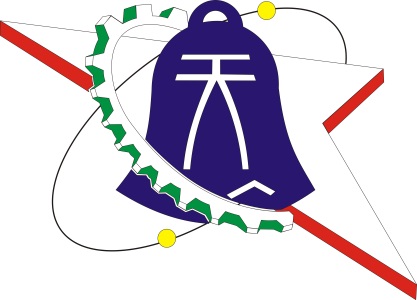
**國立彰化師範大學技術及職業教育學院**

**工業教育與技術學系**

****

**程式設計**

**期末專題**

**題目名稱**

檔案加密器

**班級：**生一

**學號：**S0724008

**姓名：**余紹華

**中華民國108年6月19日**

**目錄**

## 系統功能，輸入及輸出資料

## 應用層面說明

## 資料結構說明

## 程式剖析

## 程式執行範例

## 完整的程式

1. 系統功能，輸入及輸出資料

透過凱薩加密，對文字進行加密與解密。分為兩個部分，分別為加密與解密。

1. 加密

會輸入一個plaintext.txt的檔案，檔案的內容為你想要加密的文字，接著程式會要求你輸入密碼(長度在100個字以內)，進行加密。待加密完成後，會顯示「完成了」，並輸出一的檔名為ciphertext.txt的檔案，裡面的內容將會是一段加密後的文字。

1. 解密

如果要進行加密，則須輸入一個檔名為ciphertext.txt的檔案，內容為加密過後的文字，接著輸入與加密時相同的密碼，即進行解密解密的動作。解密完成以後，程式會顯示「完成了」，並輸出一個plaintext-recovered的檔案，檔案內容將會顯示解密完成的文字。

1. 應用層面說明

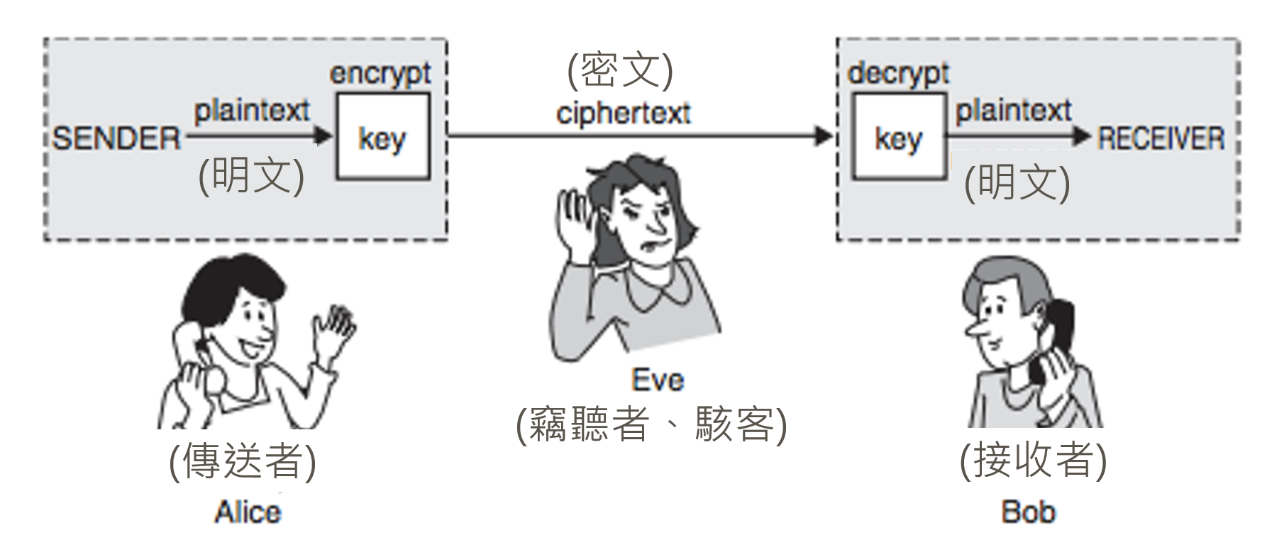


Fig.1加密與解密

當Alice(傳送者)要傳送一則訊息給Bob(接收者)時，將欲傳送的訊息(明文)透過金鑰進行加密，就可以避免被Eve(竊聽者)竊取。收到訊息的Bob也必須具有與傳送者相同的金鑰，才可以進行解密，獲取訊息。

