1 Problem 1

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

```python
def cypher_freq(f_path):
    freq = {}
    with open(f_path, "r") as file:
        for l in file:
            for c in l:
                if c.isalpha():
                    freq[c] = freq.get(c, 0) + 1

    return freq

f_path = "./Quiz1/cyphertext.txt"
unsorted_freq = cypher_freq(f_path)
sorted_freq = {k: v for k, v in sorted(unsorted_freq.items(),
                                       key=lambda item: item[1], reverse=True)}
print(sorted_freq)
```

   Output: {'M': 19, 'C': 12, 'Y': 12, 'P': 12, 'R': 9, 'Z': 9, 'W': 9, 'V': 7, 'U': 6, 'X': 6, 'D': 6, 'G': 5, 'N': 5, 'I': 4, 'E': 4, 'H': 3, 'S': 3, 'A': 2, 'B': 2, 'Q': 2, 'K': 2, 'T': 1, 'O': 1, 'L': 1}

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

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	Q	M	P	S	J	Y	B	E
	20	23	0	3	6	16	12	15	18	9	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

   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

   Plaintext: 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

   Step：

   (a) Guess M corresponds to E and C corresponds to A based on the common frequency of letters appearance.

   (b) Guess RNM corresponds to THE based on context.

   (c) And so on to get the final result.

3. Assume C is ciphertext, and P is plaintext. Can you find a particular relationship between C and P?
   It can be observed that most of the index of ciphertext increases by 1, the index value of plaintext will increase by 3, and the maximum index is not greater than 25.

4. Suppose "$f(x) = ax + b \ mod \ 26$", where x is plaintext, please solve the value of a and b.
   From the observation of the question 3, we can get $f(x) = \begin{cases} 9x + 2 \ mod \ 26 \ (x \neq 9, \ 21) \\ 9 \ (x = 9) \\ 16 \ (x = 21) \end{cases}$
5. What is the key size of the Mono-Alphabetic Substitution Cipher? Such a size makes exhaustive search becomes difficult?
   Key size: 26!
   Exhaustive search time: $\frac{26!}{60 \times 60 \times 24 \times 365 \times 10^7} \approx 1.28 \times 10^{12}$ years (Suppose checking 10^7 keys/second).
6. (Bonus) Please try to see if it is possible to decipher this problem with ChatGPT or another tool.
   (a) Substitution Solver (Possible)

Substitution Solver

This tool solves monoalphabetic substitution ciphers, also known as cryptograms. These are ciphers where each letter of the clear text is replaced by a corresponding letter of the cipher alphabet.

As an example here is an English cryptogram this tool can solve:

```
Rbo rpktigo vcrb bwucja wj kloj hcjd, km sktpqo, cq rbwr loklgo
vcgg cjqcqr kj skhcja wgkja wjd rpycja rk ltr rbcjaq cj cr.
-- Roppy Lpwrsborr
```

A Python implementation of this breaker is provided on GitLab.

If you want to break a polyalphabetic cipher instead try the Vigenère Solver.

