CRYPTOGRAPHY

(ELEC6242)

Coursework Answer Sheet

Name: Shasini Umesha Jasenthu Liyana

Student ID: 32476981

Outline

Please note that Question 1 and 3 were done manually, while a python script was used to decrypt the Question 2

Question 01

Solution for Cipher 1

The role of the assessments was traditionally to test outcomes of teaching in order to grade students. Another function of the assessments is to support the learning process, the latter purpose has not always been emphasised. Evidence shows that students define a curriculum based on the assessment and use it to guide their use of time, attention, and resources.

Decryption Key

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
-	y	u	w	b	v	u	t	s	r	-	p	o	n	m	l	-	-	i	h	c	g	f	e	d	a

🟦 - Represents the key to each letter

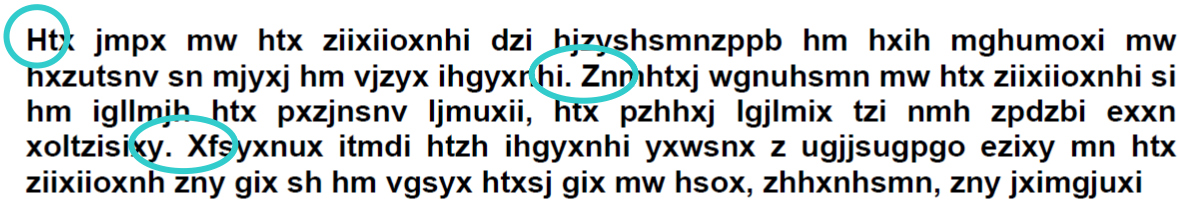
Analysis

Main Assumption – Plain text is English Language

Step 01

At a quick glance, it can be seen that the structure of the sentence is preserved due to subsequent reasons.

1. The spaces between words
2. Word Lengths
3. Having punctuations
4. Having capital letters at a beginning of a new sentence (as shown in figure1)

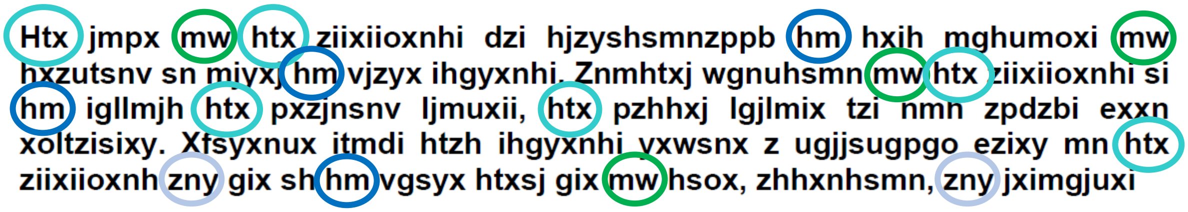


Htx jmpx mw htx ziixiioxnhi dzi hjzyshsmnzppb hm hxih mghumoxi mw hxzutsnv sn mjyxj hm vjzyx ihgyxnhi. Znnhtxj wgnuhsmn mw htx ziixiioxnhi si hm igllmjh htx pxzjnsnv ljmuxii, htx pzhhxj lgjlmix tzi nmh zpdzbi exxn xoltzisixy. Xfsyxnux itmdi htzh ihgyxnhi yxwsnx z ugjjsugpgo ezixy mn htx ziixiioxnh zny gix sh hm vgsyx htxsj gix mw hsox, zhhxnhsmn, zny jximgjuxi

Figure 1 Cipher Text - Emphasized with punctuations

Step 02

The cipher text lacks vowel letters compared to normal letters. Further, having ‘x, y, z’ very often in the text, is not normal in English. Hence, this is not a permutation cipher but can be a substitution cipher. Moreover, as depicted in the figure 2 below, it can be seen that several words are repeated throughout the text. Therefore, a frequency analysis was conducted and plotted on a graph as shown in figure 3.



Htx jmpx mw htx ziixiioxnhi dzi hjzyshsmnzppb hm hxih mghumoxi mw
hxzutsnv sn miyxj hm vjzyx ihgyxnhi. Znmhtxj wgnuhsmn mw htx ziixiioxnhi si
hm igllmjh htx pxzjnsnv ljmuxii, htx pzhhxj lgjlmix tzi nmn zpdzbi exxn
xoltzisixy. Xfsyxnux itmdi htzh ihgyxnhi vxwsnx z ugjjsugpgo ezixy mn htx
ziixiioxnh zny gix sh hm vgsyx htxsj gix mw hsox, zhhxnhsmn, zny jximgjuxi

Figure 3 - Repeated Ciphers in the Cipher Text

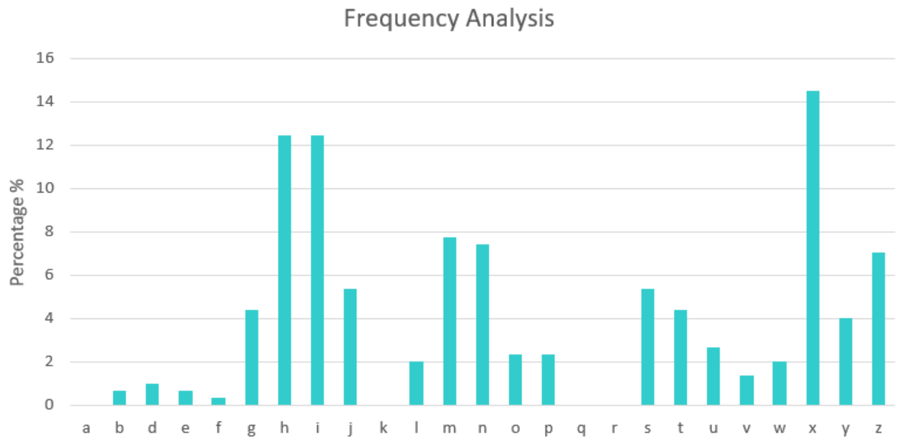
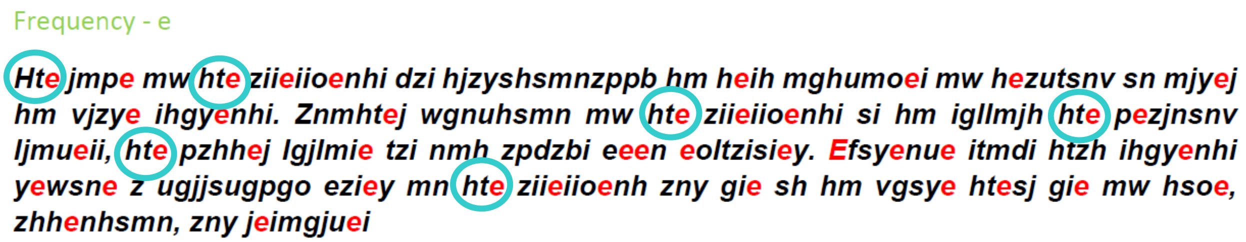


