮，決定以後就用這台電報機**利用摩斯密**碼傳遞訊息給程式設計的助教。

- 而**Mike**老師也知道現在的學生實在太厲害了**!!**所以為了不讓傳遞的內容外洩，**Mike**老師決定使用**維吉尼亞密碼**加密。

- 這天，班上的同學聽到小道消息說**: Mile**老師傳送一份攸關全班程式設計總分的訊息給助教。於是聰明的你們製作了攔截器，在資料傳遞時攔截下了這份訊息**...**並且透過觀察發現老師所使用的**keyword**是自己的名字。**(mikemayer)**

- 到底**...**電報的內容會是甚麼呢**???**

程式

- 為了解開電報內容，你們必須撰寫一個程式：
  - **1.** 程式要從 **decode.txt** 內讀入數筆 **“摩斯密碼”**。
  - **2.** 將摩斯密碼利用 **mos.txt** 內的密碼表轉譯成自元。
  - **3.** 讓使用者輸入**Keyword . (**僅一個全英文單字**)**
  - **4.** 再利用**維吉尼亞密碼**將原資料還原。
  - **5.** 將結果輸出到**output_decode.txt** 中。

- 而為了不讓助教發現你們已經破解密碼了所以：
  - **1.** 程式要從 **encode.txt** 讀入訊息。
  - **2.** 讓使用者輸入**Keyword . (**僅一個全英文單字**)**
  - **3.** 先將訊息利用**維吉尼亞密碼**加密。
  - **4.** 再將其利用 **mos.txt** 內的密碼表轉成**摩斯密碼**。
  - **5.** 最後將結果輸出到**output_encode.txt** 中。

要求

- **Encode、Decode：**
  - 所有input大小寫不限，但輸出皆須統一為**大寫**。
  - 輸出格式請遵照後頁規定。
- **摩斯密碼與字元間的轉換工作：**
  - 需放在**副函式**中執行。
- **使用者介面：**
  - 選項需防錯，**需考慮輸入字元**的情況。
  - 顯示翻譯完或讀入的英文字串。
  - 顯示加解密後的結果。
- **不須擔心：**
  - Encode.txt 、 Decode.txt 中的任何格式錯誤。

TXT檔內資料排法

- **Decode.txt :**
  - **1. 類別 :** 摩斯密碼
  - **2. 排法 :** 每組密碼代表**一個字元**，每組密碼間用**空白鍵**區隔。
  - **3. 特殊密碼 :**
    - **|**代表**輸出時**，**單字間**的空白鍵。其他不在 **mos.txt** 中的資料皆直接維持原樣。

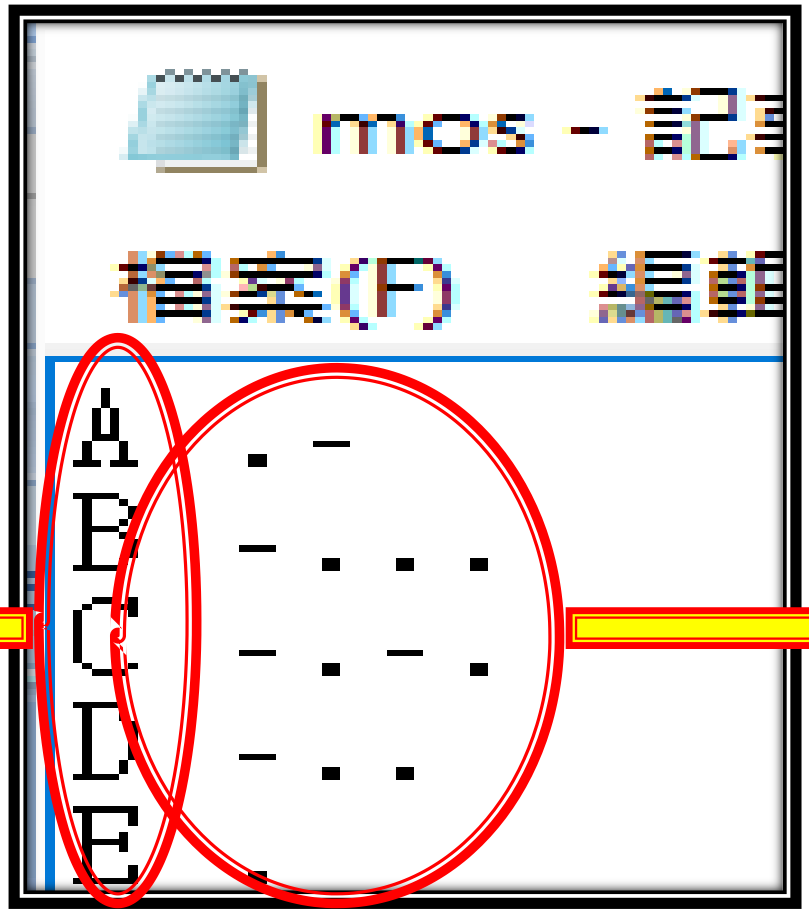
- **Encode.txt :**
  - **1. 類別 :** 一串訊息
  - **2. 排法 :** 一串訊息，字根字之間利用**'-'**間隔。
  - **3. 特殊密碼 :**
    - 僅數字跟英文字元需轉成摩斯密碼、**'-'**轉成**'|'**、其餘維持原樣。

