Quiz2

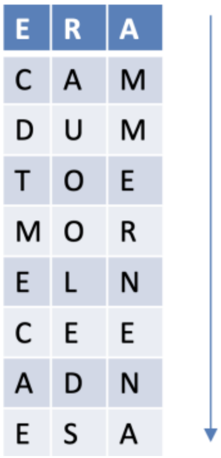
Please write a program including the answers to the following questions.

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

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



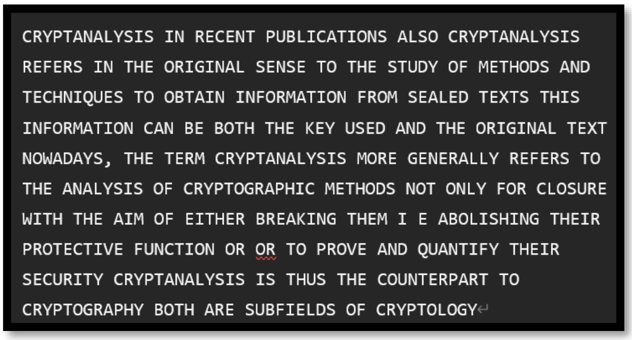
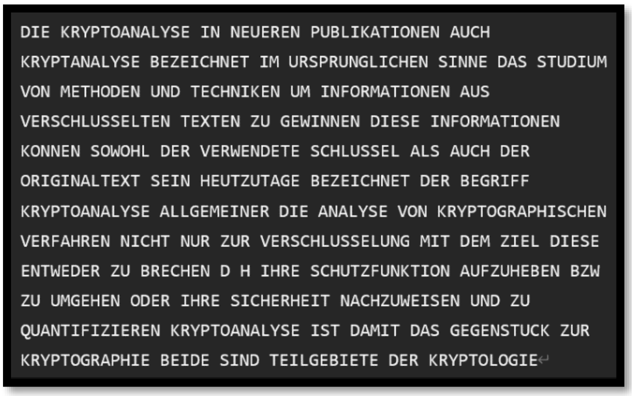
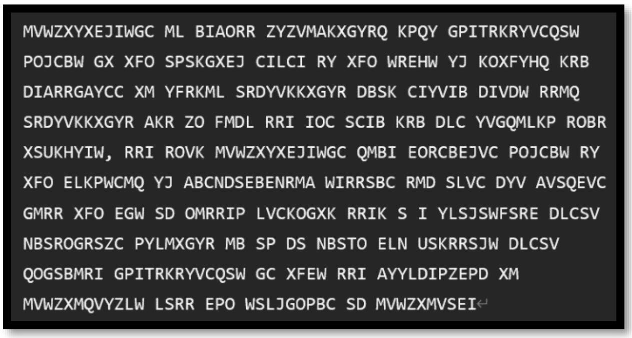
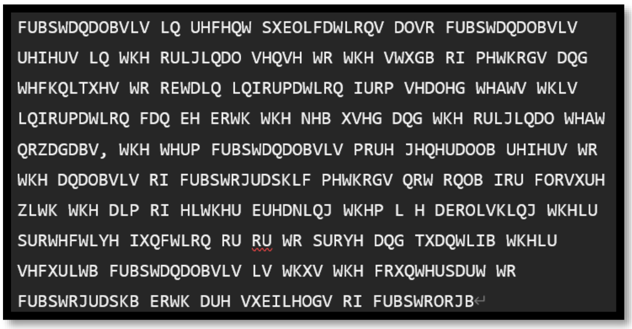
E	R	A
C	A	M
D	U	M
T	O	E
M	O	R
E	L	N
C	E	E
A	D	N
E	S	A

A :