Figure 3 Frequency Analysis of the cipher text

Step 03

According to the character frequency shown in figure 3, the distribution of cipher letters appears to be normal as of an English text. Hence, it is certain that this is a monoalphabetic substitution. Above basic frequency analysis shows that letter ‘x’ is most common letter in this cipher. Therefore, it could be letter ‘e’ which is the most common used letter in the English alphabet. The result after substituting letter e is shown in figure 4.



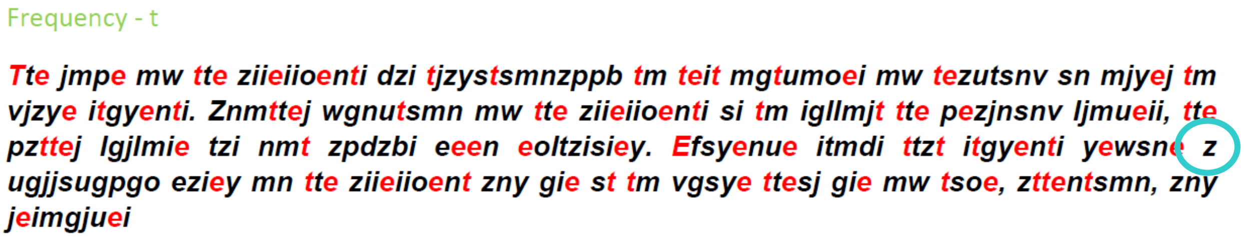
Frequency - e

Hte jmpe mw hte ziieiioenhi dzi hjzyshsmnzppb hm heih mghumoei mw hezutsnv sn mjyej hm vjzye ihgyenhi. Znmhtej wgnuhsmn mw hte ziieiioenhi si hm igllmjh hte pezjnsnv ljmueii, hte pzhhej lgjlmie tzi nmh zpdzbi eeen eoltzisiey. Efsyenue itmdi htzh ihgyenhi yewsne z ugjjsugpgo eziey mn hte ziieiioenh zny gie sh hm vgsye htesj gie mw hsoe, zhhenhsmn, zny jeimgjuei

Figure 4 Cipher Text after substituting letter 'e'

Step 04

In English language second most frequently, used letter is ‘t’. However, as shown in the graph (figure 3), letter ‘h’ and ‘i’ have the same frequency. Word ‘hte’ has appeared six times (3 letter sequence) as shown in the figure 4; hence we can assume of that word to be ‘the’. Therefore, there is a higher chance ‘h’ represents as ‘t’ than ‘i’ being ‘t’.



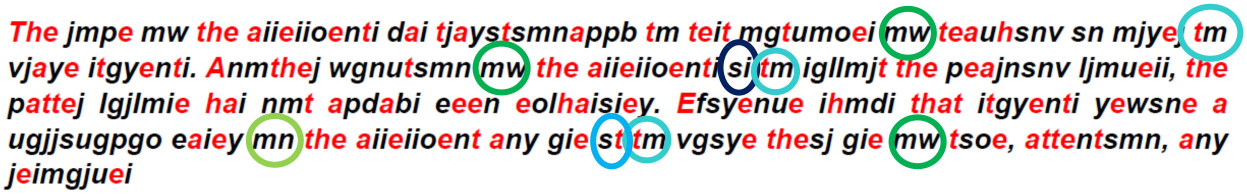
Frequency - t

Tte jmpe mw tte ziieiioenti dzi tjzystsmnzppb tm teit mgtumoei mw tezutsnv sn mjyej tm vjzye itgyenti. Znmttej wgnutsmn mw tte ziieiioenti si tm igllmjt tte pezjnsnv ljmueii, tte pzttej lgjlmie tzi nmt zpdzbi eeen eoltzisiey. Efsyenue itmdi ttzt itgyenti yewsne z ugjjsugpgo eziey mn tte ziieiioent zny gie st tm vgsye ttesj gie mw tsoe, zttentsmn, zny jeimgjuei

Figure 5 Cipher Text after substituting letter 't'

Step 05

Having said that, in English the letter ‘h’ most of the time appear after letter ‘t’ (crib). Therefore, it can be assumed that ‘t’ in cipher text represents ‘h’. Further, there are only two single word in English i.e.: I and a (preposition). ‘I’ always written in Uppercase while ‘a’ preposition is written in lower case unless otherwise it starts a sentence. Therefore, in this context, lower case ‘z’ (refer figure 5) should be ‘a’ preposition.



The jmpe mw the aiieiioenti dai tjaystsmnappb tm teit mgtumoei mw teauhsnv sn mjyej tm vjaye itgyenti. Anmthej wgnutsmn mw the aiieiioenti si tm igllmjt the peajnsnv ljmueii, the pattej lgjlmie hai nmt apdabi eeen eolhaisiey. Efsyenue ihmdi that itgyenti yewsne a ugjjsugpgo eaiey mn the aiieiioent any gie st tm vgsye thesj gie mw tsoe, attentsmn, any jeimgjuei

Figure 6 Cipher Text after substituting letter 'a'

Step 05

According to two letter sequence, two letter words can be easily identified. ‘tm’ has repeated for 3 times, as ‘t’ is already known this word should be ‘to’ in English language. As shown in below figure 7 when one piece of two letter word rectified, eventually other group of two letter words can be recognized as below.