OUTPUT格式(請遵照格式輸出)

- **Output_encode.txt (同decode.txt) :**
  - **1. 類別 :** 摩斯密碼
  - **2. 排法 :** 每組密碼代表**一個字元**，每組密碼間用**空白鍵**區隔。
  - **3. 特殊密碼 :**
    - **|**代表**輸出時**，**單字間**的空白鍵。其他不在 **mos.txt** 中的資料皆直接維持原樣。

- **Output_decode.txt :**
  - **1. 類別 :** 一串訊息
  - **2. 排法 :** 一串訊息，字根字之間利用 **空白鍵**間隔。
  - **3. 特殊密碼 :**
    - **Decode.txt**內**'|'**轉成**空白建**。
    - **Decode.txt**內不在**mos.txt**內的皆維持原樣。

Mos.txt

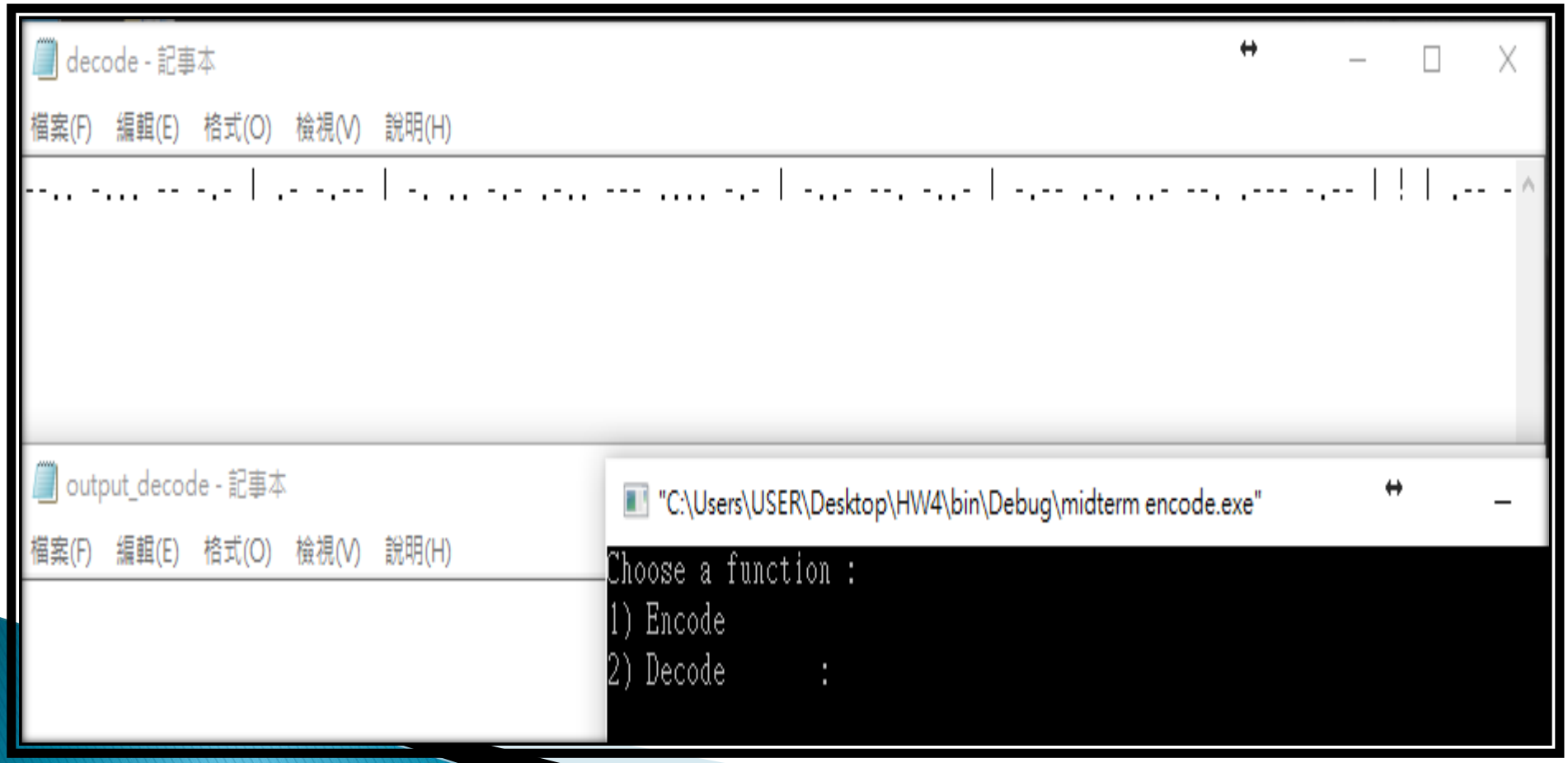


代表字元

摩斯密碼

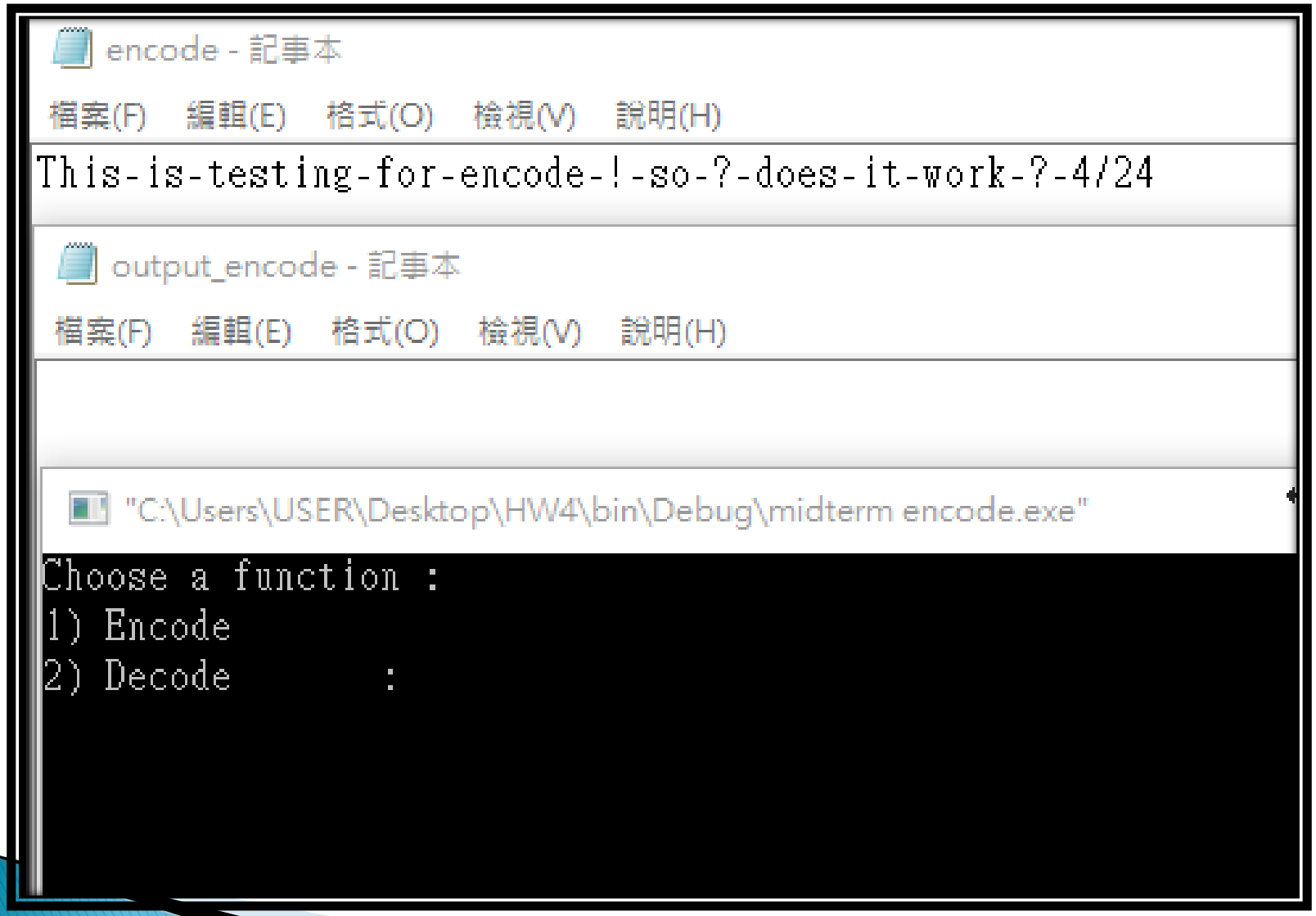
範例圖

- **Decode :**


decode - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
--.. -... -- -.- | .- -.-- | -. .. -.- .-.. --- .... -.- | -..- --. -..- | -.-- .-. ..- --. .--- -.-- | ! | .-- -
output_decode - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
"C:\Users\USER\Desktop\HW4\bin\Debug\midterm encode.exe"
