Problem 1

a)

```
Letter frequencies in the ciphertext:
A: 2
B: 2
C: 12
D: 6
E: 4
F: 0
G: 5
H: 3
I: 4
J: 0
K: 2
L: 1
M: 19
N: 5
O: 1
P: 12
Q: 2
R: 9
S: 3
T: 1
U: 6
V: 7
W: 9
X: 6
Y: 12
Z: 9
```

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/q	m	p	s	j/q	y	b	e
	20	23	0	3	6	9/16	12	15	18	9/16	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

c) by d) $C = 9P + 2$ #

F和J在題目中沒有出現，不能確定對應到哪個字母

d) 思路：①先代式看手算
②跑程式

$f(x) = (ax+b) \bmod 26$

Ⓐ 2 | b → $b = 2 \,\|\, 28 \,\|\, \cdots$
Ⓑ 11 | $a+b$ → $a+b = 11 \,\|\, 37 \,\|\, \cdots$
Ⓒ 20 | $2a+b$ → $2a+b = 20 \,\|\, 46 \,\|\, \cdots$

try $b=2$, $a+b=11 \Rightarrow a=9$

驗証 $2a+b = 18+2 = 20$

$\therefore a=9, b=2$, $f(x) = (9x+2) \bmod 26$ #

e) 26! #

f) 我試了很多次都沒辦法用GPT
(只給定義和參考的英文字母使用頻率的話)
它會把空白自動省略，再重新斷句，
有可能要更多提示 ex. 加密方法 ... 它才能處理 #

Problem 2

a) a要和30互質 → Z_{30}^* (1, 7, 11, 13, 17, 19, 23, 29)
b可為0-29任一數 → Z_{30} (0-29)
⇒ $|Z_{30}^*| \times |Z_{30}| = 8 \times 30 = 240$ #

b)

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

其他的沒有 multiple inverse #

c) $\begin{cases} 8 = (4a+b) \% 30 \\ 7 = (27a+b) \% 30 \end{cases}$ ⇒ $23a \% 30 = 29$
⇒ $a = 29 \times 17 \% 30 = 13$

$a = 13 \Rightarrow (13 \times 4 + b) \% 30 = 8 \Rightarrow b = 16$

驗證 $26 = (10a+b) \% 30$
$130 + 16 = 146$
$146 \% 30 = 26$ ✓

⇒ $(a, b) = (13, 16)$ #

d) ∵ 13的 multiplicative inverse 是 7
∴ $4 = (18 \times 7 + d) \% 30 \Rightarrow d = 8$

驗證 ① $10 = (26 \times 7 + 8) \% 30$
$182 + 8 = 190$
$190 \% 30 = 10$ ✓
② $27 = (7 \times 7 + 8) \% 30$
$49 + 8 = 57$
$57 \% 30 = 27$ ✓
⇒ $(a, b) = (7, 8)$ #