Quiz 2

Department: 資工 **14** **Student ID: 110550091** **Name:** 吳承瑀

1. Please determine the dimension of the rectangle for this encryption cipher.

   Sum of difference for each dimension is as follows:

3x21:	1.4
21x3:	13.8
7x9:	11.4
9x7:	6.2

   According to the vowel percentage, the program suggests that the dimension of the rectangle should be 3x21. However, vowel percentage is just something to consider, not to obey. 3x21 turns out to not be the correct answer. Thus, we try the second-best choice, which is 9x7 and it is indeed correct.

   In the code, I first put each letter into a vector and counted its length, then factorized the length into different pairs (aka 63 = (3x21), (21x3), (7x9), (9x7)). Then I used these dimensions to find the vowel percentage of each dimensions listed above.

2. Please Solve this following transposition cipher which involves a completely filled rectangles from the HINT below.

The code deciphers to "LASER BEAMS CAN BE MODULATED TO CARRY MORE INTELLIGENCE THAN RADIOWAVES QR".

In the code, I printed each dimension along with each row's respective vowel count and count difference for better visualization. After switching columns around, I realized that 3x21 isn't a reasonable result. Thus, I switched to the 9x7 one and quickly found the key to be "4523617" as written below.

4	5	2	3	6	1	7
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

1	2	3	4	5	6	7
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

3. Please count Index of Coincidence (IC) for each message. The IC of English is around 0.066.

    1. IC = 0.0642208
    2. IC = 0.0667898
    3. IC = 0.0494258
    4. IC = 0.0642210

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.

    IC = 0.0397811

    Since the IC of a normal English text should be around 0.066 and the given text has an IC of around 0.04, I assume it is not a monoalphabetic but rather a polyalphabetic cipher since a polyalphabetic cipher doesn't keep the original letter count.

5. Bonus: Suppose a columnar transposition cipher is not 10 columns by 5 rows, please break this message and state your method! If you can provide your own algorithm will be plus.

    This code deciphers to "LOOK IF I CALLED THE WRONG NUMBER WHY DID YOU ANSWER THE PHONE".

We really had to think outside the ‘box’ on this one. Since the ‘L’, ‘O’, ‘O’, ‘K’, are highlighted in the slides and they are each 6 letters apart, it is obvious that there would be 6. However, the total length of the message was 50, so it is not divisible by 6. Thus, the last row cannot be filled completely. If the last right-most 4 are empty, some cells are off. So, it should be the last bottom 4 that are empty. In order to do so, I programmed it to only fill the first 5 (50%9=5) columns normally and only fill the first 5 (6-1) spots after the first 5 columns.

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