Quiz 2 revised

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

9

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

How to determine the dimension of the rectangle?

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

9

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.
- Let us note the difference between this estimate and the actual count.

Either

A	I	T	M	T	S	E	
S	R	F	I	K	O	E	
A	I	N	M	L	I	M	

or

A	F	L
S	N	S
A	M	O
I	I	I
R	M	E
I	T	E
T	K	M

.

40% vowels. Consider our choice between 3×7 and 7×3.

For a 3×7 rectangle, each row should contain approximately 2.8 vowels. Let us note the difference between this estimate and the actual count:

							Number of vowels	Difference
A	I	T	M	T	S	E	3	0.2
S	R	F	I	K	O	E	3	0.2
A	I	N	M	L	I	M	3	0.2

The sum of the differences is 0.6.

For a 7×3 rectangle:

			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

The sum of the differences is 6.2. It appears that the 3×7 rectangle is more likely.

1.Please write a program to determine the dimension of the rectangle for this encryption transposition cipher.

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

9

2. Please Break the following transposition cipher which involves a completely filled rectangles with our HINT.

9

E R A S B L E
C A M S N A B
D U M O L E A
T O E D C T A
M O R Y R R E
E L N T L I I
C E E N T G H
A D N R I A O
E S A V Q W R

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

We assume that this encrypted message is using completely filled rectangle with 9 rows and 7 columns.

9

Please Break the following transposition cipher which involves a completely filled rectangles from next HINT. (CONT)

L	A	S				
A	M	S				
E	M	O				
T	E	D				
R	R	Y				
I	N	T				
G	E	N				
A	N	R				
W	A	V				

Decrypted partially

9

2022/3/8

11

3. Please count Index of Coincidence (IC) for each messages.
Usually, The I. C. of English is around 0.066

Dan Boneh

$f_a, f_b, f_c, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots f_z,$

$\frac{(f_a)}{(N)} \frac{(f_a-1)}{(N-1)}$

$\frac{(f_i)}{(N)} \frac{(f_i-1)}{(N-1)}$

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

Dan Boneh

message1

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

Dan Boneh

message2

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

Dan Boneh

Message 3

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

Dan Boneh

Message 4

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 TXDQWLB WKHLU VHFXULWB
FUBSWDQDOBVLV LV WKXV WKH FRXQWHUSDUW WR
FUBSWRJUDSKB ERWK DUH VXEILHOGV RI FUBSWRRORJB

Dan Boneh

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 (I.C).

Dan Boneh

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

Dan Boneh