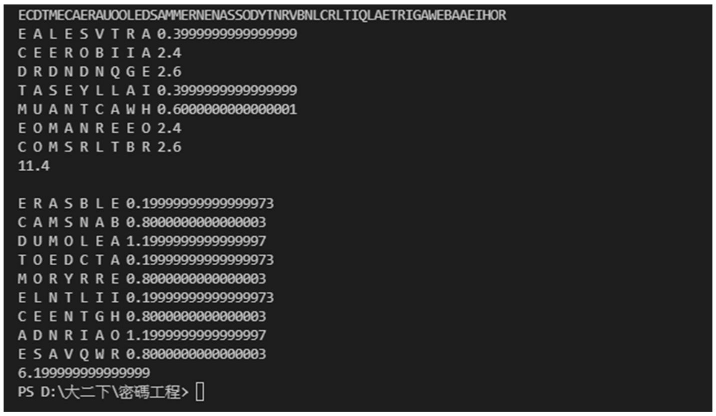
密碼工程 Quiz2

Problem-1



```
ECDTMECAERAUOOLEDSAMMERNENASSODYTNRVBNLCRLTIQLAETRIGAWEBAAEIHOR
E A L E S V T R A 0.3999999999999999
C E E R O B I I A 2.4
D R D N D N Q G E 2.6
T A S E Y L L A I 0.3999999999999999
M U A N T C A W H 0.6000000000000001
E O M A N R E E O 2.4
C O M S R L T B R 2.6
11.4

E R A S B L E 0.19999999999999973
C A M S N A B 0.800000000000003
D U M O L E A 1.1999999999999997
T O E D C T A 0.19999999999999973
M O R Y R R E 0.800000000000003
E L N T L I I 0.19999999999999973
C E E N T G H 0.800000000000003
A D N R I A O 1.1999999999999997
E S A V Q W R 0.800000000000003
6.199999999999999
PS D:\大二下\密碼工程> ▯
```

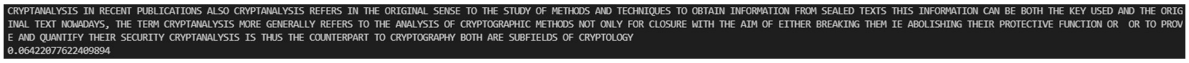
From the result, we can easily find that the sum of the difference of dimension 7x9 is 11.4, and the sum of the difference of dimension 9x7 is approximately 6.2. So, we consider that the 9x7 rectangle is more likely.

Problem-2

LASERBE
AMSCANB
EMODULA
TEDTDCA
RRYMORE
INTELLI
BENCETH
ANRADIO
WAVESRR

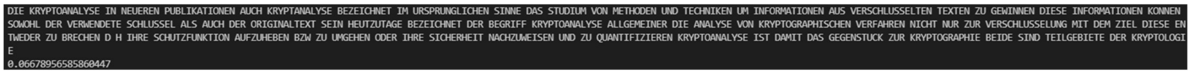
Problem-3

IOC in Message1 is approximately 0.064.



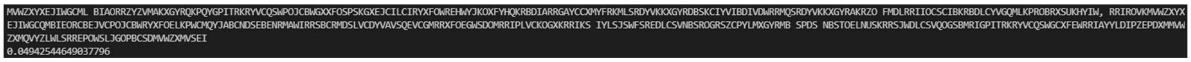
```
CRYPTANALYSIS IN RECENT PUBLICATIONS ALSO CRYPTANALYSIS REFERS IN THE ORIGINAL SENSE TO THE STUDY OF METHODS AND TECHNIQUES TO OBTAIN INFORMATION FROM SEALED TEXTS THIS INFORMATION CAN BE BOTH THE KEY USED AND THE ORIG
INAL TEXT NOWADAYS, THE TERM CRYPTANALYSIS MORE GENERALLY REFERS TO THE ANALYSIS OF CRYPTOGRAPHIC METHODS NOT ONLY FOR CLOSURE WITH THE AIM OF EITHER BREAKING THEM IE ABOLISHING THEIR PROTECTIVE FUNCTION OR  OR TO PROV
E AND QUANTIFY THEIR SECURITY CRYPTANALYSIS IS THUS THE COUNTERPART TO CRYPTOGRAPHY BOTH ARE SUBFIELDS OF CRYPTOLOGY
0.06422077622409894
```

IOC in Message2 is approximately 0.067.



