

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 IGAW E BAAEI HOR

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



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

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
KÖNNEN 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 ODER IHRE SCHUTZFUNKTION AUFZUHEBEN BZW
ZU UMGEHEN ODER IHRE SICHERHEIT NACHZUWEISEN UND ZU
QUANTIFIZIEREN KRYPTOANALYSE IST DAMIT DAS GEGENSTÜCK ZUR
KRYPTOGRAPHIE BEIDE SIND TEILGEBIETE DER KRYPTOLOGIE

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
MVWZXMVQVYZLW 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
QRZDGBV, WKH WHUP FUBSWDQDOBVLV PRUH JHQHUDO 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 TXDQWLIV WKHLU
VHFXULWB FUBSWDQDOBVLV LV WKXV WKH FRXQWHUSDW WR
FUBSWRJUDSKB ERWK DUH VXEILHOGV RI FUBSWRORJB

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
ACLFH	AYDPP	JBAHV	MXPNF	LNWQB	WUGOU	LGFMQ	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

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

Suppose a columnar transposition cipher is not 10 column by 5 row

LLOWA POLNH NHOEG YSOKD NDWNI TUIEE FHMDR IEBYT CWE OH ARRUE.

Please break this message and state your method! If you can provide your own algorithm will be plus

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.
- ECDDTM ECAER AUOOL EDSAM MERNE NASSO DYTNR VBNLC RLTIQ LAETR IGAWEBAAEI 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	or	A	F	L
	S	R	F	I	K	O	E		S	N	S
	A	I	N	M	L	I	M		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)

$$f_a, f_b, f_c, \dots \dots \dots f_z,$$

$$\frac{(f_a)}{(N)} \quad \frac{(f_{a-1})}{(N-1)}$$

$$\frac{(f_i)}{(N)} \quad \frac{(f_{i-1})}{(N-1)}$$

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