ooxWord://word/media/image2.jpeg

Quiz2

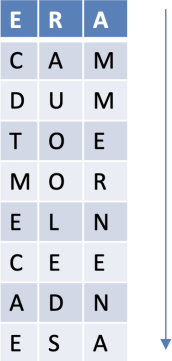
Please write a program including the answers to the following questions.

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

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

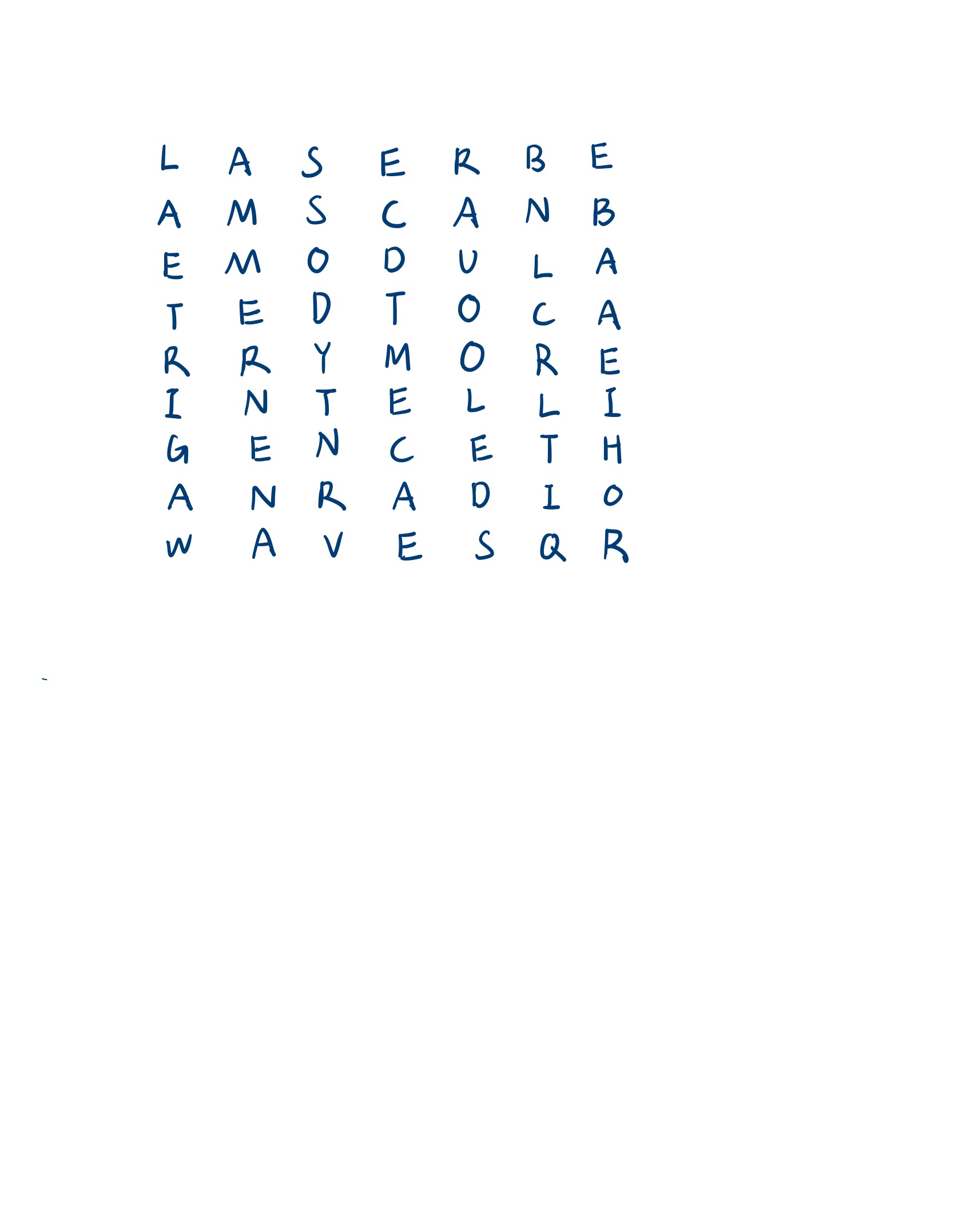
A : Since there are 63 letters , determine the dimension of rectangle as 9\*7

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



A :

4 5 2 3 6 1 7



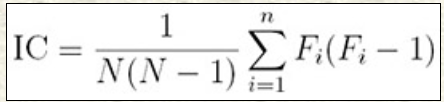
→ Laserbeams can be modulated to carry more intelligence than radio waves .