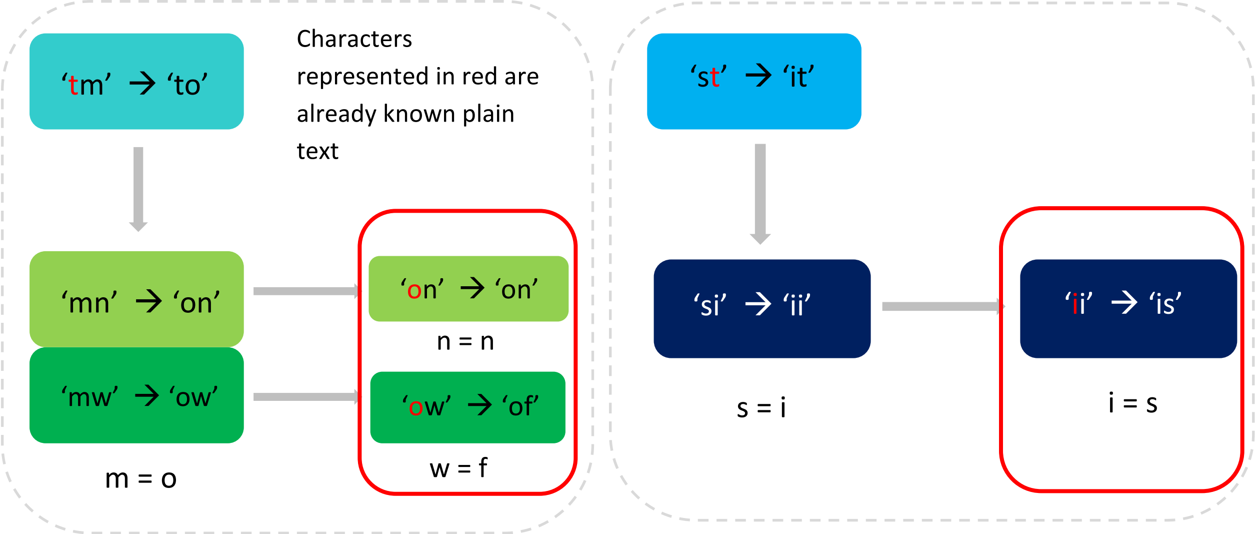


Figure 7 Process of identifying two letter words

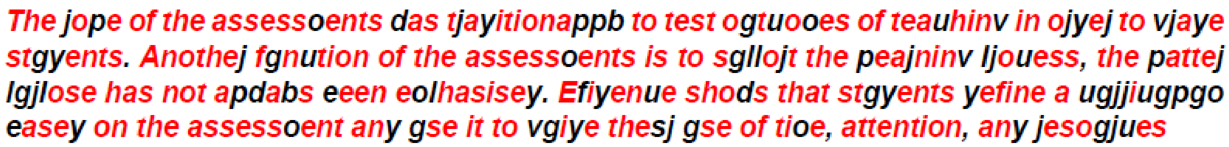
However, the outputs inside the red outlined boxes (in figure 7), were decided based on following assumptions (Table 1)

Table 1 Clarification for letters 'n' and 'w'

Assumption	Intermediate cipher texts which confirms the assumption (figure6)	Reasons
n → n	‘on’, ‘any’, ‘attentsmn’ (already identified letters are represented in red)	There is higher chance of ‘any’ being ‘and’, as it is located in a sentence after ‘,’ separated words. Further, ‘attentsmn’ could be representing the word ‘attention’ Hence, it can be assumed that ‘n’ letter is represented as letter ‘n’ itself.
w → f	‘ow’	As, ‘on’ represents ‘on’, ‘ow’ should be word ‘of’ as most of the time ‘ok’ word in English does not appear in the middle of a sentence.

i → s	‘ii’, ‘teit’, ‘hai’	It is certain that it should be letter ‘s’, any other letter cannot output meaningful mentioned below 3 words at the same time with already identified combinations. ‘is’, ‘test’ and ‘has’

Therefore, by substituting above identified letters to other words figure 8 can be seen as the output.



The jope of the assessoents das tjayitionappb to test ogtuooes of teauhinv in ojyej to vjaye stgyents. Anothej fgnution of the assessoents is to sgllojt the peajninv ljouess, the pattej lgjlose has not apdabs eeen eolhasisey. Efiyenue shods that stgyents yefine a ugjjiugpgo easey on the assessoent any gse it to vgiye thesj gse of tioe, attention, any jesogjues

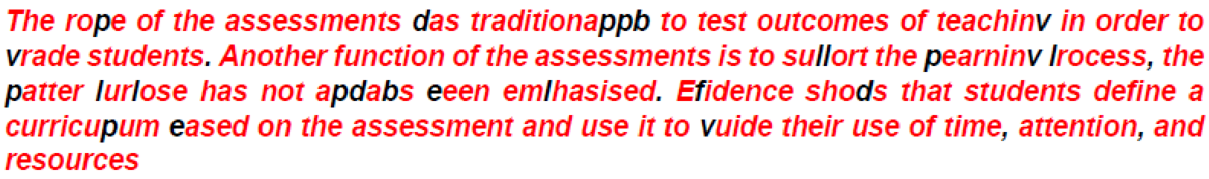
Figure 8 Cipher Text, after substituting step 05 values

Step 06

Now, that words can be easily simplified as below (Table 2) by guessing.

Table 2 Terms which can be guessed in the cipher text

	Plain Text
Anothej	Another
fgnution	function
yefine	define
assessoents	assessments



The rope of the assessments das traditionappb to test outcomes of teachinv in order to vrade students. Another function of the assessments is to sullort the pearninv lrocess, the patter lurlose has not apdabs eeen emlhasised. Efidence shods that students define a curricupum eased on the assessment and use it to vuide their use of time, attention, and resources

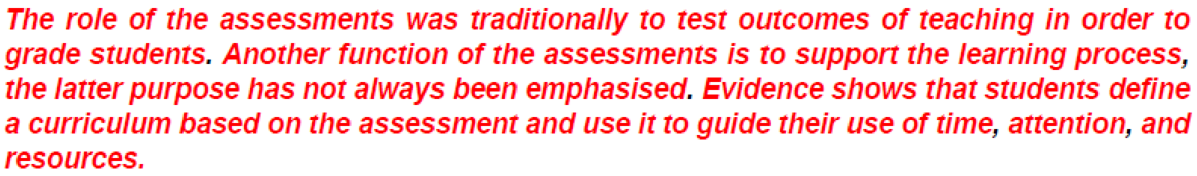
Figure 9 Cipher Text, after substituting step 06 values

Step 07

As the final step, above step can be repeated to guess the remaining letters.