Input

Cipher Text *

```
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
```

Language

English

Break Cipher | Clear Cipher Text

Result

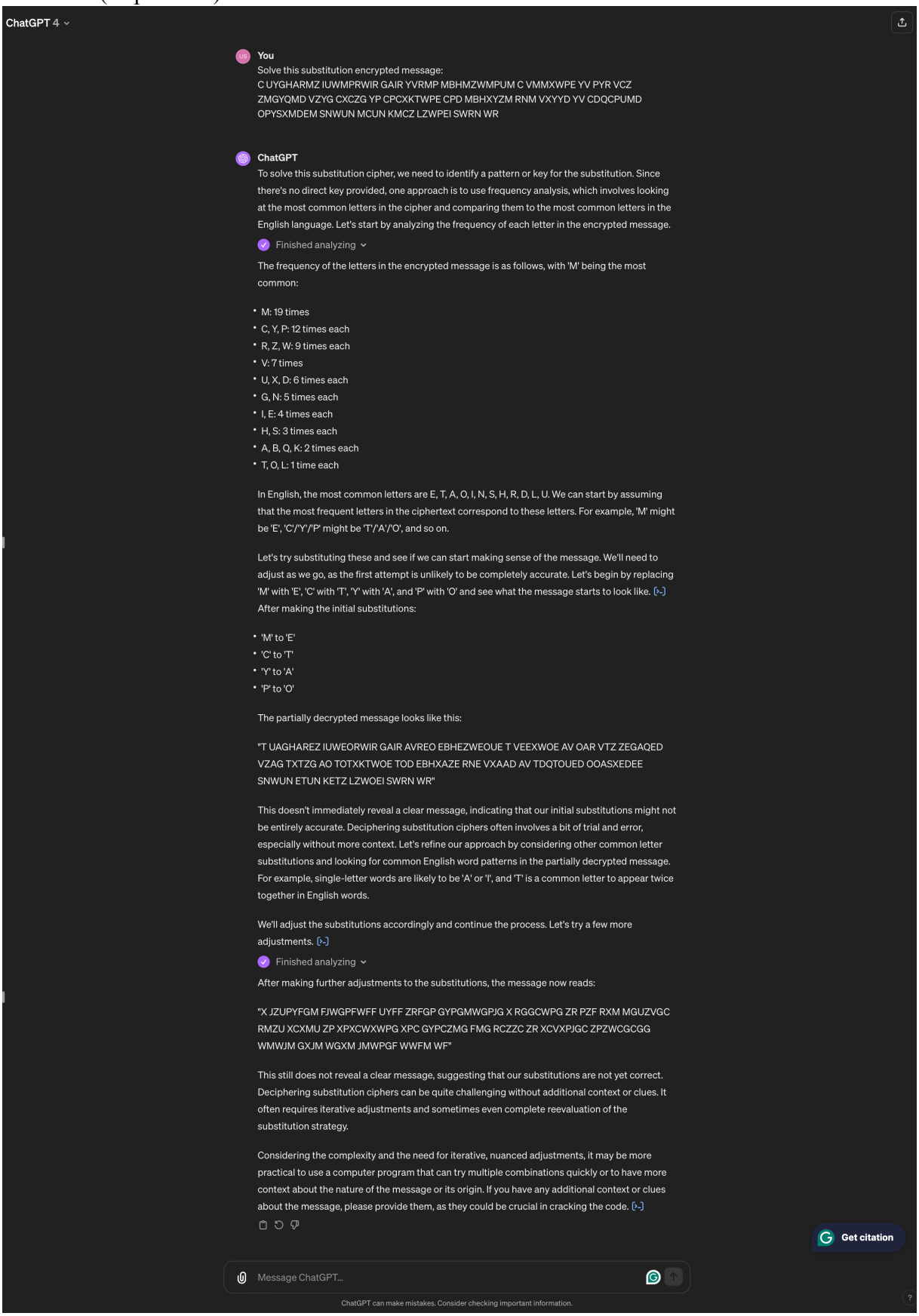
Key	abcdefghijklmnopqrstuvwxyz	This clear text ...
	uxadgqmpsjybehknvtwzcfilor	... maps to this cipher text

```
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
```

▸ Details

Runtime: 0.010 seconds

(b) ChatGPT (Impossible)



2 Problem 2

1. Determine the size of the key space (that is, the total number of keys).
   We must have $gcd(30,\ a) = 1$, and also $1 \leq b \leq 30$. $\varphi(30) = \varphi(2 \times 3 \times 5)$
   $= (2-1) \times (3-1) \times (5-1) = 8$, therefore we have $8 \times 30 = 240$ possible keys.
2. Determine all values in $\mathbb{Z}_{30}$ that have inverses and, by trail-and-error, determine the inverses.

Value	0	1	2	3	4	5	6	7	8	9
Inverse	x	1	x	x	x	x	x	13	x	x
Value	10	11	12	13	14	15	16	17	18	19
Inverse	x	11	x	7	x	x	x	23	x	19
Value	20	21	22	23	24	25	26	27	28	29
Inverse	x	x	x	17	x	x	x	x	x	29

3. Determine the encryption key $k_{enc} = (a, b)$.
$$\begin{cases} 4a + b \ mod\ 30 = 8 \\ 10a + b \ mod\ 30 = 26 \\ 27a + b \ mod\ 30 = 7 \end{cases} \Rightarrow \begin{cases} a = 13 \\ b = 16 \end{cases}$$
4. Determine the decryption key $k_{dec} = (c, d)$, where "$x = cy + d \ mod\ 30$".
$$\begin{cases} 8c + d \ mod\ 30 = 4 \\ 26c + d \ mod\ 30 = 10 \\ 7c + d \ mod\ 30 = 27 \end{cases} \Rightarrow \begin{cases} c = 7 \\ d = 8 \end{cases}$$