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

For 9*7 rectangle, each row is about 2.8 vowels, and for 7*9 rectangle, each row is about 3.6 vowels. According to the result below, the rectangle is more likely to be 9*7.

9*7 rectangle -> sum of difference: 6.2

							Frequency	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

7*9 rectangle -> sum of difference: 11.4

									Frequency	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

```
PS D:\nycu\密碼工程\311605012_hw2> python .\311605012_Q1.py
Please input your cipher text:
ECDTM ECAER AUOOL EDSAM MERNE NASSO DYTNR VBNLC RLTIQ LAETR IGAWE BAAEI HOR
For 1*63 triangle, the sum of the difference is 0.2
For 3*21 triangle, the sum of the difference is 1.4
For 21*3 triangle, the sum of the difference is 13.8
For 9*7 triangle, the sum of the difference is 6.2
For 7*9 triangle, the sum of the difference is 11.4
For 63*1 triangle, the sum of the difference is 30.2
```

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

   According to the frequency with the pair of the alphabet, we can construct it in the ciphertext, and keep switching to find the plaintext.

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

➔ Laser beam can be modulated to carry more intelligence than radiowavesqr

Picture below is using the program try to find the high frequency pair constructed with two alphabets in the ciphertext, but it still needs to keep switching until finding the plaintext.
(0,1) (2,3) (4,5) are the ciphertext column index that can construct the high frequency pair with two alphabets.

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

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

➔ 0.06422

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

➔ 0.06679

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

➔ 0.04943

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

➔ 0.06422

```
PS D:\nycu\密碼工程\311605012_hw2> python .\311605012_Q3.py
Please input your case number: Q3_1
0.06422
Please input your case number: Q3_2
0.06679
Please input your case number: Q3_3
0.04943
Please input your case number: Q3_4
0.06422
```

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

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

➔ 0.03978

```
PS D:\nycu\密碼工程\311605012_hw2> python .\311605012_Q3.py
Please input your case number: Q4
0.03978
```

The IC of the monoalphabetic cipher is close to 0.067, and the IC of the polyalphabetic cipher is close to 0.0385. According to the IC counting by the program, this encrypted message is enciphered by using a polyalphabetic cipher.