1. 資料結構說明(流程圖)
2. 加密

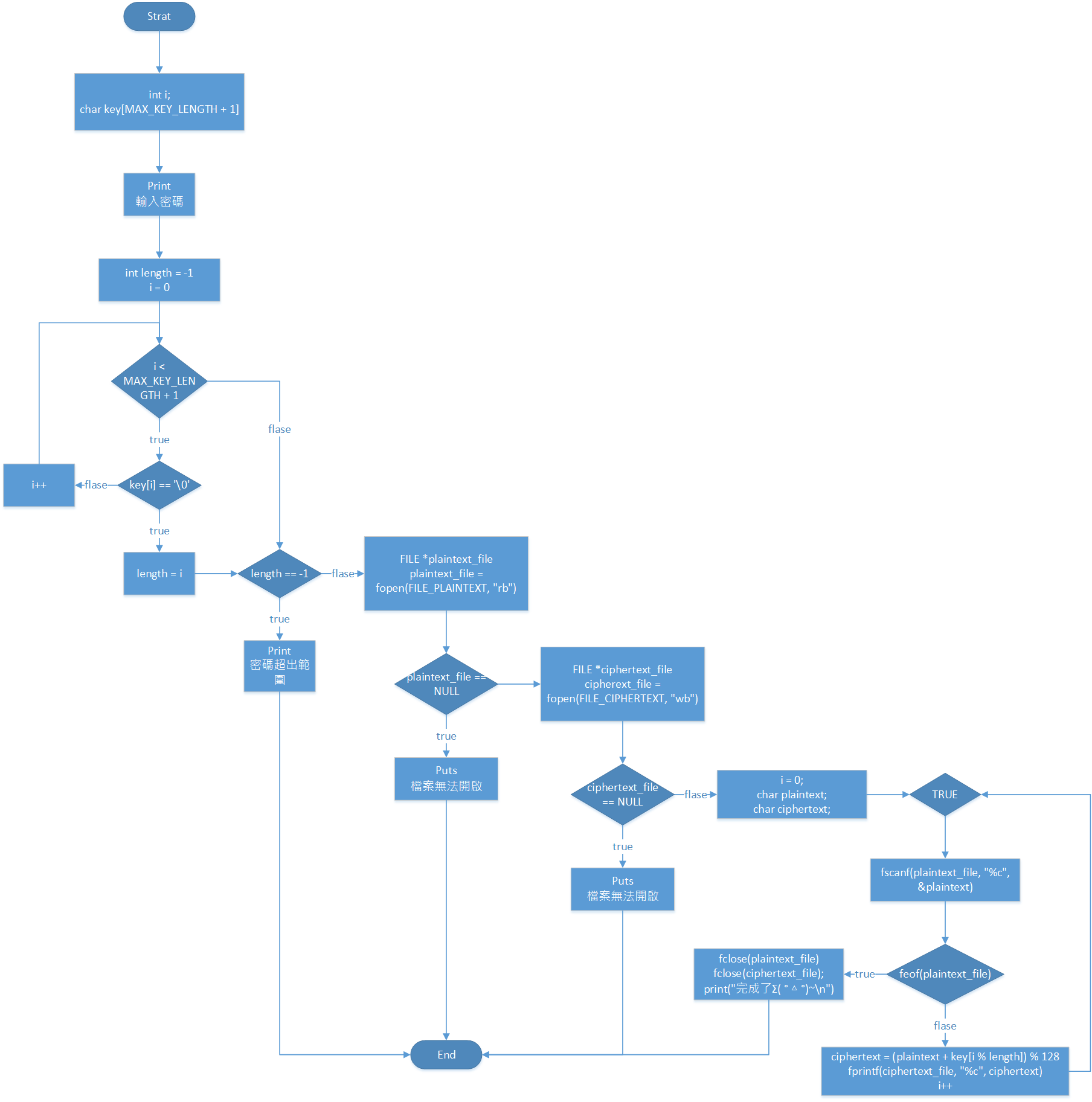


Fig.2加密流程圖

1. 解密

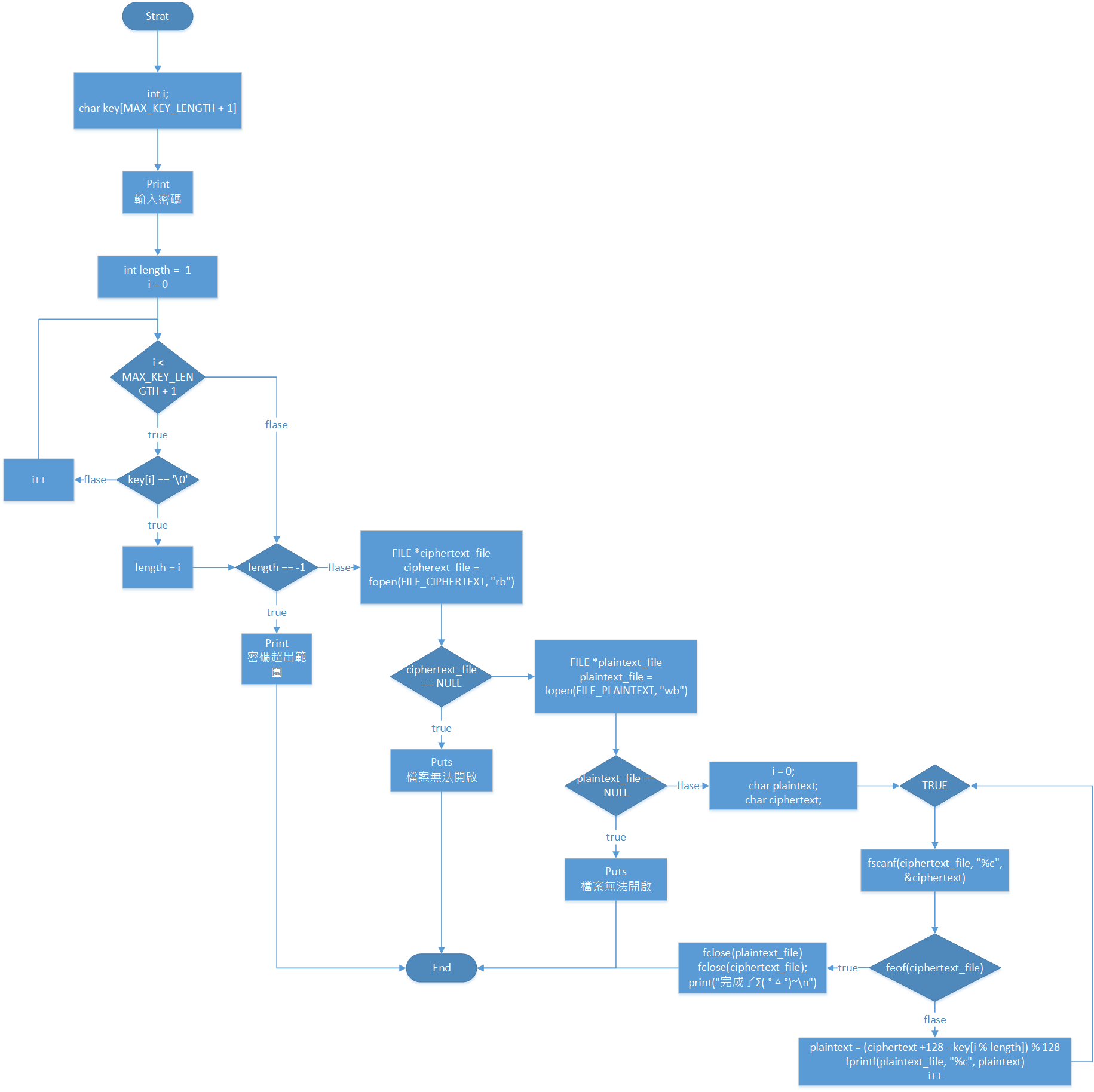


Fig.3流程圖-解密

1. 程式剖析
2. 加密

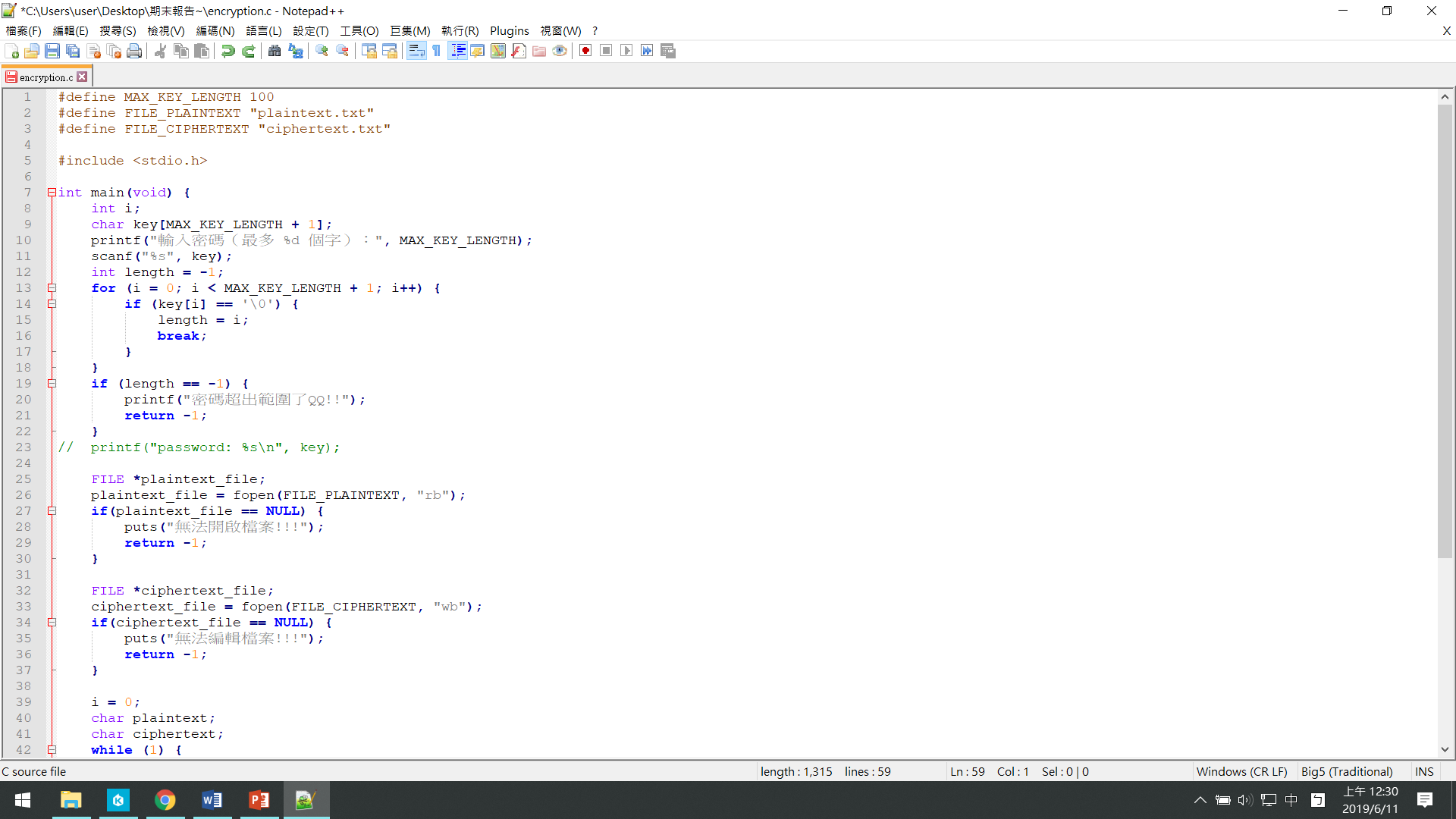


Fig.4加密程式(1)

第1~3行，以第1行為例，只要在這個程式內看到Max\_Key\_Length皆會自動代入100。

第7行，開始main函式。

第9行，宣告一陣列可以存放100 + 1個字元，指定密碼長度為100個字(第1行)，電腦會自動在字串的最後加上/0，故需要多要一格記憶體。

第12~22行，將length的初始值設為-1，利用for迴圈來檢測密碼的長度，一旦看到\0(字串的結尾)，表示密碼在合理範圍內，就會更新length值，若到檢查完都沒有更新此變數，那就會維持-1，代表長度超過設定之最大值。