4	5	2	3	6	1	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

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

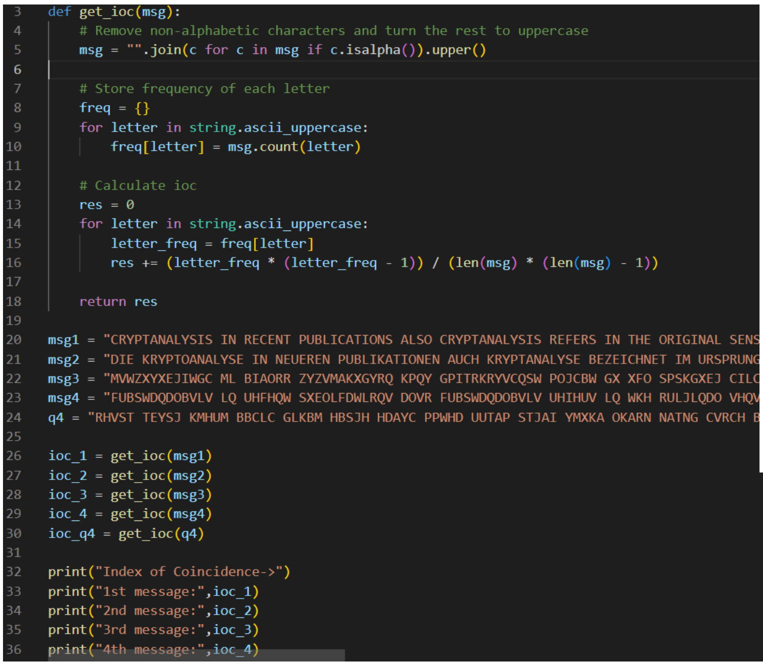
3. Please count Index of Coincidence (IC) for each message. The IC of English is around 0.

Message 1	Message 2
 CRYPTANALYSIS IN RECENT PUBLICATIONS ALSO CRYPTANALYSIS REFERS IN THE ORIGINAL SENSE TO THE STUDY OF METHODS AND TECHNIQUES TO OBTAIN INFORMATION FROM SEALED TEXTS THIS INFORMATION CAN BE BOTH THE KEY USED AND THE ORIGINAL TEXT NOWADAYS, THE TERM CRYPTANALYSIS MORE GENERALLY REFERS TO THE ANALYSIS OF CRYPTOGRAPHIC METHODS NOT ONLY FOR CLOSURE WITH THE AIM OF EITHER BREAKING THEM I E ABOLISHING THEIR PROTECTIVE FUNCTION OR OR TO PROVE AND QUANTIFY THEIR SECURITY CRYPTANALYSIS IS THUS THE COUNTERPART TO CRYPTOGRAPHY BOTH ARE SUBFIELDS OF CRYPTOLOGY	 DIE KRYPTOANALYSE IN NEUEREN PUBLIKATIONEN AUCH KRYPTANALYSE BEZEICHNET IM URSPRUNGLICHEN SINNE DAS STUDIUM VON METHODEN UND TECHNIKEN UM INFORMATIONEN AUS VERSCHLUSSELTEN TEXTEN ZU GEWINNEN DIESE INFORMATIONEN KONNEN SOWOHL DER VERWENDETE SCHLUSSEL ALS AUCH DER ORIGINALTEXT SEIN HEUTZUTAGE BEZEICHNET DER BEGRIFF KRYPTOANALYSE ALLGEMEINER DIE ANALYSE VON KRYPTOGRAPHISCHEN VERFAHREN NICHT NUR ZUR VERSCHLUSSELUNG MIT DEM ZIEL DIESE ENTWEDER ZU BRECHEN D H IHRE SCHUTZFUNKTION AUFZUHEBEN BZW ZU UMGEHEN ODER IHRE SICHERHEIT NACHZUWEISEN UND ZU QUANTIFIZIEREN KRYPTOANALYSE IST DAMIT DAS GEGENSTUCK ZUR KRYPTOGRAPHIE BEIDE SIND TEILGEBIETE DER KRYPTOLOGIE
Message 3	Message 4
 MVWZXYXEJIWGC ML BIAORR ZYZVMAKXGYRQ KPQY GPITRKRYVCQSW POJCBW GX XFO SPSKGXEJ CILCI RY XFO WREHW YJ KOXFYHQ KRB DIARRGAYCC XM YFRKML SRDYVKKXGYR DBSK CIYVIB DIVDW RRMQ SRDYVKKXGYR AKR ZO FMDL RRI IOC SCIB KRB DLC YVGQMLKP ROBR XSUKHYIW, RRI ROVK MVWZXYXEJIWGC QMBI EORCBEJVC POJCBW RY XFO ELKPWCMQ YJ ABCNDSEBENRMA WIRRSBC RMD SLVC DYV AVSQEVC GMRR XFO EGW SD OMRRIP LVCKOGXK RRIK S I YLSJSWFSRE DLCSV NBSROGRSZC PYLMXGYR MB SP DS NBSTO ELN USKRRSJW DLCSV QOGSBMRI GPITRKRYVCQSW GC XFEW RRI AYYLDIPZEPD XM MVWZXMQVYZLW LSRR EPO WSLJGOPBC SD MVWZXMVSEI	 FUBSWDQDOBVLV LQ UHFHQW SXEOLFDWLRQV DOVR FUBSWDQDOBVLV UHIHUV LQ WKH RULJLQDO VHQVH WR WKH VWXGB RI PHWKRGV DQG WHFKQLTXHV WR REWDLQ LQIRUPDWLRQ IURP VHDOHG WHAWV WKLV LQIRUPDWLRQ FDQ EH ERWK WKH NHB XVHG DQG WKH RULJLQDO WHAW QRZDGDBV, WKH WHUP FUBSWDQDOBVLV PRUH JHQHUDOOB UHIHUV WR WKH DQDOBVLV RI FUBSWRJUDSKLF PHWKRGV QRW RQOB IRU FORVXUH ZLWK WKH DLP RI HLWKHU EUHDNLQJ WKHP L H DEROLVKLQJ WKHLU SURWHFWLYH IXQFWLRQ RU RU WR SURYH DQG TXDQWLIB WKHLU VHFXULWB FUBSWDQDOBVLV LV WKXV WKH FRXQWHUSDUW WR FUBSWRJUDSKB ERWK DUH VXEILHOGV RI FUBSWRORJB

