Quiz 1

111550113 謝語承晴

Problem 1

a) Please write a program to find out the frequencies of letters in the ciphertext.

```python
def Count_letter_frequency(ciphertext):
    letter_frequency={}
    total_length=0
    for character in ciphertext:
        if character.isalpha():
            if character in letter_frequency:
                letter_frequency[character]+=1
            else:
                letter_frequency[character]=1
            total_length+=1

    #sort
    sorted_frequency=sorted(letter_frequency.items(), key=lambda c:c[1], reverse=True)

    #print
    for letter, frequency in sorted_frequency:
        print(f"{letter}'s frequency: {(frequency/total_length)*100:.2f}%")

ciphertext="C UYGHARMZ IUWMPRWIR GAIR YVRMP MBHMZWMPUM C VMMXWPE YV PYR VCZ ZMGYQMD VZYG

Count_letter_frequency(ciphertext)
```

```
M's frequency: 13.38%
C's frequency: 8.45%
Y's frequency: 8.45%
P's frequency: 8.45%
R's frequency: 6.34%
Z's frequency: 6.34%
W's frequency: 6.34%
V's frequency: 4.93%
U's frequency: 4.23%
X's frequency: 4.23%
D's frequency: 4.23%
G's frequency: 3.52%
N's frequency: 3.52%
I's frequency: 2.82%
E's frequency: 2.82%
H's frequency: 2.11%
S's frequency: 2.11%
A's frequency: 1.41%
B's frequency: 1.41%
Q's frequency: 1.41%
K's frequency: 1.41%
T's frequency: 0.70%
O's frequency: 0.70%
L's frequency: 0.70%
```

b) Use the plaintext frequency count information below as a reference to break this encrypted messages.

Table 2: Common frequency of letters appearance: (%)

E	A	R	I	O	T	N	S	L	C	U	D	P
11.16	8.5	7.58	7.54	7.16	6.95	6.65	5.74	5.49	4.54	3.63	3.38	3.17
M	H	G	B	F	Y	W	K	V	X	Z	J	Q
3.01	3.0	2.47	2.07	1.81	1.78	1.29	1.10	1.01	0.29	0.27	0.20	0.20

A COMPUTERSCIENTIST MUST OFTEN
C UYGHARMZ IUWMPRWIR GAIR YVRMP

EXPERIENCE A FEELING OF NOT FAR
MBHMZWMPUM C VMMXWPE YV PYR VCZ

REMOVED FROM ALARM ON ANALYZING AND EXPLORE
ZMGYQMD VZYG CXCZG YP CPCXKTWPE CPD MBHXYZM

THE FLOOD OF ADVANCED KNOWLEDGEWHICH EACH
RNM VXYYD YV CDQCPUMD OPYSXMDEM SNWUN MCUN

YEAR BRINGS WITH IT
KMCZ LZWPEI SWRN WR

Table 3: Ciphertext to plaintext mapping

Ciphertext	A	B	C	D	E	F	G	H	I	J	K	L	M
	0	1	2	3	4	5	6	7	8	9	10	11	12
Plaintext	U	X	A	D	G		M	P	S		Y	B	E
Ciphertext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	13	14	15	16	17	18	19	20	21	22	23	24	25
Plaintext	H	K	N	V	T	W	Z	C	F	I	L	O	R

1. RNM = THE
   將 R、N、M 都用 T、H、E 替代

2. C = A
   會出現在句中自己單一字母

3. 由 MCUN 和 WR 推得 U 是 C，W 是 I
   再由 SWRN(_ITH) 推得 S 是 W

4. WPE 作為結尾，推得是 ING
   並可容易看出 EXPERIENCE

5. 由 Y 的 frequency 和 YV 和 YP 可知
   Y 應為 O，V 應為 F

6. 接著由 CPD(AN_) 推得 D 應為 D

⋮

持續對照 frequency 或觀察英文單字
推得所有字母

c) Assume C is ciphertext, and P is plaintext. Can you find a particular relationship between C and P?

Using the equation in (d), $f(x) = (9x+2) \bmod 26$, we can complete this table.

Table 3: Ciphertext to plaintext mapping

Ciphertext	A	B	C	D	E	F	G	H	I	J	K	L	M
	0	1	2	3	4	5	6	7	8	9	10	11	12
Plaintext	U	X	A	D	G	J	M	P	S	Q	Y	B	E
	20	23	0	3	6	9	12	15	18	16	24	1	4
Ciphertext	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
	13	14	15	16	17	18	19	20	21	22	23	24	25
Plaintext	H	K	N	V	T	W	Z	C	F	I	L	O	R
	7	10	13	21	19	22	25	2	5	8	11	14	17

但 ciphertext $\left[\begin{array}{l}Q\\J\end{array}\right.$ 对应到 plaintext $\left[\begin{array}{l}V\\Q\end{array}\right.$ 有例外.