1. Please count Index of Coincidence (IC) for each message. The IC of English is around 0.

|  |  |
| --- | --- |
| Message 1 | Message 2 |
|  |  |
| Message 3 | Message 4 |
|  |  |

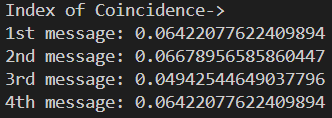
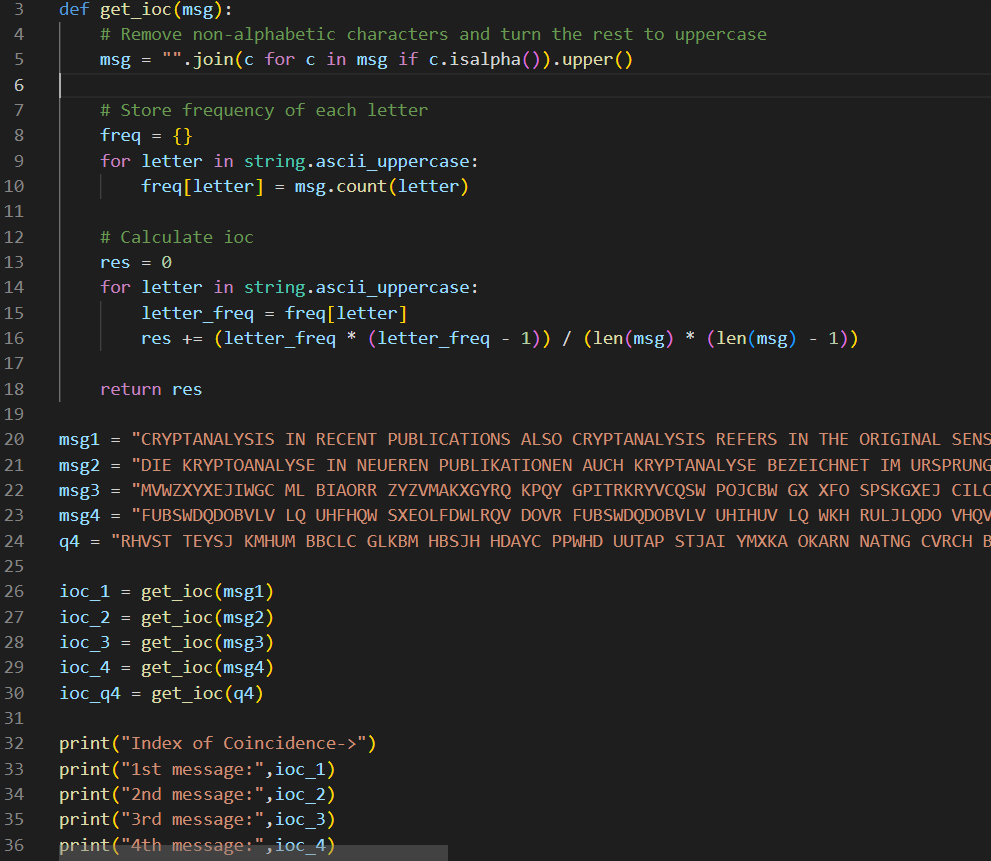
A :

As the picture of “109550135.py” shows , I calculate ioc through the “get\_ioc” function . In the function , first remove non-alphabetic characters and turn the rest to uppercase , then this code can be applied to different common messages . Then , store

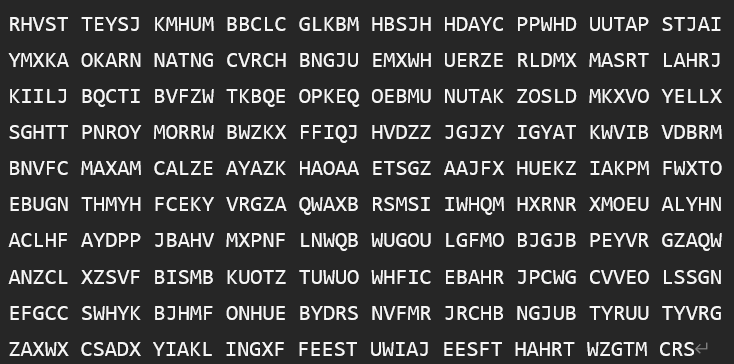
frequency of each letter for latter use .