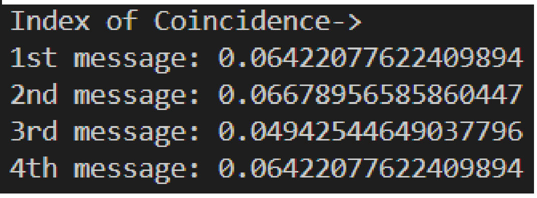
A :

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 $\mathrm{IC} = \frac{1}{N(N-1)} \sum_{i=1}^{n} F_i(F_i - 1)$, then return the result .

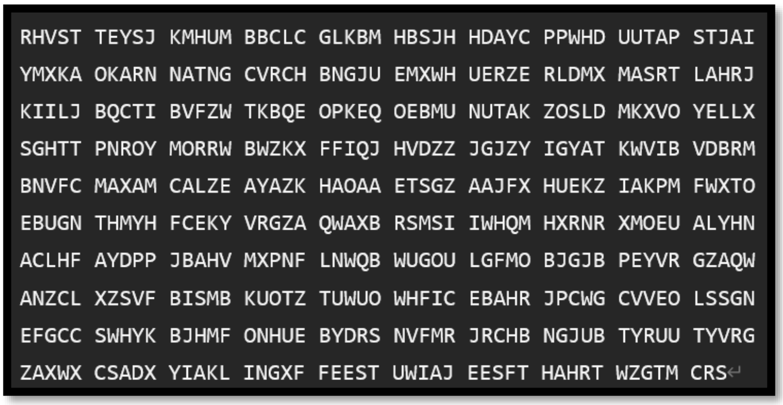


```python
def get_ioc(msg):
    # Remove non-alphabetic characters and turn the rest to uppercase
    msg = "".join(c for c in msg if c.isalpha()).upper()

    # Store frequency of each letter
    freq = {}
    for letter in string.ascii_uppercase:
        freq[letter] = msg.count(letter)

    # Calculate ioc
    res = 0
    for letter in string.ascii_uppercase:
        letter_freq = freq[letter]
        res += (letter_freq * (letter_freq - 1)) / (len(msg) * (len(msg) - 1))

    return res

msg1 = "CRYPTANALYSIS IN RECENT PUBLICATIONS ALSO CRYPTANALYSIS REFERS IN THE ORIGINAL SENS
msg2 = "DIE KRYPTOANALYSE IN NEUEREN PUBLIKATIONEN AUCH KRYPTANALYSE BEZEICHNET IM URSPRUNG
msg3 = "MVWZXYXEJIWGC ML BIAORR ZYZVMAKXGYRQ KPQY GPITRKRYVCQSW POJCBW GX XFO SPSKGXEJ CILC
msg4 = "FUBSWDQDOBVLV LQ UHFHQW SXEOLFDWLRQV DOVR FUBSWDQDOBVLV UHIHUV LQ WKH RULJLQDO VHQV
q4 = "RHVST TEYSJ KMHUM BBCLC GLKBM HBSJH HDAYC PPWHD UUTAP STJAI YMXKA OKARN NATNG CVRCH B

ioc_1 = get_ioc(msg1)
ioc_2 = get_ioc(msg2)
ioc_3 = get_ioc(msg3)
ioc_4 = get_ioc(msg4)
ioc_q4 = get_ioc(q4)

print("Index of Coincidence->")
print("1st message:",ioc_1)
print("2nd message:",ioc_2)
print("3rd message:",ioc_3)
print("4th message:",ioc_4)
```



```
Index of Coincidence->
1st message: 0.06422077622409894
2nd message: 0.06678956585860447
3rd message: 0.04942544649037796
4th message: 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’sindex of coincidence



