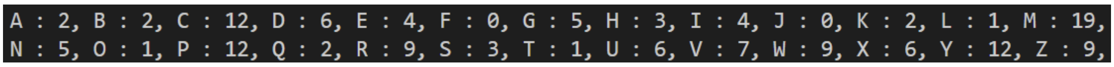
密碼工程 quiz1

110550108 施柏江

Problem 1

a) Please write a program to find out the frequencies of letters 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) Use the plaintext frequency count information below as a reference to break this encrypted messages.

我從找出 THE 下手。ciphertext 當中字母出現最多次的是 M，推測 M->E(4)。ciphertext 當中以 M 結尾且為 3 個字母單字只有 RNM，推測 R->T(19)，N->H(7)。發現 ciphertext 當中 M 和 N 相差 1，對應的 plaintext E 和 H 相差 3；ciphertext 當中 N 和 R 相差 4，對應的 plaintext H 和 T 相差 12，推測加密方式可能是平移之後以 3 為間隔填入新字母。得出的 plaintext 為：

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

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

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

d) Suppose “f(x) = ax + b mod 26”, where x is plaintext, please solve the value of a and b.

f(0) = b mod 26 = 2 => b = 2

f(1) = a + b = 11 mod 26 => a + 2 = 11 => a = 9

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

26!，大約是 10^26，因此使用暴力解需要花上許多時間。

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

ChatGPT 在算 ciphertext 當中每個字母出現頻率時就已經是錯的了，因此最後的答案也截然不同，不確定是否具有某種規律。

Problem 2

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

a 必須要小於 30 且與 30 互質，符合此條件的有 1, 7, 11, 13, 17, 19, 23, 29，共 8 個。

b 必須要小於 30，符合此條件的有 0~29，共 30 個。

所以 key space 的大小為 a*b = 8*30 = 240。

b) Determine all values in Z30 that have inverses and, by trail-and-error, determine the inverses.

必須和 30 互質才有 inverse，符合此條件的有 1, 7, 11, 13, 17, 19, 23, 29。

For 1, 1 * 1≡1 mod 30, so the inverse is 1.

For 7, 7 * 13≡1 mod 30, so the inverse is 13.

For 11, 11 * 11≡1 mod 30, so the inverse is 11.

For 13, 13 * 7≡1 mod 30, so the inverse is 7.

For 17, 17 * 23≡1 mod 30, so the inverse is 23.

For 19, 19 * 19≡1 mod 30, so the inverse is 19.

For 23, 23 * 17≡1 mod 30, so the inverse is 17.

For 29, 29 * 29≡1 mod 30, so the inverse is 29.

c) Determine the encryption key kenc = (a, b).

We have 8 = a*4 + b mod 30;   26 = a*10 + b mod 30;   7 = a*27 + b mod 30

=>   6*a = 18 mod 30   and   17*a = -19 mod 30   and   23*a = -1 mod 30

=>   a = 13

=>   8 = 52 + b mod 30;   26 = 130 + b mod 30;   7 = 351 + b mod 30

=>   b = 16

=>   (a, b) = (13, 16)

d) Determine the decryption key kdec = (c, d), where "x = cy + d mod 30".

We have 4 = 8*c + d mod 30;   10 = 26*c + d mod 30;   27 = 7*c + d mod 30

=>   18*c = 6 mod 30   and   19*c = -17 mod 30;   c = -23 mod 30

=>   c = 7

=>   4 = 56 + d mod 30;   10 = 182 + d mod 30;   27 = 49 + d mod 30

=>   d = 8

=>   (c, d) = (7, 8)