Finally , calulate ioc with formula , then return

the result .



1. 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



A :

Through “109550135.py” , the ioc of this message is around 0.03978 , which is apparently lower than the expected IoC for a monoalphabetic cipher(around ) , so this message was likely enciphered using a polyalphabetic cipher.

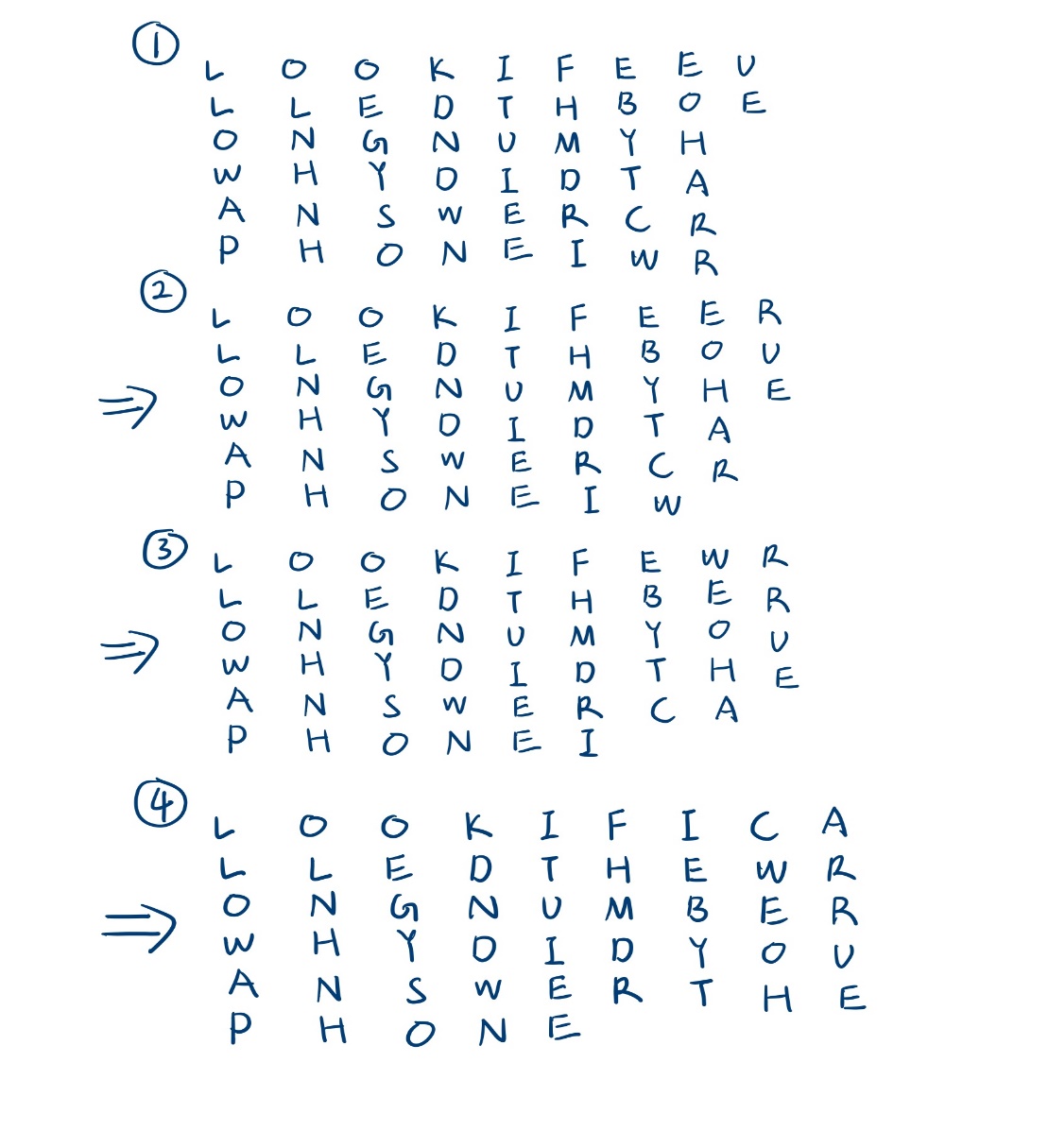
* Bonus: (Please provide another program if you would like to submit it)

Suppose a columnar transposition cipher is not 10 column by 5 row

LLOWA POLNH NHOEG YSOKD NDWNI TUIEE FHMDR IEBYT CWEOH ARRUE.