还是要由 article 語意判斷

d) Suppose "$f(x) = ax + b \bmod 26$", where x is plaintext, please solve the value of a and b.

By RNM = THE, $(f(x), x) = (17, 19)、(13, 7)、(12, 4)$

$$\begin{cases} 17 = (19a+b) \bmod 26 \\ 13 = (7a+b) \bmod 26 \\ 12 = (4a+b) \bmod 26 \end{cases} \Rightarrow \begin{cases} 4 = 12a \bmod 26 \\ 1 = 3a \bmod 26 \end{cases} \Rightarrow a = 9 \qquad \therefore (a, b) = (9, 2) \ \#$$

$$12 = (36+b) \bmod 26, \quad b = 2$$

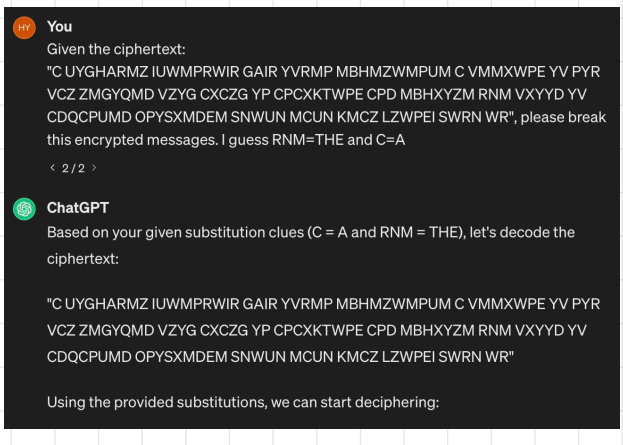
e) What is the key size of the Mono-Alphabetic Substitution Cipher? ① Such a size makes exhaustive search becomes difficult? ②

① The key size is 26! (factorial of 26) #

② 26! is a large number, it may make exhaustive search be difficult, but with frequency analysis attacks, the cipher can be vulnerable. Some letters occur more frequently than others.

f) (Bonus) Please try to see if it is possible to decipher this problem with ChatGPT or another tool.

① Using ChatGPT 3.5, it seems that it's not possible to decipher. It turns out to be a weird answer.



You

Given the ciphertext:
"C UYGHARMZ IUWMPRWIR GAIR YVRMP MBHMZWMPUM C VMMXWPE YV PYR VCZ ZMGYQMD VZYG CXCZG YP CPCXKTWPE CPD MBHXYZM RNM VXYYD YV CDQCPUMD OPYSXMDEM SNWUN MCUN KMCZ LZWPEI SWRN WR", please break this encrypted messages. I guess RNM=THE and C=A

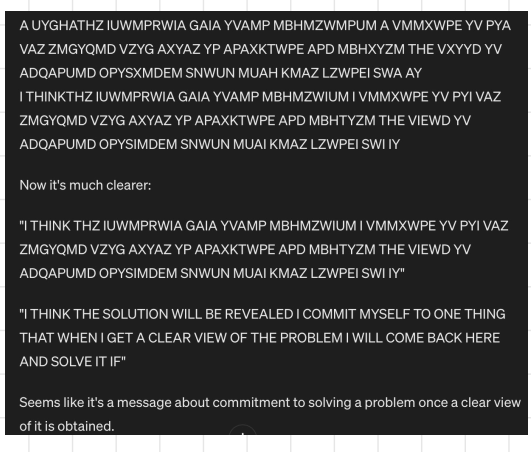
‹ 2 / 2 ›

ChatGPT

Based on your given substitution clues (C = A and RNM = THE), let's decode the ciphertext:

"C UYGHARMZ IUWMPRWIR GAIR YVRMP MBHMZWMPUM C VMMXWPE YV PYR VCZ ZMGYQMD VZYG CXCZG YP CPCXKTWPE CPD MBHXYZM RNM VXYYD YV CDQCPUMD OPYSXMDEM SNWUN MCUN KMCZ LZWPEI SWRN WR"

Using the provided substitutions, we can start deciphering:



