Quiz. 1

111550057 莊婷馨 資工15

Problem 1

a)

```
Alphabet Frequency:
A: 1.41%
B: 1.41%
C: 8.45%
D: 4.23%
E: 2.82%
G: 3.52%
H: 2.11%
I: 2.82%
K: 1.41%
L: 0.70%
M: 13.38%
N: 3.52%
O: 0.70%
P: 8.45%
Q: 1.41%
R: 6.34%
S: 2.11%
T: 0.70%
U: 4.23%
V: 4.93%
W: 6.34%
X: 4.23%
Y: 8.45%
Z: 6.34%
```

b)

A COMPUTER SCIENTIST MUST OFTEN EXPERIENCE A FEELING OF NOT FAR REMOVED FROM ALARM ON ANALYZING AND EXPLORE THE FLOOD OF ADVANCED KNOWLEDGE WHICH EACH YEAR BRINGS WITH IT

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	L	F	I	L	O	R
	7	10	13	21	19	22	25	2	5	8	11	14	17

How to solve:

如下圖所示，不同顏色為不同次填入的字母。

Step 1. 根據 frequency 的資料和字串長短填入 A 和 THE，再根據 frequency 資料填入 R

Step 2. 觀察到有兩個字串為 WPE 結尾，推測是 ING

Step 3. 觀察到有三個字串為 Y 開頭而且只有兩個字母，推測是 OF 和 ON

Step 4. 許多字串已經完成一半或更多，可以根據推測直接填入

A computer scientist 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 knowledge which each
RNM VXYYD YV CDQCPUMD OPYSXMDEM SNWUN MCUN

year brings with it
KMCZ LZWPEI SWRN WR

c)

C 和 P 的字母是一對一的關係，屬於 substitution cipher，對應關係如上題 table 3 所示。

d)

$$\begin{cases} a+b \equiv 11 \pmod{26} \\ 2a+b \equiv 20 \pmod{26} \end{cases}$$

$$a \equiv 9 \pmod{26}$$

$$b \equiv 2 \pmod{26}$$

$$f(x) = 9x+2 \pmod{26}$$

但根據此對應方法，plaintext Q 應該會對應到 ciphertext Q，plaintext V 應該會對應到 ciphertext J，和 table 3 的結果不相符。

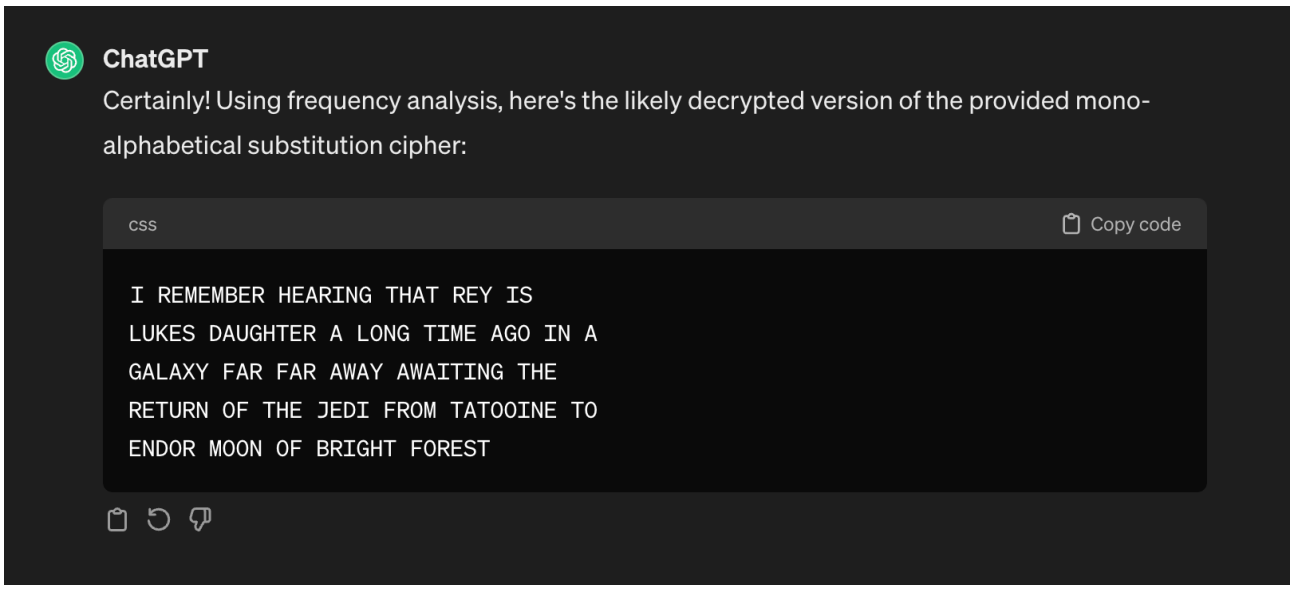
e)