未來在執行時，有可能會出錯，所以必須告訴使用者，並結束程式。

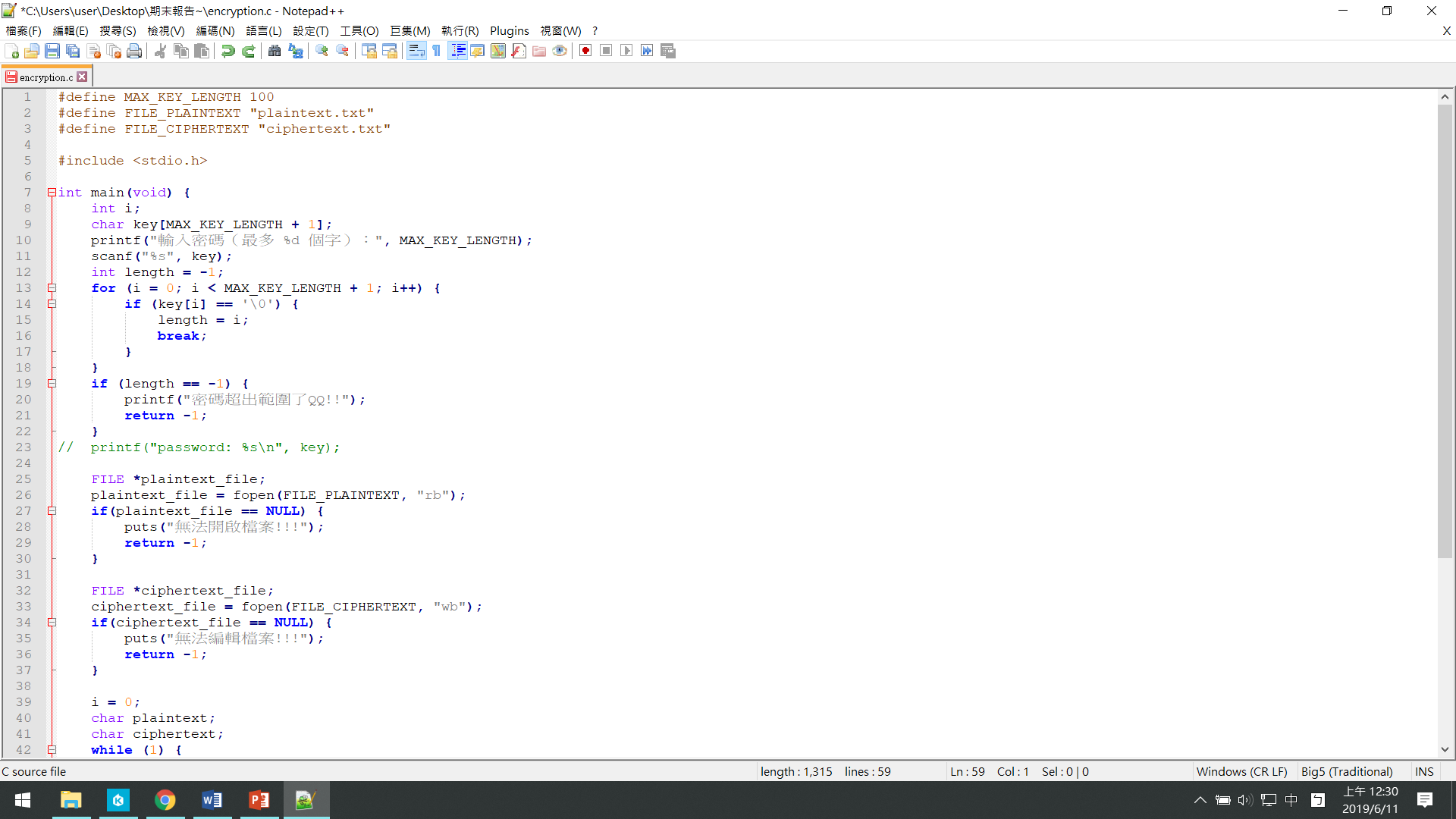


Fig.5加密程式(2)

第25~30行，會以二進位的方式讀取一個檔名plaintext.txt的檔案，接著會判斷檔案是否可以讀取，若檔案無法讀取，則會告訴使用者並結束程式。

第32~37行，會以二進位的方式將內容寫入ciphertext.txt的檔案中，接著會判斷檔案是否能寫入，若檔案無法寫入，則會告訴使用者並結束程式。

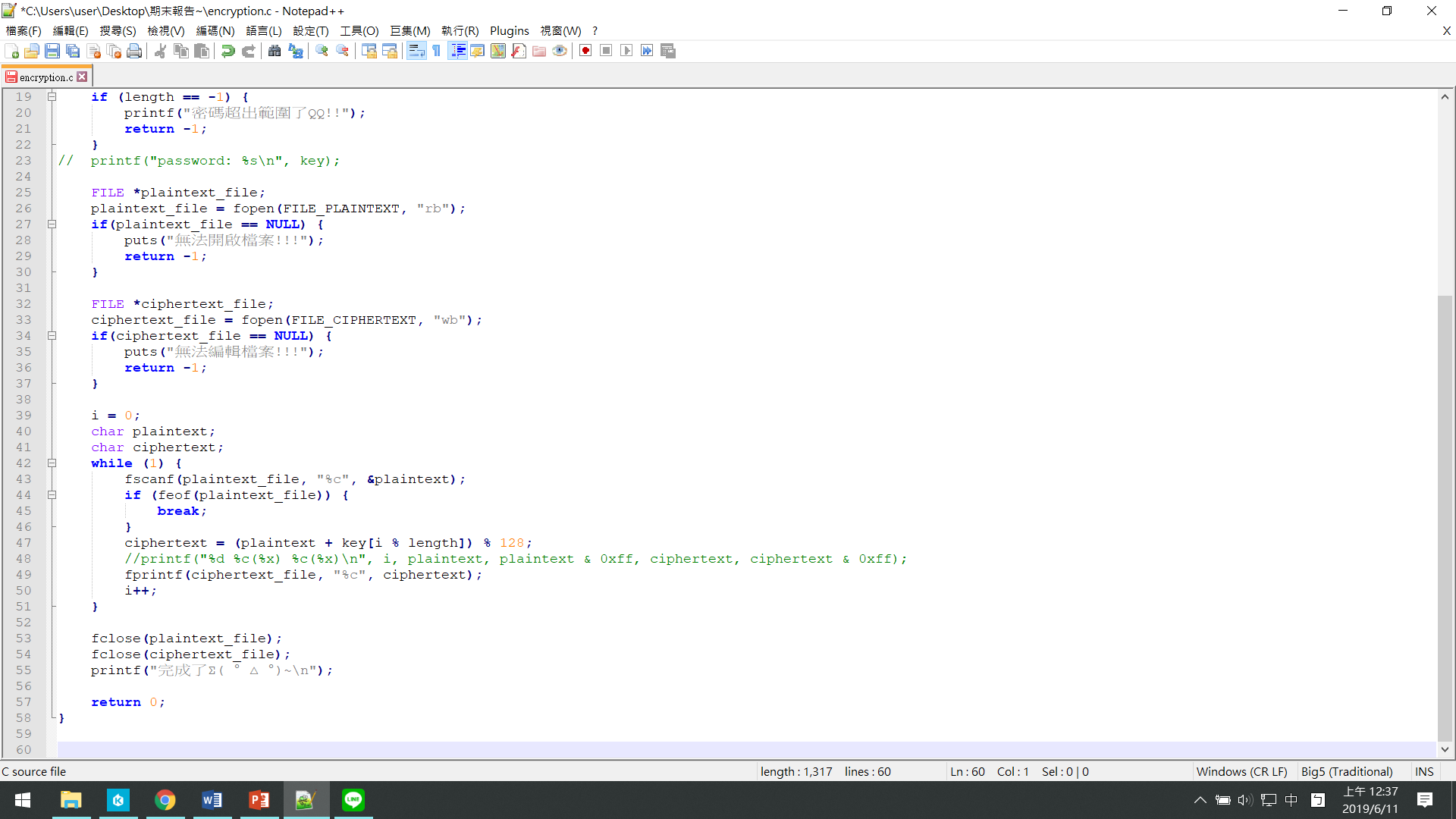


Fig.6加密程式(3)

第42~51行，設了一個while(1)迴圈，一次讀一個字元，直到讀到檔案的最後，跳出迴圈，否則繼續。

第47行，(可參考Fig.6)電腦會自動將讀到的字元轉為一組數字儲存，加上密碼轉換的數字，除以128取餘數(能夠加密的範圍在ASCII code表上的00~127，共128個字)。理論上密碼的長度會小於被加密文字的長度，密碼會不斷重複，故除以密碼本身的長度取餘數。