Table 3 Terms which can be guessed in the cipher text

	Plain Text
traditionappb	traditionally
teachinv	teaching
Efidence	evidence
shods	shows
eased	based



The role of the assessments was traditionally to test outcomes of teaching in order to grade students. Another function of the assessments is to support the learning process, the latter purpose has not always been emphasised. Evidence shows that students define a curriculum based on the assessment and use it to guide their use of time, attention, and resources.

Figure 10 Plain Text - Decrypted Message

Question 02

Solution for Cipher 2

Lord Byron kept a pet bear in his dorm room while studying at Cambridge University

Decryption Key

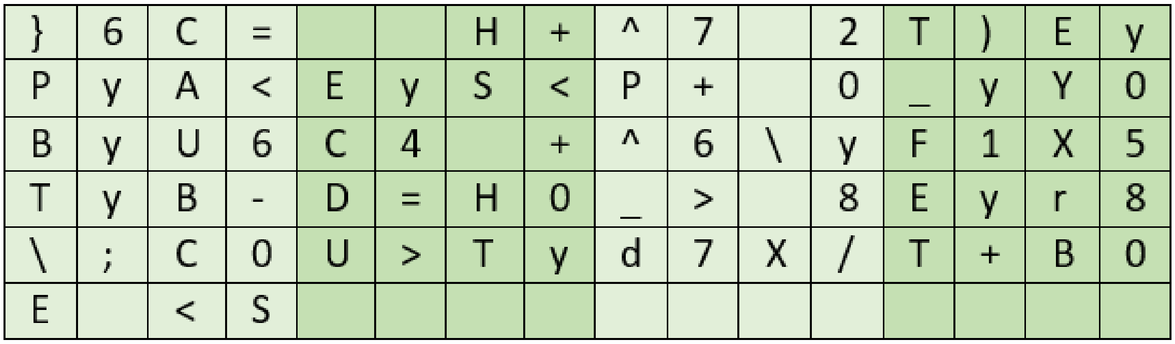
Key 01		Key 02	
Hex Value	ASCII	Hex Value	ASCII
0x31	1	0x59	Y

Analysis

Main Assumption – Plain text is English Language

Step 01

To have a better idea regarding the cipher text, initially the hex file was opened via a hex file editor (figure 11) and then plotted as below.



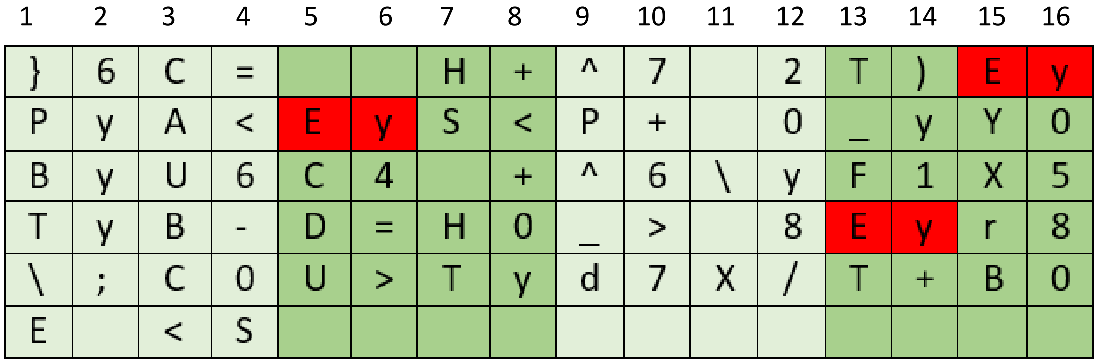
}	6	C	=			H	+	^	7		2	T	)	E	y
P	y	A	<	E	y	S	<	P	+		0	_	y	Y	0
B	y	U	6	C	4		+	^	6	\	y	F	1	X	5
T	y	B	-	D	=	H	0	_	>		8	E	y	r	8
\	;	C	0	U	>	T	y	d	7	X	/	T	+	B	0
E		<	S												

Figure 11 Cipher Text 2

As the hint describes that the first letter of the plain text of this cipher is 'L', it is certain that this does not fall under to the category of permutation ciphers (Since, permutation cipher contains the plain text in different order and in this context no such letter appear to be in the cipher text). As the numerical values and alphabetical characters both present in the cipher text, it can be assumed that this not a substitution cipher either. Therefore, there is a possibility this cipher text being a steganography, which means that the value of the plain text could be masked by a key.

Step 02

Having said that, below pattern (figure 12) was identified in the cipher text.



1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
}	6	C	=			H	+	^	7		2	T	)	E	y
P	y	A	<	E	y	S	<	P	+		0	_	y	Y	0
B	y	U	6	C	4		+	^	6	\	y	F	1	X	5
T	y	B	-	D	=	H	0	_	>		8	E	y	r	8
\	;	C	0	U	>	T	y	d	7	X	/	T	+	B	0
E		<	S												

Figure 12 Pattern presented in the cipher text

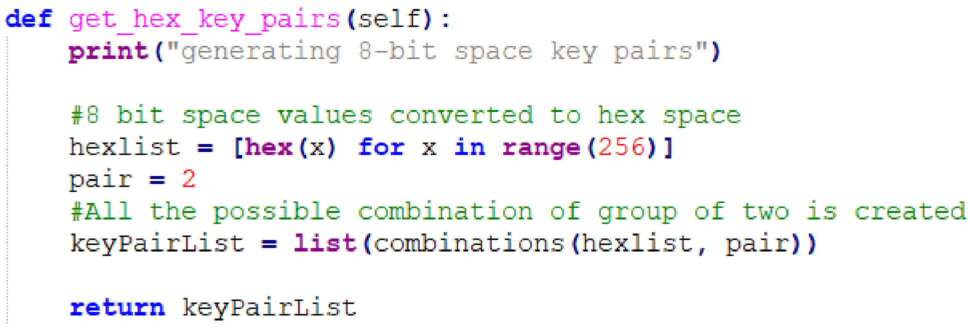
There are 84 characters (up to S) in this cipher text. Further, it can be seen that identified pattern (which is group of 2) is finishing in even columns (refer bullet points). Hence, the distance between each pattern is multiple of the size of the pattern (in this case it is multiple of 2). Therefore, it can be assumed that the key may consist of two values.