```
RHVST TEYSJ KMHUM BBCLC GLKBM HBSJH HDAYC PPWHD UUTAP STJAI
YMXKA OKARN NATNG CVRCH BNGJU EMXWH UERZE RLDMX MASRT LAHRJ
KIILJ BQCTI BVFZW TKBQE OPKEQ OEBMU NUTAK ZOSLD MKXVO YELLX
SGHTT PNROY MORRW BWZKX FFIQJ HVDZZ JGJZY IGYAT KWVIB VDBRM
BNVFC MAXAM CALZE AYAZK HAOAA ETSGZ AAJFX HUEKZ IAKPM FWXTO
EBUGN THMYH FCEKY VRGZA QWAXB RSMSI IWHQM HXRNR XMOEU ALYHN
ACLHF AYDPP JBAHV MXPNF LNWQB WUGOU LGFMO BJGJB PEYVR GZAQW
ANZCL XZSVF BISMB KUOTZ TUWUO WHFIC EBAHR JPCWG CVVEO LSSGN
EFGCC SWHYK BJHMF ONHUE BYDRS NVFMR JRCHB NGJUB TYRUU TYVRG
ZAXWX CSADX YIAKL INGXF FEEST UWIAJ EESFT HAHRT WZGTM CRS
```

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.

- <u>Bonus: (Please provide another program if you would like to submit it)</u>

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 :

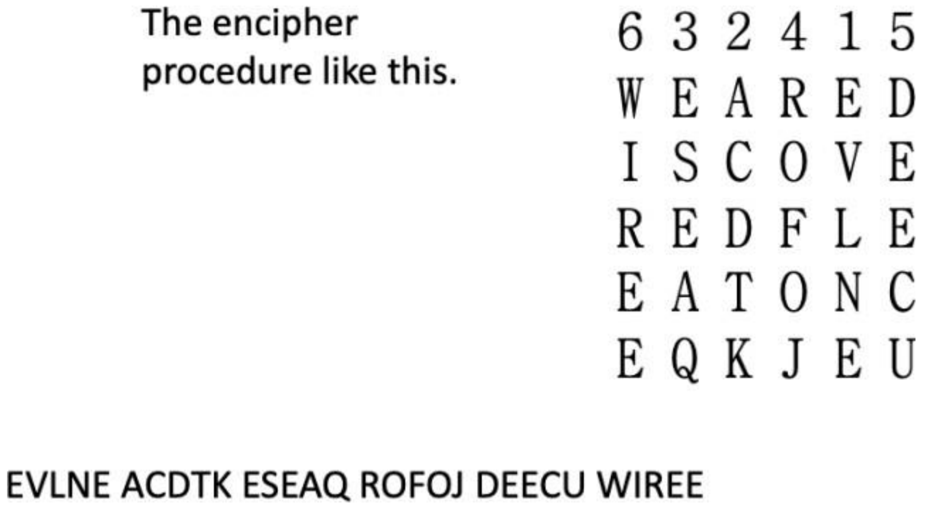
```
①  L O O K I F E E U
   L L E D T H B O E
   O N G N U M Y H
   W H Y O I D T A
   A N S W E R C R
   P H O N E I W R