第53~58行，待讀取與輸入完畢後，關閉檔案，結束程式。



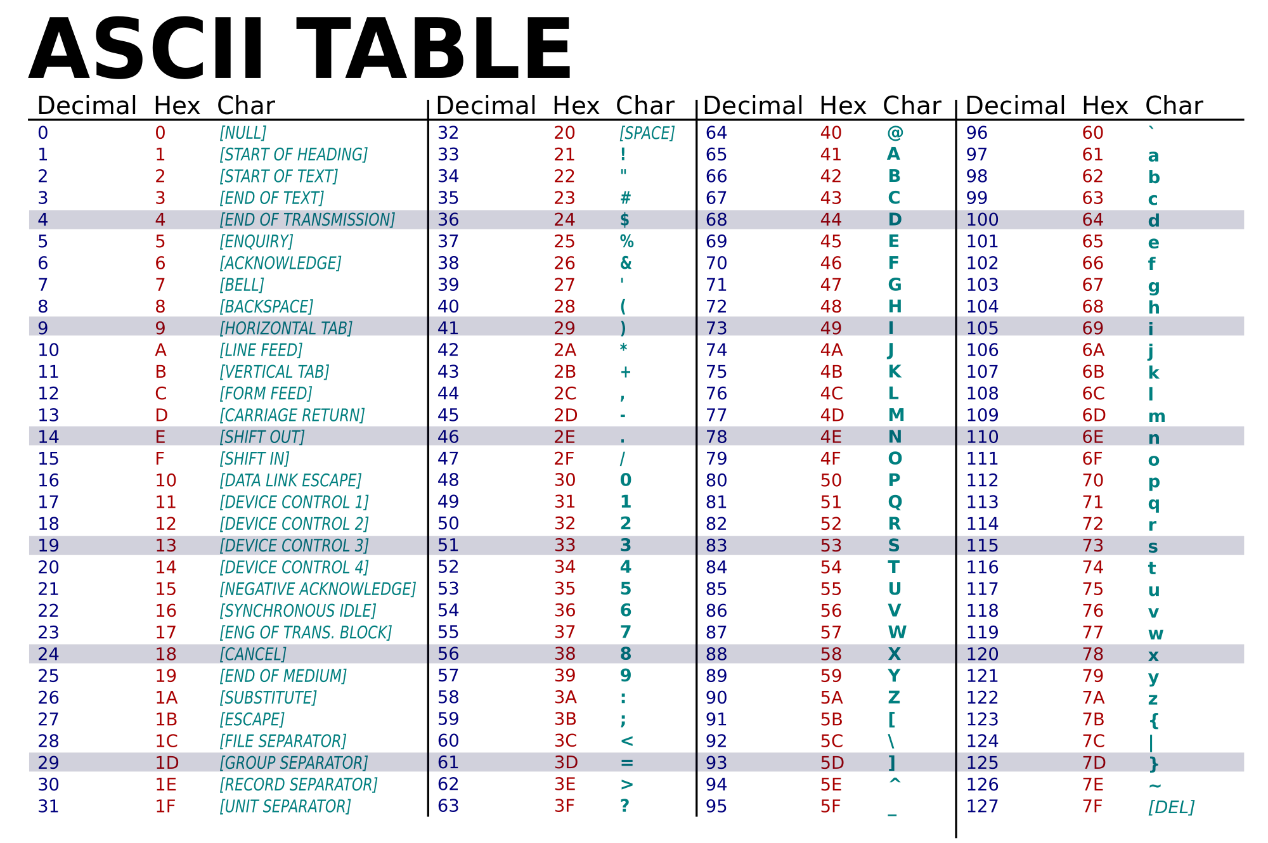
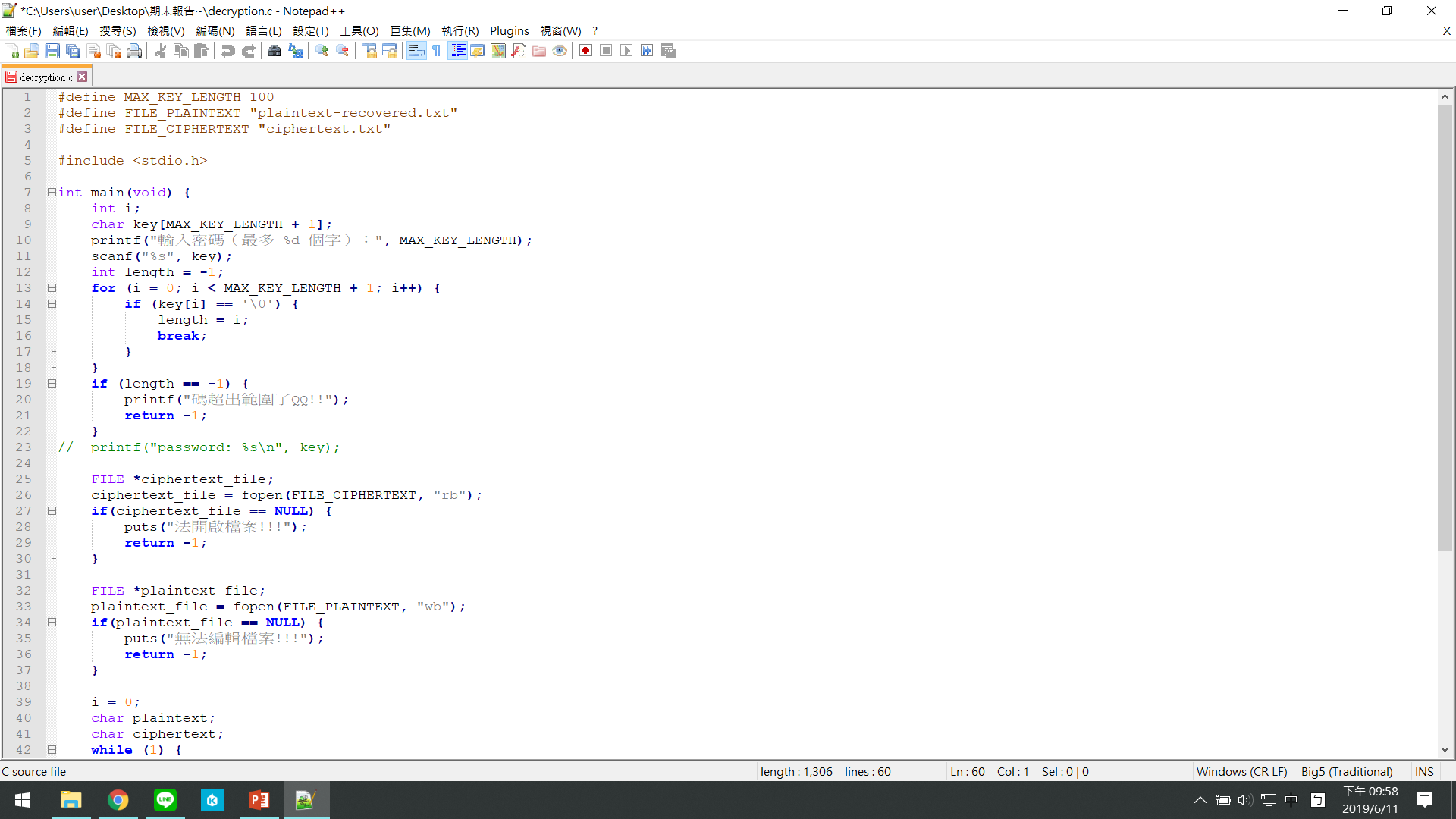
Fig.7加密程式第47行轉換機制

