Cryptography Engineering Quiz2 310555004 呂佳柔

Ciphertext:
ECDTM ECAER AUOOL EDSAM MERNE NASSO DYTNR VBNLC RLTIQ LAETR IGAWE BAAEI HOR

Appearance Frequency:

A	B	C	D	E	F	G	H	I	J	K	L	M
8	2	3	3	9	0	1	1	3	0	0	4	3
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
4	4	0	1	6	3	4	1	1	1	0	1	0

Total 63 character

1. For a 9x7 rectangle, each row should contain approximately 2.8 vowels, and for a 7x9 rectangle it is about 3.6 vowels. Because the sum of the difference is 6.2 for 9x7 rectangle, it appears that the 9x7 rectangle is more likely.

   9x7 rectangle, the sum of the difference is 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

   7x9 rectangle, the sum of the difference is 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

From the results of the program, it can be seen that the sum of the difference in other dimensions rectangles, and 9 x 7 rectangle would be the best option.

```
/Desktop/310555004_q1.py
For 1 x 63 rectangle, the sum of the difference is 0.2
For 3 x 21 rectangle, the sum of the difference is 1.4
For 7 x 9 rectangle, the sum of the difference is 11.4
For 9 x 7 rectangle, the sum of the difference is 6.2
For 21 x 3 rectangle, the sum of the difference is 13.8
For 63 x 1 rectangle, the sum of the difference is 30.2
```

2. Transposition cipher

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

Plan Text:

Laser beams can be modulated to carry more intelligence than radio waves qr.

3. Count Index of Coincidence (IC) for each message.

I. 0.06422

```
PS C:\Users\jasmi\Desktop> & C:/Users/jasmi/AppData/Local/Microsoft/Wi
ndowsApps/python3.10.exe c:/Users/jasmi/Desktop/310555004.py
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 (0.06422077622409894)
```

II. 0.06679

```
ndowsApps/python3.10.exe c:/Users/jasmi/Desktop/310555004.py
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
KRYPTOGRAPHIE BEIDE SIND TEILGEBIETE DER KRYPTOLOGIE
0.06679 (0.06678956585860447)
```

III. 0. 04943

```
10.exe c:/Users/jasmi/Desktop/310555004.py
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 SRDYVKK
XGYR AKR ZO FMDL RRI IOC SCIB KRB DLC YVGQMLKP ROBR XSUKHYIW, RRI ROVK MVWZXYXEJIWGC QMB
I EORCBEJVC POJCBW RY XFO ELKPWCMQ YJ ABCNDSEBENRMA WIRRSBC RMD SLVC DYV AVSQEVC GMRR XF
O EGW SD OMRRIP LVCKOGXK RRIK S I YLSJSWFSRE DLCSV NBSROGRSZC PYLMXGYR MB SP DS NBSTO EL
N USKRRSJW DLCSV QOGSBMRI GPITRKRYVCQSW GC XFEW RRI AYYLDIPZEPD XM MVWZXMQVYZLW LSRR EPO
 WSLJGOPBC SD MVWZXMVSEI
0.04943 (0.04942544649037796)
```

IV. 0.06422

```
PS C:\Users\jasmi\Desktop> & C:/Users/jasmi/AppData/Local/Microsoft/WindowsApps/python3.
10.exe c:/Users/jasmi/Desktop/310555004.py
FUBSWDQDOBVLV LQ UHFHQW SXEOLFDWLRQV DOVR FUBSWDQDOBVLV
UHIHUV LQ WKH RULJLQDO VHQVH WR WKH VWXGB RI PHWKRGV DQG WHFKQLTXHV WR REWDLQ LQIRUPDWLR
Q 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 S
URWHFWLYH IXQFWLRQ RU RU WR SURYH DQG TXDQWLB WKHLU VHFXULWB FUBSWDQDOBVLV LV WKXV WKH
FRXQWHUSDUW WR FUBSWRJUDSKB ERWK DUH VXEILHOGV RI FUBSWRORJB
0.06422 (0.06422077622409894)
```

4. Please determine if this encrypted message was enciphered using a monoalphabetic or polyalphabetic cipher based on the message's index of coincidence.

```
PS C:\Users\jasmi\Desktop> & C:/Users/jasmi/AppData/Local/Microsoft/WindowsApps/python3.
10.exe c:/Users/jasmi/Desktop/310555004.py
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 (0.039780853797483695)
```

Normally, the IC of monoalphabetic cipher is closer to 0.067, and the IC of polyalphabetic cipher is closer to 0.0385. Judging from the IC in the above figure is 0.03978, this cipher text should be polyalphabetic cipher.