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

```
EALESVTRA 0.3999999999999999
CEEROBIIA 2.4
DRDNDNQGE 2.6
TASEYLLAI 0.3999999999999999
MUANTCAWH 0.6000000000000001
EOMANREEO 2.4
COMSRLTBR 2.6
dim: (7, 9) error: 11.4
```

```
ERASBLE 0.19999999999999973
CAMSNAB 0.8000000000000003
DUMOLEA 1.1999999999999997
TOEDCTA 0.19999999999999973
MORYRRE 0.8000000000000003
ELNTLII 0.19999999999999973
CEENTGH 0.8000000000000003
ADNRIAO 1.1999999999999997
ESAVQWR 0.8000000000000003
dim: (9, 7) error: 6.199999999999999
```

因 3*21 和 21*3 無法得出答案，所以只考慮 7*9 和 9*7，運用母音在單字中佔 40%來推斷，9*7 的誤差只有 6.2 比 7*9 的 11.4 小，得出 9*7 的機率可能性較高。

程式碼：

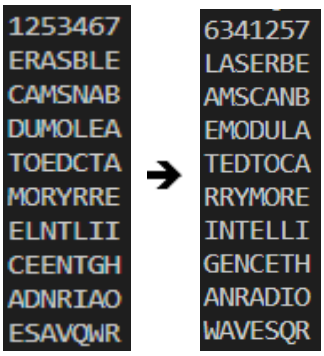
```python

def vowel_rate(words,dim):
    diff = 0
    for i in range(0,dim[0]):
        vow = 0
        for j in range(0,dim[1]):
            print(words[j*dim[0]+i],end="")
            if words[j*dim[0]+i] in 'AEIOU':
                vow+=1
        print("",abs(vow-dim[1]*0.4))
        diff += abs(vow-dim[1]*0.4)
        #print(vow-dim[1]*0.4)
    return diff
if __name__ == "__main__":
    words = "ECDTM ECAER AUOOL EDSAM MERNE NASSO DYTNRVBNLC RLTIQ LAETR IGAWE BAAEI HOR".replace(" ","")
    dim1 = (7,9)
    dim2 = (9,7)
    print("dim:",dim1,"error:",vowel_rate(words,dim1))
    print()
    print("dim:",dim2,"error:",vowel_rate(words,dim2))

```

根據不同的 dimension 分割為若干個 row，並分別計算出現的母音數和平均值的誤差。

2. 原本的 rectangle 和 交換 column 解密後的 rectangle 分別為：



LASER BEAMS CAN BE MODULATED TO CARRY MORE INTELLIGENCE THAN RADIO WAVES QR 為解密出來的明文

3. Index of coincidence:

Message1：0.06422

```
CRYPTANALYSIS IN RECENT PUBLICATIONS ALSO CRYPTANALYSIS REFERS IN THE ORIGINAL S
ENSE TO THE STUDY OF METHODS AND TECHNIQUES TO OBTAIN INFORMATION FROM SEALED TE
XTS THIS INFORMATION CAN BE BOTH THE KEY USED AND THE ORIGINAL TEXT NOWADAYS, TH
E TERM CRYPTANALYSIS MORE GENERALLY REFERS TO THE ANALYSIS OF CRYPTOGRAPHIC METH
ODS NOT ONLY FOR CLOSURE WITH THE AIM OF EITHER BREAKING THEM I E ABOLISHING THE
IR PROTECTIVE FUNCTION OR OR TO PROVE AND QUANTIFY THEIR SECURITY CRYPTANALYSIS
IS THUS THE COUNTERPART TO CRYPTOGRAPHY BOTH ARE SUBFIELDS OF CRYPTOLOGY
0.06422077622409894
```