- First 'Ey' → column 15, 16
- Second 'Ey' → column 5, 6
- Third 'Ey' → column 13, 14

Even though, the first letter of the plain text is known, it cannot be guaranteed that the first letter of the plain text is placed under the first cipher text (In this case it's '}').

Step 03

As the first step in decrypting, hex file was extracted using a python script. Under the assumption of plain text is covered by xor using a key pair. Each hex value was placed inside a python list in order to xor with the key pair. Having such consideration, in the 8-bit space all the possible



```
def get_hex_key_pairs(self):
    print("generating 8-bit space key pairs")

    #8 bit space values converted to hex space
    hexlist = [hex(x) for x in range(256)]
    pair = 2
    #All the possible combination of group of two is created
    keyPairList = list(combinations(hexlist, pair))

    return keyPairList
```

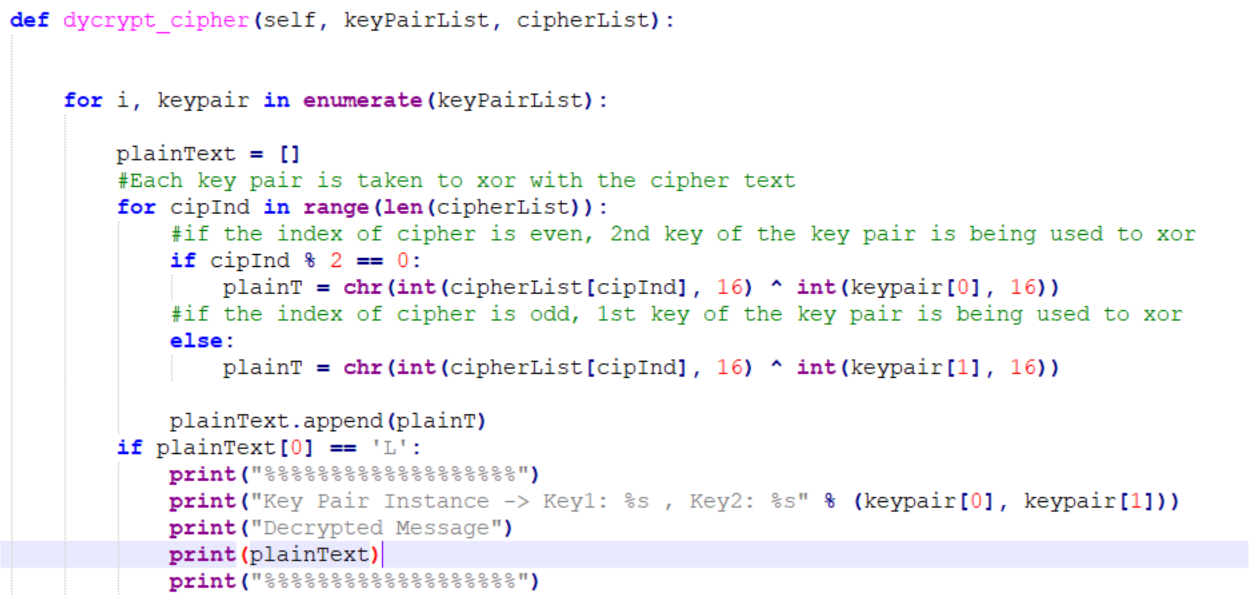
Figure 13 Function to generate hex key pairs

combination of group of two were gathered into a python list. Reason to consider the 8-bit space is, in these context ascii characters are presented and each ascii character is presented in 8 bits. Further, each key pair is then converted to hexadecimal value (Below function in figure 13 was used to create key pair list).

Step 04

Then each two key pair were taken to XOR with the cipher text. In order to achieve this, the key pair should be extended (repeated) until the length of the cipher text. This was done using following logic.

- If the index of cipher text is odd, 1st key inside the key pair is used to xor
- Else if, the index of cipher text is even 2nd key inside the key pair is used to xor

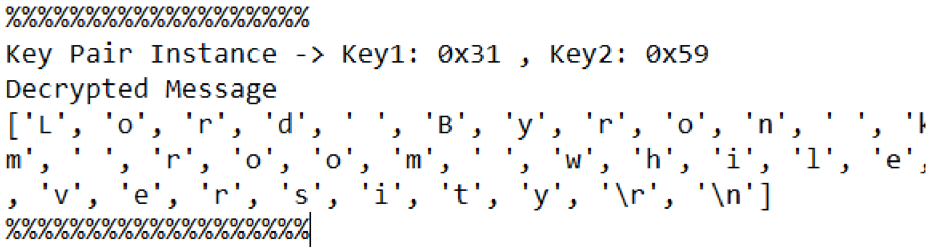


```
def dycrypt_cipher(self, keyPairList, cipherList):


    for i, keypair in enumerate(keyPairList):

        plainText = []
        #Each key pair is taken to xor with the cipher text
        for cipInd in range(len(cipherList)):
            #if the index of cipher is even, 2nd key of the key pair is being used to xor
            if cipInd % 2 == 0:
                plainT = chr(int(cipherList[cipInd], 16) ^ int(keypair[0], 16))
            #if the index of cipher is odd, 1st key of the key pair is being used to xor
            else:
                plainT = chr(int(cipherList[cipInd], 16) ^ int(keypair[1], 16))

            plainText.append(plainT)
        if plainText[0] == 'L':
            print("%%%%%%%%%%%%%%%%%%%%")
            print("Key Pair Instance -> Key1: %s , Key2: %s" % (keypair[0], keypair[1]))
            print("Decrypted Message")
            print(plainText)
            print("%%%%%%%%%%%%%%%%%%%%")
```

Figure 14 Function to decrypt the cipher

Step 05

As the result scheme is vague, ‘if condition’ was placed to output plaintext starting from L only (Here assuming the first location is L). As the final step, the results were manually identified to check a realistic sentence.



```
%%%%%%%%%%%%%%%%%%%%
Key Pair Instance -> Key1: 0x31 , Key2: 0x59
Decrypted Message
['L', 'o', 'r', 'd', ' ', 'B', 'y', 'r', 'o', 'n', ' ', '
m', ' ', 'r', 'o', 'o', 'm', ' ', 'w', 'h', 'i', 'l', 'e',
, 'v', 'e', 'r', 's', 'i', 't', 'y', '\r', '\n']
%%%%%%%%%%%%%%%%%%%%
```

Figure 15 Plaint Text - Decrypted Message of Cipher 2

Question 03

Solution for Cipher 3

The Milky Way began as a series of dense regions in the early universe not long after the Big Bang

Decryption Key

8	2	5	4	1	7	3	6
V	E	R	K	A	U	F	T

Analysis

Main Assumption – Plain text is English Language

Step 01

It can be seen that letters presented in the cipher text (figure 16) has same sort of a same frequency analysis as appeared in normal English. In this context letter 'e' has the highest frequency while letter 'a' has the second highest. Hence, it can be assumed that this is not substitution but a permutation cipher.