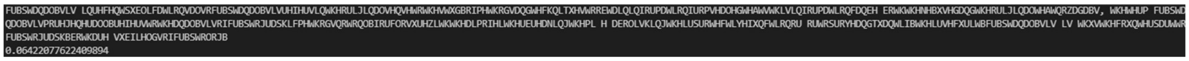
```
DIE KRYPTOANALYSE IN NEUEREN PUBLIKATIONEN AUCH KRYPTANALYSE BEZEICHNET IM URSPRUNGLICHEN SINNE DAS STUDIUM VON METHODEN UND TECHNIKEN UM INFORMATIONEN AUS VERSCHLUSSELTEN TEXTEN ZU GEWINNEN DIESE INFORMATIONEN KONNEN 
SOWOHL DER VERWENDETE SCHLUSSEL ALS AUCH DER ORIGINALTEXT SEIN HEUTZUTAGE BEZEICHNET DER BEGRIFF KRYPTOANALYSE ALLGEMEINER DIE ANALYSE VON KRYPTOGRAPHISCHEN VERFAHREN NICHT NUR ZUR VERSCHLUSSELUNG MIT DEM ZIEL DIESE EN
TWEDER 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 KRYPTOLOGI
E
0.06678956585860447
```

IOC in Message3 is approximately 0.049.



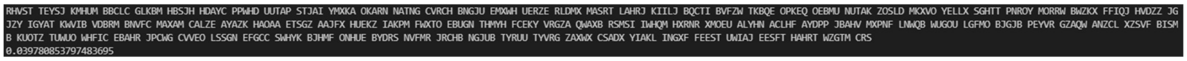
```
MVWZXYXEJIWGCML BIAORRZYZVMAKXGYRQKPQYGPITRKRYVCQSWPOJCBWGXXFOSPSKGXEJCILCIRYXFOWREHWYJKOXFYHQKRBDIARRGAYCCXMYFRKMLSRDYVKKXGYRDBSKCIYVIBDIVDWRRMQSRDYVKKXGYRAKRZO FMDLRRIIOCSCIBKRBDLCYVGQMLKPROBRXSUKHYIW, RRIROVKMVWZXYX
EJIWGCQMBIEORCBEJVCPOJCBWRYXFOELKPWCMQYJABCNDSEBENRMAWIRRSBCRMDSLVCDYVAVSQEVCGMRRXFOEGWSDOMRRIPLVCKOGXKRRIKS IYLSJSWFSREDLCSVNBSROGRSZCPYLMXGYRMB SPDS NBSTOELNUSKRRSJWDLCSVQOGSBMRIGPITRKRYVCQSWGCXFEWRRIAYYLDIPZEPDXMMVW
ZXMQVYZLWLSRREPOWSLJGOPBCSDMVWZXMVSEI
0.04942544649037796
```

IOC in Message4 is approximately 0.064.



```
FUBSWDQDOBVLV LQUHFHQWSXEOLFDWLRQVDOVRFUBSWDQDOBVLVUHIHUVLQWKHRULJLQDOVHQVHWRWKHVWXGBRIPHWKRGVDQGWHFKQLTXHVWRREWDLQLQIRUPDWLRQIURPVHDOHGWHAWVWKLVLQIRUPDWLRQFDQEH ERWKWKHNHBXVHGDQGWKHRULJLQDOWHAWQRZDGDBV, WKHWHUP FUBSWD
QDOBVLVPRUHJHQHUDOOBUHIHUVWRWKHDQDOBVLVRIFUBSWRJUDSKLFPHWKRGVQRWRQOBIRUFORVXUHZLWKWKHDLPRIHLWKHUEUHDNLQJWKHPL H DEROLVKLQJWKHLUSURWHFWLYHIXQFWLRQRU RUWRSURYHDQGTXDQWLIBWKHLUVHFXULWBFUBSWDQDOBVLV LV WKXVWKHFRXQWHUSDUWWR
FUBSWRJUDSKBERWKDUH VXEILHOGVRIFUBSWRORJB
0.06422077622409894
```

Problem-4



```
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 JG
JZY 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 BISM
B 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
0.039780853797483695
```

Using the analysis of index of coincidence, this message has the IOC approximately 0.04. As we know the IOC of English is about 0.066. So, we can have the conclusion that this message is used polyalphabetic cipher.

Because if this message is used monoalphabetic cipher, the IOC of the cipher text would also approximately at 0.066.