Message2：0.06679

```
DIE KRYPTOANALYSE IN NEUEREN PUBLIKATIONEN AUCH KRYPTANALYSE BEZEICHNET IM URSPR
UNGLICHEN SINNE DAS STUDIUM VON METHODEN UND TECHNIKEN UM INFORMATIONEN AUS VERS
CHLUSSELTEN TEXTEN ZU GEWINNEN DIESE INFORMATIONEN KONNEN SOWOHL DER VERWENDETE
SCHLUSSEL ALS AUCH DER ORIGINALTEXT SEIN HEUTZUTAGE BEZEICHNET DER BEGRIFF KRYPT
OANALYSE ALLGEMEINER DIE ANALYSE VON KRYPTOGRAPHISCHEN VERFAHREN NICHT NUR ZUR V
ERSCHLUSSELUNG MIT DEM ZIEL DIESE ENTWEDER ZU BRECHEN D H IHRE SCHUTZFUNKTION AU
FZUHEBEN BZW ZU UMGEHEN ODER IHRE SICHERHEIT NACHZUWEISEN UND ZU QUANTIFIZIEREN
KRYPTOANALYSE IST DAMIT DAS GEGENSTUCK ZUR KRYPTOGRAPHIE BEIDE SIND TEILGEBIETE
DER KRYPTOLOGIE
0.06678956585860447
```

Message3：0.04943

```
MVWZXYXEJIWGC ML BIAORR ZYZVMAKXGYRQ KPQY GPITRKRYVCQSW POJCBW GX XFO SPSKGXEJ C
ILCI RY XFO WREHW YJ KOXFYHQ KRB DIARRGAYCC XM YFRKML SRDYVKKXGYR DBSK CIYVIB DI
VDW RRMQ SRDYVKKXGYR AKR ZO FMDL RRI IOC SCIB KRB DLC YVGQMLKP ROBR XSUKHYIW, RR
I ROVK MVWZXYXEJIWGC QMBI EORCBEJVC POJCBW RY XFO ELKPWCMQ YJ ABCNDSEBENRMA WIRR
SBC RMD SLVC DYV AVSQEVC GMRR XFO EGW SD OMRRIP LVCKOGXK RRIK S I YLSJSWFSRE DLC
SV NBSROGRSZC PYLMXGYR MB SP DS NBSTO ELN USKRRSJW DLCSV QOGSBMRI GPITRKRYVCQSW
GC XFEW RRI AYYLDIPZEPD XM MVWZXMQVYZLW LSRR EPO WSLJGOPBC SD MVWZXMVSEI
0.04942544649037796
```

Message4：0.06422

```
FUBSWDQDOBVLV LQ UHFHQW SXEOLFDWLRQV DOVR FUBSWDQDOBVLV UHIHUV LQ WKH RULJLQDO V
HQVH WR WKH VWXGB RI PHWKRGV DQG WHFKQLTXHV WR REWDLQ LQIRUPDWLRQ IURP VHDOHG WH
AWV WKLV LQIRUPDWLRQ FDQ EH ERWK WKH NHB XVHG DQG WKH RULJLQDO WHAW QRZDGDBV, WK
H WHUP FUBSWDQDOBVLV PRUH JHQHUDOOB UHIHUV WR WKH DQDOBVLV RI FUBSWRJUDSKLF PHWK
RGV QRW RQOB IRU FORVXUH ZLWK WKH DLP RI HLWKHU EUHDNLQJ WKHP L H DEROLVKLQJ WKH
LU SURWHFWLYH IXQFWLRQ RU RU WR SURYH DQG TXDQWLB WKHLU VHFXULWB FUBSWDQDOBVLV
LV WKXV WKH FRXQWHUSDUW WR FUBSWRJUDSKB ERWK DUH VXEILHOGV RI FUBSWRORJB
0.06422077622409894
```