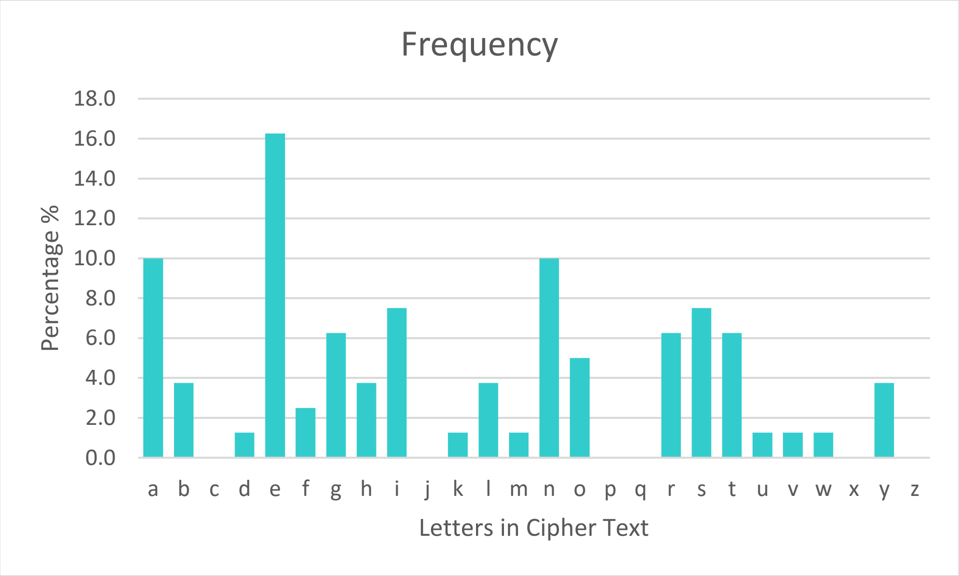


Figure 16 Frequency Analysis of cipher text 3

Step 02

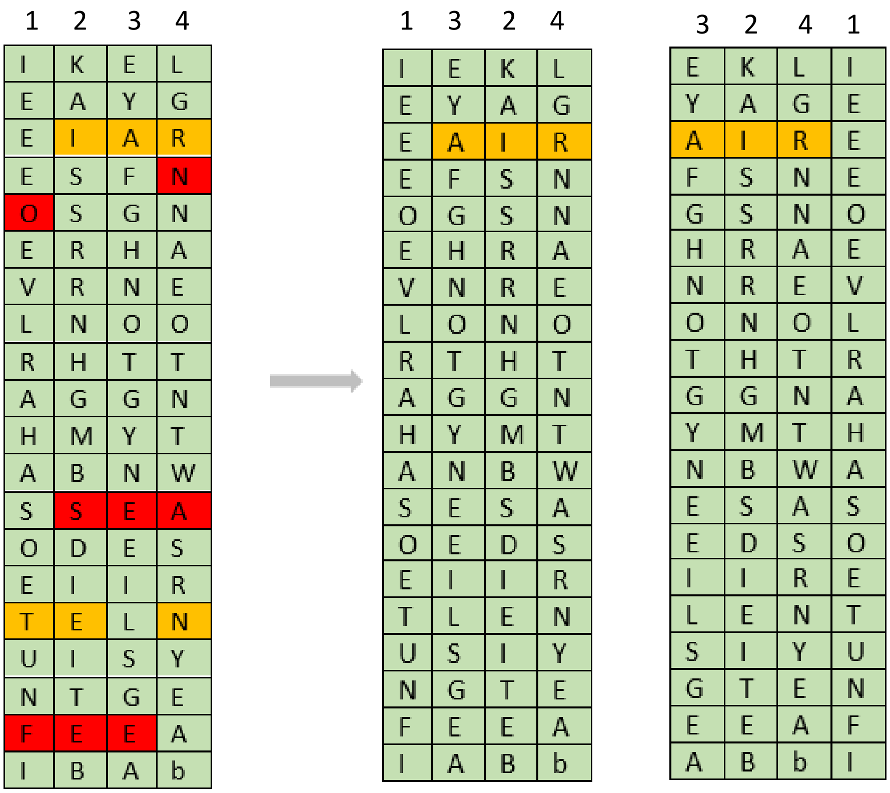
The total number of letters presented in this cipher text is 80. It has been assumed this is a transposition cipher not any other methods that can be found in permutation ciphers. Having said that, length of the key should be devisor of 80 (which are as mentioned below).

1. 4 x 20
2. 5 x 16
3. 8 x 10

Each key length was taken in ascending order until a meaningful sentence is identified.