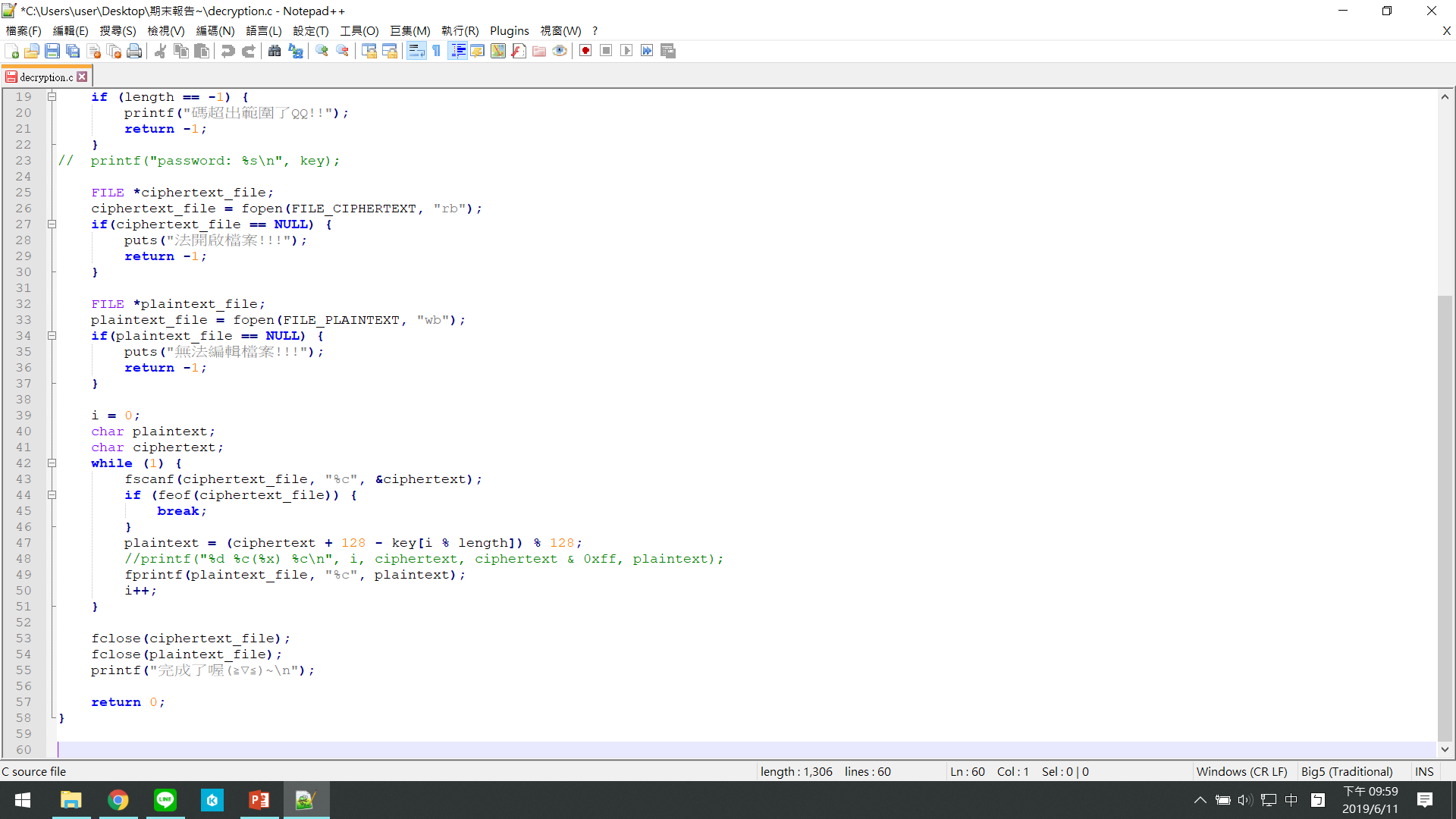
Fig.8 ASCII code

1. 解密

Fig.9解密程式(1)

此部分與加密程式相同!!!(可參考加密程式(1))

檢測密碼的長度，若密碼超出範圍，告知使用者後結束程式。

Fig.10解密程式(2)

第25~30行，會以二進位的方式讀取一個檔名ciphertext.txt的檔案，接著會判斷檔案是可以讀取，若檔案無法讀取，會告訴使用者並結束程式。

第32~37行，會以二進位的方式將內容寫入plaintext-recovered.txt的檔案中，接著會判斷檔案是否可以寫入，若檔案無法寫入，會告訴使用者並結束程式。

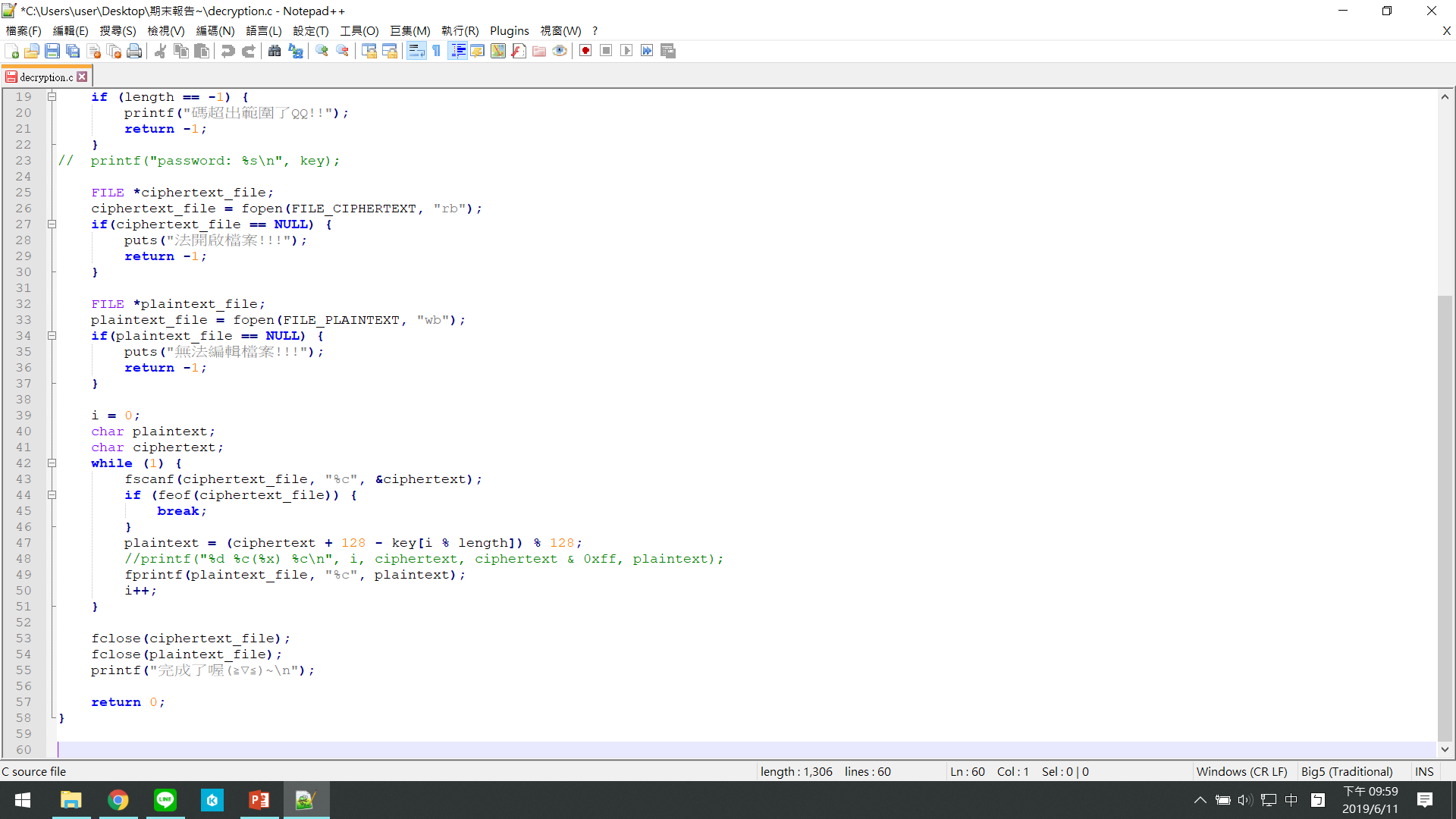


Fig.11解密程式(3)