26!

因為可能的 key 有很多，所以要進行 exhaustive search 比較有難度，但現今可能受到量子電腦的威脅。

f)

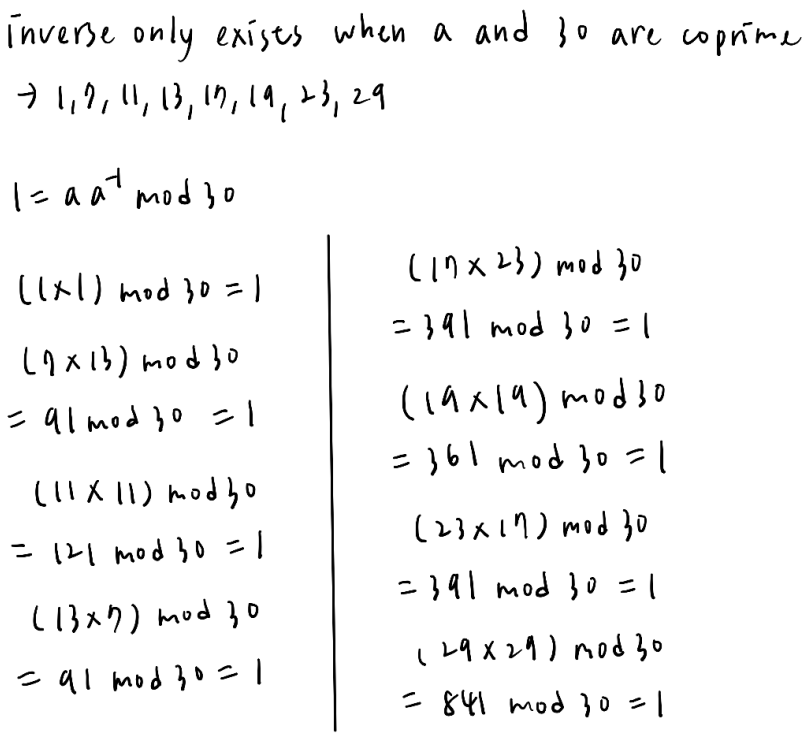
ChatGPT 會給一段長度差不多的 text，但完全不正確。



Problem 2

a)
a has to be coprime with 30
-> 8 possible a's and 30 possible b's
-> 8*30=240
There are 240 keys.

b)



	1	7	11	13	17	19	23	29
inverse	1	13	11	7	23	19	17	29

c)

$$4a + b \equiv 8 \pmod{30}$$
$$10a + b \equiv 26 \pmod{30}$$
$$27a + b \equiv 7 \pmod{30}$$

$$6a \equiv 18 \pmod{30}$$
$$23a \equiv -1 \pmod{30}$$
$$\equiv 29 \pmod{30}$$
$$a \equiv 29 \times 17 \pmod{30}$$
$$\equiv 13 \pmod{30}$$

$$13 \times 4 + b \equiv 8 \pmod{30}$$
$$b \equiv 16 \pmod{30}$$

$$k_{enc} = (13, 16)$$ ☆

d)

$$y \equiv ax + b \pmod{30}$$

$$x \equiv a^{-1}(y - b) \pmod{30}$$
$$\equiv 7(y - 16) \pmod{30}$$
$$\equiv 7y + 8 \pmod{30}$$

$$k_{dec} = (7, 8)$$ ☆