Step 03

Assuming that the key length is 4 (k = 4), cipher letters were arranged in the following grid as shown below (figure 17)



1	2	3	4
I	K	E	L
E	A	Y	G
E	I	A	R
E	S	F	N
O	S	G	N
E	R	H	A
V	R	N	E
L	N	O	O
R	H	T	T
A	G	G	N
H	M	Y	T
A	B	N	W
S	S	E	A
O	D	E	S
E	I	I	R
T	E	L	N
U	I	S	Y
N	T	G	E
F	E	E	A
I	B	A	b

1	3	2	4
I	E	K	L
E	Y	A	G
E	A	I	R
E	F	S	N
O	G	S	N
E	H	R	A
V	N	R	E
L	O	N	O
R	T	H	T
A	G	G	N
H	Y	M	T
A	N	B	W
S	E	S	A
O	E	D	S
E	I	I	R
T	L	E	N
U	S	I	Y
N	G	T	E
F	E	E	A
I	A	B	b

3	2	4	1
E	K	L	I
Y	A	G	E
A	I	R	E
F	S	N	E
G	S	N	O
H	R	A	E
N	R	E	V
O	N	O	L
T	H	T	R
G	G	N	A
Y	M	T	H
N	B	W	A
E	S	A	S
E	D	S	O
I	I	R	E
L	E	N	T
S	I	Y	U
G	T	E	N
E	E	A	F
A	B	b	I

Figure 17 Cipher Text presented in a 4x20 grid. 2nd, and 3rd (from left to right) grids show intermediate steps of column transpositions

Highlighted in red (in figure 17), words were identified without juggling the columns. However, it is not correct as other letters do not make any sensible sentence. Further search was taken place to identify anagrams to obtain a meaningful English term by trans positioning the columns. Highlighted in orange, anagrams were gathered to make following words

- IAR – AIR
- TEN – TEN / NET

By taking each word at a time, columns were swapped to make the possible word. Even if the columns were arranged to make the word ‘IAR’ highlighted in orange (even if columns swapped or changed the location of word ‘air’ to start from column 1), it will not create a reasonable sentence which is correct in English. It was same with other aforementioned words as well. Hence, assumption of key length is equal to 4 is incorrect.

Step 04

1	2	3	4	5
I	U	S	T	N
E	N	D	G	A
E	F	I	Y	E
E	I	E	N	O
O	K	I	E	T
E	A	T	E	N
V	I	E	I	T
L	S	B	L	W
R	S	E	S	A
A	R	Y	G	S
H	R	A	E	R
A	N	F	A	N
S	H	G	L	Y
O	G	H	G	E
E	M	N	R	A
T	B	O	N	B

1	2	3	5	4
I	U	S	N	T
E	N	D	A	G
E	F	I	E	Y
E	I	E	O	N
O	K	I	T	E
E	A	T	N	E
V	I	E	T	I
L	S	B	W	L
R	S	E	A	S
A	R	Y	S	G
H	R	A	R	E
A	N	F	N	A
S	H	G	Y	L
O	G	H	E	G
E	M	N	A	R
T	B	O	B	N

1	4	3	5	2
I	T	S	N	U
E	G	D	A	N
E	Y	I	E	F
E	N	E	O	I
O	E	I	T	K
E	E	T	N	A
V	I	E	T	I
L	L	B	W	S
R	S	E	A	S
A	G	Y	S	R
H	E	A	R	R
A	A	F	N	N
S	L	G	Y	H
O	G	H	E	G
E	R	N	A	M
T	N	O	B	B

4	3	5	2	1
T	S	N	U	I
G	D	A	N	E
Y	I	E	F	E
N	E	O	I	E
E	I	T	K	O
E	T	N	A	E
I	E	T	I	V
L	B	W	S	L
S	E	A	S	R
G	Y	S	R	A
E	A	R	R	H
A	F	N	N	A
L	G	Y	H	S
G	H	E	G	O
R	N	A	M	E
N	O	B	B	T

Figure 18 Cipher Text presented in a 5x16 grid. 2nd, 3rd, and 4th (from left to right) grids show intermediate steps of column transpositions

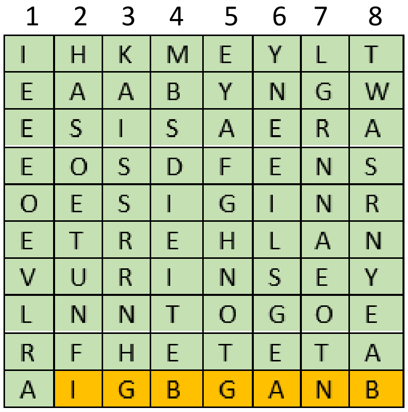
Therefore, assumption was changed to key length is equal to 5. Having said that, 5 x 16 grid was arranged to place the letters and repeated the same procedure (figure 18). Even if proper English words appear in the cipher text which is in red color, it does not provide a meaningful sentence across rows. Further, following anagrams were identified (in Orange color).

- KIET – KITE
- SEA – SEA
- ARYG - GRAY

The same steps which were taken when analyzing key = 4, had been applied here. Further, the word ‘sea’ highlighted in orange, even if two ‘s’ columns swapped or change the location of word ‘sea’ to column 1, it will not create a reasonable sentence which is correct in English. Hence, assumption of key length is equal to 5 was incorrect.

Step 05

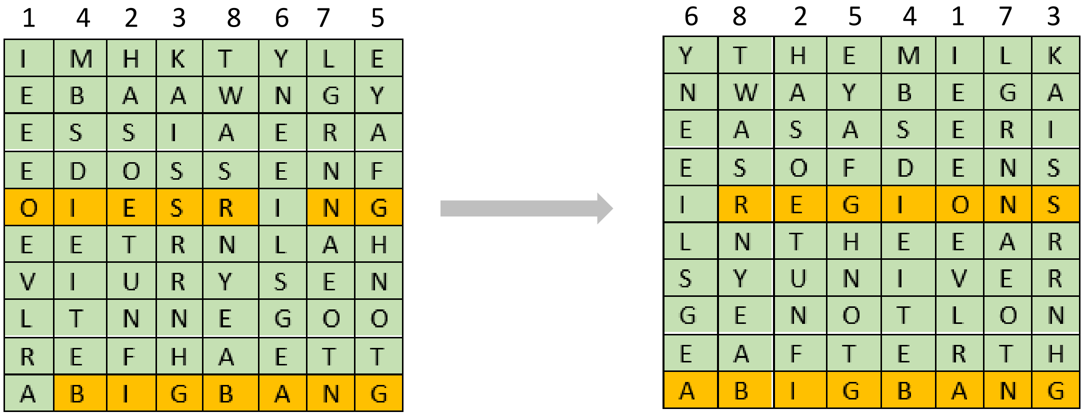
Therefore, assumption was changed to key length is equal to 8 and 8 x 10 grid was organized to place the letters and repeated the same procedure (figure 18).