第47行，先加上128確保數值在減掉密碼的長度後仍為正數，最後除以128是為了避面有超過128的疑慮。

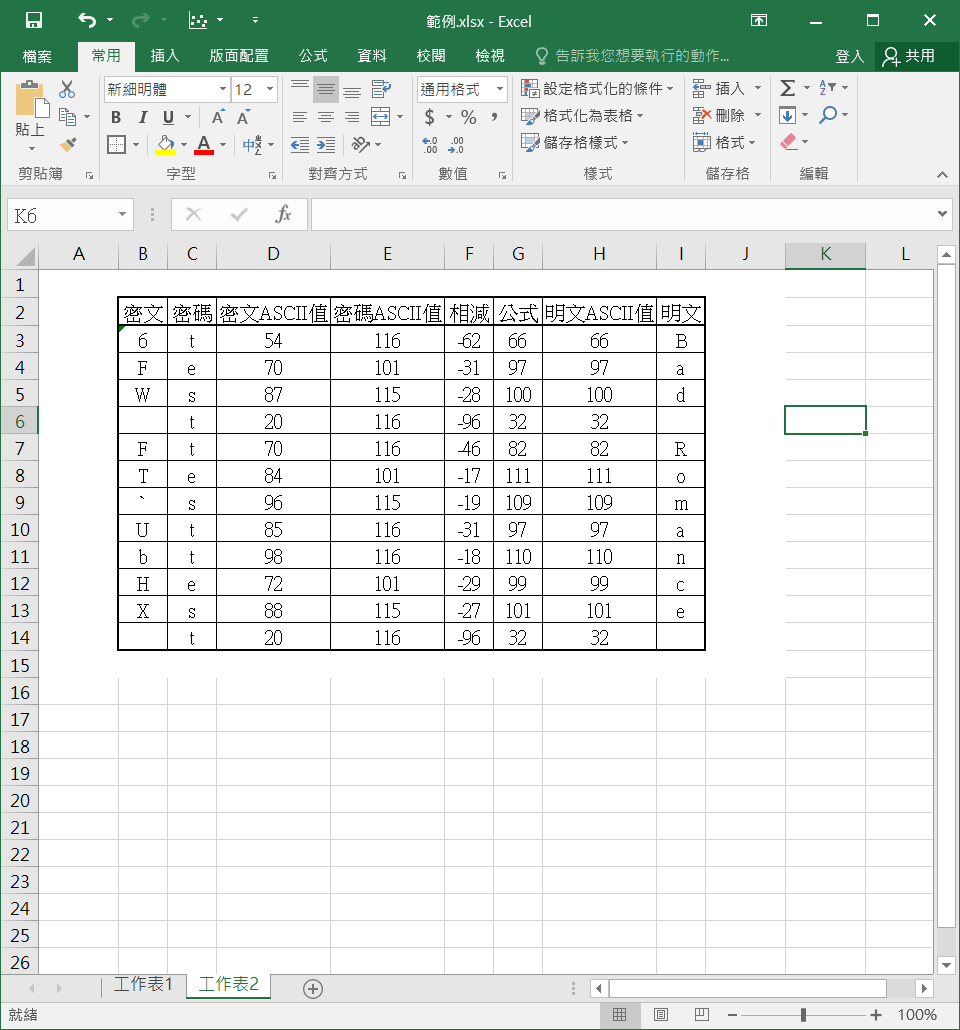


Fig.12解密程式第47行轉換機制

1. 程式執行範例

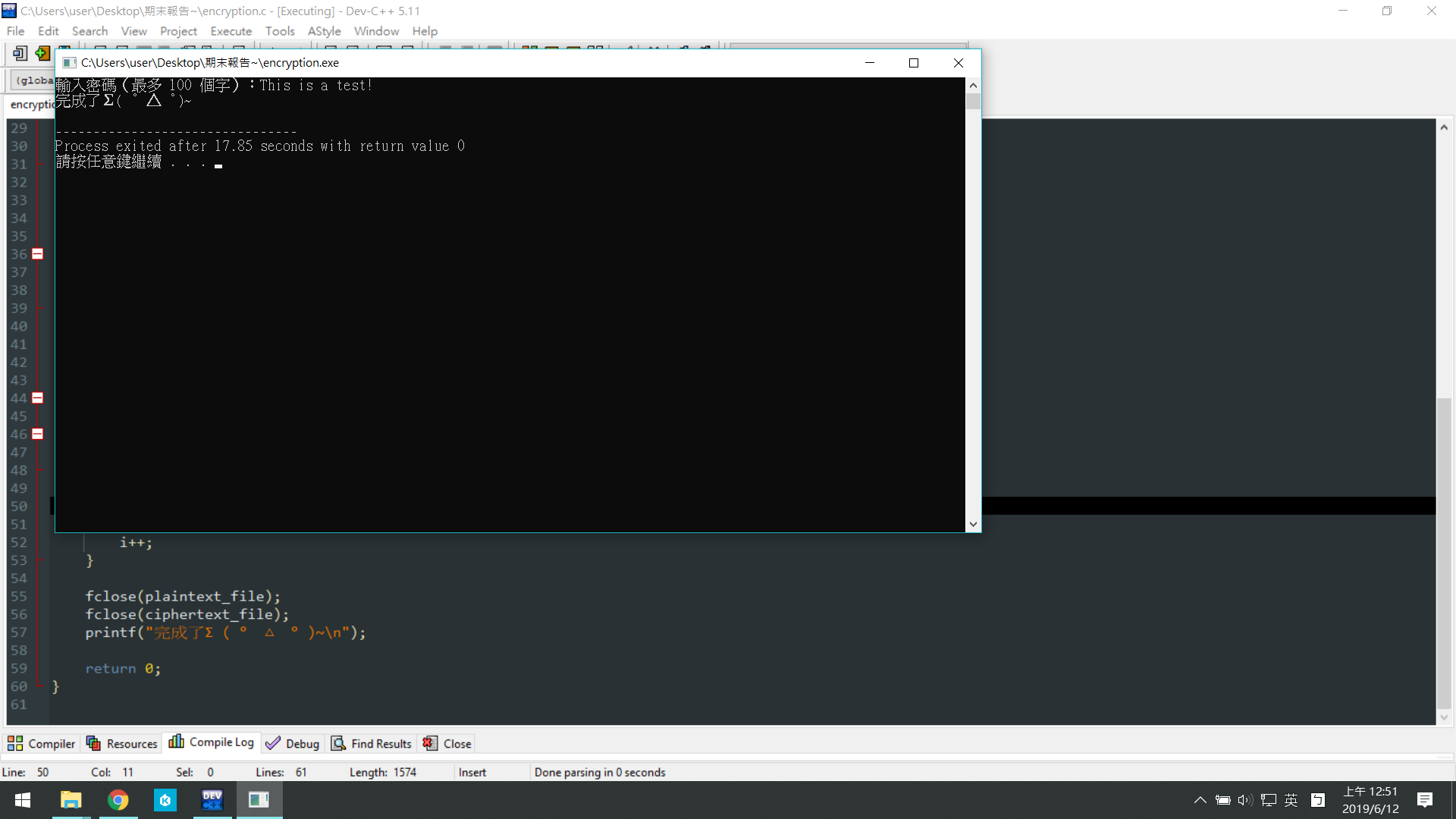


Fig.13加密的執行結果

使用者需要輸入一段密碼，若密碼在指定長度內，加密完成後會告知使用者「完成了」。

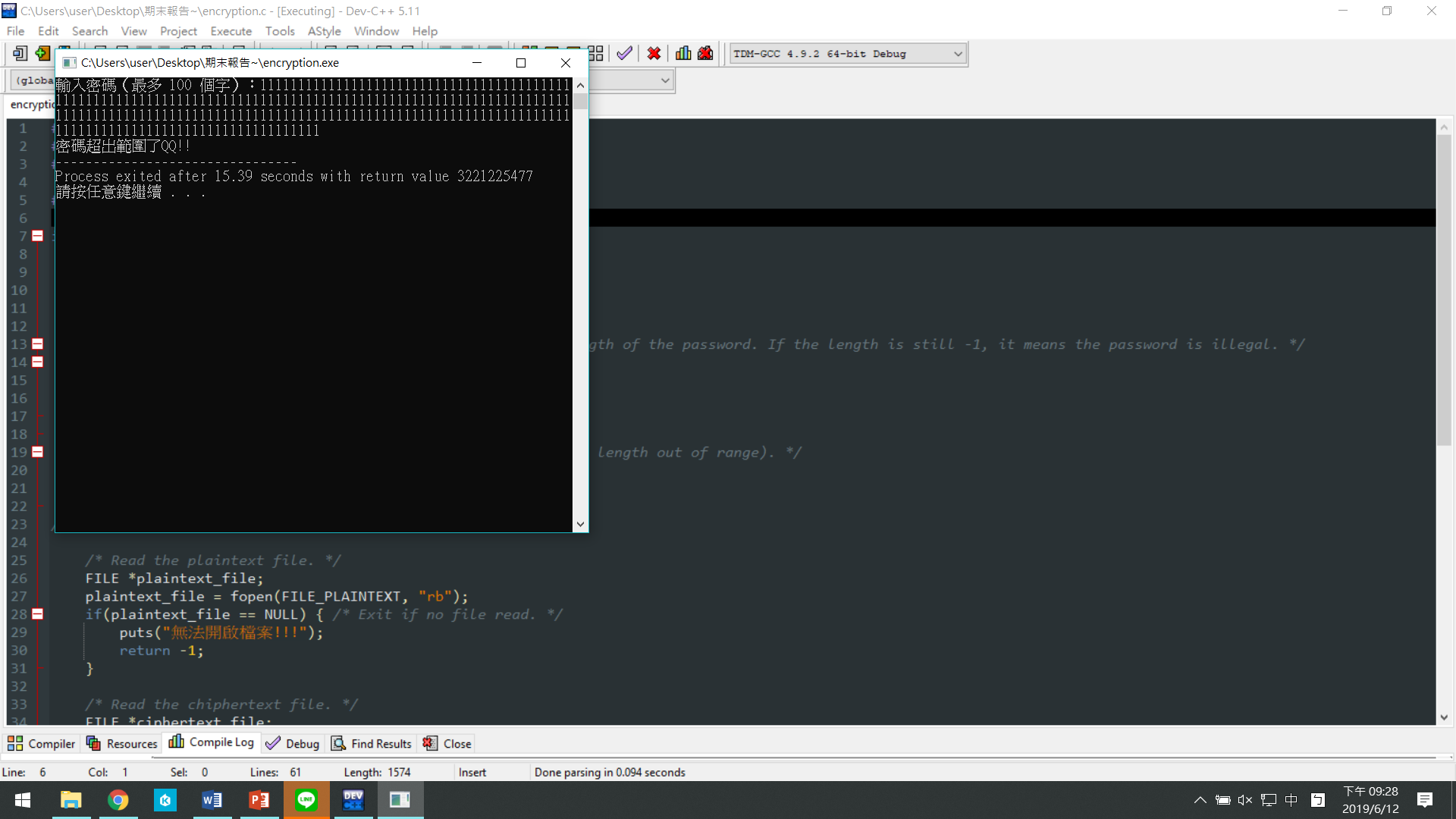


Fig.14密碼超過長度

