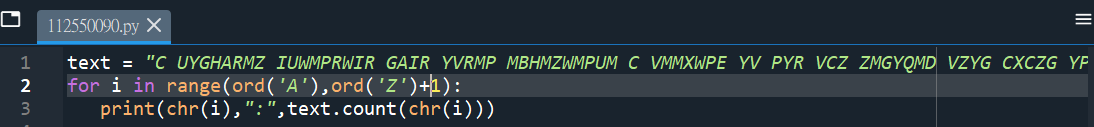
密碼工程Quiz1

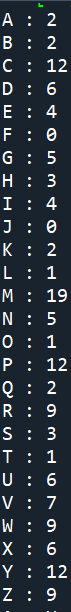
學號:112550090 姓名:曾士珍

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：





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 REMOQED FROM ALARM ON ANALYZING AND EXPLORE THE FLOOD OF ADQANCED 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 | 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 |

d) Suppose “f(x) = ax + b mod 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\*0+b)%26 (A加密變為C)

24=(a\*14+b)%26 (O加密變為Y)

21=(a\*5+b)%26 (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!=26×25×24×…×3×2×1

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。

一張含有 文字, 字型, 螢幕擷取畫面, 白色 的圖片

自動產生的描述

**一張含有 文字, 螢幕擷取畫面, 字型, 代數 的圖片

自動產生的描述**

Problem2

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

a要在Z30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 8×30=240

b) Determine all values in Z30 that have inverses and, by trail-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⋅1≡1(mod30) 7⋅13≡1(mod30)

11⋅11≡1(mod30) 13⋅7≡1(mod30) 17⋅23≡1(mod30)

19⋅19≡1(mod30) 23⋅17≡1(mod30) 29⋅29≡1(mod30)

An attacker intercepts the following plaintext/ciphertext pairs:

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

8=(4\*a+b)%30

26=(10\*a+b)%30

7=(27\*a+b)%30

解方程式得(a, b)=(13, 16)

d) Determine the decryption key kenc = (c, d), where “x = cy + d mod 30”

4=(8\*c+d)%30

10=(26\*c+d)%30

27=(7\*c+d)%30

解方程式得(c, d)=(7, 8)