1	2	3	4	5	6	7	8
I	H	K	M	E	Y	L	T
E	A	A	B	Y	N	G	W
E	S	I	S	A	E	R	A
E	O	S	D	F	E	N	S
O	E	S	I	G	I	N	R
E	T	R	E	H	L	A	N
V	U	R	I	N	S	E	Y
L	N	N	T	O	G	O	E
R	F	H	E	T	E	T	A
A	I	G	B	G	A	N	B

Figure 18 Cipher Text presented in an 8x10 grid

The last row of this block seemed to have a possible anagram for the word 'BIGBANG'. As the next step, columns were exchanged to create the word (figure). After that step, another anagram was recognized, which is 'OIESRNG' to make the word 'REGION'. It was possible to create the word 'REGION' without damaging the order of word 'BIGBANG' in the context, as there were couple of 'B', 'G', and 'A' and both the words have the same length.



1	4	2	3	8	6	7	5
I	M	H	K	T	Y	L	E
E	B	A	A	W	N	G	Y
E	S	S	I	A	E	R	A
E	D	O	S	S	E	N	F
O	I	E	S	R	I	N	G
E	E	T	R	N	L	A	H
V	I	U	R	Y	S	E	N
L	T	N	N	E	G	O	O
R	E	F	H	A	E	T	T
A	B	I	G	B	A	N	G

6	8	2	5	4	1	7	3
Y	T	H	E	M	I	L	K
N	W	A	Y	B	E	G	A
E	A	S	A	S	E	R	I
E	S	O	F	D	E	N	S
I	R	E	G	I	O	N	S
L	N	T	H	E	E	A	R
S	Y	U	N	I	V	E	R
G	E	N	O	T	L	O	N
E	A	F	T	E	R	T	H
A	B	I	G	B	A	N	G

Figure 19 Intermediate steps

However, it is clear that if the first column is moved to the end of the block, the right message would appear (column 6 should appear at the end). The following output was obtained (figure 20). It is certain that the letter ‘A’ had been chosen as a redundant value to make the length total in to 80.

8	2	5	4	1	7	3	6
T	H	E	M	I	L	K	Y
W	A	Y	B	E	G	A	N
A	S	A	S	E	R	I	E
S	O	F	D	E	N	S	E
R	E	G	I	O	N	S	I
N	T	H	E	E	A	R	L
Y	U	N	I	V	E	R	S
E	N	O	T	L	O	N	G
A	F	T	E	R	T	H	E
B	I	G	B	A	N	G	A

Figure 20 Decrypted Message of Cipher Text 3

Order of the key is → 8 2 5 4 1 7 3 6

Corresponding Word → VERKAUFT

It is worth stating that, after thorough research, searching [*] and using the own knowledge in English, I could not able to find a matching English term with the above-mentioned sequence. However, I was able to find the above word ‘VERKAUFT’ which is a German term and have a meaning of ‘sold’ in English.

**https://www.bestwordlist.com/allwords.htm*

Appendixes

Appendix A

Table 4 Source to frequency analysis for the cipher text 1

Letter	Count	Frequency (%)
a	0	0.0
b	2	0.7
c	0	0.0
d	3	1.0
e	2	0.7
f	1	0.3
g	13	4.3
h	37	12.4
i	37	12.4
j	16	5.4
k	0	0.0
l	6	2.0
m	23	7.7
n	22	7.4
o	7	2.3
p	7	2.3
q	0	0.0
r	0	0.0
s	16	5.4
t	13	4.3
u	8	2.7
v	4	1.3
w	6	2.0
x	43	14.4
y	12	4.0
z	21	7.0
Total	299	

Appendix B

```
import binascii
from itertools import combinations

ciphlist = []

class HexDecryptor():

    def __init__(self):
        print("Script Started..")

    def get_extract_hexfile(self):
        print("Extracting Hex File")
        with open('113.hex', 'rb') as file:
            hexChunk = iter(lambda: file.read(1), b'')
            hexCiph = map(binascii.hexlify, hexChunk)

            #each value is extracted from hexCiph and placed in a list
            for hexVal in hexCiph:
                ciphlist.append('0x' + hexVal.decode('utf-8'))

        return ciphlist

    def get_hex_key_pairs(self):
        print("generating 8-bit space key pairs")

        #8 bit space values converted to hex space
        hexlist = [hex(x) for x in range(256)]
        pair = 2
        #All the possible combination of group of two is created
        keyPairList = list(combinations(hexlist, pair))

        return keyPairList

    def dycrypt_cipher(self, keyPairList, cipherList):


        for i, keypair in enumerate(keyPairList):

            plainText = []
            #Each key pair is taken to xor with the cipher text
            for cipInd in range(len(cipherList)):
            #if the index of cipher is even, 2nd key of the key pair is being used to xor
                if cipInd % 2 == 0:
                    plainT = chr(int(cipherList[cipInd], 16) ^ int(keypair[0], 16))
                #if the index of cipher is odd, 1st key of the key pair is being used to xor
                else:
                    plainT = chr(int(cipherList[cipInd], 16) ^ int(keypair[1], 16))

                plainText.append(plainT)
            if plainText[0] == 'L':
                print("%%%%%%%%%%%%%%%%%%%")
                print("Key Pair Instance -> Key1: %s , Key2: %s" %(keypair[0], keypair[1]))
                print("Decrypted Message")
                print(plainText)
                print("%%%%%%%%%%%%%%%%%%%")

if __name__ == '__main__':
    m = HexDecryptor()
    cipherList = m.get_extract_hexfile()
    keyPairList = m.get_hex_key_pairs()
    possiblePlainT = m.dycrypt_cipher(keyPairList, cipherList)
```

Appendix C

Table 5 Source to frequency analysis for the cipher text 3

Letter	Count	Frequency
a	8	10.0
b	3	3.8
c	0	0.0
d	1	1.3
e	13	16.3
f	2	2.5
g	5	6.3
h	3	3.8
i	6	7.5
j	0	0.0
k	1	1.3
l	3	3.8
m	1	1.3
n	8	10.0
o	4	5.0
p	0	0.0
q	0	0.0
r	5	6.3
s	6	7.5
t	5	6.3
u	1	1.3
v	1	1.3
w	1	1.3
x	0	0.0
y	3	3.8
z	0	0.0
Total	80	

*****