若使用者輸入的密碼超過指定長度，則會顯示「密碼超出範圍」，結束程式

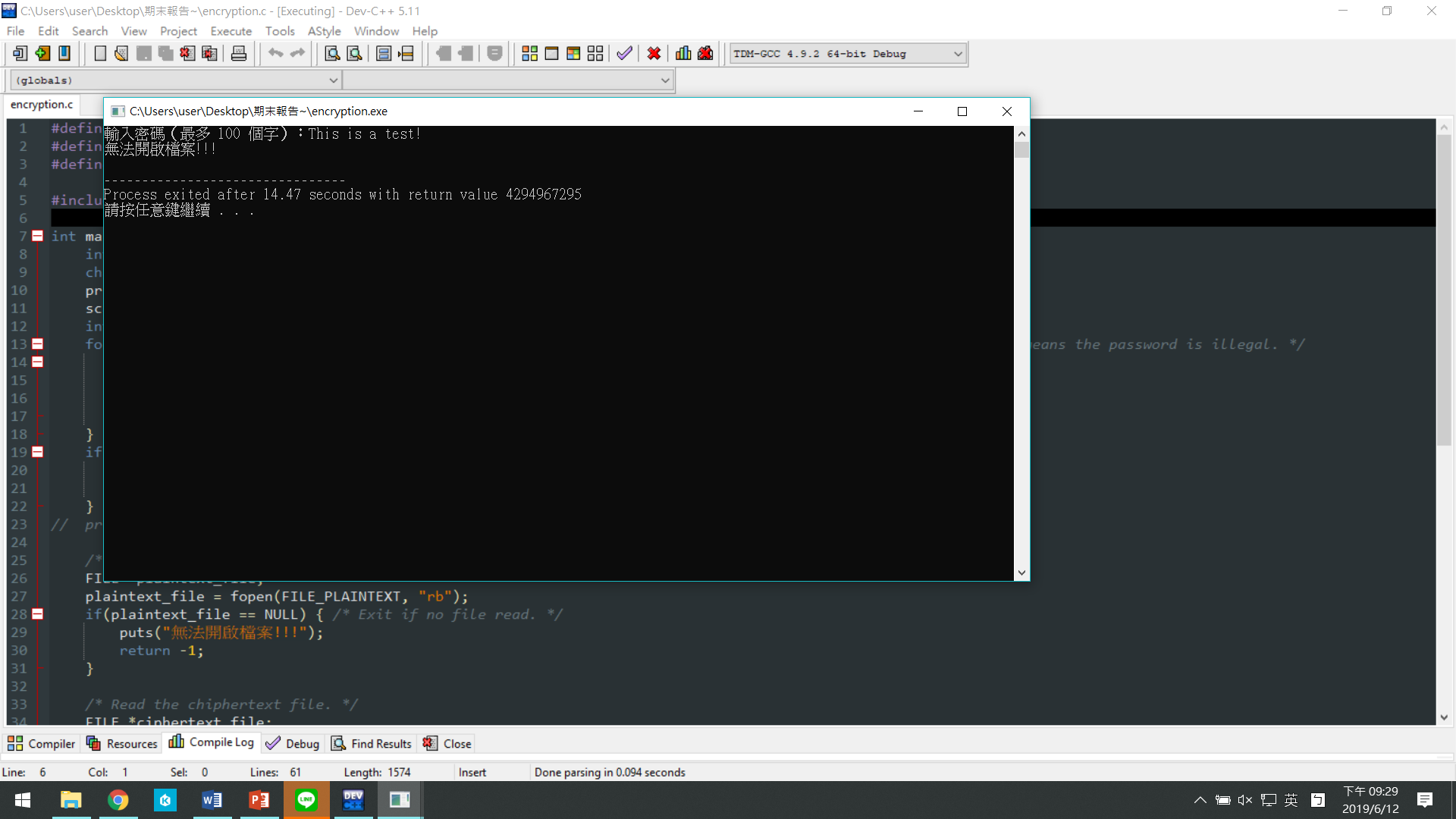


Fig.15檔案不存在

若檔案不存在，也會告知使用者，然後結束程式。

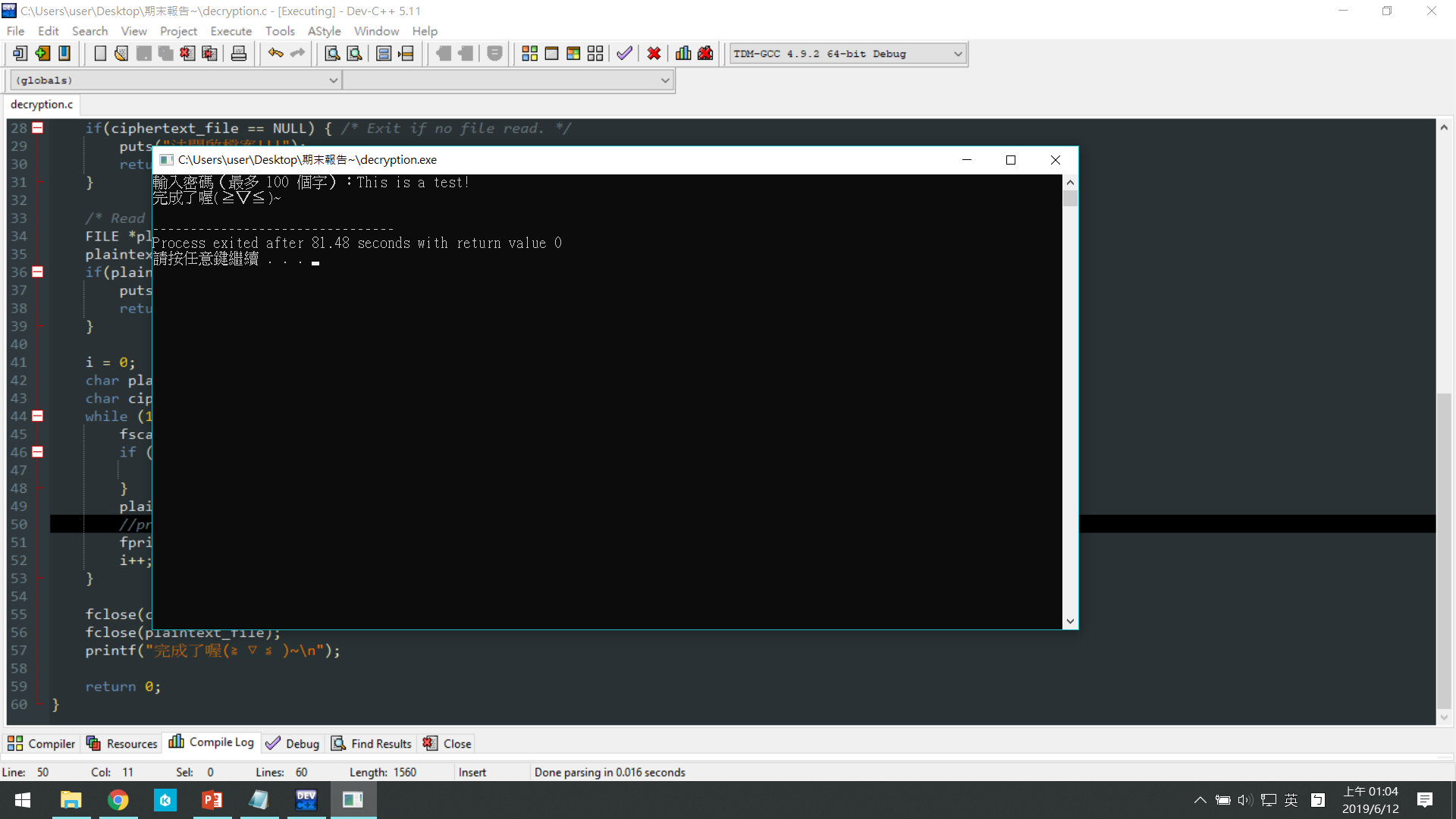


Fig.16解密的執行結果

使用者需要輸入與加密時相同的密碼，解密完成後會告知使用者「完成了」。

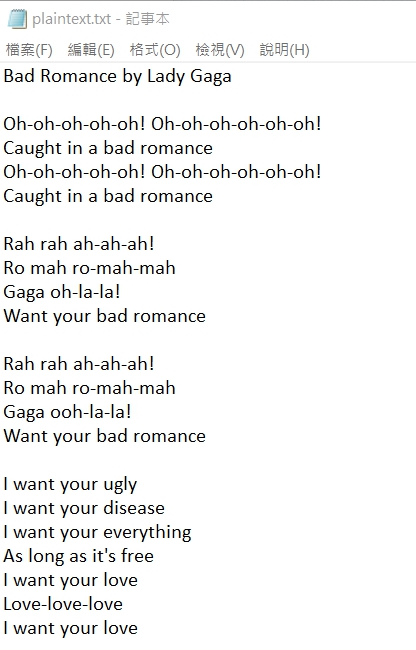
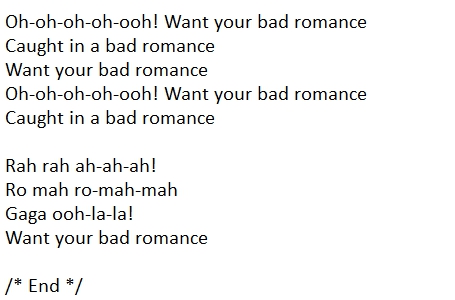
 

