

# 密碼工程 Quiz1

學號:112550090 姓名:曾士珍

## Problem1

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

把密文存成一個 list，取名為 **text**，再用迴圈跑 **text** 裡面的字母並用 **count** 印出其出現的次數，下圖為程式碼跟其結果：

```
112550090.py X
1 text = "C UYGHARMZ IUWMPRIWR GAIR YVRMP MBHMZWMPUM C VMMXWPE YV PYR VCZ ZMGYQMD VZYG CX CZG YP
2 for i in range(ord('A'),ord('Z')+1):
3     print(chr(i),":",text.count(chr(i)))
```

```
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

對照常見的字母頻率表及常用單字。密文 **C** 自己便可組成一個單字推測可能為 **A** 或 **I**，**A** 在字母表中的頻率較常出現，先猜測是 **A**。兩個字的單字之密文有 **YV** 跟 **YP**，推測 **Y** 大機率應該是 **O**，**V** 大機率對到 **F**。

以推測的字再推得公式後，可以還原密文，還原後的明文如下：

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?

<b>Ciphertext</b>	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
<b>Plaintext</b>	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
<b>Ciphertext</b>	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
<b>Plaintext</b>	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

d) Suppose " $f(x) = ax + b \bmod 26$ ", where x is plaintext, please solve the value of a  
and b.

由 b) 的推論可得到三條方程式

$$2 = (a \cdot 0 + b) \bmod 26 \quad (\text{A 加密變為 C})$$

$$24 = (a \cdot 14 + b) \bmod 26 \quad (\text{O 加密變為 Y})$$

$$21 = (a \cdot 5 + b) \bmod 26 \quad (\text{F 加密變為 V})$$

可解得  $a=9, b=2$

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

單字替換密碼的密鑰大小指的是可用於加密訊息的可能密鑰數量。在單字替換密碼中，明文中的每個字母都被字母表中的另一個字母替換。如果我們考慮一個包含 26 個字母的標準英文字母表，則每個字母都可以被替換為其他 25 個字母中的任意一個（不包括它本身），結果會有  $n$  個不同對象的排列組合數量。對於一個 26 個字母的字母表來說  $26! = 26 \times 25 \times 24 \times \dots \times 3 \times 2 \times 1$

$$26! = 403,291,461,126,605,635,584,000,000$$

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

以下為使用 **chatgpt** 嘗試解密文的結果，再給予其較詳細的說明後，前半段的敘述看起來挺對的，後續他給了一個找(a, b)的程式碼看起來不太正常，感覺計算出(a, b)有點超過他目前所能執行的運算能力。



**You**

User

可以試可能拼湊出的單字(A加密後為C以及D加密後為D)來猜測對應明文的可能性，代碼轉換(A對到O，Z對到25)再以這兩組關係解出加密方程式( $a \times \text{明文代碼} + b \text{ 除以 } 26 \text{ 的餘數} = \text{密文代碼}$ )中的a及b(a, b是整數)，密文如下:C UYGHARMZ IUWMPRWIR GAIR YVRMP  
MBHMZWMPUM C VMMXWPE YV PYR VCZ  
ZMGYQMD VZYG CX CZG YP CPCXKTWPE CPD MBHXYZM  
RNM VXYD YV CDQCPUMD OPYSXMDM SNWUN MCUN  
KMCZ LZWP EI SWRN WR請嘗試解密



**ChatGPT**

讓我們按照你提供的信息來解密這段密文。首先，我們需要找到一些可能拼湊出的單字，其中"A"加密後為"C"，"D"加密後為"D"。

假設我們選擇 "AND" 作為可能的單字。根據密文的對應關係，我們可以得到：

- "A" 加密後為 "C"，因此我們可以推測  $a \times 0 + b \bmod 26 = 2$ ；
- "N" 加密後為 "P"，因此我們可以推測  $a \times 13 + b \bmod 26 = 15$ ；
- "D" 加密後為 "D"，因此我們可以推測  $a \times 3 + b \bmod 26 = 3$ 。

現在，我們可以解這個方程組以找到 a 和 b 的值。解方程組的一種方法是使用模數的性質，這裡我們可以將方程組表示為矩陣形式，然後求逆。

## Problem2

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

a 要在  $\mathbb{Z}_{30}$  中，且必須與 30 互質（即  $\gcd(a, 30) = 1$ ），確保每個明文符號都映射到唯一的密文符號。

0-29 中與 30 互質的整數共有 8 個(1, 7, 11, 13, 17, 19, 23, 29)，故 a 有 8 種選擇。

對於 b，由於是對 30 取模，b 可以有 0-29，30 種選擇。

密鑰空間的大小（密鑰的總數）是 a 和 b 的可能值的乘積，即  $8 \times 30 = 240$

b) Determine all values in  $\mathbb{Z}_{30}$  that have inverses and, by trial-and-error, determine the inverses.

在模 30 情況下，只有  $\gcd(x,30)=1$  的  $x$  會具有 inverse。故在 0-29 中與 30 互質的 8 個數字(1, 7, 11, 13, 17, 19, 23, 29)中找出他們的模逆元，結果如下：

$$1 \cdot 1 \equiv 1(\text{mod}30) \quad 7 \cdot 13 \equiv 1(\text{mod}30)$$

$$11 \cdot 11 \equiv 1(\text{mod}30) \quad 13 \cdot 7 \equiv 1(\text{mod}30) \quad 17 \cdot 23 \equiv 1(\text{mod}30)$$

$$19 \cdot 19 \equiv 1(\text{mod}30) \quad 23 \cdot 17 \equiv 1(\text{mod}30) \quad 29 \cdot 29 \equiv 1(\text{mod}30)$$

An attacker intercepts the following plaintext/ciphertext pairs:

c) Determine the encryption key  $k_{\text{enc}} = (a, b)$ .

$$8 = (4 \cdot a + b) \% 30$$

$$26 = (10 \cdot a + b) \% 30$$

$$7 = (27 \cdot a + b) \% 30$$

解方程式得  $(a, b) = (13, 16)$

d) Determine the decryption key  $k_{\text{enc}} = (c, d)$ , where “ $x = cy + d \text{ mod } 30$ ”

$$4 = (8 \cdot c + d) \% 30$$

$$10 = (26 \cdot c + d) \% 30$$

$$27 = (7 \cdot c + d) \% 30$$

解方程式得  $(c, d) = (7, 8)$