程式碼：

```python
def index_of_coincidence(words):
    words = words.replace(" ","")
    words = words.upper()
    freq = [0]*26
    n = 0
    ans =0
    for i in range(0,26):
        now = chr(ord('A')+i)
        freq[i] = words.count(now)
        n+= freq[i]
    for i in freq:
        ans +=i*(i-1)
    ans /= n*(n-1)

    print(ans)

if __name__ =="__main__":
    word1 ="CRYPTANALYSIS IN RECENT PUBLICATIONS ALSO CRYPTANALYSIS REFERS IN THE ORIGINAL SENSE TO
    word2 ="DIE KRYPTOANALYSE IN NEUEREN PUBLIKATIONEN AUCH KRYPTANALYSE BEZEICHNET IM URSPRUNGLICHE
    word3 ="MVWZXYXEJIWGC ML BIAORR ZYZVMAKXGYRQ KPQY GPITRKRYVCQSW POJCBW GX XFO SPSKGXEJ CILCI RY
    word4 ="FUBSWDQDOBVLV LQ UHFHQW SXEOLFDWLRQV DOVR FUBSWDQDOBVLV UHIHUV LQ WKH RULJLQDO VHQVH WR
    print(word1)
    index_of_coincidence(word1)
    print()
    print(word2)
    index_of_coincidence(word2)
    print()
    print(word3)
    index_of_coincidence(word3)
    print()
    print(word4)
    index_of_coincidence(word4)
    print()
    word5 = "RHVST TEYSJ KMHUM BBCLC GLKBM HBSJH HDAYC PPWHD UUTAP STJAI YMXKA OKARN NATNG CVRCH BNG
    print(word5)
    index_of_coincidence(word5)
```

將文章掃過一遍，計算出個字母出現的個數，和總字母數，並按照公式計算出 index of coincidence

4. Index of coincidence of this message is 0.03978，遠小於 English 的 0.066，因此，此密碼是使用 polyalphabetic cipher

```
RHVST TEYSJ KMHUM BBCLC GLKBM HBSJH HDAYC PPWHD UUTAP STJAI YMXKA OKARN NATNG CV
RCH BNGJU EMXWH UERZE RLDMX MASRT LAHRJ KIILJ BQCTI BVFZW TKBQE OPKEQ OEBMU NUTA
K 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 VR
GZA QWAXB RSMSI IWHQM HXRNR XMOEU ALYHN ACLHF AYDPP JBAHV MXPNF LNWQB WUGOU LGFM
O 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 IN
GXF FEEST UWIAJ EESFT HAHRT WZGTM CRS
0.039780853797483695
```

5. Bonus:

   LLOWA POLNH NHOEG YSOKD NDWNI TUIEE FHMDR IEBYT CWEOH ARRUE.

   將此密文直的填橫的讀最後 1 row 不足的補空格，補到完整的 rectangle。

   將可能的解列出後，

```
==================6*9==================
LOOKIFICA
LLEDTHEWR
ONGNUMBER
WHYDIDYOU
ANSWERTHE
PHONE
```

   6*9 會是可以得出可以得到明文，

   LOOK IF I CALLED THE WRONG NUMBER WHY DID YOU ANSWER THE PHONE

   程式碼

```python
import math
def decode(words,dim):
    ans = [""]*dim[0]
    rest = dim[1]-(dim[0]*dim[1]-50)
    if rest <0 or rest==0:
        print(dim, "is not avaliable")
        return
    for i in range(0,rest*dim[0]):
        ans[i%dim[0]]+=words[i]
    at = 0
    for i in range(rest*dim[0],50):
        ans[at%(dim[0]-1)]+=words[i]
        at+=1
    for i in ans:
        print(i)

if __name__ == "__main__":
    words = "LLOWA POLNH NHOEG YSOKD NDWNI TUIEE FHMDR IEBYT CWEOH ARRUE".replace(" ","
    for i in range(6,15):
        temp = math.ceil(50/i)
        print("=================="+str(i)+"*"+str(temp)+"==================")
        decode(words,(i,temp))
        print("==================================================")

```

先計算出目標 dimension 需要多少 dimension 和多少空格，若是此矩陣可以正常顯現則計算密文需填到矩陣的哪個位子後，最後人工判斷哪個矩陣可以解出明文。