Choose a function :
1) Encode
2) Decode :


decode - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
-.. -... -- -.- | .- -.-- | -. .. -.- .-.. --- .... -.- | -..- --. -..- | -.-- .-. ..- --. .--- -.-- | ! | .-- -
output_decode - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
THIS IS TESTING FOR ENCODE ! SO ? DOES IT WORK ? 4/24
"C:\Users\USER\Desktop\HW4\bin\Debug\midterm encode.exe"
Choose a function :
1) Encode
2) Decode : 2
Keyword : guess
The data is : ZBMK|AY|NIKLOHK|XGX|YRUGJY|!|WG|?|VUYW|AL|CIVC|?|4/24
Result : THIS IS TESTING FOR ENCODE ! SO ? DOES IT WORK ? 4/24

- **Encode :**


encode - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
This-is-testing-for-encode-!-so-?-does-it-work-?-4/24
output_encode - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
"C:\Users\USER\Desktop\HW4\bin\Debug\midterm encode.exe"
Choose a function :
1) Encode
2) Decode :


encode - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
This-is-testing-for-encode-!-so-?-does-it-work-?-4/24
output_encode - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)
--.. -... -- -.- | .- -.-- | -. .. -.- .-.. --- .... -.- | -..- --. -..- | -.-- .-. ..- --. .--- -.-- | ! | .-- -
"C:\Users\USER\Desktop\HW4\bin\Debug\midterm encode.exe"
Choose a function :
1) Encode
2) Decode : 1
Keyword : guess
The data is : THIS-IS-TESTING-FOR-ENCODE-!-SO-?-DOES-IT-WORK-?-4/24
Result : ZBMK|AY|NIKLOHK|XGX|YRUGJY|!|WG|?|VUYW|AL|CIVC|?|4/24

配分

- **程式完成的程度有不同的得分：**

可以將txt檔內的摩斯密碼轉換成英文字元、數字	20%
可以Encode，且功能正確	30%
可以Decode，且功能正確	30%
讀檔寫檔功能正常 (能讀、寫進資料)	10%
程式簡潔、有註解、User Interface	10%

- **使用暴力破解法** **得分*0.8**

到底Mike老師跟助教說了些甚麼呢？
故事的結局就讓同學們自己去發現吧!