Fig.17輸入的檔案(Plaintext.txt)擷取頭、尾兩部分。

完整檔案的內容為Lady Gaga 的 Bad Romance。

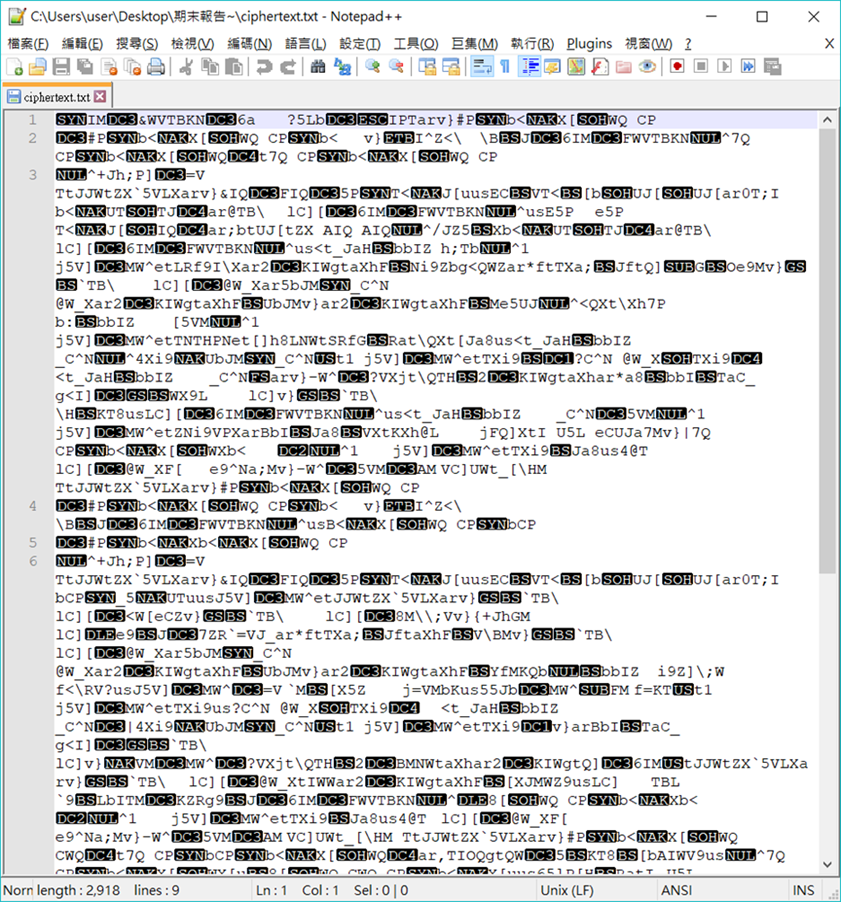


Fig.18加密後輸出的檔案/解密時輸入的檔案(ciphertext.txt)。

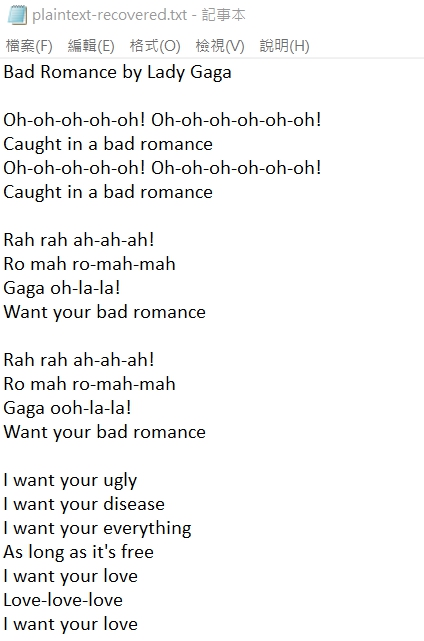
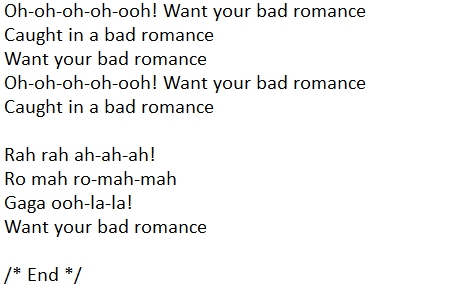
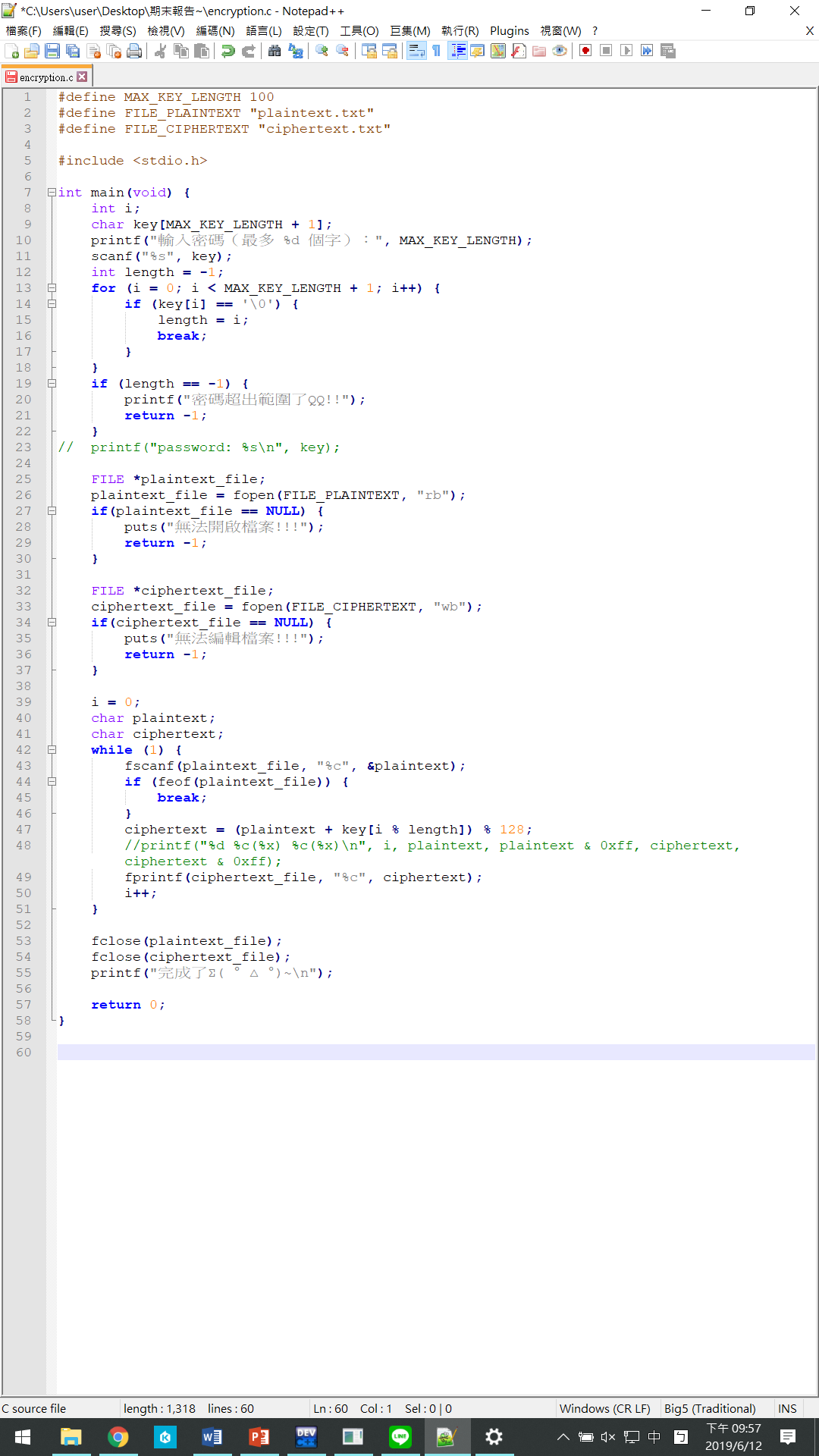
 

Fig.19解密後輸出的檔案(Plaintext-recovered.txt)擷取頭、尾兩部分。

可與Fig.17做比較，內容是相同的。

1. 完整的程式碼
2. 加密



1. 解密

