Quiz 2

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

The number of characters in this cipher is 63, so the possible dimension can be either 7X9 or 9X7.

For 7X9 : each row should be approximately 9 X 0.4 = 3.6 vowels

	Number of vowels	Difference
E A L E S V T R A	4	0.4
C E E R O B I I A	6	2.4
D R D N D N Q G E	1	2.6
T A S E Y L L A I	4	0.4
M U A N T C A W H	3	0.6
E O M A N R E E O	6	2.4
C O M S R L T B R	1	2.6

Difference Count Average = (0.4 + 2.4 + 2.6 + 0.4 + 0.6 + 2.4 + 2.6) / 7 = 11.4 / 7 = 1.62857143

For 9X7 : each row should be approximately 7 X 0.4 = 2.8 vowels

	Number of vowels	Difference
E R A S B L E	3	0.2
C A M S N A B	2	0.8
D U M O L E A	4	1.2
T O E D C T A	3	0.2
M O R Y R R E	2	0.8
E L N T L I I	3	0.2
C E E N T G H	2	0.8
A D N R I A O	4	1.2
E S A V Q W R	2	0.8

Difference Count Average = (0.2 + 0.8 + 1.2 + 0.2 + 0.8 + 0.2 +

0.8 + 1.2 + 0.8) / 9 = 6.2 / 9 = 0.68888889

As the result, 9X7 has the smaller difference count average, so the dimension should be row = 9, col = 7.

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

From the result of Part 1, we get :

E R A S B L E

C A M S N A B

.

.

.

We can observe that there is a word “LASER” in row 1 after rearrangement, and a word “BEAM” in row 1 and row 2 after rearrangement. According to the observation, we can find that the decryption order is 4 5 2 3 6 1 7. The result will be :

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.

We use the given function to calculate IC and get the result of each message :

Message 1 IC : 0.064220776224098 94

Message 2 IC : 0.066789565858604 47

Message 3 IC : 0.049425446490377 96

Message 4 IC : 0.064220776224098 94

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.

We calculate the IC of message, which is 0.039780853797483695. Thus, the result is closer to polyalphabetic cipher.

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

The cipher is encrypted with an incomplete rectangle, so we rearrange the cipher by this :

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

After rearrangement, we break the message by reading row by row.