A UYGHATHZ IUWMPRWIA GAIA YVAMP MBHMZWMPUM A VMMXWPE YV PYA VAZ ZMGYQMD VZYG AXYAZ YP APAXKTWPE APD MBHXYZM THE VXYYD YV ADQAPUMD OPYSXMDEM SNWUN MUAH KMAZ LZWPEI SWA AY
I THINKTHZ IUWMPRWIA GAIA YVAMP MBHMZWIUM I VMMXWPE YV PYI VAZ ZMGYQMD VZYG AXYAZ YP APAXKTWPE APD MBHTYZM THE VIEWD YV ADQAPUMD OPYSIMDEM SNWUN MUAI KMAZ LZWPEI SWI IY

Now it's much clearer:

"I THINK THZ IUWMPRWIA GAIA YVAMP MBHMZWIUM I VMMXWPE YV PYI VAZ ZMGYQMD VZYG AXYAZ YP APAXKTWPE APD MBHTYZM THE VIEWD YV ADQAPUMD OPYSIMDEM SNWUN MUAI KMAZ LZWPEI SWI IY"

"I THINK THE SOLUTION WILL BE REVEALED I COMMIT MYSELF TO ONE THING THAT WHEN I GET A CLEAR VIEW OF THE PROBLEM I WILL COME BACK HERE AND SOLVE IT IF"

Seems like it's a message about commitment to solving a problem once a clear view of it is obtained.

② Using online decryption tool: https://www.dcode.fr/affine-cipher

By part (d)'s equation, it can generate the answer but is not 100% correct.

Problem 2

a) Determine the size of the key space (that is, the total number of keys).

$y = ax + b \bmod 30$, a must be coprime with 30 and less than 30

$30 = 2 \times 3 \times 5$, $\phi(30) = (2-1)(3-1)(5-1) = 8$, a has 8 possible choices

b can have 30 possible choices (from 0 to 29)

size of key space $= 8 \times 30 = 240$ #

1. 2.

b) Determine all values in $\mathbb{Z}_{30}$ that have inverses and, by trail-and-error, determine the inverses.

In $\mathbb{Z}_{30}$, element a has inverse if a is coprime with 30.

1. 1、7、11、13、17、19、23、29 have inverse #

2. $1 = aa^{-1} \bmod 30$, ① $1^{-1} = 1$ #

② $7a^{-1} \bmod 30 = 1$, $(7 \times 13) \bmod 30 = 1$, $7^{-1} = 13$ #

③ $11a^{-1} \bmod 30 = 1$, $(11 \times 11) \bmod 30 = 1$, $11^{-1} = 11$ #

④ $13a^{-1} \bmod 30 = 1$, $(13 \times 7) \bmod 30 = 1$, $13^{-1} = 7$ #

⑤ $17a^{-1} \bmod 30 = 1$, $(17 \times 23) \bmod 30 = 1$, $17^{-1} = 23$ #

⑥ $19a^{-1} \bmod 30 = 1$, $(19 \times 19) \bmod 30 = 1$, $19^{-1} = 19$ #

⑦ $23a^{-1} \bmod 30 = 1$, $(23 \times 17) \bmod 30 = 1$, $23^{-1} = 17$ #

⑧ $29a^{-1} \bmod 30 = 1$, $(29 \times 29) \bmod 30 = 1$, $29^{-1} = 29$ #

c) An attacker intercepts the following plaintext/ciphertext pairs:

x	y
4	8
10	26
27	7

Determine the encryption key $k_{\text{enc}} = (a, b)$.

$y = (ax + b) \bmod 30$,

$8 = (4a + b) \bmod 30$ — ①

$26 = (10a + b) \bmod 30$ — ②

$7 = (27a + b) \bmod 30$ — ③

(substitute the possible a into these 2 equations)

②-①: $18 = 6a \bmod 30$, ⇒ $a = 13$.

①-③: $1 = -23a \bmod 30$,

∵ a must be value that has inverse in $\mathbb{Z}_{30}$ ∴ $a = 13$

$8 = (4 \times 13 + b) \bmod 30 = (52 + b) \bmod 30$, $b = 16$

∴ $k_{enc} = (a, b) = (13, 16)$ #

d) Determine the decryption key $k_{\text{dec}} = (c, d)$, where "$x = cy + d \bmod 30$".

$y = (ax + b) \bmod 30 = (13x + 16) \bmod 30$

$x = [a^{-1}(y - b)] \bmod 30$

$= [13^{-1}(y - 16)] \bmod 30$

$= (7y - 112) \bmod 30$

$= (7y - 112 + 30 \times 4) \bmod 30$

$= (7y + 8) \bmod 30$

∴ $k_{dec} = (c, d) = (7, 8)$ #