②  L O O K I F E E R
   L L E D T H B O U
⇒  O N G N U M Y H E
   W H Y O I D T A
   A N S W E R C R
   P H O N E I W

③  L O O K I F E W R
   L L E D T H B E R
⇒  O N G N U M Y O U
   W H Y O I D T H E
   A N S W E R C A
   P H O N E I

④  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 O I D Y O U
   A N S W E R T H E
   P H O N E
```

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



The encipher procedure like this.

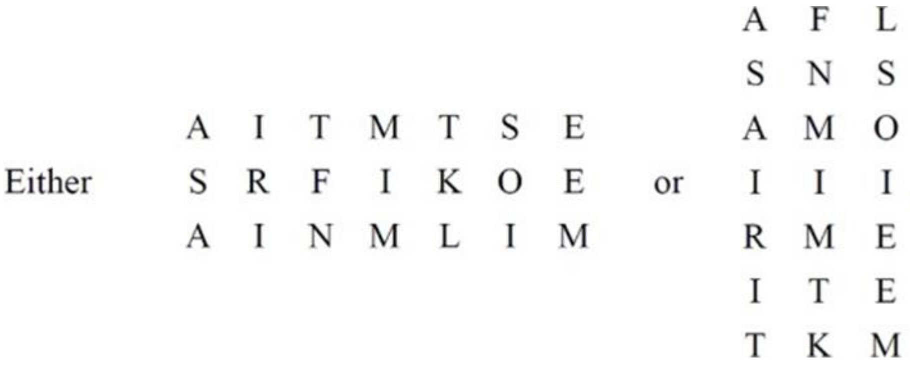
6	3	2	4	1	5
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	F	L	E
E	A	T	O	N	C
E	Q	K	J	E	U

EVLNE ACDTK ESEAQ ROFOJ DEECU WIREE

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



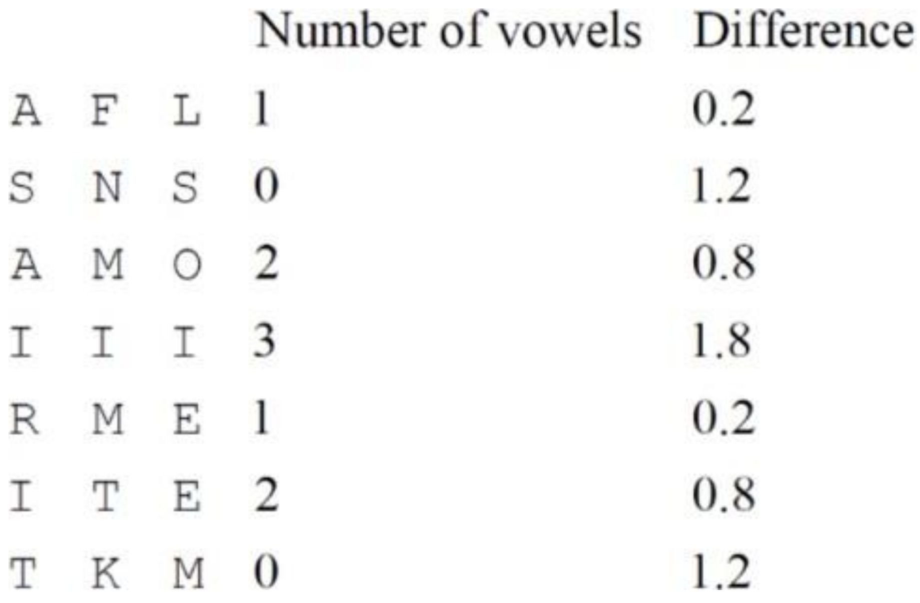
Either

A	I	T	M	T	S	E
S	R	F	I	K	O	E
A	I	N	M	L	I	M

or

A	F	L
S	N	S
A	M	O
I	I	I
R	M	E
I	T	E
T	K	M

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



			Number of vowels	Difference
A	F	L	1	0.2
S	N	S	0	1.2
A	M	O	2	0.8
I	I	I	3	1.8
R	M	E	1	0.2
I	T	E	2	0.8
T	K	M	0	1.2

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

3. Index of Coincidence (IC)

$$f_a,\ f_b, f_c,\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ .\ f_z,$$

$$\frac{(f_a)}{(N)}\ \frac{(f_a-1)}{(N-1)}$$

$$\frac{(f_i)}{(N)}\ \frac{(f_i-1)}{(N-1)}$$

$$\text{Index of Coincidence I.C.} = \frac{\sum_{i=A}^{i=Z}(f_i)(f_i-1)}{(N)(N-1)}$$