

1. (a)

```
PS C:\Users\borac\Desktop\school\selective_course\Cryptograhpy_Engineering\HW\HW1> python3 .\P1_frequency.py
{'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}
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
```

(b)

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	V	Y	B	E
	20	23	0	3	6	9	12	15	18	21	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	Q	T	W	Z	C	F	I	L	O	R
	7	10	13	16	19	22	25	2	5	8	11	14	17

(c)  $(3C+20) \bmod 26 = P$

(d)

$$\begin{aligned}
 (3f(x) + 20) \bmod 26 &= x \\
 \Rightarrow 3f(x) + 20 &= 26k + x \\
 \Rightarrow f(x) &= 3^{-1}(26k + x - 20) \bmod 26 \\
 &= 9(26k + x - 20) \bmod 26 \quad \because (3 \times 9) \bmod 26 = 1 \text{ (multiplicative inverse)} \\
 &= (9x - 180) \bmod 26 \\
 &= (9x + 2) \bmod 26 \\
 \hline
 a &= 9, b = 2
 \end{aligned}$$

(e) 26!. Yes, as the cost of trying all the permutations is too high.

(f) Gemini: failed to decode. Below is the prompt and response:

can you give me the mapping based on frequency analysis?

While we can attempt a mapping based on frequency analysis, it's crucial to understand that **this mapping is not guaranteed to be correct** nor are there the limitations mentioned earlier. Here's a possible mapping based solely on frequency analysis:

**Ciphertext Letter	Frequency	Possible Mapping**
Z	13	E (Most frequent letter in English)
M	12	T (Second most frequent)
Y	10	A
C	9	O
V	8	I
W	7	N
P	6	S
X	5	H

2. (a)  $a$  must be co-prime with 30 and less than 30, while  $b$  is the number of shifts.  $\#(a) = 8$ ,  $\#(b) = 30$ . Therefore, the key space is  $8 \times 30 = 240$ .

(b)  $1^{-1} = 1$ ,  $7^{-1} = 13$ ,  $11^{-1} = 11$ ,  $13^{-1} = 7$ ,  $17^{-1} = 23$ ,  $19^{-1} = 29$ ,  $23^{-1} = 17$ ,  $29^{-1} = 19$ .

(c)

$$\begin{cases} 4a + b \equiv 8 \pmod{30} \\ 10a + b \equiv 26 \pmod{30} \\ 27a + b \equiv 7 \pmod{30} \end{cases}$$
$$\Rightarrow \begin{cases} 6a \equiv 18 \pmod{30} \\ 17a \equiv 11 \pmod{30} \end{cases} \quad (17 \text{ has multiplicative inverse})$$
$$a = (17^{-1} \times 11) \pmod{30}$$
$$= 13$$
$$b = 30 \times 2 + 8 - 13 \times 4 = 16$$
$$key = (13, 16) \neq$$

(d)

$$\begin{aligned}y &= (13x + 16) \bmod 30 \\ \Rightarrow y + 30k &= 13x + 16 \\ \Rightarrow x &= 13^{-1}(y + 30k - 16) \bmod 30 \\ \Rightarrow x &= (7y - 112) \bmod 30 \\ &= (7y + 8) \bmod 30 \\ k_{dec} &= (7, 8) \quad \# \end{aligned}$$