Please break this message and state your method! If you can provide your own algorithm will be plus

A :



Since the hint showed the first 4 letters of the plaintext , we can know that each

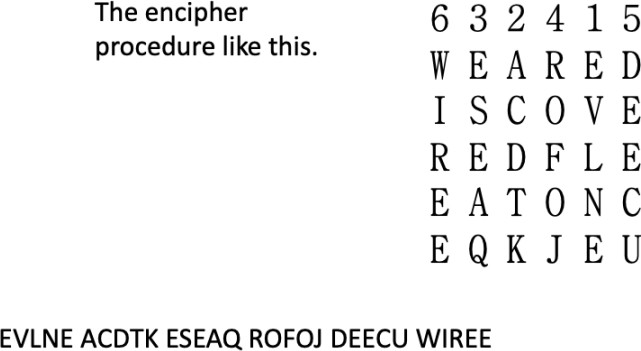
column has 6 letters at most . However , only the last row can have less letters than all

other ones , while the last column can’t . Thus , make each row having 9 letters except

for the last one , then we obtained the result :

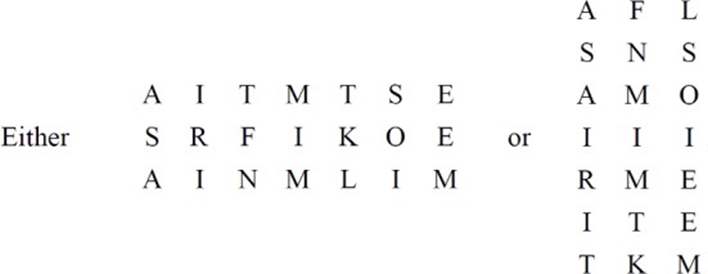
Look if I called the wrong number , why did you answer the phone ?

**Some knowledges related to Quiz2…**

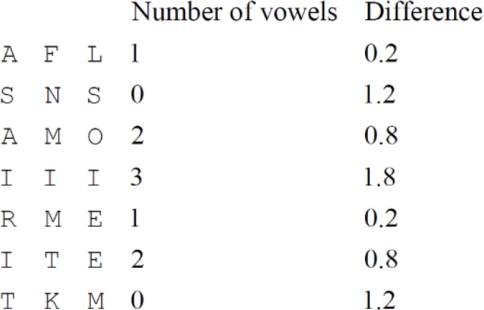
1. **Transposition cipher**: The transposition cipher quite different in substitution It does not change the identities of the letter but rearrange their position
2. **Determine the dimension of the rectangle**

How to determine the dimension of the rectangle?

* + In this case we have 63 letters.
  + Vowel Frequencies can help us to determine the dimensions of the rectangle.
  + In English approximately 40% of plaintext consists of vowels. Therefore, for the correct dimension,
  + each row of the rectangle should be approximately 40% vowels.
  + For example, there are 21 letters in the ciphertext.
  + Because we know that the message completely fills the rectangle, this suggests either a 3X7 or a 7X3
  + array.
  + Consider our choice between 3X7 and 7X3 as an example.
  + For a 3X7 rectangle, each row should contain approximately 2.8 vowels.
  + ECDTM ECAER AUOOL EDSAM MERNE NASSO DYTNR VBNLC RLTIQ LAETR IGAWE BAAEI HOR
  + Let us note the difference between this estimate and the actual count to find the right dimension
    - For a 7 \* 3 or 3 \* 7 rectangle



* + - Sum of 3 \* 7: 0.6, Sum of 7 \* 3: 6.2



* + - It appears that the 3 \* 7 rectangle is more likely.

# Index of Coincidence (IC)