# Quiz 2 revised

2022/3/8

1.Please write a program to determine the dimension of the rectangle for this encryption transposition cipher.

ECDTM ECAER AUOOL
EDSAM MERNE NASSO
DYTNR VBNLC RLTIQ
LAETR IGAWE BAAEI
HOR

程式邏輯：

　把字串只留A-Z後，轉換成 col * row 的二維陣列，在對此二維陣列取transport，得到想要的編碼方式，再對此編碼方式計算總共的difference。

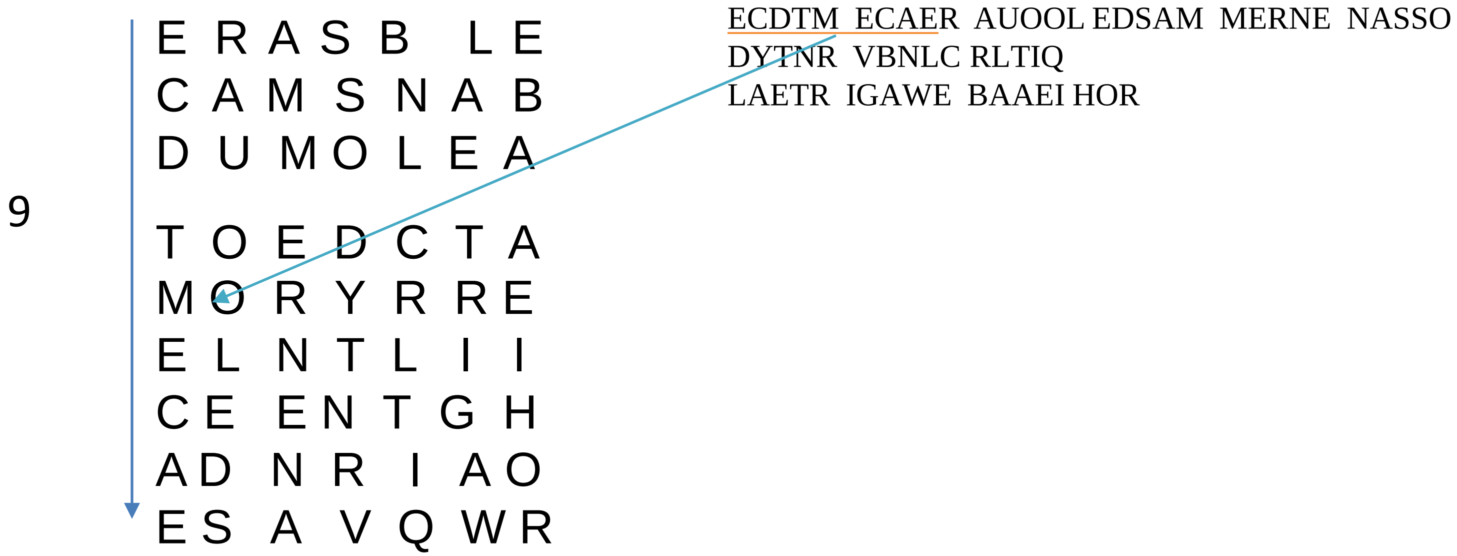
　最後比較7*9和9*7的difference，發現9*7的difference較小所以取9*7。

發現：

　因為63還可以拆成3*21和21*3，所以我測試這兩種後發現反而是3*21的difference最小。這是因為40%母音一個統計數據，所以當一個row的長度變長時，母音的的佔比會越來越趨近於統計的數值，才會造成這個情況。

　所以助教說程式中只要測試7*9和9*7即可。

## 2. Please Break the following transposition cipher which involves a completely filled rectangles with our HINT.



ECDTM ECAER AUOOL EDSAM MERNE NASSO
DYTNR VBNLC RLTIQ
LAETR IGAWE BAAEI HOR

9

E R A S B L E
C A M S N A B
D U M O L E A
T O E D C T A
M O R Y R R E
E L N T L I I
C E E N T G H
A D N R I A O
E S A V Q W R

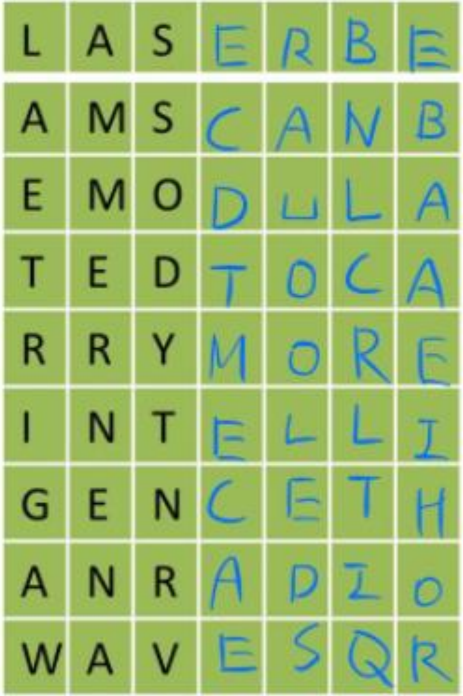
We assume that this encrypted message is using completely filled rectangle with 9 rows and 7 columns.

9

# Please Break the following transposition cipher which involves a completely filled rectangles from next HINT. (CONT)

| | | | | | | |
|---|---|---|---|---|---|---|
| L | A | S | | | | |
| A | M | S | | | | |
| E | M | O | | | | |
| T | E | D | | | | |
| R | R | Y | | | | |
| I | N | T | | | | |
| G | E | N | | | | |
| A | N | R | | | | |
| W | A | V | | | | |

答案：



| | | | | | | |
|---|---|---|---|---|---|---|
| L | A | S | E | R | B | E |
| A | M | S | C | A | N | B |
| E | M | O | D | U | L | A |
| T | E | D | T | O | C | A |
| R | R | Y | M | O | R | E |
| I | N | T | E | L | L | I |
| G | E | N | C | E | T | H |
| A | N | R | A | D | I | O |
| W | A | V | E | S | Q | R |

9

3. Please count Index of Coincidence (IC) for each messages.

Usually, The I. C. of English is around 0.066

程式邏輯：

把字串只留A-Z後，紀錄A-Z分別的數量，最後把A-Z數量的值帶入ic的計算公式。

發現：

每個語言平均的IC值不同，而第一個和第四個訊息的IC剛好一樣。

```
message1's ic = 0.06422077622409894
message2's ic = 0.06678956585860447
message3's ic = 0.04942544649037796
message4's ic = 0.06422077622409894
```

4. Given the following ciphertext, please determine if this encrypted message was enciphered using a monoalphabetic or polyalphabetic cipher based on the message's index of coincidence (I.C).

IC = 0.039780853797483695 ≒ 1/26

此訊息IC值趨近於1/26，而經過polyalphabetic加密後的訊息的字母機率分布會差不多，
所以此訊息應該是用polyalphabetic加密。